



Sistema de naves y aeronaves no tripuladas e inteligencia artificial: innovaciones estratégicas para el futuro militar

Colección
Estrategia,
Geopolítica y
Cultura

Editor
David
Barrero-Barrero

Sistema de naves y aeronaves no tripuladas e inteligencia artificial: Innovaciones estratégicas para el futuro militar



Sistema de naves y aeronaves no tripuladas e inteligencia artificial: Innovaciones estratégicas para el futuro militar

DAVID BARRERO-BARRERO
(EDITOR)

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., 2026

Catalogación en la publicación – Escuela Superior de Guerra “General Rafael Reyes Prieto”

Sistema de naves y aeronaves no tripuladas e inteligencia artificial: innovaciones estratégicas para el futuro militar / David Barrero-Barrero, Editor – Bogotá D.C.: Sello Editorial ESDEG, 2026

180 páginas: ilustraciones y tablas; 24 cm

Incluye referencias al final de cada capítulo

ISBN impreso: 978-628-7818-56-9

E-ISBN digital: 978-628-7818-62-0

(Colección Estrategia, Geopolítica y Cultura)

1. Poder aéreo – Colombia 2. Ciberespacio – Colombia 3. Ámbito militar – Colombia 4. Innovación – Colombia i. Caro Cancelado, Fabio Leonardo, Mayor General, (prefacio) ii. Barrero-Barrero, David, (autor) iii. Baquero Valdés, Fabio, (autor) iv. Tavera Flórez, Carlos Andrés, (autor) v. González Carrasco, Leonardo, (autor) vi. Conde Mesa, Javier Hernando, (autor) vii. Riaño Pérez, Felipe Alfredo, (autor) viii. Meléndez Riveros, Daniel Alberto, (autor) ix. Quiroga Cruz, Robert Santiago, (autor) x. Poveda Zamora, Guillermo Alberto, (autor) xi. Colombia Escuela Superior de Guerra “General Rafael Reyes Prieto” (ESDEG)

SCLC UG479 2026
SCDD355.84

Registro Catalográfico SIBFuP 991409933807231



Archivo descargable en formato MARC en: <https://short.do/f68HGK>

Sistema de naves y aeronaves no tripuladas e inteligencia artificial: innovaciones estratégicas para el futuro militar

Primera edición, 2026

Editor:

David Barrero-Barrero

Cubierta:

Lina Marcela Manrique Lozada con base en
imágenes de la Fuerza Aeroespacial Colombiana.

2026 Escuela Superior de Guerra

“General Rafael Reyes Prieto”

Vicedirección de Investigación

Sello Editorial ESDEG

Carrera 11 N°. 102-50 Bogotá D.C., Colombia

www.esdeglibros.edu.co

Colección Estrategia, Geopolítica y Cultura

ISBN impreso: 978-628-7818-56-9

E-ISBN digital: 978-628-7818-62-0

DOI: <https://doi.org/10.25062/9786287818620>

Libro electrónico publicado a través de la plataforma

Open Monograph Press.

Tiraje de 100 ejemplares

Impreso en Colombia

Libro resultado de investigación de la Escuela Superior de Guerra “General Rafael Reyes Prieto”.

El contenido de este libro corresponde exclusivamente al pensamiento de los autores y es de su absoluta responsabilidad. Las posturas y aseveraciones aquí presentadas son resultado de un ejercicio académico e investigativo que no representa necesariamente la posición oficial ni institucional de las instituciones participantes, la Escuela Superior de Guerra “General Rafael Reyes Prieto”, las Fuerzas Militares de Colombia y el Ministerio de Defensa Nacional.



Los libros publicados por el Sello Editorial ESDEG son de acceso abierto bajo una licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.

<https://creativecommons.org/licenses/by-nc-nd/4.0/>



Mayor General
Fabio Leonardo Caro Cancelado
DIRECTOR

Brigadier General
Jaime Andrés Valencia Monsegny
SUBDIRECTOR

Coronel
Aldemar Serrano Cuervo
VICEDIRECTOR DE INVESTIGACIÓN



Coronel
Aldemar Serrano Cuervo
JEFE SELLO EDITORIAL ESDEG

Erika Ramírez Benítez
EDITORA LIBROS ESDEG

Jorge Hernando Aristizábal Gáfaró
CORRECTOR DE ESTILO

Rubén Alberto Urriago Gutiérrez
DIAGRAMADOR

Contenido

Prefacio	09-10
MG. Fabio Leonardo Caro Cancelado	
Introducción	11-14
David Barrero-Barrero	
Capítulo 1	
La nueva era de la guerra: autonomía, UAS e inteligencia artificial en el campo de batalla	15-39
David Barrero-Barrero	
Capítulo 2	
UAS, inteligencia artificial y toma de decisiones en tiempo real	41-66
Fabio Baquero Valdés	
Capítulo 3	
Tecnología antidrones C-UAS	67-86
Carlos Andrés Tavera Flórez	
Capítulo 4	
UAS/RPAS en el silencio de la batalla moderna del ciberespacio	87-111
Leonardo González Carrasco	
Capítulo 5	
Interoperabilidad de UAS: desafíos, estrategias y oportunidades en operaciones conjuntas y multinacionales	113-136
Javier Hernando Conde Mesa	
Felipe Alfredo Riaño Pérez	

Capítulo 6

La sinfonía de la guerra: inteligencia de enjambre y la transformación del poder aéreo

137-158

Daniel Alberto Meléndez Riveros

Robert Santiago Quiroga Cruz

Capítulo 7

Naves autónomas en el espacio: poder, tecnología y desafíos de seguridad

159-185

Guillermo Alberto Poveda Zamora

Prefacio

Mayor General Fabio Leonardo Caro Cancelado

Director de la Escuela Superior de Guerra "General Rafael Reyes Prieto"

En el siglo XXI, el conocimiento estratégico es una herramienta de poder tan decisiva como la fuerza misma. Las guerras ya no se libran únicamente en trincheras físicas, sino también en los dominios del espacio, el ciberespacio y la información. La velocidad de los avances tecnológicos y la creciente complejidad del entorno operacional exigen nuevas capacidades, nuevas doctrinas y, sobre todo, nuevas formas de pensamiento.

La Escuela Superior de Guerra "General Rafael Reyes Prieto", como institución de educación superior líder en la formación de los líderes de alto nivel del sector defensa, tiene el deber de anticiparse a estos cambios, orientar el análisis de sus implicaciones y preparar a sus oficiales para actuar con eficacia, responsabilidad y visión de largo plazo.

Con ese espíritu nace esta obra, resultado de un proyecto de investigación formal adelantado por el Departamento Fuerza Aeroespacial Colombiana (DEFAC), desarrollado en el marco de las líneas institucionales de ciencia, tecnología e innovación de nuestra Escuela. Su propósito es contribuir al estudio profundo de los desafíos que implican la integración de tecnologías disruptivas como la inteligencia artificial (IA), los sistemas autónomos y los sistemas aéreos no tripulados (UAS) en la seguridad y defensa nacionales.

Cada capítulo de esta obra es testimonio del compromiso investigativo y doctrinal de nuestros oficiales. El trabajo que aquí se presenta no solo examina el impacto de estas tecnologías en el campo de batalla moderno, sino que también plantea preguntas de fondo sobre la ética, la gobernanza, la interoperabilidad y la regulación del poder militar en la era digital. Este libro es, por tanto, un ejercicio académico riguroso, una contribución intelectual pertinente y una guía estratégica para quienes tienen la misión de liderar nuestras instituciones de defensa.

Reconozco y valoro el esfuerzo colectivo del equipo de investigación que ha hecho posible esta publicación. Su trabajo aporta a la consolidación de una

doctrina nacional que responde a los retos de la cuarta revolución industrial en el ámbito militar. Asimismo, invita al lector —sea este militar, académico, formulador de políticas o ciudadano comprometido con la seguridad— a pensar con visión crítica y estratégica sobre el papel que Colombia debe jugar en la configuración del orden global emergente. Este libro no es solo una reflexión sobre el futuro; es una herramienta para construirlo.

Introducción

David Barrero-Barrero

Editor Escuela Superior de Guerra "General Rafael Reyes Prieto"

En el umbral de una nueva era tecnológica, el poder militar se redefine a partir de la integración de sistemas autónomos, sistemas de naves y aeronaves no tripuladas (*Unmanned Aerial System, UAS*) e inteligencia artificial (IA). El presente libro hace parte del proyecto de investigación "Sistema de naves y aeronaves no tripuladas e inteligencia artificial: innovaciones estratégicas para el futuro militar", del grupo de investigación del Departamento Fuerza Aeroespacial Colombiana (DEFAC) de la Escuela Superior de Guerra "General Rafael Reyes Prieto".

El objetivo general de este trabajo es investigar y analizar el impacto de los UAS y de la IA en las estrategias y tácticas militares contemporáneas, con el fin de proponer soluciones y recomendaciones que garanticen su implementación efectiva, segura y ética en el ámbito militar.

Esta obra está estructurada en siete capítulos y aborda los retos y oportunidades que implican estas tecnologías disruptivas. El texto fue desarrollado por un equipo multidisciplinario de investigadores militares, pertenecientes al grupo de investigación Masa Crítica de la Escuela Superior de Guerra "General Rafael Reyes Prieto", en colaboración con otros investigadores militares pertenecientes a los siguientes grupos de investigación: Estudios Aeroespaciales (GIEA), Productividad, Innovación y Tecnología (PIT) y Ciencias Militares Aeronáuticas (GIGMA) de la Escuela Militar de Aviación "Marco Fidel Suárez", y Productividad, Innovación y Tecnología (PIT) de la Universidad Militar Nueva Granada.

La investigación se apoya en un enfoque metodológico mixto, articulando el paradigma hermenéutico con el empírico-analítico. Desde la perspectiva cualitativa, se analizan las percepciones, experiencias y significados estratégicos atribuidos por los actores militares al uso de IA y UAS en conflictos contemporáneos. Desde la dimensión cuantitativa, se recolectan y analizan datos sobre efectividad

operativa, casos documentados, algoritmos aplicados y métricas de desempeño para comprender cómo estas herramientas impactan los resultados tácticos y estratégicos.

El capítulo 1, titulado *“La nueva era de la guerra: autonomía, UAS e inteligencia artificial en el campo de batalla”*, examina cómo la incorporación masiva de tecnologías inteligentes ha revolucionado el concepto de *guerra moderna*. Se evidencian tres ejes de transformación: la autonomía operativa, la disuasión estratégica descentralizada y la guerra en mosaico. A través de estudios de caso como el conflicto de Nagorno-Karabaj o la guerra ruso-ucraniana, se demuestra que la superioridad ya no reside en el poder de fuego, sino en la agilidad operativa, la inteligencia algorítmica y la capacidad de adaptación en entornos multidominio. Este capítulo sienta las bases teóricas y doctrinales sobre el uso de IA en combate, subrayando la redefinición de la toma de decisiones, la logística y la estrategia.

El capítulo 2, *“UAS, inteligencia artificial y toma de decisiones en tiempo real”*, profundiza en las capacidades técnicas que permiten a los UAS actuar con creciente independencia humana. Se analizan los algoritmos de aprendizaje supervisado, no supervisado y por refuerzo que posibilitan la navegación autónoma, la detección de amenazas y la ejecución de misiones en entornos dinámicos. Al mismo tiempo, se abordan los dilemas éticos y de gobernanza derivados de delegar decisiones críticas a máquinas. El capítulo plantea la urgencia de implementar marcos de supervisión responsables, basados en la transparencia, la explicabilidad y la rendición de cuentas.

En el capítulo 3, denominado *“Tecnología antidrones C-UAS”*, se aborda el desarrollo de sistemas de defensa diseñados para contrarrestar amenazas provenientes de drones hostiles. Ante el incremento de UAV accesibles y modificables por actores no estatales o criminales, los sistemas C-UAS representan una respuesta tecnológica compleja que combina sensores multiespectrales, IA, inhibidores de señal y algoritmos de neutralización. Se analizan los componentes técnicos de estos sistemas y su aplicabilidad en el contexto colombiano, donde la geografía y el conflicto interno demandan soluciones adaptadas y eficientes.

En el capítulo 4, *“UAS como plataformas de guerra cibernética”*, se explora la convergencia entre UAS, IA y guerra electrónica. El capítulo documenta cómo los UAS pueden ser empleados para realizar ataques cibernéticos, interferencias electromagnéticas o actividades de inteligencia, transformándose en armas aéreas digitales. Se estudian las arquitecturas de radio definida por *software* (SDR), módulos SIGINT, algoritmos de *spoofing* y *jamming*, así como técnicas de detección y

respuesta autónoma. El capítulo también alerta sobre los riesgos de vulnerabilidad en redes militares y civiles, proponiendo una regulación urgente y estrategias de ciberdefensa integradas.

El capítulo 5, titulado *“Interoperabilidad de UAS: desafíos, estrategias y oportunidades en operaciones conjuntas y multinacionales”*, analiza las barreras normativas, técnicas y operativas que dificultan la integración de UAS en entornos cooperativos. Se examinan metodologías como SORA, STPA y FRAM para evaluar riesgos operacionales, así como tecnologías emergentes como el 5G, la computación en el borde (*edge computing*) y la inteligencia colectiva de enjambres. El capítulo destaca la necesidad de estandarizar protocolos de comunicación, aumentar la ciberseguridad y fomentar el desarrollo de capacidades interoperables a nivel internacional.

En el capítulo 6, denominado *“La sinfonía de la guerra: inteligencia de enjambre y la transformación del poder aéreo”*, se analiza la transformación que ha tenido el poder aéreo respecto a las vulnerabilidades de los nuevos sistemas aéreos centralizados frente a las amenazas asimétricas y la guerra electrónica. Sobre la base de la IA colaborativa, plantea la inteligencia de enjambre como una respuesta disruptiva que en el mundo contemporáneo podrá reemplazar las plataformas costosas por redes autónomas y resilientes. A partir de fundamentos técnicos y estudios de casos planteados como el de las operaciones Spiderweb y Manticora, se demuestran sus aplicaciones tácticas y estratégicas. Además, aborda los desafíos éticos, legales y de seguridad, proponiendo finalmente recomendaciones para una integración responsable que garantice seguridad y estabilidad.

Por último, el capítulo 7, *“Naves autónomas en el espacio: poder, tecnología y desafíos de seguridad”*, traslada el análisis al dominio espacial. Se examinan las capacidades operacionales de plataformas como el X-37B (EE.UU.), el Shijian-21 (China) o los satélites rusos Posmos, y se evalúan sus implicaciones geopolíticas. Identifica como amenazas emergentes: la militarización del espacio, la vulnerabilidad ante ciberataques y la carencia de marcos regulatorios adecuados. A su vez, se proponen estrategias basadas en ciberseguridad cuántica, monitoreo orbital y cooperación internacional para garantizar una gobernanza responsable del entorno espacial.

Finalmente, este libro ofrece un panorama comprensivo sobre la transformación tecnológica de la guerra moderna, abordando sus dimensiones técnicas, estratégicas, éticas y regulatorias. Entre los resultados más destacados se encuentran los siguientes: la identificación de los principales algoritmos y arquitecturas tecnológicas que definen el uso de UAS e IA en operaciones militares, y la

sistematización de riesgos operacionales, dilemas éticos y vulnerabilidades en el ciberespacio y el espacio orbital. Igualmente, se plantean algunas propuestas concretas de interoperabilidad, gobernanza ética y normativas aplicables a contextos nacionales y multinacionales, así como se hacen algunas recomendaciones para fortalecer la toma de decisiones, la doctrina militar y las capacidades de defensa frente a amenazas híbridas y multidominio.

Este libro no solo constituye una contribución académica al debate sobre la guerra futura, sino también una herramienta práctica para tomadores de decisiones, planificadores estratégicos, académicos y desarrolladores tecnológicos en defensa. Frente a un entorno global en permanente evolución, su lectura resulta indispensable para entender, anticipar y moldear el rol de la tecnología en los conflictos del siglo XXI.

Capítulo 1

La nueva era de la guerra: autonomía, UAS e inteligencia artificial en el campo de batalla*

DOI: <https://doi.org/10.25062/9786287818620.01>

David Barrero-Barrero

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo analiza la transformación del campo de batalla contemporáneo mediante la integración de sistemas aéreos no tripulados (UAS) e inteligencia artificial (IA). El objetivo es examinar cómo estas tecnologías están redefiniendo la estrategia militar, la toma de decisiones y la doctrina operativa. Se utiliza un enfoque metodológico mixto, que combina análisis cualitativo y cuantitativo a través de estudios de caso en conflictos como Nagorno-Karabaj y Ucrania. Los resultados destacan una revolución tecnológica caracterizada por autonomía algorítmica, guerra en enjambre y disuasión estratégica descentralizada. Las operaciones se tornan multidominio, fluidas y adaptativas, desafiando los paradigmas clásicos de la guerra. Se concluye que la superioridad militar ya no depende del volumen de fuego, sino de la flexibilidad, la velocidad y la capacidad de reorganización operativa en redes inteligentes autónomas. La IA redefine la fricción, la disuasión y la estructura del combate, exigiendo nuevas formas de pensamiento estratégico y doctrina militar.

Palabras clave: autonomía; disuasión; enjambres; inteligencia artificial; superioridad estratégica; *Unmanned Aircraft Systems*

* Capítulo de libro resultado del proyecto de investigación "Sistema de naves y aeronaves no tripuladas e inteligencia artificial: innovaciones estratégicas para el futuro militar" del grupo de investigación Masa Crítica de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado en A1 por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) (código COL0123247). Los puntos de vista y los resultados de este capítulo pertenecen a su autor y no reflejan necesariamente los de las instituciones participantes.

David Barrero-Barrero

Coronel (R) de la Fuerza Aeroespacial Colombiana. Doctor en bioética, Universidad Militar Nueva Granada, Colombia. M.Sc. en defensa y seguridad interamericana, Colegio Interamericano de Defensa, Estados Unidos. Docente ocasional asociado e investigador asociado por MinCiencias del grupo de investigación Masa Crítica, Escuela Superior de Guerra “General Rafael Reyes Prieto”, Colombia.

Orcid: <https://orcid.org/0000-0003-0412-1371> - Contacto: david.barrero@esdeg.edu.co

Citación APA: Barrero-Barrero, D. (2026). La nueva era de la guerra: autonomía, UAS e inteligencia artificial en el campo de batalla. En D. Barrero-Barrero (Ed.), *Sistema de naves y aeronaves no tripuladas e inteligencia artificial: innovaciones estratégicas para el futuro militar* (pp. 15-39). Sello Editorial ESDEG.
<https://doi.org/10.25062/9786287818620.01>

SISTEMA DE NAVES Y AERONAVES NO TRIPULADAS E INTELIGENCIA ARTIFICIAL: INNOVACIONES ESTRATÉGICAS PARA EL FUTURO MILITAR

ISBN impreso: 978-628-7818-56-9

E-ISBN digital: 978-628-7818-62-0

DOI: <https://doi.org/10.25062/9786287818620>

Colección Estrategia, Geopolítica y Cultura

Sello Editorial ESDEG

Escuela Superior de Guerra “General Rafael Reyes prieto”

Bogotá D.C., Colombia

2026



Introducción

Los avances tecnológicos de las últimas décadas han reconfigurado profundamente el panorama de los conflictos armados, introduciendo cambios radicales en la forma en que se planean y ejecutan las operaciones militares. Entre estos avances se destacan las aeronaves no tripuladas (UAS) y la inteligencia artificial (IA), tecnologías que han dejado de ser elementos complementarios para convertirse en piezas centrales de las estrategias de defensa contemporáneas. Estas herramientas no solo amplifican las capacidades militares, sino que también están redefiniendo los principios tradicionales de la estrategia y alterando la dinámica del poder en los conflictos internacionales.

La convergencia entre UAS e IA ha permitido crear sistemas autónomos que operan con un nivel de eficacia y precisión nunca antes visto. Estos sistemas han cambiado radicalmente la percepción del tiempo y el espacio en los conflictos armados, haciendo posible la ejecución de operaciones en múltiples frentes de manera simultánea. Además, su capacidad para procesar y analizar datos en tiempo real ha transformado el ciclo de decisión militar, acelerando la respuesta a amenazas y optimizando el uso de recursos estratégicos.

En esta nueva era de la autonomía en el campo de batalla, definida como “la capacidad de un agente para llevar a cabo una misión de forma independiente sin necesidad de intervención humana” (Gupta et al., 2013, p. 1650), los UAS habilitados por la IA han alcanzado niveles de sofisticación que les permiten ejecutar misiones críticas sin intervención humana directa. Estas capacidades, que incluyen la vigilancia constante, el reconocimiento de objetivos y los ataques selectivos, han reducido significativamente las bajas humanas y han redefinido las reglas de compromiso en la guerra moderna. En este contexto, los comandantes militares deben adaptarse a un entorno en el que la tecnología juega un papel determinante en la toma de decisiones.

La incorporación de estas tecnologías ha tenido un impacto significativo en las doctrinas militares de las principales potencias del mundo. Las estrategias de defensa se han rediseñado para integrar estas herramientas, priorizando la flexibilidad operativa y la capacidad de respuesta inmediata. Esta transformación ha dado lugar a un replanteamiento de las tácticas tradicionales, fomentando un enfoque más dinámico y adaptativo en los conflictos contemporáneos.

Un aspecto crucial de esta transformación es la forma en que los UAS y la IA han alterado las dinámicas de poder en los conflictos internacionales. Si bien estas tecnologías eran inicialmente exclusivas de las grandes potencias, su accesibilidad ha permitido que actores estatales y no estatales las utilicen para nivelar las asimetrías de poder. Este fenómeno ha dado lugar a un entorno de confrontación más competitivo donde los conflictos asimétricos y las guerras híbridas son cada vez más frecuentes.

A medida que estas tecnologías se consolidan, el pensamiento estratégico tradicional también se ve desafiado. Conceptos como la superioridad aérea, el control territorial y el poder disuasorio están siendo reformulados en un contexto donde las operaciones remotas y autónomas dominan el campo de batalla. La capacidad de operar a distancia y de manera simultánea en diferentes dominios ha redefinido las prioridades estratégicas de los Estados y las fuerzas armadas.

En este panorama, la superioridad tecnológica se ha convertido en un elemento estratégico para garantizar la victoria en los conflictos modernos. Los países que lideran la innovación en IA y UAS están consolidando su influencia en el ámbito global, fortaleciendo su capacidad de disuasión y proyectando poder con una eficiencia sin precedentes. Esta nueva carrera tecnológica ha desencadenado una competencia feroz entre las potencias mundiales, en la que la inversión en investigación y desarrollo desempeña un papel crucial.

Además de transformar los conflictos convencionales, estas tecnologías han dado lugar a nuevos escenarios de confrontación, como la guerra cibernética y las operaciones en dominios híbridos. En un mundo cada vez más interconectado, las amenazas ya no se limitan al ámbito físico, sino que se extienden al espacio digital y al espectro electromagnético, ampliando el alcance de las operaciones militares y las implicaciones estratégicas.

Sin embargo, esta revolución tecnológica plantea también retos significativos en el ámbito ético y legal. El uso de UAS e IA para tomar decisiones autónomas en el campo de batalla genera interrogantes fundamentales sobre la delegación de decisiones de vida o muerte a sistemas no humanos. Este debate afecta tanto a

las políticas de defensa nacionales como a las normas internacionales que regulan los conflictos armados, desafiando el marco ético establecido.

El objetivo del presente capítulo es introducir el contexto actual de la guerra y cómo los UAS y la IA están redefiniendo las operaciones militares, abordando la transformación del campo de batalla, el impacto estratégico de los UAS e IA y el concepto emergente de la guerra en mosaico. A través de un enfoque que combina análisis cualitativo y cuantitativo, se exploran las experiencias y percepciones de los actores militares, así como los datos operacionales sobre la efectividad de estas tecnologías en misiones específicas. La metodología empleada, basada en un paradigma mixto de investigación, articula elementos hermenéuticos y empírico-analíticos mediante un análisis de casos seleccionados en contextos estratégicos relevantes. Este enfoque permite integrar significados interpretativos y métricas cuantitativas para generar conclusiones fundamentadas sobre el impacto de estas tecnologías en la defensa y seguridad global.

En consecuencia, y como se muestra en la Figura 1, se analizan tres apartados en torno a la nueva era de la guerra. En el primero, se aborda la transformación de las capacidades operativas en el campo de batalla contemporáneo, las cuales, al permitir mayor autonomía, precisión y velocidad en la ejecución de misiones, han revolucionado la vigilancia, el reconocimiento y la toma de decisiones tácticas en tiempo real. En el segundo, se describe el impacto de la militarización de la IA en la redefinición de la estrategia militar, al optimizar la toma de decisiones, mejorar la autonomía en combate y aumentar la efectividad operativa, lo que, a su vez, plantea nuevos desafíos en la disuasión estratégica del conflicto. Finalmente, en el tercer apartado, se aborda la guerra en mosaico como una de las estrategias fragmentadas en un mundo interconectado, resultado de la combinación UAS/IA, que emplea estrategias descentralizadas y sistemas autónomos interconectados para mayor adaptabilidad y eficacia táctica en entornos dinámicos. Al final, se plantean algunas conclusiones.

Transformación de las capacidades operativas en el campo de batalla como resultado de la disrupción tecnológica

Si bien es cierto que los inicios de la IA se remontan hasta la década de 1950, su consolidación como tecnología para la guerra se dio a partir de los años noventa (Gupta et al., 2013), considerando como punto de inflexión histórico la guerra del

Figura 1. Tres aspectos a tratar en torno a la nueva era de la guerra



Fuente: Elaboración propia

Golfo, donde la tecnología no solo apoyó la estrategia, sino que la rediseñó desde entonces. Los primeros avances de la IA pudieron verse en los misiles guiados por computadora, también llamados misiles de crucero, a través del uso de algoritmos para aumentar la precisión de sus ataques. También surgieron los vehículos aéreos no tripulados (VANT), más conocidos como drones, que fueron utilizados en reconocimiento y ataques selectivos. Es así como "la inteligencia que se puede integrar en un UAS está directamente relacionada con la complejidad de la tarea que puede realizar e inversamente relacionada con el nivel de supervisión que requiere por parte de los operadores humanos" (Gupta et al., 2013, p. 1648).

De acuerdo con el U.S. Department of Defense, "la IA está transformando rápidamente una amplia gama de negocios e industrias. También está a punto de cambiar la naturaleza del futuro campo de batalla y el ritmo de las amenazas que debemos enfrentar" (2018, p. 18). La IA comenzó no solo a desarrollarse, sino a integrarse con otros sistemas avanzados de tecnología militar, como los vehículos autónomos y los sistemas de defensa antimisiles. Lo anterior pudo verse reflejado en las guerras de Irak y Afganistán con el empleo de las aeronaves remotamente tripuladas MQ-1 Predator, "una aeronave pilotada remotamente, armada, multimisión, de altitud media y gran autonomía, que se emplea principalmente como un

activo de recopilación de inteligencia y, secundariamente, contra objetivos de ejecución dinámicos" (United States Air Force, s.f.), en los ataques estratégicos contra estructuras o cabecillas del terrorismo. Además, la IA ha resultado útil en ámbitos civiles como el control de tráfico aéreo, el entrenamiento en simuladores de vuelo, el análisis de datos y las mejoras en ciberseguridad (United States Air Force, s.f.).

Esto se denomina *disrupción tecnológica*: la aparición de tecnologías que han cambiado radicalmente la forma en que funcionan los sistemas existentes, desplazando los métodos tradicionales, las estrategias y tácticas de combate y los modelos doctrinales establecidos. De hecho, esta disrupción de la tecnología, en palabras de Yuval Harari, "podría perturbar la sociedad humana y el sentido mismo de la vida humana de numerosas maneras, desde la creación de una clase global inútil hasta el auge del colonialismo de datos y las dictaduras digitales" (2020).

Los UAS y la IA deben ser considerados tecnologías disruptivas, ya que están alterando los fundamentos de la guerra convencional mediante cuatro características que, en el siglo XXI, hacen posible lo que antes era impensable:

- La velocidad y la precisión en la toma de decisiones en tiempo real
- La autonomía en el campo de batalla a partir de algoritmos
- El equilibrio/desequilibrio estratégico entre actores estatales y no estatales
- La necesidad de adaptación de las doctrinas operacionales a las realidades emergentes

Es así como la IA, junto con los UAS, ha llevado al planeta a una verdadera revolución tecnológica que ha generado grandes transformaciones en los conflictos armados que se libran en diferentes partes del mundo. La teoría militar y la noción de superioridad en el campo de batalla se redefinen permanentemente, puesto que estas tecnologías rompen con los paradigmas tradicionales y plantean nuevos desafíos estratégicos. Lo aquí tratado será abordado desde tres dimensiones conforme a la evolución de la "cascada de disrupciones" (Harari, 2020): el análisis de la IA en la planificación estratégica, referido a la automatización y precisión; el alcance de la transformación operativa de los UAS y las nuevas capacidades en el dominio del campo de batalla, la vigilancia y el reconocimiento en tiempo real; y la revisión de la guerra asimétrica y el acceso a capacidades tecnológicas emergentes.

La IA en la planificación estratégica: automatización y precisión

El desarrollo de la IA aplicada al campo de combate redefine el concepto de *superioridad* en el campo de batalla, por cuanto aumenta la capacidad en la toma

de decisiones tácticas y estratégicas en tiempo real, la optimización de recursos militares, el empleo de armas y mayor precisión en misiones de ataque, además de una total automatización de sistemas de defensa, entre otros (Tabla 1), a partir de lo establecido en el informe *The impact of artificial intelligence on military defence and security* (Araya & King, 2022), que destaca también la optimización de la logística militar y la minimización de riesgos que aporta la IA.

En suma, estas capacidades potencializadas por la IA son determinantes en cualquier conflicto contemporáneo. Como se ha visto en los conflictos en el Medio Oriente desde la última década del siglo XX, la búsqueda, delimitación, identificación y ataque a “objetivos de alto valor, fugaces y sensibles al tiempo” (United States Air Force, s.f.) se ha logrado con la mayor precisión posible.

Tabla 1. *Aplicaciones de la IA y su impacto en la superioridad en el campo de batalla*

Aplicaciones de la IA en el campo de combate	Impacto en la superioridad en el campo de batalla
Mejora de la toma de decisiones en tiempo real	Incrementa la velocidad y precisión en la respuesta ante situaciones dinámicas.
Optimización de recursos militares	Permite un uso más eficiente de los recursos disponibles, reduciendo desperdicios.
Aumento de la precisión en ataques y misiones	Minimiza los errores en las operaciones, mejorando la efectividad de las fuerzas.
Automatización de sistemas de defensa	Proporciona un control más ágil y autónomo de las defensas, aumentando la capacidad reactiva.
Mejora en la gestión logística y de suministros	Agiliza la distribución de recursos y la planificación de suministros en el terreno.
Reducción del riesgo para las fuerzas humanas	Permite el uso de unidades no tripuladas, disminuyendo las bajas en combate.
Capacidad para detectar y neutralizar amenazas más rápido	Mejora la rapidez y exactitud en la identificación de amenazas, actuando de forma más eficiente.
Mejora en la interoperabilidad entre sistemas y unidades	Facilita la coordinación entre diferentes fuerzas y tecnologías, optimizando las operaciones conjuntas.
Análisis predictivo para anticipar movimientos enemigos	Aumenta la capacidad de anticipación y planificación estratégica frente a los enemigos.
Apoyo en la guerra cibernética y la protección de infraestructuras	Refuerza las capacidades defensivas contra ataques cibernéticos y protege los sistemas críticos.

Fuente: Elaboración propia con base en Araya y King (2022)

Esto no desconoce los retos que enfrenta la IA al integrarse a sistemas de automatización y precisión en el campo de batalla, pues estos dependen de datos de alta calidad, así que los errores en esos datos pueden conllevar consecuencias desastrosas. Además, la mayor amenaza es que actores no estatales puedan acceder a estas tecnologías, con consecuencias potencialmente desastrosas (Kumar, 2020).

Los UAS y la transformación operativa: nuevas capacidades en el dominio del campo de batalla

En general, los sistemas no tripulados han pasado de ser simples plataformas de reconocimiento y vigilancia, a medios estratégicos en la reconfiguración de capacidades empleadas en el campo de batalla. Además de cumplir funciones tradicionales de reconocimiento y ataque, “son adecuados para situaciones demasiado peligrosas y arriesgadas donde no es posible la monitorización directa” (Gupta et al., 2013, p. 1646), por lo que han evolucionado lo suficiente para convertirse en nodos de interconexión en redes de guerra multidominio; una capacidad que permite a las fuerzas armadas extender alcance de combate y superioridad.

Así es como se entiende la integración de enjambres autónomos a través de procesos de IA, donde una multiplicidad de drones opera, inclusive, de forma descentralizada, lo que permite una alta flexibilidad y cambio de misiones durante el transcurso de las operaciones, facilitando la reevaluación de amenazas y la redistribución de funciones según la evolución del conflicto. Todo lo anterior, sumado a características clásicas como el sigilo y las altas velocidades de vuelo, rompe con las estrategias tradicionales de combate aéreo, detección y guerra electrónica.

Los UAS han resultado esenciales en conflictos recientes, como Siria, Libia, Nagorno-Karabaj (Jordán, 2021) y Afganistán, demostrando su capacidad de generar impactos desproporcionados en relación con los recursos empleados y cómo permiten a fuerzas con recursos limitados, como Ucrania, desafiar a potencias como Rusia.

Además, los UAS están cambiando la lógica operacional y doctrinal de las estrategias empleadas. En lugar de depender de ataques masivos, las fuerzas pueden utilizar enjambres de drones para abrumar las defensas enemigas. Esta táctica, coordinada por algoritmos de IA, maximiza los efectos mientras minimiza el uso de recursos. Sin embargo, como señala Javier Jordán (2021), la dependencia de estos sistemas también introduce vulnerabilidades, tales como “las interferencias de un enemigo tecnológicamente avanzado” (p. 7).

Guerra asimétrica y acceso a capacidades tecnológicas emergentes

Un primer aspecto de la asimetría tecnológica es la facilidad de acceso a esta. En este sentido, las guerras asimétricas, definidas como aquellas que se producen “entre varios contendientes de capacidades militares normalmente distintas y con diferencias básicas en su modelo estratégico” (Fernández-Montesinos, 2018), tradicionalmente son el resultado de tácticas insurgentes, cuyo propósito es contrarrestar la superioridad de oponentes más fuertes o potencias militares. Sin embargo, a través del acceso a la IA y los UAS, las fuerzas irregulares, organizaciones terroristas y criminales, han encontrado formas y medios de equilibrar las capacidades de combate en el campo de batalla, de una manera sin precedentes en la historia.

La incorporación de capacidades de IA en la planificación y ejecución de tácticas insurgentes y terroristas introduce una evolución significativa en la forma en que los grupos no estatales diseñan y llevan a cabo sus operaciones. Estas tecnologías les permiten incrementar los niveles de precisión, reducir errores operativos, acortar los tiempos de despliegue y maximizar el impacto mediático de sus acciones, lo que representa un desafío creciente para la seguridad nacional de los Estados afectados.

Si bien el acceso pleno a drones autónomos, ataques en enjambre o infraestructuras descentralizadas basadas en *blockchain* aún no es generalizado, estas capacidades no pueden considerarse inalcanzables. La existencia de mercados negros de armas, *software* y servicios tecnológicos especializados facilita el acceso progresivo a este tipo de recursos, configurando un problema estratégico de alta complejidad para los países que enfrentan fenómenos persistentes de terrorismo e insurgencia en su territorio.

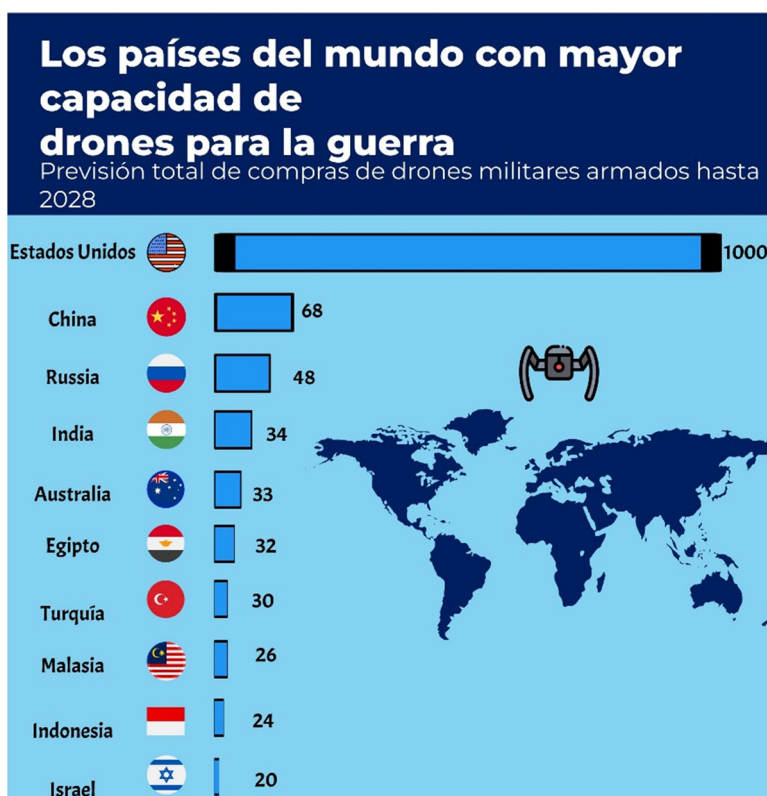
Un segundo punto de la asimetría tecnológica consiste en el desarrollo desbordado de capacidades por parte de las potencias, definido por Javier Jordán (2021), como:

Los importantes avances logrados en IA, enjambres, armas hipersónicas, armas de energía dirigida, etc., podrían hacer que los campos de batalla se vuelvan tan complejos y asombrosamente rápidos que superen la capacidad humana para gestionarlos eficazmente, lo que obligará a la IA a tomar la mayor parte de las decisiones. (p. 7)

Para citar algún ejemplo, Estados Unidos posee en inventarios aeronaves desarrolladas y probadas en diferentes escenarios como el Kratos XQ-58 para escolta de los F-22 y F-35 en misiones de combate, el Boeing MQ-25 Stingray cuya función es la de servir como sistema aéreo de la Navy, el Northrop Grumman X-47B para misiones de reconocimiento y penetración en ambientes denegados en búsqueda de objetivos y lógicamente el MQ-1 Predator ya mencionado.

Adicionalmente, tan solo diez países en el mundo dominan las capacidades UAS para la guerra, siendo Estados Unidos el principal superando en determinados escenarios la capacidad de algunos de sus seguidores, lo que deja al resto de países del mundo en la expectativa de cómo se desarrollará la guerra en el futuro del presente siglo XXI, y cómo serán los acontecimientos que marcarán las estrategias militares.

Figura 2. Los países del mundo con mayor capacidad de drones para la guerra



Fuente: Elaboración propia a partir de datos de Statista (McCarthy, 2019) mediante Freepik

El impacto de la militarización de la IA en la estrategia militar

La IA puede socavar la disuasión al inducir a los Estados a usar deliberadamente sus armas nucleares. De acuerdo con Greg Allen y Taniel Chan, “es probable que la tecnología de IA sea una capacidad militar transformadora, a la par de la invención de los aviones y las armas nucleares” (2017, p. 1); en palabras de la Oficina de Asuntos de Desarme de las Naciones Unidas, la IA podría llevar a los Estados a decidir usar sus armas nucleares de forma intencional (United Nations Office for Disarmament Affairs et al., 2019). Por tanto, la incorporación de la IA en el ámbito militar, además de revolucionar la dimensión táctica del combate, ha comenzado a redefinir los fundamentos estratégicos que históricamente han guiado la planificación y la conducción de la guerra. La IA está aún muy “lejos de alcanzar su máximo potencial” (Harari, 2020), al integrarse con plataformas autónomas, sensores interconectados y algoritmos de decisión avanzada. Como señalan Allen y Chan (2017), la IA se ha convertido en eje central de la transformación estratégica al permitir una proyección de poder más eficiente y adaptativa por parte de los Estados, asegurando ventajas operacionales y moldeando el comportamiento del adversario, con la necesidad de aprovechar “la agilidad operativa para adaptarse rápidamente a cualquier situación o acción enemiga” (Department of the Air Force, 2015, p. 7).

Por otra parte, tal como lo afirma James Lewis (2014), “las nuevas tecnologías militares son desestabilizadoras. Cuando una de las partes introduce una nueva tecnología, los adversarios potenciales creen estar en riesgo hasta que puedan igualar o contrarrestar la innovación” (p. 1). Esta transformación impacta directamente en tres ejes estratégicos clave: la reducción de la fricción operativa tradicional, la expansión hacia un dominio multidimensional adaptativo y la reconfiguración de la disuasión en un entorno algorítmico. A continuación, se desarrollan estos tres vectores para ilustrar cómo la IA está alterando la arquitectura misma de la estrategia militar contemporánea.

Transformación de la fricción operativa en entornos autónomos

Uno de los conceptos que más influye en la teoría clásica de la guerra es el de *fricción*, desarrollado por Carl von Clausewitz dos siglos atrás (2024, p. 804). Este concepto se refiere a las variables imprevisibles —errores humanos, fallos

mecánicos, confusión, miedo, fatiga y clima, entre otros—, que hacen de la guerra un fenómeno caótico y con incertidumbres, particularmente en el planeamiento, lo que la convierte en una actividad profundamente humana, imperfecta e inestable (2024, p. 804).

La fricción en el siglo XXI no solamente persiste, sino que se ha transformado y complejizado. En la era contemporánea, la fricción se evidencia en la saturación informativa, los ciberataques, los errores algorítmicos y las interferencias electromagnéticas, entre muchas más, por lo que “confiar demasiado en las máquinas podría provocar accidentes y errores de cálculo, incluso antes de que comience una guerra” (United Nations Office for Disarmament Affairs et al., 2019, p. 14). Esta fricción se manifiesta ahora en los dominios físicos, virtuales y cognitivos. De hecho, “la introducción del ámbito cibernético benefició a todo tipo de actores [...]; actores no estatales hostiles, incluyendo tanto criminales como terroristas, han hecho un uso eficaz de las herramientas cibernéticas” (Allen & Chan, 2017, p. 15).

La idea de fricción puede referirse entre otros aspectos, a la militarización de la IA y el despliegue de los UAS con capacidad autónoma de decisión, que particularmente la redefinen y la amplifican en formas nuevas y profundas. Según Saylor (2020), aunque la IA mejora la precisión táctica, también introduce nuevas vulnerabilidades que amplifican la fricción desde lo cibernético y algorítmico. Por lo anterior, “ninguna tecnología ni técnica eliminará la niebla y la fricción metafóricas de la guerra, y ninguna ventaja militar quedará sin oposición” (Department of the Air Force, 2015, p. 5), debido a que la guerra siempre será incierta y desafiante, sin importar los avances tecnológicos, porque los enemigos siempre responderán.

En este sentido, la incorporación de sistemas autónomos controlados por IA contribuye en doble sentido a reducir (cuando permiten decisiones más informadas y precisas) o aumentar (cuando fallan, se vulneran o son mal usados) las implicaciones de la fricción operativa de una forma supremamente acelerada, a través de plataformas aéreas como los drones kamikaze *loitering munitions* (municiones merodeadoras), como el Hero 30 israelí o los enjambres de microdrones —por citar tan solo unos pocos—, que son el resultado de tecnología disruptiva capaz de llevar a cabo misiones complejas, con alto grado de criticidad y con niveles mínimos de intervención humana.

Estas capacidades de la tecnología contribuyen a la reducción de la multiplicidad de errores que pueden asociarse a los operadores humanos, lo que conduce a mejores grados de precisión, sincronización y agilidad en las operaciones,

en especial gracias a la reducción de la intervención humana y el aumento de la autonomía algorítmica de la IA. Sin embargo, “si los sistemas de IA funcionan a la perfección, un desafío que podrían enfrentar las naciones es la incapacidad de predecir qué medidas podrían tomar en una crisis” (United Nations Office for Disarmament Affairs et al., 2019, p. 14).

Es así como la planificación militar poco a poco va asumiendo el control del entorno operacional, donde los márgenes de error, improvisación y lentitud —propios de la fricción— se minimizan gracias a la intervención de la IA, por lo que “la IA puede generar y ayudar a los comandantes a explorar nuevas opciones para que puedan seleccionar los cursos de acción que mejoren los resultados de la misión, minimizando los riesgos tanto para las fuerzas desplegadas como para los civiles” (U.S. Department of Defense, 2018, p. 11). Esto implica cambios estructurales en la doctrina militar como mecanismo de transformación, debido a que la estrategia no se orienta solo a neutralizar un enemigo o a proteger las tropas, sino la optimización continua en el combate, buscando como resultado la adaptación de los procesos por encima de la incertidumbre. Por ende, el teatro de operaciones es el resultado de una red interconectada capaz de detectar, decidir y actuar en tiempo real, priorizando la eficiencia del sistema antes que cualquier postulado de improvisación en la táctica o heroísmos individuales.

Sin embargo, la reducción de la fricción humana no implica la eliminación de todos los riesgos, puesto que podrían surgir restricciones algorítmicas, como los errores en la predicción y las vulnerabilidades cibernéticas. Estas, como las explotadas en casos históricos de intrusión en sistemas industriales —por ejemplo, el gusano *Stuxnet*, que afectó instalaciones en Irán— y en campañas recientes de ataques dirigidos contra infraestructura financiera y servicios en redes, demuestran la magnitud potencial de las exposiciones tecnológicas en contextos geopolíticos complejos. Además de lo anterior, también deben considerarse los sesgos en los modelos de decisión y los fallos sistémicos. Un ejemplo orientador sería considerar que, en lugar de un soldado con cansancio o un piloto desorientado, el nuevo punto crítico podría ser un algoritmo mal entrenado, interferencias en la comunicación o interpretaciones erráticas o erróneas de datos en tiempo real. A pesar de ello, “la niebla y la fricción de la guerra persisten, pero las interfaces hombre-sistema óptimas ayudan a los planificadores y operadores a detectar rápidamente las lagunas de comprensión y a superar con prontitud los impedimentos para el cumplimiento de la misión” (Department of the Air Force, 2015, p. 16).

Por tanto, la militarización de la IA no solo plantea redefinir la eficiencia en el combate, sino también los fundamentos de la epistemología doctrinal de la guerra. Por ello, es importante que las Fuerzas Armadas replanteen su arquitectura operativa, sus niveles y estructura de mando, y diseñen fuerzas capaces de actuar en escenarios más allá de la fricción tradicional, evolucionando hacia las fricciones de la tecnología disruptiva y considerando que la transformación del concepto de *fricción* ha trascendido hacia nuevos terrenos de incertidumbre estratégica.

Dominio multidimensional y arquitectura adaptativa del combate

De acuerdo con el Departamento de la Fuerza Aérea de los Estados Unidos, “las Operaciones Multidominio Integradas [...] abarcan la interoperabilidad total entre las capacidades aéreas, espaciales y ciberespaciales, de modo que el efecto combinado sea mayor que la suma de las partes” (Department of the Air Force, 2015, p. 8). Es así como la realidad de la militarización de la IA apunta hacia una transformación profunda, en la que las operaciones militares en el mundo contemporáneo deben concebirse, estructurarse y ejecutarse de manera diferente. Lo anterior implica dejar atrás los enfoques unidimensionales, centrados en la supremacía de los poderes terrestre, naval y aéreo, inclusive por separado, y apuntar a enfoques de dominio multidimensional, donde las operaciones se desarrollan de manera simultánea y coordinada en todos los dominios: terrestre, naval, aéreo, espacial, ciberespacial y cognitivo, o más allá. Así lo especifica la tabla multidominio presentada en la Figura 3, tomada de un documento doctrinario del Departamento de Defensa de EE.UU., que establece la visión estratégica de cómo las Fuerzas Armadas deben operar de forma conjunta y adaptativa en entornos futuros complejos y cambiantes, justificando los cambios en la forma de pensar las operaciones conjuntas, especialmente en escenarios futuros o de incertidumbre estratégica. Esta visión, a manera de ejemplo, ha sido adoptada formalmente por el Departamento de Defensa de EE.UU. (2018), que plantea un enfoque de operaciones conjuntas donde la IA es un integrador clave de dominios. El resultado de esta sinergia de dominios, facilitada por la IA, conlleva la exigencia de una nueva forma de entender la estructura de la guerra, que se ha denominado la *arquitectura adaptativa del combate*.

Cuando los sistemas autónomos operan en red a través de algoritmos de aprendizaje y control distribuido, permiten a las fuerzas militares actuar como un sistema vivo, con capacidad de reorganizarse en el tiempo para hacer frente a la

Figura 3. Nuevos dominios de confrontación en el siglo XXI

Físico	Virtual	Humano
Tierra	Ciberespacio Información	Social
Mar		Moral
Aire		Cognitivo
Espacio		

Dominios tradicionales

Dominios evolutivos del siglo XXI

Fuente: U.S. Department of Defense (2005)

evolución cambiante de las amenazas. “Los UAS suelen constar de varias aeronaves, puestos de control en tierra (C3), terminales de datos, cargas útiles modulares, [...] un sistema mucho más complejo que la simple aeronave” (Gupta et al., 2013, p. 1646). Este tipo de operación distribuida y autónoma ha sido visualizada por la Fuerza Aérea de Estados Unidos (2015) como parte de su concepto operativo para el año 2035. Así, el nuevo modelo arquitectónico de la guerra moderna redefine las estrategias en términos de maniobra, control y superioridad, aumentando los niveles de agilidad, flexibilidad y velocidad, y dejando por fuera las respuestas tácticas de las doctrinas convencionales.

Esta arquitectura adaptativa conlleva una necesaria evolución doctrinaria, puesto que la batalla no puede concebirse como una línea secuencial de fases, sino como un entorno fluido de nodos de un sistema que puede mutar de vigilancia a ataque, y de defensa a reconocimiento, de forma inmediata. Esto es comprensible debido a las grandes capacidades de aprendizaje de la IA, que refuerzan la lógica adaptativa de los sistemas tecnológicos actuales, los cuales no solo ejecutan órdenes, sino que también mejoran su rendimiento durante las operaciones.

Ejemplos de esta evolución se han visto recientemente en Nagorno-Karabaj, Ucrania y Gaza. La multiintegración de los UAS con IA, guerra electrónica, enlace satelital, *data link* y comunicación con estaciones terrenas, navales o aéreas permite la coordinación para el desarrollo de operaciones de mucha precisión, y también erosiona la capacidad del enemigo para adaptarse a estos nuevos escenarios de

confrontación. La IA almacena grandes volúmenes de información, lo que la convierte en una ventaja operacional en el combate, al desplegar esta capacidad de interoperabilidad y autoorganización.

Este nuevo enfoque rompe la rigidez doctrinal del siglo XXI y exige a las Fuerzas Armadas repensar nuevos diseños de lógica sistémica para reemplazar la jerárquica. La nueva guerra ahora se gana por la capacidad de operar con inteligencia distribuida simultáneamente en todos los dominios, a diferencia de lo anterior, donde la victoria se medía por el tamaño de los arsenales, la ocupación territorial y la persistencia en el combate. La arquitectura adaptativa corresponde, entonces, a la manifestación estructural que debe adoptar la estrategia multidominio contemporánea.

Reconfiguración de la disuasión estratégica en la era algorítmica

La disuasión, entendida como “una variable relacional, resultado de una interacción en la que el disuadido opta por no llevar a cabo una acción —que de otro modo sí realizaría— al estimar los costes que puede entrañar” (Jordán, 2021), también puede verse como “el arte y la ciencia que los estrategas deben emplear para evitar ataques externos o, simplemente, mantener una imagen de peligrosidad en caso de que alguien intente agredir” (Barrero-Barrero, 2020, p. 170).

Esta capacidad intrínseca de influir en las decisiones de un adversario a través de la amenaza creíble de represalias inaceptables ha sido parte fundamental de la estrategia militar de la Guerra Fría. En el siglo XXI, la incorporación de la IA, la robótica, los satélites en el espacio y los sistemas autónomos, entre muchos otros elementos del planeamiento y la ejecución de la guerra, modifica radicalmente las teorías y fundamentos sobre los que se ha venido construyendo la disuasión, desde el modelo tradicional del siglo anterior hasta la presente centuria. “Los futuros UAV ejecutarán misiones más complejas, como ataques electrónicos, ataque/supresión de la defensa aérea enemiga [...] coordinadas con sistemas inteligentes tácticos y estratégicos” (Gupta et al., 2013, p. 1656).

Tal como lo expone James Lewis (2014), la irrupción de tecnologías disruptivas como la IA está erosionando las bases tradicionales de la disuasión estratégica a partir de la acción algorítmica, donde las variables humanas de la racionalidad, la percepción y el cálculo político han venido siendo reemplazadas o condicionadas por las decisiones automatizadas y los ciclos acelerados de reacción, que dan sustento a la teoría del aceleracionismo de la vida y la descentralización del tiempo de Hartmut Rosa (2011).

Como se mencionó, uno de los elementos disruptivos de este nuevo escenario de confrontación es la velocidad con la que los sistemas autónomos detectan, identifican y responden a las amenazas. Las decisiones que toma la IA en milisegundos determinan de forma significativa la ventaja en todos los niveles de la guerra. Sin embargo, “en lugar de exigir inteligencia ‘perfecta’, las fuerzas militares deben poder tomar decisiones precisas a un ritmo que proporcione ventajas sobre los adversarios” (Department of the Air Force, 2015, p. 9). Lo anterior plantea un dilema inédito para la teoría y la práctica de la disuasión: ¿cómo disuadir a sistemas que no operan bajo los parámetros tradicionales de la racionalidad humana? A diferencia de los Estados y actores del siglo XX, cuya conducta estratégica estaba condicionada por el tiempo político, las emociones, los cálculos ideológicos y el temor a la destrucción, los sistemas algorítmicos no comparten estos marcos de referencia.

En consecuencia, la lógica clásica de la disuasión, construida sobre la previsibilidad racional de actores humanos, pierde efectividad en un entorno donde los principales decisores pueden ser sistemas no humanos, diseñados para operar de forma lógica, reactiva y orientada a objetivos, sin considerar costos políticos, emocionales o existenciales.

En este sentido, el carácter opaco de muchos sistemas de la IA, alimentados por *big data* y aprendizaje profundo, dificulta conocer con certeza cuáles son sus parámetros de decisión. Por lo tanto, la incertidumbre técnica que esto genera podría denominarse disuasión ambigua, en la que ni siquiera un adversario podrá conocer completamente la forma de actuar y comportarse de un sistema autónomo. Esta ambigüedad, muy lejos de aumentar la estabilidad estratégica, puede generar errores de cálculo, daños sistémicos o represalias automáticas no autorizadas por el liderazgo político.

Además, la IA es capaz de sostener la disuasión al operar con baja detectabilidad y alta capacidad de vigilancia persistente, lo que se traduce en una proyección de poder significativa. En palabras de Gupta et al. (2013), “los UAS son más adecuados para misiones aburridas, sucias o peligrosas que las aeronaves tripuladas [...] evitando el coste humano de perder vidas si la misión no tiene éxito” (p. 1654). De esta forma, los Estados no requieren el despliegue de tropas que puedan visibilizarse, así como tampoco realizar demostraciones de poder y fuerza. La disuasión debe proyectarse más allá: en la generación de efectos a través de la activación de una red de sensores, enjambre de drones, despliegue de una constelación de satélites y acciones de ciberdefensa en modo latente y letal. “Las ciberarmas de

IA altamente destructivas podrían estar ampliamente disponibles y ser difíciles de controlar” (Allen & Chan, 2017, p. 26), por lo que, en el campo de batalla del siglo XXI, la IA “cambiará principalmente los aspectos cognitivos de la guerra” (United Nations Office for Disarmament Affairs et al., 2019, p. 13).

Es por todo lo anterior que las estrategias de disuasión se deben adaptar a las nuevas lógicas en los dominios de confrontación. Por tanto, en la guerra moderna, la credibilidad no depende solo del poder que se tenga, de las amenazas o de los discursos políticos, sino de la reputación algorítmica, la residencia cibernética y la interoperabilidad sistémica que se posea. Las amenazas a la seguridad global del presente y del futuro de la humanidad no solo provienen de los ataques nucleares o las guerras convencionales, sino de la eventual posibilidad de ser neutralizado por una máquina que no requiere permiso para actuar. Esta nueva reconfiguración exige repensar y proyectar la doctrina y las estrategias de la disuasión por medio de la interdisciplinariedad tecnológica, la teorización de sistemas complejos de la tecnología disruptiva y el pensamiento estratégico contemporáneo: “Este es un problema estratégico complejo; [...] construir más armas no generará estabilidad, [...] el viejo paradigma de disuasión y estabilidad ha sido dañado y debe ser renovado” (Lewis, 2014, p. 2).

Guerra en mosaico: estrategias fragmentadas en un mundo interconectado

Uno de los resultados más sorprendentes de la evolución tecnológica y la estrategia militar, particularmente de la segunda década del presente siglo XXI, es la guerra en mosaico, un modelo de confrontación que ha podido verse en el conflicto de 2020 de Nagorno-Karabaj entre Armenia y Azerbaiyán, pero especialmente en el conflicto ruso-ucraniano iniciado en 2022.

Esta estrategia emergente es la combinación de los modelos de “letalidad distribuida” (Pulido, 2022, p. 37), los algoritmos adaptativos y los sistemas autónomos interconectados, que redefinen, como se ha dicho, el campo de batalla en un formato descentralizado, dinámico y fragmentado, puesto que la guerra, particularmente la que se libra entre Ucrania y Rusia, ha dejado de ser una confrontación lineal entre bandos definidos, para convertirse, además, en un conjunto de acciones simultáneas y autónomas que interactúan de manera fluida y coordinada a través del multidominio y los niveles de la estrategia, en un formato completamente híbrido.

Es así como este enfoque de confrontación “por debajo del nivel de guerra abierta a plena escala” (Pulido, 2022, p. 43) permite explotar ventajas decisivas, en el que las aeronaves tripuladas o no tripuladas actúan como un nodo autónomo inmerso en una red táctica mayor. Una de las grandes diferencias entre la guerra en mosaico y las operaciones jerárquicas tradicionales es la arquitectura diseñada para una operatividad de alta adaptabilidad, integración de capacidades y velocidad de respuesta, lo que conlleva plantear la guerra en mosaico como la base de la estrategia de superioridad militar contemporánea.

Por tanto, puede afirmarse que:

La guerra en mosaico es un nuevo concepto de combate propuesto por el ejército estadounidense para la guerra de información, inteligencia y no tripulada del futuro. Su objetivo es obtener una ventaja asimétrica sobre los principales oponentes en combate. Basándose en el análisis de los antecedentes de la guerra en mosaico, este artículo resume sus características básicas, la compara con la operación en enjambre de UAV y concluye sus similitudes. (Qi et al., 2021, p. 79)

Descentralización táctica y disolución del frente tradicional

Con el advenimiento de la guerra en mosaico, uno de sus efectos más disruptivos ha sido la desaparición del frente tradicional, es decir, de la estructuración lineal de las operaciones, para dar paso a una multiplicidad de trayectorias convergentes ejecutadas por plataformas independientes, que pueden actuar simultáneamente en los entornos físicos y virtuales; como “un organismo colectivo, que comparte un cerebro distribuido para la toma de decisiones y se adapta entre sí como enjambres en la naturaleza” (Scharre, 2018, p. 28). Esta descentralización, como parte de las llamadas guerras sin contacto o de sexta generación (Scharre, 2018), implica afirmar que en este modelo de confrontación deja de existir un solo centro de gravedad, dependiente de un esfuerzo clásico y doctrinario de planificación, puesto que la red de sistemas interconectados está dedicada a la toma de decisiones locales con objetivos globales.

Este enfoque, que fragmenta la planificación clásica, no implica caos, sino la necesidad de pensamiento creativo a través de la inteligencia sistémica distribuida, conformada por la integración de la IA, los sensores autónomos y los sistemas avanzados de comunicación. Cada unidad de estos UAS tiene la capacidad de redefinir en tiempo real su misión, conforme a la evolución del conflicto, lo que en definitiva proyecta una resiliencia operativa sin precedentes.

Por lo anterior, el campo de batalla contemporáneo deja de ser un escenario físico para convertirse en un entorno multidominio, flexibilizado y de recomposición permanente. En este sentido, “los enjambres de drones están a punto de dominar el campo de batalla” (King, 2023), donde las nuevas fases del conflicto serán las de “competir, desintegrar, explotar y recompetir” (Scharre, 2018, p. 56).

Sistemas autónomos en red y la lógica del enjambre distribuido

La capacidad de conectar y coordinar sistemas autónomos en red es la principal característica de la guerra en mosaico, dada su contribución a la operación sin jerarquía fija y con autonomía táctica. Este principio se materializa a través de lo que se denomina *lógica del enjambre distribuido*, donde múltiples plataformas, bien sean terrestres, aéreas, marítimas o cibernéticas, actúan como un organismo colectivo, tomando decisiones sincronizadas sin que exista un comando central.

Este concepto fue inspirado en los enjambres de abejas y adoptado como modelo táctico de integración y sincronización para la ejecución de una diversidad de operaciones, como ataques, maniobras defensivas y engaño, entre otras. En este sentido, la IA juega un papel importante en el diagrama planteado anteriormente, tanto como mecanismo para la toma de decisiones como esquema de aprendizaje colectivo. Los enjambres son capaces de redistribuir las funciones, realizar cambios en la misión y reorganizar su propia configuración, dependiendo del entorno operacional, lo que los convierte en armas totalmente disruptivas.

Este tipo de operaciones ya ha sido puesto en práctica. Desde el uso de enjambres en Nagorno-Karabaj hasta la guerra ruso-ucraniana y el conflicto de Gaza, la combinación de estos UAS con la guerra electrónica, una gran variedad de sensores y el respaldo de ataques cibernéticos deja en evidencia el poder de las redes distribuidas en relación con las doctrinas tradicionales de concentración de fuerza.

Además de producir efectos cinéticos, la guerra en mosaico produce efectos cognitivos en todos los vectores, como la sobrecarga mental del adversario (confusión, estrés, toma de decisiones erráticas y agotamiento cognitivo, entre otras), la desorganización del mando y control, la ilusión de omnipresencia, la desigualdad cognitiva y hasta la manipulación del comportamiento del enemigo. Esta función cognitiva:

Comprende todas aquellas actividades comunicacionales, emocionales, educativas y sensoriales, utilizadas permanentemente para inculcar la cultura,

modismos, ideales e intereses de quien la ejecuta a la población en general, con la intención de que, de forma consciente, respalde y defienda todos sus intereses y objetivos, sin importar los de su propia nación. (Viloria, 2024, p. 111)

Superioridad adaptativa: velocidad, flexibilidad y disrupción

La estrategia del enjambre es considerada “un nuevo concepto de combate propuesto por el ejército estadounidense para la guerra de información, inteligencia y no tripulada del futuro. Su objetivo es obtener una ventaja asimétrica sobre los principales oponentes en combate” (Qi et al., 2021). A partir de las capacidades tecnológicas, otorga a los militares la capacidad de desplegar una gran cantidad de unidades en el campo de batalla con la mínima intervención humana. El comportamiento coordinado de estas unidades permite, entre otras ventajas, la reducción significativa de los tiempos de reacción, lo que a su vez posibilita una gran ventaja en su adaptación rápida a situaciones cambiantes, algo indudablemente difícil de lograr cuando cada unidad opera individualmente (Scharre, 2018, p. 25).

Un aspecto importante por mencionar es el de la superioridad adaptativa — como eje central de la guerra en mosaico—, que representa la capacidad de ajustar el curso de las operaciones con cualidades superiores al adversario, como la velocidad y la flexibilidad, gracias a que “todos los elementos del enjambre se comunican entre sí simultáneamente y deciden colectivamente un curso de acción” (Scharre, 2018). Este concepto de *adaptabilidad* no puede considerarse simplemente como un atributo organizacional, sino como una ventaja estratégica estructural, resultado de la estructura algorítmica del combate, así como de la autonomía táctica de los nodos y, consecuentemente, del poder distribuido en tiempo real.

Por otra parte, la IA contribuye a reducir de forma radical el ciclo OODA (Observar-Orientar-Decidir-Actuar) de John Boyd; más aún desde la perspectiva de contribuir a la parálisis estratégica de un adversario (Fadok, 1995), lo que bien puede traducirse en un mayor dominio de la iniciativa operacional. Esto implica que quien logra adaptarse más rápido toma decisiones en segundos y, por tanto, impone el ritmo de las operaciones, desorganiza al enemigo y desestabiliza su planificación. Esta superioridad, hoy en día, no depende del volumen de fuego o de la cantidad de tropas que se posea, sino de la velocidad con que un sistema reorganiza su arquitectura operativa frente al cambio.

Esta ventaja en el campo de combate requiere la evolución hacia nuevas formas de enfrentamiento, de planificación y, en consecuencia, de liderazgo militar.

La guerra en mosaico que se libra actualmente en algunas partes del mundo exige cada vez más una mentalidad sistémica, algoritmos confiables y, lógicamente, un ecosistema tecnológico robusto, capaz de resistir interferencias, ataques cibernéticos e irrupciones en su entorno complejo. Esto se denomina *adaptabilidad*, que ya no es solo una respuesta a los cambios tecnológicos del siglo XXI, sino un principio y requisito en la organización de la estrategia contemporánea.

Conclusiones

La incorporación de la IA y los UAS en las últimas décadas ha transformado radicalmente la arquitectura del combate contemporáneo. La evolución de estas tecnologías ha dejado atrás su uso como herramientas complementarias y las ha convertido en un epicentro operativo que redefine los fundamentos del pensamiento estratégico en la guerra, amplía las capacidades militares y modifica considerablemente los tiempos y espacios de confrontación.

Además, la militarización de la IA genera un impacto evidente en la automatización de los procesos de toma de decisiones, el aumento de la precisión en la ejecución de operaciones, así como en su capacidad de adaptación en entornos complejos. Es así como la velocidad con la que se toman decisiones, la interoperabilidad de los sistemas y el uso de inteligencia predictiva sustituyen los enfoques clásicos de la doctrina, dando paso a una lógica de combate mucho más fluida, ágil y capaz de dar respuesta en tiempo real a cualquier amenaza.

En este orden de ideas, la integración de los UAS con la IA ha transformado las plataformas en nuevos activos dentro de la red de combate multidominio. Consecuentemente, la fricción operativa pasó del error humano a los fallos algorítmicos o a las saturaciones informáticas, lo que representa un cambio profundo en la forma como se planifican las operaciones en el ambiente actual, donde la incertidumbre ha sido desplazada hacia nuevas dimensiones, como la cognitiva.

Por otra parte, la denominada guerra en mosaico, llevada a cabo en los conflictos contemporáneos de Nagorno-Karabaj y Ucrania, plantea un nuevo modelo descentralizado y adaptativo en el combate, por lo que este enfoque propone la ejecución de las operaciones a través de sistemas interconectados que toman decisiones localmente con impacto global. De esta manera, el entorno operacional se hace dinámico, flexible y en recomposición permanente, por lo que el pensamiento estratégico clásico muta hacia nuevas formas de lógica en redes inteligentes.

Por todo lo anterior, la superioridad militar deja de medirse por el volumen de fuego, la cantidad de hombres en armas o la extensión del territorio ocupado, y pasa a medirse por la adaptación algorítmica, la flexibilidad táctica y, consecuentemente, la velocidad de la reorganización operativa. Las operaciones en enjambre se fundamentan en una lógica distribuida, operada por la IA, que reduce significativamente el control humano, lo que le da una ventaja disruptiva siempre presente, por cuanto reconfigura las funciones y sincroniza las acciones en tiempo real. Esta superioridad adaptativa impone una nueva forma de generación de estrategia militar contemporánea, la cual se centra cada vez más en la agilidad y la inteligencia distribuida, fundamentos clave en el poder militar del siglo XXI.

Referencias

- Allen, G., & Chan, T. (2017). *Artificial intelligence and national security*. Belfer Center for Science and International Affairs, Harvard Kennedy School. <https://www.belfercenter.org/publication/artificial-intelligence-and-national-security>
- Araya, D., & King, M. (2022). *The impact of artificial intelligence on military defence and security* (CIGI Papers No. 263). Centre for International Governance Innovation. <https://www.cigionline.org/publications/the-impact-of-artificial-intelligence-on-military-defence-and-security/>
- Barrero-Barrero, D. (2020). La estrategia de la disuasión: una variable independiente y potencializadora frente al poder aéreo integral del Estado nación en el siglo XXI. En F. Baquero-Valdés (Ed.), *El poder aéreo integral del Estado nación en el siglo XXI* (pp. 167-183). Sello Editorial ESDEG. <https://doi.org/10.25062/9789584289018.08>
- Clausewitz, C. von. (2024). *De la guerra: versión íntegra*. Ediciones MI-LLA.
- Department of the Air Force. (2015). *Air Force future operating concept: A view of the Air Force in 2035*. United States Air Force. <https://www.af.mil/Portals/1/images/air-power/AFFOC.pdf>
- Fadok, D. S. (1995). *John Boyd and John Warden: Air power's quest for strategic paralysis*. Air University Press.
- Fernández-Montesinos, F. A. (2018). Repensando la guerra asimétrica. *bie3: Boletín IEEE*, (9), 214-239.
- Gupta, S. G., Ghonge, M. M., & Jawandhiya, P. M. (2013). Review of unmanned aircraft system (UAS). *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 2(4), 1646-1658. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3451039
- Harari, Y. N. (2020, 24 de enero). *Read Yuval Harari's blistering warning to Davos in full*. World Economic Forum. <https://www.weforum.org/stories/2020/01/yuval-harari-warning-davos-speech-future-predictions/>

- Jordán, J. (2021). The future of unmanned combat aerial vehicles: An analysis using the Three Horizons framework. *Futures*, 134, 102848. <https://doi.org/10.1016/j.futures.2021.102848>
- King, A. (2023). Artificial intelligence and urban operations. *Journal of Strategic Security*, 16(3), 100-115. <https://doi.org/10.5038/1944-0472.16.3.2157>
- Kumar, A. (2020). Drone proliferation and security threats: A critical analysis. *Indian Journal of Asian Affairs*, 33(1/2), 43-62. <https://www.jstor.org/stable/27003434>
- Lewis, J. A. (2014). *Disruptive technologies and the future of deterrence*. Center for Strategic and International Studies. <https://www.csis.org/analysis/disruptive-technologies-and-future-deterrence>
- McCarthy, N. (2019, 19 de noviembre). *The countries set to dominate drone warfare*. Statista. <https://www.statista.com/chart/20005/total-forecast-purchases-of-weaponized-military-drones/>
- Pulido, G. (2022). *Guerra multidominio y mosaico: El nuevo pensamiento militar estadounidense*. Los Libros de la Catarata.
- Qi, D., Zhang, J., Liang, X., Li, Z., Zuo, J., & Lei, P. (2021). Autonomous reconnaissance and attack test of UAV swarm based on mosaic warfare thought. En *2021 6th International Conference on Robotics and Automation Engineering (ICRAE)* (pp. 79-83). IEEE. <https://doi.org/10.1109/ICRAE53653.2021.9657810>
- Rosa, H. (2011). Aceleración social: consecuencias éticas y políticas de una sociedad de alta velocidad desincronizada. *Persona y Sociedad*, 25(1), 9-49.
- Sayler, K. M. (2020). *Artificial intelligence and national security* (CRS Report No. R45178). Congressional Research Service. <https://www.congress.gov/crs-product/R45178>
- Scharre, P. (2018). *Army of none: Autonomous weapons and the future of war*. W. W. Norton & Company.
- U.S. Department of Defense. (2005). *Capstone concept for joint operations* (Version 2.0).
- U.S. Department of Defense. (2018). *Department of Defense artificial intelligence strategy*. <https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/DOD-AI-STRATEGY.PDF>
- United Nations Office for Disarmament Affairs, Stanley Center for Peace and Security, & Stimson Center. (2019). *The militarization of artificial intelligence*. <https://digitallibrary.un.org/record/3972613?ln=es&v=pdf>
- United States Air Force. (s.f.). *MQ-1B Predator*. <https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104469/mq-1b-predator/>
- Vloria, J. (2024). *¿Cómo es la guerra? Conceptualización del conflicto, multiforme, multidimensional y difuso*. Editorial Hormiguero.

Capítulo 2

UAS, inteligencia artificial y toma de decisiones en tiempo real*

DOI: <https://doi.org/10.25062/9786287818620.02>

Fabio Baquero Valdés

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo analiza el impacto de la inteligencia artificial (IA) en los sistemas de aeronaves no tripuladas (UAS), centrando su objetivo en evaluar cómo la IA mejora la toma de decisiones autónomas en tiempo real en operaciones militares. Mediante una revisión analítica de fuentes documentales sobre los algoritmos de aprendizaje supervisado, no supervisado y por refuerzo, se examina su efectividad para enfrentar escenarios dinámicos y adaptarse a condiciones operativas complejas. De igual forma, incluye el análisis de simulaciones computacionales como herramienta clave para validar y optimizar el rendimiento de los UAS. Los resultados evidencian avances en la autonomía operativa, como también desafíos éticos y técnicos asociados a la delegación de decisiones críticas. Finalmente, plantea la necesidad de un marco de gobernanza robusto —ético, técnico y jurídico— que garantice el uso responsable de estos sistemas, con base en principios de transparencia, explicabilidad y rendición de cuentas en entornos de alta incertidumbre.

Palabras clave: autonomía; ciberseguridad; inteligencia artificial; simulación; sistemas de armas; toma de decisiones

* Capítulo de libro resultado del proyecto de investigación "Sistema de naves y aeronaves no tripuladas e inteligencia artificial: innovaciones estratégicas para el futuro militar" del grupo de investigación Masa Crítica de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado en A1 por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) (código COL0123247). Los puntos de vista y los resultados de este capítulo pertenecen a su autor y no reflejan necesariamente los de las instituciones participantes.

Fabio Baquero Valdés

Coronel (R) de la Fuerza Aeroespacial Colombiana. Magíster en educación, Universidad Santo Tomás, Colombia. Profesional en administración aeronáutica, Escuela Militar de Aviación “Marco Fidel Suarez”, Colombia. Docente ocasional asociado e investigador Junior por MinCiencias del grupo de investigación Masa Crítica, Escuela Superior de Guerra “General Rafael Reyes Prieto”, Colombia.

Orcid: <https://orcid.org/0000-0002-5509-322X> - Contacto: fabio.baquero@esdeg.edu.co

Citación APA: Baquero Valdés, F. (2026). UAS, inteligencia artificial y toma de decisiones en tiempo real. En D. Barrero-Barrero (Ed.), *Sistema de naves y aeronaves no tripuladas e inteligencia artificial: innovaciones estratégicas para el futuro militar* (pp. 41-66). Sello Editorial ESDEG.
<https://doi.org/10.25062/9786287818620.02>

SISTEMA DE NAVES Y AERONAVES NO TRIPULADAS E INTELIGENCIA ARTIFICIAL: INNOVACIONES ESTRATÉGICAS PARA EL FUTURO MILITAR

ISBN impreso: 978-628-7818-56-9

E-ISBN digital: 978-628-7818-62-0

DOI: <https://doi.org/10.25062/9786287818620>

Colección Estrategia, Geopolítica y Cultura

Sello Editorial ESDEG

Escuela Superior de Guerra “General Rafael Reyes prieto”

Bogotá D.C., Colombia

2026



Introducción

El desarrollo de los sistemas de aeronaves no tripuladas (UAS) ha revolucionado las operaciones mediante la aplicación de la inteligencia artificial (IA). Estos sistemas, entre otras capacidades, mejoran la toma de decisiones complejas en tiempo real con la integración de la IA, mediante el empleo de algoritmos de planificación de misión; también optimizan la navegación y la respuesta en combate con la aplicación de modelos de aprendizaje profundo, entre otros (Smith & Brown, 2023).

De este modo, la inteligencia artificial se convierte en una herramienta tecnológica que mejora el rendimiento y la autonomía de los UAS cuando se emplea en escenarios de alta complejidad. La toma de decisiones en tiempo real es una capacidad crítica en estos sistemas, puesto que deben procesar grandes volúmenes de datos en condiciones cambiantes, lo que exige una rápida adaptación para operar con altos niveles de precisión.

En consecuencia, surgen dilemas éticos y dificultades técnicas por la aplicación de la IA en los UAS, puesto que, al emplearse algoritmos, se trasladan a estos sistemas responsabilidades de autonomía en la toma de decisiones y en la forma de sortear las complejidades que se presentan en ambientes inconstantes de alto riesgo, como las operaciones militares.

A fin de dar cuenta tanto de los dilemas éticos como de los problemas técnicos y de los avances en materia de simulación que permiten evaluar el rendimiento de UAS de forma autónoma —enfrentándolos a situaciones complejas para examinar su respuesta en la toma de decisiones y en otros procesos igualmente complejos—, y de plantear modelos de gobernanza integral, este capítulo busca responder al siguiente interrogante de investigación: cómo los UAS mejoran su capacidad y rendimiento en las operaciones militares modernas y en la toma de decisiones autónomas en tiempo real con la aplicación de la IA.

Con este fin, se desarrollan temas específicos relacionados con las categorías de análisis extraídas del estado del arte del objeto de investigación.

El primer apartado explica cómo los algoritmos actuales de la IA utilizados en la toma de decisiones en los UAS mejoran su efectividad en situaciones dinámicas, toda vez que han desarrollado capacidades de autonomía mediante el procesamiento de grandes volúmenes de datos en tiempo real, en condiciones complejas y con altos niveles de precisión.

La segunda parte advierte sobre los problemas técnicos y éticos derivados de la toma de decisiones en los UAS —como la precisión en la percepción del entorno y la robustez de los algoritmos de decisión—, así como sobre los dilemas éticos significativos que plantea la delegación de decisiones críticas, con implicaciones profundas en la responsabilidad y la moralidad.

El tercer apartado plantea el uso de simulaciones para evaluar el rendimiento de UAS autónomos en situaciones complejas y cómo estas pueden mejorar la toma de decisiones. Finalmente, se presentan las conclusiones del análisis como respuesta al interrogante de investigación planteado.

Algoritmos de IA usados en la toma de decisiones de UAS y su efectividad en situaciones dinámicas

Los algoritmos de inteligencia artificial empleados en los UAS son estructuras computacionales diseñadas para procesar información del entorno, evaluar alternativas de acción y seleccionar la más adecuada en función de un objetivo determinado, de manera autónoma o semiautónoma. Estos algoritmos pueden incluir desde modelos de aprendizaje supervisado, no supervisado y por refuerzo hasta redes neuronales profundas, sistemas expertos y lógica difusa.

Como lo señalan García et al. (2021), “los algoritmos de IA aplicados en UAS permiten interpretar datos del entorno en tiempo real y ejecutar decisiones tácticas sin intervención humana directa, aumentando su autonomía y efectividad operativa” (p. 45). Además, León et al. (2022) argumentan que estos algoritmos no solo replican patrones aprendidos, sino que también pueden adaptarse dinámicamente a condiciones cambiantes, especialmente en contextos militares, donde “la capacidad de aprendizaje autónomo incrementa el valor estratégico de los UAS en escenarios hostiles e impredecibles” (p. 67).

Los algoritmos más utilizados en la toma de decisiones aplicadas a los UAS y su efectividad en situaciones cambiantes muestran cómo la inteligencia artificial ha transformado la capacidad de autonomía de estos sistemas, al permitirles actuar con creciente independencia del control humano, incluso en entornos complejos y dinámicos. Esto mejora su rendimiento en ambientes de alta complejidad y favorece una toma de decisiones rápida y precisa. Sin embargo, la toma de decisiones en tiempo real continúa siendo un componente crítico en los UAS, puesto que deben procesar grandes volúmenes de datos en condiciones cambiantes y con alta exigencia de operación y precisión.

Entre los principales modelos utilizados se encuentran los algoritmos de aprendizaje profundo, los sistemas de control basados en lógica difusa y los métodos de refuerzo (Fernández et al., 2020). Estudios recientes plantean que los algoritmos de aprendizaje profundo emplean redes neuronales convolucionales (CNN, por sus siglas en inglés) y redes neuronales recurrentes (RNN, por sus siglas en inglés), y demuestran su efectividad en el reconocimiento de patrones y en la predicción de trayectorias óptimas para la navegación de los UAS en entornos no estructurados (García & Ramírez, 2021).

En lo que respecta a los enfoques basados en lógica difusa, estos han sido aplicados para mejorar la estabilidad y maniobrabilidad de los UAS en condiciones meteorológicas adversas, facilitando la adaptación de los parámetros de vuelo en tiempo real (López et al., 2019). Por otro lado, los métodos de aprendizaje por refuerzo, como el algoritmo *Deep Q-Network* (DQN), han sido empleados para la optimización de trayectorias y la evitación de obstáculos en entornos dinámicos. De este modo, los UAS equipados con IA pueden ajustar su comportamiento en función de las condiciones del ambiente, mediante modelos híbridos que combinan aprendizaje profundo con sistemas expertos.

En términos de efectividad, las simulaciones han demostrado que la combinación de redes neuronales con algoritmos de optimización evolutiva mejora la capacidad de reacción de los UAS ante amenazas imprevistas, como sistemas de interferencia electrónica o la presencia de aeronaves hostiles (Rodríguez et al., 2023). Este tipo de integración entre IA y modelos de control autónomo es fundamental para la evolución de los sistemas de aeronaves no tripuladas en operaciones militares.

Modelos de IA en la toma de decisiones de UAS

La toma de decisiones en tiempo real en los UAS depende de algoritmos avanzados de IA que permiten procesar datos y adaptarse a escenarios dinámicos. Entre los principales modelos se encuentran los siguientes:

Algoritmos de aprendizaje profundo

Los algoritmos de aprendizaje profundo han demostrado ser efectivos en el reconocimiento de patrones y en la predicción de trayectorias óptimas para la navegación de UAS en entornos no estructurados (Fernández et al., 2020). Entre estos se destacan:

- Redes Neuronales Convolucionales (CNN): utilizadas para el procesamiento de imágenes captadas por sensores de los UAS, permitiendo la identificación de obstáculos, terrenos y objetivos.
- Redes Neuronales Recurrentes (RNN): aplicadas en la predicción de trayectorias y del comportamiento de objetos en movimiento, permitiendo a los UAS ajustar su ruta en función del entorno (García & Ramírez, 2021, p. 89).

El MQ-9 Reaper (Figura 1) es una plataforma utilizada por la Fuerza Aérea de los EE.UU. e incorpora redes neuronales convolucionales (CNN) para el procesamiento de imágenes en tiempo real. Este sistema ha sido entrenado para detectar y clasificar amenazas, como vehículos blindados o insurgentes armados, incluso en áreas urbanas densas, lo que permite acelerar la toma de decisiones y reducir la carga cognitiva de los operadores (Sayler, 2020).

En el caso del sistema naval Sea Hunter (Figura 2), la IA basada en redes neuronales recurrentes y aprendizaje por refuerzo permite al sistema patrullar de forma autónoma durante semanas, evitar colisiones y seguir embarcaciones sin intervención humana, lo cual ha revolucionado la vigilancia marítima estratégica (Leidos, 2020).

Sistemas de control basados en lógica difusa

La lógica difusa ha sido aplicada para mejorar la estabilidad y maniobrabilidad de los UAS en condiciones meteorológicas adversas. Este enfoque permite que los UAS ajusten sus parámetros de vuelo en tiempo real según las condiciones ambientales (López et al., 2019, p. 112). Un ejemplo de ello es su implementación en sistemas de control autónomo para el aterrizaje en terrenos no preparados.

Figura 1. MQ-9 Reaper de la USAF



Fuente: Aeroweb, 27 de noviembre de 2015

Figura 2. Buque de superficie no tripulado de desplazamiento medio Sea Hunter



Fuente: Marina de los EE.UU., foto por el especialista en comunicación de masas de tercera clase Aleksandr Freutel

El RQ-4 Global Hawk (Figura 3), un UAS de gran altitud, utiliza controladores basados en lógica difusa para mantener la estabilidad de vuelo ante condiciones meteorológicas adversas. Esta tecnología permite adaptar el comportamiento del UAS de manera continua según cambios en variables como la turbulencia o la presión atmosférica, lo cual ha demostrado ser efectivo en misiones de vigilancia transoceánica (Núñez-Mata et al., 2018).

Figura 3. RQ-4 Global Hawk de la USAF



Fuente: U.S. Air Force, foto por Bobbi Zapka

El MQ-1 Predator (Figura 4), antecesor del Reaper, integró modelos híbridos de lógica difusa con redes neuronales para la priorización de objetivos. Durante operaciones en Irak y Afganistán, permitió gestionar múltiples amenazas al mismo tiempo, ajustando el plan de ataque según la información sensorial recibida (González et al., 2019).

Algoritmos de aprendizaje por refuerzo

Los métodos de aprendizaje por refuerzo profundo (DRL, *deep reinforcement learning*), como el algoritmo *Deep Q-Network* (DQN), han sido empleados para la optimización de trayectorias y la evitación de obstáculos en entornos dinámicos.

Figura 4. MQ-1 de la USAF



Fuente: Fuerza Aérea de EE.UU. / Teniente Coronel Leslie Pratt

Estos algoritmos permiten a los UAS ajustar su comportamiento en función de las recompensas obtenidas por acciones previas, mejorando así su capacidad de decisión en tiempo real (Rodríguez et al., 2023, p. 134).

El XQ-58A Valkyrie, desarrollado por la USAF y la Defense Advanced Research Projects Agency (DARPA), emplea DRL para realizar maniobras autónomas de combate y evasión. Entrenado en simuladores y posteriormente validado en vuelos reales, aprende a optimizar decisiones tácticas frente a amenazas cambiantes, como radares enemigos o misiles SAM (DARPA, 2021).

Efectividad de los algoritmos en operaciones militares

En términos de efectividad, las simulaciones han demostrado que la combinación de redes neuronales con algoritmos de optimización evolutiva mejora la capacidad de reacción de los UAS ante amenazas *imprevistas*, como sistemas de interferencia electrónica o la presencia de aeronaves hostiles (Rodríguez et al., 2023, p. 157) (Tabla 1). Ejemplo de ello es la integración de IA en sistemas de defensa aérea, donde los UAS equipados con algoritmos de aprendizaje profundo han sido utilizados para patrullas autónomas y respuestas a amenazas sin intervención humana.

Figura 5. XQ-58A Valkyrie



Fuente: USAF, foto por el aviador superior Joshua Hoskins

Tabla 1. Comparación de UAS por algoritmo IA aplicado, toma de decisiones, resultado y contexto operacional.

UAS	Algoritmo IA aplicado	Aplicación en toma de decisiones	Resultados y contexto operacional
MQ-9 Reaper	CNN (Deep Learning)	Detección y clasificación de amenazas visuales	Ataques precisos y rápidos en Siria y Afganistán
RQ-4 Global Hawk	Control basado en lógica difusa	Navegación autónoma en mal clima	Éxito en misiones de reconocimiento transoceánicas
XQ-58A Valkyrie	Deep Reinforcement Learning	Maniobras evasivas y combate autónomo	Adaptación dinámica frente a amenazas simuladas (USAF, DARPA)
MQ-1 Predator	Algoritmos híbridos (NN + fuzzy)	Priorización de objetivos múltiples	Eficiencia táctica en conflictos asimétricos
Sea Hunter	RNN + RL	Patrullaje y seguimiento de embarcaciones	Navegación autónoma continua en misiones de semanas

Fuente: Elaboración propia

Clasificación de algoritmos utilizados en los UAS

Los algoritmos empleados en los UAS se clasifican en tres categorías principales. En primer lugar, el aprendizaje supervisado permite entrenar modelos predictivos a partir de datos etiquetados. En segundo lugar, el aprendizaje no supervisado facilita la identificación de patrones en datos no etiquetados, lo que facilita la adaptación de los UAS a escenarios complejos. Por último, el aprendizaje por refuerzo permite optimizar maniobras y estrategias de vuelo con base en experiencias previas.

Algoritmos de aprendizaje supervisado

Los algoritmos de aprendizaje supervisado cumplen un papel central en la toma de decisiones de los UAS, pues utilizan datos etiquetados para entrenar modelos capaces de predecir resultados a partir de nuevas entradas. En este campo, los *algoritmos de clasificación* permiten identificar objetos, como vehículos enemigos o estructuras clave, mientras que los *algoritmos de regresión* se emplean para predecir trayectorias de vuelo y condiciones atmosféricas adversas. Estas aplicaciones explican su amplio uso en tareas de reconocimiento visual, clasificación y predicción. Como ejemplo, Smith (2022) reporta que los UAS con aprendizaje supervisado han logrado mejorar la precisión en el reconocimiento de objetivos en un 30 % en comparación con métodos tradicionales (p. 78) (Tabla 2).

Tabla 2. Algoritmos de aprendizaje supervisado

Algoritmo	Función	Ejemplo en UAS	Plataforma / caso de uso
Redes Neuronales Convolucionales (CNN)	Clasificación de imágenes	Reconocimiento de objetivos (vehículos enemigos, estructuras) en imágenes térmicas	MQ-9 Reaper, usado para identificar amenazas
Support Vector Machine (SVM)	Clasificación binaria o multiclase	Clasificación de terreno: urbano, desértico, montañoso	Drones tácticos para planificación de misión ISR
Random Forest	Clasificación y predicción robusta	Detección de eventos anómalos en vuelos (fallos de motor, interferencias GPS)	UAVs de reconocimiento técnico en zonas urbanas
Regresión Lineal / Logística	Predicción de variables continuas o probabilidades	Predicción de fallas de vuelo o necesidad de mantenimiento preventivo	UAS logísticos en zonas de conflicto
k-NN (k-Nearest Neighbors)	Clasificación basada en vecinos más cercanos	Detección de patrones de tráfico aéreo hostil	Drones de vigilancia para defensa aérea (p. ej., en Ucrania)

Fuente: Elaboración propia

Algoritmos de aprendizaje no supervisado

El aprendizaje no supervisado permite a los UAS identificar patrones en datos no etiquetados, lo que resulta especialmente útil en contextos donde no se cuenta con información previa suficiente. Entre sus principales aplicaciones se encuentran el *clustering*, empleado para agrupar datos similares, como tipos de terreno o formaciones enemigas, y la *reducción de dimensionalidad*, orientada a simplificar grandes volúmenes de datos y facilitar su procesamiento en tiempo real. Por ello, este tipo de aprendizaje es particularmente valioso en misiones exploratorias, tareas de vigilancia y procesos de minería de datos. Como ejemplo, Zhang (2020) analizó cómo los algoritmos de *clustering* han mejorado la detección de formaciones hostiles en zonas de conflicto (p. 92) (Tabla 3).

Tabla 3. Algoritmos de aprendizaje no supervisado

Algoritmo	Función	Ejemplo en UAS	Plataforma / caso de uso
K-Means Clustering	Agrupamiento automático	Identificación de grupos de calor (aglomeraciones humanas o animales) desde sensores infrarrojos	Drones ISR de control fronterizo (CBP USA)
Autoencoders	Reducción dimensional, detección de anomalías	Identificación de trayectorias de vuelo no convencionales	Drones autónomos para vigilancia de infraestructura crítica
PCA (Análisis de componentes principales)	Reducción de ruido de datos multidimensionales	Limpieza y combinación de señales LIDAR, radar y cámaras	UAV en escenarios costeros y de vigilancia aérea-marítima
DBSCAN (Density-Based Spatial Clustering)	Agrupamiento en datos no lineales	Detección de convoyes enemigos o movimientos sospechosos en el terreno	Simulaciones para guerra irregular o urbana
t-SNE (t-distributed Stochastic Neighbor Embedding)	Visualización de datos complejos	Análisis de grandes volúmenes de datos ISR	UAS estratégicos para análisis posterior de inteligencia

Fuente: Elaboración propia

Algoritmos de aprendizaje por refuerzo

El aprendizaje por refuerzo es fundamental para la toma de decisiones en tiempo real, ya que permite que los UAS optimicen sus estrategias de vuelo a partir de recompensas y penalizaciones derivadas de su interacción con el entorno. En este marco, algoritmos como *Q-learning* y *Deep Q-Network* (DQN) se utilizan en

el entrenamiento de maniobras evasivas, la planificación de rutas seguras, la navegación autónoma, el combate aire-aire y las operaciones en enjambre. Como ejemplo, García (2023) reportó que los UAS equipados con DQN mejoraron su capacidad de navegación en entornos urbanos en un 40 % (p. 110) (Tabla 4).

Tabla 4. Algoritmos de aprendizaje por refuerzo

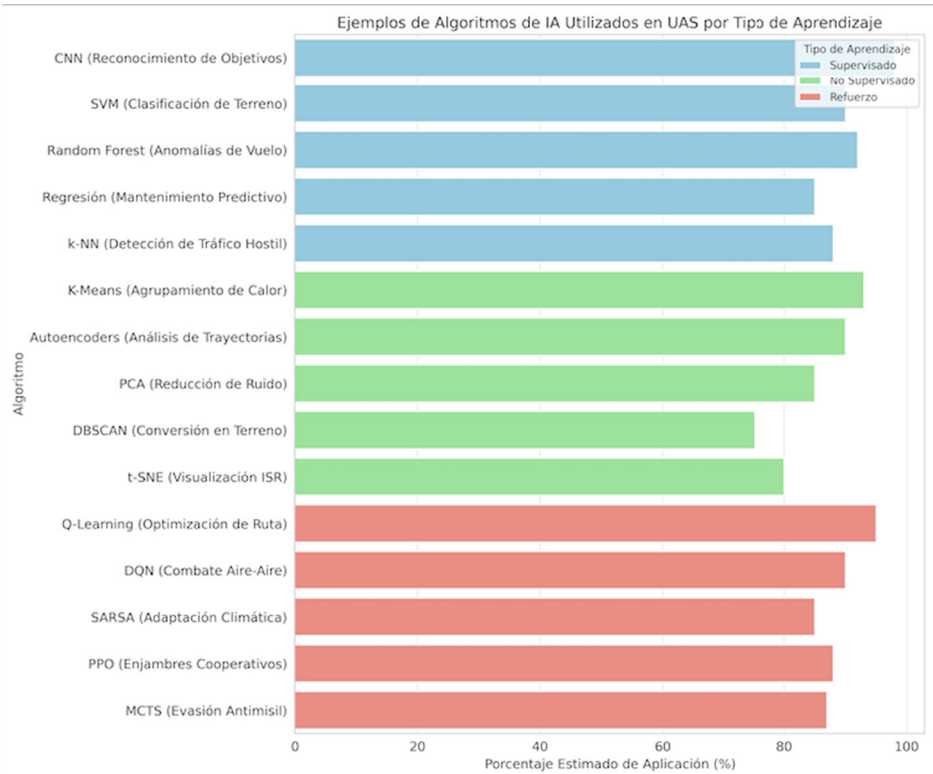
Algoritmo	Función	Ejemplo en UAS	Plataforma / caso de uso
<i>Q-Learning</i>	Aprendizaje por ensayo y error	Optimización de rutas de vuelo para evitar amenazas	UAV tácticos desplegados en áreas hostiles
<i>Deep Q-Networks (DQN)</i>	Aprendizaje profundo con estados visuales	Simulación de combate aire-aire en entornos realistas	Proyecto AlphaDogfight de DARPA
SARSA	Mejora de decisiones en entornos dinámicos	Adaptación de comportamiento según clima y obstáculos móviles	UAV de largo alcance en zonas desérticas
<i>Proximal Policy Optimization (PPO)</i>	Coordinación multiagente, estabilidad de políticas	Enjambres de drones autónomos que dividen tareas (vigilancia, ataque, transporte)	Simulaciones NATO de enjambres ofensivo-defensivos
Monte Carlo Tree Search (MCTS)	Planificación de decisiones en escenarios inciertos	Simulación de trayectorias posibles frente a amenazas dinámicas	UAV con capacidades de evasión activa (antimisil)

Fuente: Elaboración propia

En conjunto, los algoritmos de IA —incluidos el aprendizaje supervisado, no supervisado y por refuerzo— han demostrado ser efectivos en la toma de decisiones de los UAS en situaciones dinámicas. Estos avances han permitido incrementar progresivamente la autonomía y la eficiencia de estos sistemas. No obstante, persisten desafíos técnicos y éticos, como la confiabilidad de los algoritmos en escenarios no previstos y la necesidad de garantizar la supervisión humana en la toma de decisiones.

La Figura 6 muestra la clasificación de algoritmos utilizados en UAS, organizada en tres tipos de aprendizaje automático, con ejemplos específicos y aplicaciones concretas en cada categoría. La gráfica representa el rendimiento estimado (en porcentaje) para aplicaciones militares o ISR (*Intelligence, Surveillance, Reconnaissance*).

Figura 6. Algoritmos de aprendizaje automático utilizados en UAS por tipo de aprendizaje



Fuente: Elaboración propia

Problemas técnicos y éticos en la toma de decisiones de UAS

Los UAS han revolucionado el campo de la aviación militar y civil, abriendo nuevas posibilidades en operaciones de vigilancia, reconocimiento, logística y combate. Sin embargo, el creciente grado de autonomía que se les confiere ha traído consigo importantes desafíos técnicos y éticos. Estos desafíos no solo afectan el rendimiento operacional, sino que también plantean interrogantes sobre la moralidad y la legalidad de las decisiones que pueden tomar estas plataformas. Este acápite desarrolla ambos tipos de problemáticas, con ejemplos y referencias que permiten comprender sus implicaciones y posibles soluciones.

Desafíos técnicos en la toma de decisiones de UAS

A medida que los UAS se integran cada vez más en operaciones complejas, tanto en entornos militares como civiles, se enfrentan a una serie de desafíos técnicos que condicionan su efectividad. Estos desafíos no solo comprometen la capacidad de las aeronaves para cumplir sus misiones, sino que también afectan la seguridad operacional y la confiabilidad de sus decisiones. La autonomía en los UAS implica que gran parte del proceso de toma de decisiones se delega a algoritmos y sensores, los cuales deben funcionar en condiciones dinámicas y, muchas veces, impredecibles. En este contexto, aspectos como la percepción del entorno, la fusión de datos, el procesamiento en tiempo real y la ciberseguridad se convierten en factores críticos para garantizar un desempeño aceptable y seguro.

Percepción del entorno

Uno de los principales desafíos técnicos que enfrentan los UAS es la comprensión precisa del entorno. Para operar de forma autónoma, estas plataformas deben interpretar correctamente la información sensorial en tiempo real, lo cual requiere sistemas de visión por computadora, sensores LIDAR, radar y otros dispositivos de percepción.

Según Patel (2022), “la percepción es crítica para evitar colisiones, identificar objetivos y navegar de forma segura” (p. 81). Sin embargo, la calidad de la información recolectada puede verse afectada por condiciones climáticas, interferencias electromagnéticas o entornos urbanos complejos. Estas limitaciones afectan directamente la capacidad de los algoritmos de toma de decisiones.

Un UAS desplegado en una zona urbana puede confundirse entre objetivos legítimos y civiles debido a sombras, estructuras complejas o movimientos impredecibles de personas, lo que pone en riesgo la precisión de sus decisiones.

Fusión de datos y robustez algorítmica

La fusión de datos es el proceso mediante el cual se combinan diversas fuentes de información para obtener una representación coherente del entorno. Este proceso es esencial en escenarios dinámicos. Patel (2022) señala que “la integración efectiva de múltiples sensores es fundamental para lograr decisiones confiables en situaciones complejas” (p. 87).

No obstante, los algoritmos actuales todavía presentan dificultades ante datos contradictorios o faltantes, así como frente a situaciones imprevistas que no fueron contempladas en su entrenamiento. Esto afecta la robustez del sistema.

Durante una misión de patrullaje marítimo, un UAS puede recibir datos contradictorios de radar y cámara térmica, lo que puede conducir a un error en la clasificación de una embarcación, con consecuencias tácticas relevantes.

Procesamiento en tiempo real y limitaciones computacionales

La toma de decisiones en tiempo real requiere una elevada capacidad de procesamiento, especialmente cuando se trata de tareas críticas como la evasión de amenazas o la selección de objetivos. Sin embargo, los UAS están limitados por el peso, el tamaño y el consumo energético de sus sistemas computacionales.

De acuerdo con Bellingham et al. (2021), “las restricciones físicas de los UAS imponen un límite significativo en los algoritmos que pueden implementarse a bordo” (p. 92). Esto obliga a priorizar entre velocidad y precisión, lo que puede generar fallos operativos en entornos altamente dinámicos.

Seguridad cibernética y resiliencia ante interferencias

La conectividad de los sistemas de aeronaves no tripuladas (UAS), tanto con los centros de mando y control como entre las propias plataformas, constituye un vector crítico de vulnerabilidad cibernética, ya que su dependencia de enlaces de comunicación —incluidas infraestructuras emergentes como redes 5G y enlaces de datos avanzados— amplía significativamente la superficie de ataque. Esta conectividad expone a los UAS a amenazas como ataques de denegación de servicio (DoS/DDoS), interceptación o manipulación de comunicaciones, *spoofing*, inyección de datos maliciosos y accesos no autorizados a los sistemas de control, lo que puede comprometer no solo la integridad de los enlaces, sino también los sistemas de apoyo a la toma de decisiones y los algoritmos que gobiernan su comportamiento, induciendo degradaciones operativas, alteraciones funcionales o decisiones perjudiciales en entornos altamente disputados.

Según Ben-Asher y Gonzalez (2020), “la ciberseguridad debe considerarse parte integral de la arquitectura de decisión de los UAS, ya que una brecha puede comprometer toda la misión” (p. 101).

Consideraciones éticas en la toma de decisiones autónoma

El avance tecnológico ha permitido que los UAS asuman funciones que antes eran exclusivas de los operadores humanos, incluidas tareas en las que está en juego la vida humana. Esta delegación de decisiones críticas plantea interrogantes éticos profundos sobre la moralidad, la legalidad y la responsabilidad asociada a las acciones de los sistemas autónomos. A diferencia de los desafíos técnicos, que

pueden abordarse mediante soluciones ingenieriles, los dilemas éticos requieren una reflexión filosófica y jurídica sobre los límites de la automatización. ¿Es éticamente aceptable que una máquina decida cuándo y cómo emplear fuerza letal? ¿Quién debe rendir cuentas por un error catastrófico en una operación autónoma? Estas preguntas se vuelven cada vez más urgentes ante el avance de los UAS con mayor capacidad de decisión.

Delegación de decisiones críticas

Uno de los debates más intensos en torno al uso de UAS autónomos es si se les debe permitir tomar decisiones críticas, como el uso de la fuerza letal, sin intervención humana. Esta posibilidad despierta preocupaciones sobre la moralidad, la responsabilidad y la legalidad de dichas acciones.

Sharkey (2012) argumenta que “delegar la decisión de matar a una máquina viola principios fundamentales del derecho internacional humanitario y la ética militar” (p. 73). Aun cuando la tecnología avance, la falta de juicio moral en los algoritmos sigue siendo un obstáculo insalvable.

Problemas de imputabilidad y responsabilidad

Cuando un UAS toma una decisión equivocada con consecuencias letales, surge la cuestión de quién es responsable: ¿el operador, el programador, el comandante o el fabricante? Este vacío de imputabilidad plantea un serio problema ético y legal.

Cummings (2020) advierte que “la cadena de responsabilidad se difumina peligrosamente cuando se introducen sistemas autónomos en funciones sensibles” (p. 58). Si nadie puede rendir cuentas, se vulnera el principio de justicia.

Un ataque ejecutado por un UAS sin intervención humana que termina afectando a civiles puede no tener un responsable claro, lo que complica la reparación a las víctimas y la sanción a los responsables.

Discriminación y proporcionalidad

El principio de discriminación exige distinguir entre combatientes y no combatientes, y el de proporcionalidad requiere que los daños colaterales no excedan el objetivo militar. Estos principios son difíciles de codificar en algoritmos.

Arkin (2009) reconoce que “aunque los sistemas automatizados pueden tener una menor tasa de error que los humanos, su capacidad para interpretar contextos morales es limitada” (p. 65). Los UAS no pueden, por ejemplo, valorar la intención de una persona o el valor simbólico de un objetivo.

Transparencia y explicabilidad

Para que las decisiones de un UAS sean aceptadas éticamente, deben ser explicables y auditables. Sin embargo, muchos algoritmos de aprendizaje profundo funcionan como “cajas negras” difíciles de entender, incluso para sus creadores. Según Mittelstadt et al. (2016), “la opacidad algorítmica socava la confianza pública y complica los procesos de revisión ética” (p. 88). Esta falta de transparencia se agrava cuando los UAS operan de forma autónoma en situaciones letales.

Hacia una gobernanza ética y técnica de los UAS

Frente a los importantes retos técnicos y éticos que plantean los UAS, resulta indispensable avanzar hacia un modelo de gobernanza integral que articule la innovación tecnológica con principios normativos y valores humanos. Este modelo debe ser capaz de establecer límites claros a la autonomía de los sistemas, asegurar la rendición de cuentas en todas las etapas del ciclo operativo y fomentar el desarrollo de tecnologías más seguras, explicables y responsables.

La gobernanza no debe limitarse a las regulaciones nacionales, sino constituirse como un esfuerzo internacional coordinado que prevenga el uso irresponsable o malintencionado de estos sistemas. Además, debe contemplar marcos éticos para orientar el diseño de algoritmos de decisión, así como mecanismos de transparencia, validación y auditoría que permitan evaluar el comportamiento de los UAS en situaciones reales. Solo mediante la integración de aspectos técnicos, éticos y políticos será posible aprovechar plenamente las capacidades de los UAS sin comprometer la seguridad, la legalidad ni los valores fundamentales que sustentan nuestras sociedades.

Para abordar estos desafíos, es necesario un enfoque multidisciplinario que combine avances tecnológicos con marcos éticos y legales robustos. En el plano *técnico*, se deben desarrollar algoritmos más robustos, explicables y resilientes, capaces de operar en entornos inciertos y dinámicos con un mínimo de errores. En el plano *ético*, se requiere definir límites claros a la autonomía de los UAS, como la necesidad de supervisión humana en decisiones letales, conforme al principio de “*human-in-the-loop*”. En el plano *político*, los Estados deben cooperar para establecer tratados y regulaciones internacionales que eviten la proliferación irresponsable de estas tecnologías.

La autonomía de los UAS en la toma de decisiones ofrece enormes ventajas operacionales, pero también genera profundas preocupaciones técnicas y éticas.

La precisión sensorial, la fusión de datos, la ciberseguridad y la imputabilidad son elementos clave que deben resolverse antes de delegar decisiones críticas a estos sistemas. Solo mediante un enfoque integral que combine tecnología, ética y regulación será posible aprovechar los beneficios de los UAS sin poner en riesgo los principios fundamentales del derecho y la humanidad.

Simulaciones para evaluar el rendimiento y la toma de decisiones de UAS en situaciones complejas

En el desarrollo de sistemas autónomos para UAS, la simulación computacional se ha consolidado como una herramienta indispensable para probar, validar y optimizar los algoritmos de inteligencia artificial en contextos operativos de alta complejidad. Las simulaciones permiten replicar escenarios reales con múltiples variables dinámicas, sin el riesgo ni el costo asociados a operaciones reales.

La capacidad de un sistema autónomo para operar de forma eficiente en entornos inciertos y adversos depende en gran medida de su entrenamiento previo en entornos controlados y de su validación en entornos virtuales realistas antes de su despliegue. Esto resulta especialmente crítico en misiones militares, donde las condiciones pueden cambiar drásticamente en cuestión de segundos.

Las simulaciones representan un campo crucial en el desarrollo de los sistemas autónomos aplicados a los UAS, en tanto permiten modelar entornos operacionales complejos, emular condiciones adversas y evaluar algoritmos de toma de decisiones sin incurrir en riesgos reales. En este contexto, la simulación actúa como una extensión experimental de la teoría de control y del aprendizaje computacional, posibilitando la validación de sistemas en escenarios imposibles o peligrosos de replicar en el mundo real (Kozierski & Cyganek, 2021).

Desde el punto de vista epistémico, la simulación constituye una forma de conocimiento que integra la racionalidad técnica con la anticipación predictiva. Su valor radica no solo en su capacidad de replicar condiciones, sino también en su poder para construir conocimiento operacional a partir del modelado y la iteración de respuestas. En otras palabras, permite observar cómo los UAS “aprenden a decidir” bajo presión e incertidumbre (Brundage et al., 2022).

Tipos de simulaciones aplicadas a UAS

Las simulaciones aplicadas a los UAS no se limitan a la representación del vuelo. También incorporan subsistemas de navegación, detección, comunicación y lógica de decisión. Entre las principales se encuentra la *simulación de hardware-in-the-loop* (HIL), que integra componentes reales, como sensores y controladores, con un entorno virtual. Esto permite validar el comportamiento real de la plataforma bajo condiciones simuladas. Su función epistemológica consiste en hibridar realidad y modelo, anticipando fallas técnicas y validando la integración de subsistemas (Hwangbo et al., 2022).

También destaca la *simulación de entorno operativo*, que reproduce variables del medio, como el clima, el terreno o la presencia de amenazas. Estas simulaciones aportan una dimensión situacional a la toma de decisiones, al replicar la complejidad contextual que enfrentan los UAS en misiones reales.

Por su parte, la *simulación multiagente* explora la interacción entre múltiples UAS, aspecto clave en operaciones de enjambre. En este ámbito se evalúan la toma de decisiones distribuida, la autonomía cooperativa y la gestión del conflicto (Koziarski & Cyganek, 2021).

Finalmente, la *simulación basada en aprendizaje* utiliza entornos generados artificialmente para entrenar redes neuronales profundas mediante técnicas de aprendizaje reforzado. Este tipo de simulación no solo permite validar el rendimiento, sino también optimizar progresivamente los algoritmos en función de los resultados obtenidos (Tabla 5).

Tabla 5. Clasificación de las simulaciones para UAS

Tipo de simulación	Características principales	Ejemplos de uso
Simulación física (hardware-in-the-loop, HIL)	Integra componentes reales con entornos simulados para pruebas precisas.	Evaluación de sensores, controles de vuelo.
Simulación de entorno operativo	Reproduce condiciones meteorológicas, geográficas y amenazas del entorno real.	Misión de reconocimiento en zonas urbanas hostiles.
Simulación de decisión autónoma (multiagente)	Permite evaluar decisiones cooperativas o competitivas entre múltiples UAS.	Coordinación en enjambres de drones.
Simulación basada en aprendizaje (entrenamiento IA)	Entrenamiento de modelos de aprendizaje profundo usando entornos sintéticos.	Detección de objetivos y evasión de amenazas.

Fuente: Hwangbo et al. (2022); Koziarski y Cyganek (2021)

Beneficios clave del uso de simulaciones

La simulación aporta una serie de beneficios estructurales y funcionales que fortalecen la robustez de la toma de decisiones de los UAS:

- Reducción del riesgo experimental: Posibilita experimentar sin comprometer recursos ni seguridad humana. Esto resulta fundamental para validar reglas de enfrentamiento, respuestas en combate o navegación en entornos hostiles.
- Optimización del aprendizaje: A través de simulaciones, se pueden realizar millones de ciclos de entrenamiento en un tiempo reducido, alimentando modelos de aprendizaje profundo con datos enriquecidos.
- Validación de escenarios raros: Algunos eventos de alta complejidad, como emboscadas, ataques cibernéticos o interferencia electromagnética, son difíciles de recrear. La simulación permite evaluarlos bajo condiciones controladas.
- Adaptación contextual: Los UAS pueden ser expuestos a escenarios específicos según la geografía o el teatro de operaciones previsto, anticipando comportamientos no deseados.

Ejemplo aplicado: simulación de enfrentamiento en entorno urbano

En una simulación desarrollada con AirSim y entornos 3D de Unreal Engine, un UAS autónomo fue entrenado mediante DRL para identificar objetivos hostiles en un entorno urbano mixto con presencia de civiles. Se evaluaron distintos protocolos de acción ante amenazas ambiguas y se monitoreó la capacidad del sistema para priorizar la no letalidad y el cumplimiento de las reglas de enfrentamiento (Tabla 6).

Tabla 6. Resultados de evaluación de enfrentamiento en entorno urbano

Métrica evaluada	Sistema sin DRL	Sistema con DRL
Identificación correcta de amenaza (%)	74,5 %	91,3 %
Tiempo medio de decisión (seg)	4,8	2,3
Error de clasificación en civiles (%)	12,4 %	3,6 %

Fuente: Lin et al. (2021)

Limitaciones de las simulaciones aplicadas a UAS autónomos

La simulación se proyecta como un componente indispensable en la arquitectura de toma de decisiones de los UAS autónomos. Su integración con modelos de IA permite desarrollar sistemas más robustos, precisos y confiables en contextos operacionales complejos. Sin embargo, sus resultados deben evaluarse con un criterio crítico que reconozca sus limitaciones epistemológicas, éticas y operativas:

- Representación incompleta de la realidad: Las simulaciones están condicionadas por los modelos que las sustentan. Si el modelo es deficiente, los resultados también lo serán.
- Baja capacidad para emular dilemas éticos reales: Si bien se puede simular el cumplimiento de reglas, resulta extremadamente complejo emular el juicio moral humano (Arkin, 2009).
- Dependencia de la calidad de los datos: La utilidad de una simulación depende de la fidelidad de sus entradas. Una simulación con datos irrelevantes o limitados puede inducir sobreentrenamiento o una falsa sensación de seguridad.
- Reproducción del sesgo algorítmico: Si los algoritmos incorporan sesgos, estos se reproducen y magnifican en la simulación, generando decisiones potencialmente injustas o peligrosas (Brundage et al., 2022).
- El uso de simulaciones en el desarrollo y evaluación de UAS autónomos constituye una fase fundamental para mejorar sus capacidades de toma de decisiones en entornos complejos. Permite reducir el riesgo, aumentar la adaptabilidad y favorecer un comportamiento predecible bajo condiciones adversas. No obstante, su aplicación debe complementarse con validaciones en escenarios híbridos e incorporar principios éticos desde su diseño. Complementar las simulaciones con estas validaciones constituye el camino más razonable hacia una autonomía responsable y eficaz.

Conclusiones

La integración de algoritmos de inteligencia artificial en los sistemas de aeronaves no tripuladas (UAS) ha generado una transformación significativa en la estrategia militar contemporánea. Gracias a su capacidad de operar de forma autónoma en

escenarios dinámicos, estas plataformas han elevado el rendimiento táctico y operativo en misiones de reconocimiento, patrullaje, combate y apoyo logístico. Esta autonomía estratégica permite a los UAS procesar datos sensoriales en tiempo real, seleccionar rutas óptimas, evitar amenazas y ejecutar decisiones con mínima intervención humana, incrementando su efectividad en ambientes hostiles o impredecibles. Este nuevo paradigma tecnológico mejora la eficiencia de las fuerzas armadas al reducir la exposición del personal humano en zonas de alto riesgo y permitir una actuación más rápida, lo cual es vital en conflictos asimétricos. En este contexto, la IA no solo puede constituir una herramienta de apoyo, sino un componente central en la toma de decisiones militares modernas, alterando las relaciones tradicionales entre el operador, el mando y el sistema automatizado.

A pesar de los avances tecnológicos en inteligencia artificial, los UAS autónomos aún enfrentan importantes limitaciones técnicas que comprometen su fiabilidad total en misiones críticas. La precisión en la percepción del entorno continúa siendo un desafío, especialmente en condiciones meteorológicas adversas, espacios urbanos complejos o bajo la influencia de contramedidas electrónicas. La integración de múltiples sensores requiere procesos robustos de fusión de datos que, en algunos casos, no responden con la suficiente rapidez ante eventos no previstos. Además, las limitaciones físicas de los sistemas computacionales embarcados restringen la implementación de modelos de IA de gran escala, lo que obliga a hacer concesiones entre rapidez y profundidad analítica. Sumado a ello, la vulnerabilidad cibernética constituye un riesgo constante, ya que cualquier interferencia externa podría comprometer la misión completa. En consecuencia, es imprescindible continuar el desarrollo de algoritmos más resilientes, modulares y adaptativos, capaces de operar con precisión bajo incertidumbre y de resistir condiciones de estrés operacional.

El uso de UAS para la toma de decisiones en operaciones militares plantea complejos desafíos éticos que no pueden resolverse únicamente desde la ingeniería o la programación. Cuando una plataforma decide de forma autónoma atacar un objetivo, se ingresa en un terreno donde los principios del derecho internacional humanitario, como la proporcionalidad y la discriminación, corren el riesgo de ser vulnerados. La imposibilidad de los algoritmos para interpretar contextos morales o intenciones humanas conlleva un margen de error ético inaceptable en situaciones que implican el uso de la fuerza. Además, la imputabilidad legal queda difuminada: ¿quién es responsable ante una decisión errónea de un UAS? ¿El operador, el programador, el comandante o el fabricante? Esta falta de claridad compromete

los fundamentos de la justicia y la rendición de cuentas. Por ello, es urgente establecer límites normativos y operacionales que garanticen siempre la intervención humana en decisiones letales, bajo el principio de *"human-in-the-loop"*.

Las simulaciones han demostrado ser herramientas indispensables para el desarrollo, validación y mejora de los algoritmos que controlan los UAS. Estos entornos virtuales permiten exponer las plataformas a escenarios de alta complejidad sin los riesgos inherentes a la operación en campo real, lo que favorece tanto la seguridad como la optimización de recursos. Mediante simulaciones basadas en aprendizaje profundo, como el DRL, se pueden realizar millones de iteraciones en poco tiempo, acelerando el proceso de entrenamiento y adaptabilidad de los sistemas. Además, es posible recrear condiciones extraordinarias, como emboscadas, ataques cibernéticos o colapsos comunicacionales, situaciones difíciles de reproducir físicamente. Esta capacidad predictiva y experimental convierte la simulación en un componente central del ciclo de desarrollo de los UAS, permitiendo una comprensión más profunda de su comportamiento bajo estrés. Sin embargo, su valor depende de la fidelidad del modelo, por lo que debe estar acompañada de validaciones en escenarios reales o híbridos.

El avance de los UAS requiere estar acompañado por un modelo de gobernanza integral que articule los avances tecnológicos con marcos normativos y valores éticos compartidos. Esta gobernanza debe establecer mecanismos de supervisión, certificación, auditoría y control que aseguren un uso responsable, transparente y verificable de estas tecnologías. La gobernanza no puede limitarse a una regulación nacional; es urgente construir acuerdos internacionales que eviten la proliferación irresponsable de UAS letales, especialmente en contextos donde no existen mecanismos de rendición de cuentas. Además, los desarrolladores y operadores deben estar sujetos a códigos éticos robustos que incluyan principios como la explicabilidad algorítmica, la trazabilidad de las decisiones y la supervisión humana obligatoria. Las decisiones tomadas por estos sistemas deben ser comprensibles, auditables y justificables ante instancias jurídicas y sociales. Solo a través de un enfoque multilateral, interdisciplinario y orientado por los derechos humanos podrá garantizarse una autonomía tecnológica que no desplace los principios fundamentales de la humanidad y del derecho internacional.

Referencias

- Arkin, R. C. (2009). *Governing lethal behavior in autonomous robots*. CRC Press. <https://doi.org/10.1201/9781420085952>
- Ben-Asher, N., & Gonzalez, C. (2020). Cognitive biases in cyber security decision making. *Cybersecurity*, 3(1), 95-105.
- Bellingham, J., Tillerson, M., Richards, A., & How, J. P. (2021). Multi-task decision-making in autonomous systems. *IEEE Transactions on Robotics*, 37(2), 89-104.
- Brundage, M., Avin, S., Wang, J., Krueger, G., Hadfield, G., & Dafoe, A. (2022). Trustworthy AI in military decision-making: Challenges and solutions. *Journal of AI Research*, 74, 453-478.
- Cummings, M. L. (2020). *Artificial intelligence and the future of warfare*. Chatham House.
- DARPA. (2021). *Autonomous air combat operations (AACO)*. Defense Advanced Research Projects Agency.
- Fernández, J., Ramírez, P., & López, M. (2020). *Aplicación de técnicas de soft computing al modelado y control de vehículos aéreos no tripulados*. Editorial Universitaria.
- García, L., Mendoza, A., & Rojas, D. (2021). *Inteligencia artificial aplicada al control de drones: un estado del arte*. Editorial UNAM.
- García, M. (2023). Mejoras en navegación urbana mediante DQN aplicado a UAS. *Autonomous Flight Studies*, 7(3), 110-125.
- García, L., & Ramírez, P. (2021). Redes neuronales para la autonomía de drones en entornos no estructurados. *Journal of Autonomous Systems*, 12(4), 78-102.
- González, J., Torres, M., & Salazar, D. (2019). Sistemas de control autónomo aplicados al Predator. *Revista de Tecnología Militar*, 45(2), 23-35.
- Hwangbo, M., Kim, J., & Park, J. (2022). Simulation-based reinforcement learning for autonomous UAVs in urban environments. *IEEE Transactions on Aerospace and Electronic Systems*, 58(3), 1421-1432.
- Leidos. (2020). *Sea Hunter: Autonomous maritime operations*. Leidos Corporation.
- León, J., Márquez, R., & Salinas, H. (2022). *Sistema experto para la ayuda en la toma de decisiones en sistemas aéreos no tripulados (UAS)*. Instituto Politécnico Nacional.
- Lin, J., Tao, M., & Zhang, L. (2021). Training autonomous aerial vehicles with deep reinforcement learning in complex scenarios. *Journal of Intelligent & Robotic Systems*, 101(1), 59-72.
- López, M., et al. (2019). Aplicación de lógica difusa en la navegación de UAS bajo condiciones adversas. *Ciencia y Aviación*, 30(3), 112-130.
- Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 1-21. <https://doi.org/10.1177/2053951716679679>

- Núñez-Mata, R., Ortega, C., & López, J. (2018). Aplicación de lógica difusa en UAS estratégicos. *Revista Aeroespacial de Sistemas Autónomos*, 10(1), 55-66.
- Koziarski, M., & Cyganek, B. (2021). Simulators in training deep learning algorithms for autonomous aerial vehicles. *Sensors*, 21(11), 3698.
- Patel, R. (2022). Technical challenges in autonomous UAVs. *Journal of Field Robotics*, 39(1), 78-102. <https://doi.org/10.1002/rob.21987>
- Rodríguez, D., et al. (2023). Optimización de trayectorias en UAS mediante aprendizaje por refuerzo. *Military AI Review*, 18(1), 134-157.
- Sayler, K. (2020). *Emerging military technologies: AI in unmanned systems*. Congressional Research Service.
- Sharkey, N. E. (2012). The evitability of autonomous robot warfare. *International Review of the Red Cross*, 94(886), 787-796.
- Smith, J. (2022). Autonomous UAV decision-making algorithms. *Journal of Intelligent & Robotic Systems*, 45(3), 123-145. <https://doi.org/10.1007/s10846-022-01345-6>
- Smith, J., & Brown, K. (2023). Inteligencia artificial en sistemas aéreos no tripulados: toma de decisiones en tiempo real y aplicaciones de combate. *Revista de Inteligencia Artificial Militar*, 25(4), 112-134.
- Zhang, L. (2020). Real-time decision-making in autonomous UAVs. *Autonomous Robots*, 34(4), 567-589. <https://doi.org/10.1007/s10514-020-09876-3>

Capítulo 3

Tecnología antidrones C-UAS*

DOI: <https://doi.org/10.25062/9786287818620.03>

Carlos Andrés Tavera Flórez

Fuerza Aeroespacial Colombiana

Resumen: El crecimiento acelerado de los sistemas aéreos no tripulados (UAS), comúnmente conocidos como drones, ha transformado significativamente los escenarios contemporáneos de seguridad y defensa. Aunque han demostrado ser herramientas de gran utilidad en ámbitos como la agricultura, la vigilancia y la logística, su uso indebido plantea una amenaza real para la seguridad nacional y la protección de infraestructuras críticas. Ante este panorama, han surgido tecnologías antidrones —conocidas como Counter-Unmanned Aerial Systems (C-UAS)— que integran detección, seguimiento, identificación y neutralización de amenazas no tripuladas. Este capítulo emplea un método descriptivo con énfasis analítico, que permite exponer de manera detallada las tecnologías involucradas y, al mismo tiempo, analizar críticamente sus implicaciones y desafíos. Este capítulo tiene como objetivo examinar el estado del arte de las tecnologías antidrones, analizar sus componentes técnicos clave y reflexionar sobre su aplicabilidad y proyección en el contexto colombiano. Para ello, se abordarán sus fases operacionales, los desafíos normativos y éticos que conllevan, así como experiencias comparadas a nivel internacional que puedan orientar futuras estrategias nacionales de defensa aérea de baja cota. Se examina además el ciclo funcional de estos sistemas, las principales herramientas tecnológicas involucradas (radares, sensores electroópticos, algoritmos de inteligencia artificial y mecanismos de neutralización), así como los desafíos regulatorios, operativos y éticos asociados a su implementación.

Palabras clave: amenaza aérea; contra-UAV; defensa tecnológica; detección; neutralización; seguridad nacional.

* Capítulo de libro resultado del proyecto de investigación "Sistema de naves y aeronaves no tripuladas e inteligencia artificial: innovaciones estratégicas para el futuro militar" en cooperación del grupo de investigación en Estudios Aeroespaciales de la Fuerza Aeroespacial Colombiana - GIEA, categorizado en B por el Ministerio de Ciencia, Tecnología e Innovación (Minciencias) y registrado con el código COL0084209. Los puntos de vista y los resultados de este capítulo pertenecen al autor y no reflejan necesariamente los de las instituciones participantes.

Carlos Andrés Tavera Flórez

Oficial Logístico de la Fuerza Aeroespacial Colombiana. Magíster en logística aeronáutica, Escuela de Posgrados FAC, Colombia. Especialista en seguridad y defensa nacionales, Escuela Superior de Guerra “Rafael Reyes Prieto”, Colombia. Ingeniero aeronáutico, Universidad San Buenaventura, Colombia. Gerente de diseño y desarrollo en la Corporación de la Industria Aeronáutica Colombiana.

Orcid: <https://orcid.org/0009-0002-0786-6432> - Contacto: carlos.tavera@fac.mil.co

Citación APA: Tavera Flórez, C. A. (2026). Tecnología Antidrones C-UAS. En D. Barrero-Barrero (Ed.), *Sistema de naves y aeronaves no tripuladas e inteligencia artificial: innovaciones estratégicas para el futuro militar* (pp. 67-86). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818620.03>

SISTEMA DE NAVES Y AERONAVES NO TRIPULADAS E INTELIGENCIA ARTIFICIAL: INNOVACIONES ESTRATÉGICAS PARA EL FUTURO MILITAR

ISBN impreso: 978-628-7818-56-9

E-ISBN digital: 978-628-7818-62-0

DOI: <https://doi.org/10.25062/9786287818620>

Colección Estrategia, Geopolítica y Cultura

Sello Editorial ESDEG

Escuela Superior de Guerra “General Rafael Reyes prieto”

Bogotá D.C., Colombia

2026



Introducción

Durante la última década, el uso de Sistemas de Aeronaves No Tripuladas (UAS) ha experimentado un crecimiento sin precedentes, impactando tanto el ámbito civil como el militar. En sectores como la agricultura de precisión, la logística, la vigilancia ambiental y las telecomunicaciones, los drones se han consolidado como herramientas de alto valor estratégico (Mogili & Deepak, 2018). Sin embargo, su facilidad de acceso, autonomía y capacidad de modificación los han convertido también en potenciales instrumentos de amenaza.

En Colombia, donde confluyen factores como una geografía compleja, la presencia de grupos armados ilegales y desafíos estructurales de seguridad, los UAV (Vehículos Aéreos No Tripulados) representan un riesgo tangible. Existen casos documentados en los que estos dispositivos han sido empleados para labores de vigilancia ilegal, transporte de sustancias ilícitas e, incluso, como armas ofensivas de bajo costo (Cubillos et al., 2020; Tavera Flórez, 2024).

Frente a estos desafíos, los sistemas antidrones, denominados *Counter Unmanned Aerial Systems* (C-UAS), han surgido como soluciones tecnológicas sofisticadas que integran radares multifrecuencia, sensores de radiofrecuencia, cámaras térmicas, *software* de reconocimiento visual y jammers electromagnéticos (Castrillo et al., 2022; Al-Dosari et al., 2023). Estas plataformas permiten detectar, identificar, seguir y neutralizar drones no autorizados, garantizando así la seguridad de infraestructuras críticas, eventos internacionales, instalaciones militares y zonas urbanas densamente pobladas. Un caso destacado de su aplicación fue el despliegue de un sistema antidrones durante la COP16 de 2024 en Cali, Colombia, donde se protegió exitosamente el espacio aéreo de la Zona Azul, neutralizando amenazas sin afectar las operaciones autorizadas (Atalayar, 2024).

No obstante, subsiste un problema fundamental: la creciente sofisticación y el bajo costo de los drones siguen superando la capacidad de respuesta de los sistemas antidrones, generando un desequilibrio tecnológico y estratégico que amenaza la seguridad nacional y la protección de infraestructuras críticas en Colombia.

Para enfrentar este desafío, el presente capítulo se propone examinar el estado del arte de las tecnologías antidrones, analizar sus componentes técnicos esenciales y reflexionar sobre su aplicabilidad y proyección en el contexto colombiano. Para tal fin, el contenido se organiza en cinco secciones:

1. La amenaza creciente de los drones, donde se describe el fenómeno global y regional del uso indebido de UAV.
2. Tecnologías antidrones actuales, que presentan las soluciones técnicas disponibles y sus capacidades.
3. Ciclo funcional de los sistemas C-UAS, detallando sus fases operativas y la integración tecnológica necesaria.
4. Desafíos en la implementación de sistemas antidrones, que abordan aspectos técnicos, económicos, legales y éticos.
5. Futuro de la tecnología antidrones, explorando tendencias emergentes y perspectivas estratégicas para Colombia.

De este modo, el capítulo pretende brindar al lector una perspectiva integral que sirva como fundamento para desarrollar estrategias nacionales de defensa aérea de baja cota, orientadas a anticipar amenazas y disminuir la vulnerabilidad del país frente al uso indebido de drones. Su propósito es presentar de manera comprensible la problemática, explicar el funcionamiento de las tecnologías diseñadas para contrarrestarla, detallar su aplicación en escenarios reales, analizar los retos técnicos, normativos y económicos que implica su implementación y reflexionar de forma crítica sobre la brecha existente entre el ritmo de avance de estas soluciones tecnológicas y la velocidad con la que evolucionan las amenazas asociadas a los UAV.

La amenaza creciente de los drones

Un indicador importante de la magnitud del desafío que representan los UAV es su inclusión, por primera vez, en la Revisión Anual de Seguridad 2024 de la Agencia Europea de Seguridad Aérea (EASA). Este informe reconoce oficialmente a los

sistemas aéreos no tripulados (UAS) como una categoría relevante para la seguridad operacional de la aviación civil. En su capítulo 6, la EASA analiza 12 incidentes graves registrados en 2023, incluyendo un accidente fatal y otros no fatales, con impactos mínimos sobre la aviación tripulada, pero con alta preocupación por la falta de datos clasificados y reportes estructurados para este tipo de sistemas. Esta iniciativa demuestra la creciente necesidad de ajustar normativas, metodologías de análisis de riesgo y registros operacionales, reflejando así el compromiso por integrar los UAS de forma segura en el espacio aéreo europeo (Infodron, 2025).

El auge de los UAV ha abierto oportunidades significativas en campos como la vigilancia, la agricultura y la logística. Sin embargo, esta misma versatilidad ha permitido su uso por actores no estatales con fines ilícitos. Su bajo costo, facilidad de adquisición, capacidad de modificación y operación remota los convierten en herramientas ideales para actividades delictivas, conflictos asimétricos y operaciones encubiertas (Cubillos et al., 2020; Chaari & Al-Maadeed, 2021):

- *Terrorismo y conflictos asimétricos:* Diversos grupos insurgentes han adaptado drones comerciales para cargar explosivos o realizar misiones de reconocimiento. Ejemplos recientes se han documentado en Medio Oriente, particularmente en Siria e Irak, donde se han utilizado drones armados con cargas improvisadas para atacar instalaciones militares y civiles (Radovanović et al., 2024).
- *Espionaje y vigilancia ilícita:* Los drones permiten la obtención de información estratégica mediante cámaras de alta definición, sensores térmicos, sistemas de visión nocturna e, incluso, tecnología de reconocimiento facial. Su reducido tamaño y la posibilidad de volar a baja altura o en trayectorias poco convencionales los convierten en herramientas ideales para operar de manera encubierta, evitando ser detectados por sistemas tradicionales de vigilancia. Esto ha dado lugar a un incremento de intentos de espionaje industrial, donde empresas rivales utilizan drones para capturar imágenes de instalaciones, procesos de producción o tecnologías patentadas, generando riesgos significativos en términos de propiedad intelectual y competitividad (Casanovas, 2016).

Al respecto, se han reportado incidentes de vigilancia sobre instalaciones gubernamentales, infraestructuras críticas y residencias de altos funcionarios, con fines que van desde la recopilación de información sensible hasta la planificación de actos delictivos o ataques. En contextos militares, drones equipados con sensores avanzados han sido empleados para obtener datos sobre despliegues tácticos,

movimientos de tropas o características de sistemas de defensa, lo que representa un grave riesgo para la seguridad nacional. Además, en el ámbito urbano, los UAV también han sido utilizados para espiar a figuras públicas, periodistas, defensores de derechos humanos o líderes sociales, alimentando preocupaciones sobre violaciones a la privacidad y la protección de datos personales.

Un caso más reciente y de alto impacto fue la denominada Operación Spiderweb, ejecutada por el Servicio de Seguridad de Ucrania el 1.º de junio de 2025, en la cual drones FPV coordinados penetraron profundamente en territorio ruso para atacar activos de la aviación estratégica en múltiples bases aéreas, incluyendo Bélaya, Dyagilevo, Ivanovo-Sévernny, Olenya y Ukrainka. Esta operación, que empleó más de cien drones no tripulados lanzados desde camiones infiltrados y alcanzó aeronaves de largo alcance como bombarderos Tu-95MS y Tu-22M3, se considera el mayor ataque con drones contra bases aéreas rusas hasta esa fecha y ha llevado a replantear paradigmas sobre las capacidades ofensivas de plataformas autónomas o semiautónomas en conflictos interestatales modernos (Plichka, 2025).

- *Narcotráfico y crimen organizado:* En el contexto latinoamericano, especialmente en Colombia y México, grupos criminales han empleado UAV para el transporte de drogas, armas o celulares a través de fronteras y hacia centros penitenciarios (Cubillos et al., 2020).
- *Interferencia en aeropuertos:* Casos como el cierre temporal del aeropuerto de Gatwick, en Londres (2018), por presencia de drones no identificados, demuestran el riesgo que representan para la aviación civil. En Colombia también se han reportado incidentes en cercanías de bases aéreas y aeropuertos regionales (Tavera Flórez, 2024). Un caso relevante se registró en 2022, cuando un dron no identificado fue detectado sobrevolando una instalación aérea militar estratégica, lo que evidenció la vulnerabilidad de infraestructuras críticas frente a incursiones no tripuladas. El UAV, de tipo comercial, fue avistado a baja altura y generó la interrupción temporal de las operaciones para garantizar la seguridad de las aeronaves en vuelo y evitar posibles riesgos de colisión o espionaje. El incidente motivó la activación de protocolos de seguridad y puso de relieve la vulnerabilidad de instalaciones militares frente al uso indebido de estos dispositivos. Aunque las autoridades lograron neutralizar el dron, evidenció la necesidad urgente de contar con sistemas antidrones más robustos y con marcos legales que regulen su operación en espacios aéreos restringidos.

- *Aplicación militar no convencional:* En el conflicto entre Rusia y Ucrania, se ha observado el uso masivo de drones tanto para vigilancia como para ataques dirigidos, así como para operaciones de desinformación (Infodefensa, 2024). Estos hechos reflejan una tendencia creciente hacia la “droneificación” del campo de batalla. Uno de los ejemplos más ilustrativos del papel transformador de los drones en conflictos modernos es la guerra entre Rusia y Ucrania. En este escenario, los UAV han sido utilizados intensamente para tareas de reconocimiento, corrección de artillería, ataques kamikaze y desinformación. Drones comerciales de bajo costo han sido modificados con explosivos y empleados con notable eficacia táctica, redefiniendo el concepto de guerra asimétrica y tecnológica (Voskuil, 2022).

El conflicto ha demostrado que los drones no solo son herramientas auxiliares, sino activos estratégicos que pueden alterar el equilibrio en el campo de batalla. Su capacidad de operar en enjambres, de forma autónoma y con apoyo de IA, ha obligado a replantear doctrinas de defensa y a acelerar el desarrollo de contramedidas tecnológicas. Esta experiencia ofrece una lección clara para países como Colombia, donde la preparación frente a amenazas emergentes es clave para garantizar la soberanía y la seguridad nacional.

Uno de los casos más notorios ocurrió en septiembre de 2019, cuando una serie de ataques coordinados con drones armados impactaron instalaciones petroleras de Saudi Aramco en Arabia Saudita, reduciendo temporalmente en un 50 % la producción nacional de crudo (Kang et al., 2020). Este ataque evidenció cómo una infraestructura crítica puede ser vulnerada con tecnología de bajo costo y fácil acceso.

En América Latina, se han documentado vuelos ilegales de drones sobre instalaciones militares, plantas de energía y eventos de alta seguridad. Fernández-Osorio (2025) señala que, en Colombia, la utilización de UAV por parte de grupos armados organizados ha evolucionado más allá de simples labores de vigilancia. Estudios recientes muestran que disidencias de las FARC, el ELN y otras facciones han incorporado drones con fines ofensivos o de apoyo táctico, intensificando los ataques contra la Fuerza Pública y otras fuerzas del orden en varias regiones del país. Evidencias académicas destacan esta adaptación tecnológica como parte de una transformación más amplia de las tácticas de los grupos ilegales en el marco de la guerra de quinta generación, incluyendo amenazas a la seguridad, control territorial y operaciones de intimidación desde el aire.

Estos casos demuestran la urgencia de contar con tecnologías avanzadas de detección y neutralización, así como con marcos legales que permitan su uso eficaz en la defensa de la soberanía y la seguridad interna.

Tecnologías antidrones actuales

Como parte de los avances contemporáneos en el diseño y operación de sistemas C-UAS, diversos autores han propuesto marcos de referencia cooperativos que faciliten una integración más eficaz entre sensores, plataformas y sistemas de mando y control. Castrillo et al. (2022) subrayan la necesidad de adoptar un enfoque modular y colaborativo, que garantice la interoperabilidad entre sistemas antidrones y otras capacidades de vigilancia o defensa aérea. Esta visión es especialmente relevante en contextos complejos como la protección de infraestructuras críticas, instalaciones gubernamentales o eventos internacionales, donde las amenazas pueden presentarse de forma simultánea y diversa (Atalayar, 2024).

La evolución de los sistemas antidrones refleja la rápida transformación tecnológica del entorno operativo. Actualmente, estas soluciones se dividen en dos grandes componentes: detección y neutralización. Las plataformas más modernas integran sensores multispectrales, algoritmos avanzados de IA y centros de mando y control automatizados, lo que permite responder con mayor velocidad y precisión ante incursiones no autorizadas (Radovanović et al., 2024; Pu, 2019).

Los sistemas C-UAS, en la práctica, funcionan siguiendo un ciclo operacional bien definido, observado tanto en doctrinas militares contemporáneas como en despliegues reales en escenarios de conflicto o grandes eventos internacionales (Infodefensa, 2024). Aunque pueden existir variaciones según el fabricante o el entorno, la secuencia funcional básica suele comprender siete fases, muchas de las cuales se gestionan ya con apoyo de procesos de decisión automatizados gracias a la IA (Al-Dosari et al., 2023).

Ciclo funcional de un sistema C-UAS

El ciclo funcional de un C-UAS constituye un componente operativo especializado dentro de arquitecturas más amplias de defensa y alerta temprana, encargado de integrar de manera electrónica y coordinada los subsistemas tecnológicos destinados a la detección, identificación, seguimiento y neutralización de amenazas aéreas de baja cota. Este ciclo describe cómo y en qué momento intervienen los

distintos componentes, desde la fase preventiva hasta el análisis posterior a un incidente, definiendo el papel que cada uno desempeña para lograr la detección temprana, la identificación precisa, el seguimiento continuo y, en caso necesario, la neutralización de UAV.

La correcta interacción entre sensores radar, sistemas de radiofrecuencia, cámaras electroópticas e infrarrojas, centros de mando y control y mecanismos de neutralización permite crear una respuesta integral y eficaz frente a la creciente amenaza que representan los drones en escenarios civiles y militares. Este apartado expone de forma estructurada cada fase del ciclo, destacando la importancia de la interoperabilidad entre las distintas fases:

1. *Detección.* Aquí intervienen sensores radar de última generación, como los AESA, y sistemas multispectrales capaces de identificar objetos con bajo perfil radar (RCS). El despliegue de radares 3D, especialmente en aeropuertos o eventos de alta seguridad, constituye una práctica habitual. Según Marta y Gamboa (2014), los radares modernos son cruciales para detectar microdrones que vuelan a baja altura y que, por sus características físicas, resultan difíciles de localizar con tecnologías convencionales. En esta etapa, los radares forman el primer anillo de defensa, creando cúpulas de cobertura de hasta 7 kilómetros, dependiendo de su configuración. Sistemas como Crow, integrados por múltiples tipos de radares 3D, han demostrado gran eficacia en escenarios complejos, proporcionando una detección activa y precisa (Atalayar, 2024).
2. *Identificación/clasificación.* Tras la detección, dispositivos pasivos basados en análisis de radiofrecuencia (RF) examinan las señales electromagnéticas, identifican frecuencias específicas y caracterizan el tipo de dron. Esta etapa permite diferenciar si se trata de un UAV comercial, modificado o de fabricación independiente, lo que resulta esencial para clasificarlo como aliado o amenaza (Chaari & Al-Maadeed, 2021). La correcta clasificación evita errores operativos costosos, como la neutralización de drones autorizados.
3. *Seguimiento.* Consiste en el rastreo continuo del objeto mediante sensores electroópticos (EO/IR), cámaras térmicas y sistemas diurnos/nocturnos. Gracias a la IA, estos sistemas pueden mantener el seguimiento de drones incluso a grandes distancias y en condiciones climáticas adversas (Contreras Henao, 2014). En esta fase se confirma visualmente si se trata de un dron enemigo, basándose en su morfología, dimensiones y patrones de vuelo.

4. *Neutralización.* En esta fase se despliegan diversas herramientas tecnológicas, como inhibidores de RF que transmiten señales de alta potencia en las frecuencias del dron para interrumpir su enlace de datos (Radovanović et al., 2024). También se emplea el *spoofing* GPS, que engaña a los UAV autónomos mediante la emisión de rutas falsas (Szabolcsi, 2014). Si estas medidas fallan, se recurre a soluciones cinéticas, como láseres de alta energía, interceptores aéreos o disparos sónicos, para neutralizar físicamente la amenaza (Pu, 2019).
5. *Centro de mando y control.* Esta fase integra todas las fuentes de información procedentes de los distintos sensores, generando una visión cartográfica en tiempo real del espacio aéreo protegido. Permite visualizar las trayectorias de los objetos detectados, tomar decisiones informadas sobre el momento óptimo de intervención y coordinar acciones con otras entidades de seguridad. Al-Dosari et al. (2023) destacan que el centro de mando es esencial para la interoperabilidad y para evitar acciones precipitadas que puedan poner en riesgo a aeronaves civiles o zonas pobladas.
6. *Postanálisis.* Finalmente, esta etapa implica la recopilación y el análisis de datos tras el incidente. Aquí se retroalimenta a los sistemas de IA, ajustando algoritmos de reconocimiento, predicción y respuesta. Además, contribuye a generar lecciones aprendidas que refuerzan futuras intervenciones (Zong-xin, 2021). Esta fase es vital para evolucionar frente a las rápidas innovaciones tecnológicas de los UAV.

Tecnologías de radares de detección y seguimiento

Un aspecto determinante en la eficacia de los sistemas antidrones es el uso de tecnologías radar especializadas. Los diferentes tipos de radar ofrecen capacidades específicas:

- PESA (*Passive Electronically Scanned Array*): utiliza matrices pasivas y es una opción más económica, aunque limitada en el seguimiento dinámico.
- MESA (*Multirole Electronically Scanned Array*): ofrece cobertura de 360°, ideal para misiones de alerta temprana.
- ESA (*Electronically Scanned Array*): permite un escaneo rápido sin partes móviles, mejorando la fiabilidad.
- AESA (*Active Electronically Scanned Array*): cuenta con módulos transmisores independientes, aportando mayor precisión, resistencia a interferencias

y la posibilidad de rastrear múltiples objetivos simultáneamente (Marta & Gamboa, 2014).

Estas tecnologías han demostrado ser cruciales en entornos urbanos y densos, donde drones pequeños, con baja sección transversal de firma radar y maniobras erráticas, exigen niveles de precisión extremadamente altos (Casanovas, 2016).

Una ilustración real de estas capacidades se observó durante la COP16 en Cali, Colombia. Allí se desplegó un sistema antidrones modular que integraba radares tridimensionales, sensores de RF, sistemas EO/IR y plataformas de mando y control. En este evento, se detectaron y neutralizaron 220 amenazas potenciales, logrando inhibir con éxito 70 de ellas, sin afectar la operatividad de los UAV autorizados. Su diseño modular y escalable demostró gran flexibilidad, validando su eficacia en escenarios de alta complejidad operativa (Atalayar, 2024).

Los componentes de este tipo de sistemas incluyen:

- Sensores activos (radares 3D): rastreo preciso de microdrones en entornos complejos.
- Sensores RF: monitoreo y triangulación de señales de UAV y estaciones base.
- EO/IR: cámaras ópticas y térmicas con algoritmos de IA para identificación automática.
- *Jammers*: inhibidores configurables para RF, GPS y enlaces de video.
- Centro de mando: plataforma integral para gestión en 2D/3D y análisis posterior a la operación.

Este enfoque modular permite adaptar los sistemas C-UAS a distintas realidades operativas (urbanas, rurales o tácticas), integrarlos con infraestructuras preexistentes y facilitar la cooperación entre agencias civiles y militares. La experiencia en la COP16 evidenció la importancia de contar con protocolos conjuntos y de mantener la capacidad de evolución tecnológica para anticipar amenazas emergentes (Castrillo et al., 2022).

Desafíos en la implementación de sistemas antidrones

A pesar de los avances tecnológicos en materia antidrones, su implementación efectiva presenta importantes desafíos técnicos, económicos, legales y operativos. Estos obstáculos deben ser comprendidos en profundidad para diseñar

estrategias sostenibles que garanticen su adopción a gran escala sin generar impactos negativos colaterales.

- *Interferencias colaterales:* Los sistemas de neutralización mediante inhibición electromagnética, conocidos como *jammers*, representan una herramienta efectiva para detener drones no autorizados. No obstante, su empleo conlleva riesgos significativos, ya que pueden interferir con otras comunicaciones legales, incluidos sistemas de navegación aérea, enlaces de comunicación de emergencia o redes comerciales (Radovanović et al., 2024). Esta limitación obliga a configurar cuidadosamente las bandas de frecuencia y a delimitar zonas de operación para evitar daños colaterales.
- *Falsos positivos y precisión de identificación:* El reconocimiento e identificación precisos de drones siguen siendo una limitación crítica, especialmente en entornos urbanos densos, donde hay múltiples objetos voladores y señales electromagnéticas. La IA aún enfrenta desafíos para diferenciar drones de aves o aeronaves convencionales, lo que puede generar falsas alarmas o neutralizaciones innecesarias (Chaari & Al-Maadeed, 2021). Estas situaciones afectan la confiabilidad del sistema y demandan mayor inversión en entrenamiento de algoritmos y fusión sensorial.
- *Costos operativos y sostenibilidad:* Uno de los mayores desafíos para los países en desarrollo es el costo elevado de los sistemas C-UAS integrales. A diferencia de los drones comerciales, cuyo precio puede ser bajo, los sistemas de defensa multidominio requieren infraestructura, sensores avanzados, personal capacitado y mantenimiento continuo. Esto puede limitar su despliegue masivo, especialmente en regiones con restricciones presupuestales (Basante, 2020). Además, la rápida evolución tecnológica puede volver obsoletos sistemas adquiridos recientemente.
- *Vacíos regulatorios y restricciones legales:* desde una perspectiva doctrinal, estudios como el de Choi et al. (2021) resaltan que la construcción efectiva de sistemas antidrones requiere no solo avances tecnológicos, sino también la creación de ecosistemas normativos que regulen su uso con claridad. Estos autores plantean que, sin una estructura legal coherente, la adopción de soluciones C-UAS puede verse limitada en su efectividad, especialmente cuando deben operar en zonas densamente pobladas o de alto valor estratégico.

La normativa internacional sobre el uso de tecnologías antidrones es aún incipiente. La mayoría de los marcos jurídicos carecen de definiciones claras sobre

la legalidad de interceptar o derribar drones, lo que puede generar conflictos entre operadores civiles, autoridades de aviación y fuerzas de seguridad (Szabolcsi, 2014). En Colombia, aunque existen esfuerzos por actualizar la legislación, persisten ambigüedades sobre la responsabilidad legal en caso de daños a terceros o invasión de privacidad (Pérez Pinzón, 2015).

Asimismo, las operaciones en zonas urbanas presentan dificultades añadidas por la densidad poblacional y la presencia de infraestructura crítica, lo que limita el uso de sistemas cinéticos o de alta potencia. La regulación debe encontrar un equilibrio entre seguridad y derechos civiles.

Diversos estudios especializados han señalado que los C-UAS pueden adaptarse a una amplia variedad de escenarios operacionales, incluidos entornos urbanos complejos, infraestructuras críticas y eventos de alto perfil. En particular, los sistemas basados en detección por radiofrecuencia, interferencia electrónica y arquitecturas multicapas permiten identificar, rastrear y mitigar amenazas de aeronaves no tripuladas, incluso en contextos caracterizados por alta densidad electromagnética y comunicaciones civiles. Este tipo de soluciones se ha consolidado como una respuesta flexible frente a la proliferación de UAV de bajo costo y uso no convencional, integrándose progresivamente en esquemas más amplios de seguridad y protección del espacio aéreo (Center for the Study of the Drone at Bard College, 2022).

Estos ejemplos evidencian que la adaptabilidad, la precisión de respuesta y el diseño modular son elementos clave en la implementación de sistemas antidrones. También reflejan la importancia de integrar estos desarrollos con organismos internacionales como la OTAN y la EASA para establecer marcos normativos consistentes y éticos que permitan operar estas soluciones sin causar daños colaterales.

Futuro de la tecnología antidrones

A medida que los UAV continúan evolucionando en capacidades, autonomía y accesibilidad, las tecnologías antidrones se enfrentan al desafío constante de adaptarse a un entorno tecnológico en rápida transformación. La demanda de soluciones más inteligentes, integradas, escalables y rentables es hoy más crítica que nunca para mantener la superioridad operativa frente a amenazas cada vez más complejas y sofisticadas (Al-Dosari et al., 2023; Radovanović et al., 2024).

Uno de los escenarios que mejor ilustra esta dinámica es el conflicto entre Rusia y Ucrania, convertido en un verdadero laboratorio de guerra tecnológica, donde ambos bandos han llevado la innovación en drones y sistemas antidrones a niveles sin precedentes (Infodefensa, 2024). Durante 2024, se observó un avance notable en los UAV ucranianos, que empezaron a incorporar enlaces de datos basados en técnicas de salto de frecuencia, conocidas como *Frequency Hopping Spread Spectrum* (FHSS) (IVCAN, 2025). Esta técnica consiste en transmitir datos variando rápidamente la frecuencia de emisión dentro de un espectro amplio, lo que reduce significativamente la vulnerabilidad de las comunicaciones frente a las interferencias o a la detección por sistemas antidrones convencionales.

Ante ello, los sistemas C-UAS se han visto obligados a integrar transmisores más potentes, junto con antenas tanto direccionales como omnidireccionales, capaces de operar en rangos que se extienden desde los 400 MHz hasta los 6 GHz. Sin embargo, este avance ha provocado un incremento considerable en los costos de los sistemas antidrones, tanto por la sofisticación de sus componentes como por la complejidad de los algoritmos necesarios para contrarrestar estas nuevas técnicas de transmisión.

Aún más significativa ha sido la respuesta tecnológica de Ucrania en 2025. Frente a las cuantiosas inversiones rusas en contramedidas electrónicas, los ingenieros ucranianos han explorado la implementación de drones equipados con enlaces de datos por fibra óptica. Esta innovación ha supuesto una ruptura en el paradigma C-UAS. Los drones ucranianos, particularmente aquellos equipados con sistemas FPV (*First Person View*), operan mediante cables de fibra óptica que permiten transmitir video y datos de control de forma directa y completamente indetectable para los sensores de radiofrecuencia enemigos.

Lima (2025) señala que la tecnología de drones con cable de fibra óptica está revolucionando el conflicto, evidenciando que los antidrones están siempre dos pasos atrás de la innovación no tripulada. Según Castillo (2025), gracias a esta tecnología se eliminan por completo las emisiones electromagnéticas que podrían ser interceptadas o bloqueadas, generando un canal de comunicación seguro y resistente a las contramedidas electrónicas.

Aunque la principal limitación de esta tecnología reside en la longitud de la fibra —actualmente disponible en carretes de hasta 50 kilómetros—, su adopción ha permitido a Ucrania desplegar drones en áreas fuertemente vigiladas, incluso más allá de las líneas de defensa enemigas. Se han documentado extensas redes de fibra óptica tendidas a lo largo del campo de batalla, utilizadas como infraestructura

para controlar drones de diversos tamaños y capacidades, tanto en misiones de reconocimiento como en ataques de precisión o sabotaje (Infodefensa, 2024).

Sin embargo, la evolución tecnológica no se detiene. Muchos de estos sistemas híbridos están comenzando a integrar capacidades avanzadas de navegación inercial y algoritmos de IA, que permiten a los drones continuar sus misiones incluso si la fibra óptica se corta o durante el tramo final hacia su objetivo. La IA dota a estos UAV de la capacidad de identificar objetivos mediante cámaras ópticas y térmicas, y de tomar decisiones autónomas en tiempo real, elevando exponencialmente la dificultad de detectarlos y neutralizarlos (Al-Dosari et al., 2023).

El conflicto entre Rusia y Ucrania ha dejado claro que la guerra de drones se libra no solo en el espacio físico, sino también en dominios invisibles como el espectro electromagnético, las redes de fibra óptica y los complejos algoritmos que gobiernan la IA. Cada innovación en el campo de los UAV genera una carrera frenética por desarrollar sistemas antidrones capaces de contrarrestarla. No obstante, en muchos casos, los sistemas C-UAS se ven obligados a reaccionar en lugar de anticiparse. Esta brecha perpetúa una desigualdad tecnológica y económica evidente: mientras los drones mantienen costos relativamente bajos y son fácilmente adaptables, las contramedidas resultan cada vez más costosas y complejas de implementar. Esta asimetría constituye una amenaza latente para la seguridad global y es una lección vital que países como Colombia deben tener presente al diseñar sus estrategias de defensa aérea (Infodefensa, 2024; Kang et al., 2020).

Dentro de este panorama, la IA y el aprendizaje automático se consolidan como los pilares sobre los que se erigen los sistemas antidrones de nueva generación. Estas tecnologías permiten detectar y clasificar UAV de forma predictiva, analizando patrones de vuelo, firmas térmicas, acústicas o señales electromagnéticas. Algoritmos avanzados son capaces de anticipar trayectorias, distinguir amenazas reales de falsos positivos y automatizar decisiones críticas en tiempo real, algo crucial para proteger entornos densamente poblados o infraestructuras críticas (Al-Dosari et al., 2023).

Además, la IA está comenzando a aplicarse en técnicas sofisticadas como el *spoofing* GPS, mediante el cual se engaña a los UAV autónomos enviándoles señales falsas que simulan rutas inexistentes. Esto se perfila como una alternativa no destructiva clave en escenarios urbanos o misiones de inteligencia, reduciendo el riesgo de daños colaterales y aumentando las posibilidades de neutralización discreta (Szabolcsi, 2014).

Por otra parte, la fusión sensorial multispectral emerge como la solución más avanzada del mercado. Estos sistemas integran radares, sensores infrarrojos, ópticos, acústicos y de radiofrecuencia en una única arquitectura capaz de detectar y rastrear UAV con precisión, incluso en entornos extremadamente complejos o con escasa visibilidad (Marta & Gamboa, 2014). Esta integración permite crear redes de defensa multisensor que minimizan las vulnerabilidades individuales de cada tecnología, reforzando la eficacia global de los sistemas C-UAS.

Las tecnologías emergentes, como los sistemas láser y las soluciones cinéticas no letales, están captando también la atención de la industria. Investigaciones como las de Mathew et al. (2020) han demostrado la viabilidad de sistemas láser de corto alcance en contextos donde la precisión y la reducción de residuos son prioritarias. Estos sistemas ofrecen una alternativa atractiva para entornos sensibles o eventos multitudinarios, donde métodos más tradicionales podrían implicar riesgos de daños colaterales. Aunque todavía están limitados por los altos costos iniciales y por las condiciones meteorológicas adversas, los sistemas láser se destacan por su bajo costo operativo por disparo y su alta precisión, convirtiéndose en una opción cada vez más valorada en el ámbito militar (Pu, 2019).

De manera paralela, el desarrollo de drones interceptores y dispositivos como redes lanzadas por UAV ha permitido capturas controladas de drones hostiles sin ocasionar daños colaterales, lo que resulta especialmente útil en entornos urbanos o durante eventos de alta seguridad (Infodefensa, 2024). Asimismo, los avances en sensores acústicos, apoyados por IA, han potenciado la capacidad de estos sistemas para filtrar el ruido ambiental y focalizarse en las firmas acústicas específicas de los motores de los UAV (Contreras Henao, 2014). Por su parte, la visión por computadora aplicada a cámaras ópticas e infrarrojas permite identificar drones incluso bajo condiciones de baja visibilidad. Alternativas más inusuales, como el uso de aves entrenadas para interceptar UAV o redes físicas, aunque limitadas en alcance y eficacia, siguen explorándose como opciones sostenibles y no electrónicas (Casanovas, 2016).

Aunque actualmente los sistemas C-UAS implican costos elevados, se espera que la economía de escala, la estandarización de componentes y el desarrollo de soluciones modulares contribuyan a una reducción significativa de costos en los próximos años. Esto podría abrir las puertas a su adopción no solo en entornos militares, sino también en infraestructuras civiles críticas y en países en desarrollo que necesitan reforzar su seguridad aérea (Tavera Florez, 2024).

Por último, el desarrollo normativo resultará tan decisivo como la innovación tecnológica. La armonización de marcos legales a nivel internacional permitirá la

operación coordinada de sistemas antidrones en espacios compartidos, zonas fronterizas o durante eventos globales. Ejemplos como la inclusión de los UAV en la Revisión Anual de Seguridad de la EASA (2024) y la colaboración con organismos como la OTAN marcan una ruta positiva hacia una gobernanza más coherente y eficaz en materia de seguridad aérea (Infodron, 2025).

En síntesis, el futuro de la tecnología antidrones dependerá no solo de la capacidad técnica para innovar, sino también de la habilidad de los Estados y las organizaciones para anticiparse a las amenazas, regular con sabiduría, cooperar internacionalmente y democratizar el acceso a soluciones eficaces. En un mundo donde los UAV avanzan en sofisticación y volumen, los sistemas C-UAS deben ser igualmente dinámicos, adaptativos y estratégicos para proteger no solo el espacio aéreo, sino también la seguridad, la soberanía y la estabilidad de las naciones.

Conclusiones

La creciente amenaza que representan los UAS ha evidenciado la urgencia de transformar de manera profunda las capacidades defensivas, sobre todo en el ámbito táctico y a baja altura. Como se ha explorado a lo largo de este capítulo, el ritmo vertiginoso con el que evoluciona la tecnología de los UAV, cada vez más autónomos, accesibles y sofisticados, está superando la capacidad de respuesta de los sistemas antidrones actuales, que con frecuencia se ven obligados a ir a la zaga.

La defensa contra drones ya no puede entenderse únicamente como un desafío técnico ni como una cuestión aislada de la ingeniería. Se trata, en realidad, de un reto estructural que se extiende por múltiples dimensiones: desde la necesidad de innovación constante, pasando por la sostenibilidad económica de estas soluciones, hasta cuestiones de gobernanza normativa y cooperación internacional. La brecha entre la velocidad con la que los UAV siguen innovando y la respuesta, siempre reactiva, que pueden ofrecer los sistemas antidrones constituye hoy el mayor desequilibrio estratégico y una amenaza latente para la eficacia de estas defensas (Radovanović et al., 2024).

El análisis también ha puesto de manifiesto limitaciones persistentes, como la falta de un marco regulatorio claro, los altos costos asociados a las tecnologías más avanzadas y las restricciones inherentes a los sistemas de detección y neutralización. Estas barreras convierten la implementación de soluciones C-UAS en un reto especialmente complejo, hoy limitado a contextos muy específicos y a

actores con alta capacidad de inversión y sofisticación tecnológica. Para países como Colombia, este escenario obliga a repensar no solo la adquisición de tecnología, sino también el desarrollo de capacidades nacionales, la formación de talento humano especializado y la integración de estas soluciones en una visión estratégica más amplia (Tavera Flórez, 2024).

No obstante, existen señales positivas y experiencias exitosas que demuestran la posibilidad de enfrentar estos retos. La implementación de sistemas antidrones en escenarios internacionales, como la COP16 en Colombia, y la participación de actores estratégicos en proyectos tecnológicos nacionales reflejan una creciente voluntad de anticiparse y prepararse frente a amenazas que, hasta hace pocos años, parecían futuristas (Atalayar, 2024). Ejemplos como el uso de drones con enlaces de fibra óptica en Ucrania, o el desarrollo de tecnologías híbridas con IA y sistemas multisensoriales, muestran que, si bien la carrera tecnológica es desafiante, también constituye una fuente de oportunidades para innovar y establecer ventajas estratégicas (Infodefensa, 2024).

De cara al futuro, las conclusiones de este capítulo apuntan a la necesidad de consolidar sistemas antidrones que sean modulares, inteligentes y económicamente accesibles. Será esencial apostar por arquitecturas flexibles, capaces de integrar distintos sensores y métodos de neutralización —radar, ópticos, acústicos, láser o cibernéticos—, así como por plataformas basadas en IA que permitan anticipar amenazas, identificar objetivos y actuar con precisión, casi en tiempo real (Al-Dosari et al., 2023).

Una de las grandes enseñanzas de la guerra moderna, expuesta con contundencia por el conflicto entre Rusia y Ucrania, es que los drones y los sistemas antidrones no son ya meros complementos tecnológicos, sino auténticas armas de guerra y piezas clave en la defensa aérea. Esta guerra tecnológica ha revelado una paradoja: mientras la IA juega a ambos bandos, impulsando tanto las capacidades ofensivas de los UAV como las defensivas de los sistemas C-UAS, la brecha de costos sigue siendo abismal. Un dron de bajo costo puede poner en jaque infraestructuras críticas, obligando a desplegar contramedidas que cuestan cientos de veces más. Esta carrera desigual está redefiniendo los conceptos tradicionales de poder aéreo y defensa.

Más allá de los avances técnicos, surge una conclusión crucial: el campo de batalla aéreo está evolucionando tan rápido que el eslabón más vulnerable empieza a ser el ser humano. Los drones de hoy superan en varios órdenes de magnitud lo que un piloto humano puede soportar: triplican las fuerzas G tolerables, alcanzan

velocidades hipersónicas, operan a temperaturas cercanas a los 400 grados, vuelan durante más de 30 horas seguidas y procesan miles de datos en tiempo real para identificar objetivos. Todo ello ha llevado a que la guerra aérea suprima progresivamente el factor humano, situando a los sistemas antidrones como el primer anillo de defensa y seguridad de cualquier nación. Este cambio está redefiniendo por completo lo que se entiende por necesidades de defensa aérea estratégica.

En definitiva, el reto que se enfrenta no es únicamente tecnológico. Defender nuestros cielos y contrarrestar la amenaza de los drones exige un enfoque verdaderamente multidimensional, en el que confluyan ciencia, política, derecho, economía y estrategia. La armonización de marcos legales a nivel internacional, la cooperación entre países y la posibilidad de democratizar estas tecnologías, para que no sean patrimonio exclusivo de unas pocas potencias, serán elementos clave para garantizar la seguridad del espacio aéreo y, más allá de ello, la protección de la soberanía, las infraestructuras críticas y, en última instancia, de la vida humana.

Colombia y otros países con desafíos similares deberán estar preparados para anticipar, innovar y cooperar, asegurando así su lugar en el nuevo paradigma de la defensa aérea que se perfila para este siglo XXI. Hoy resulta innegable que los drones y los sistemas antidrones ocuparán un rol protagónico y duradero en las guerras del futuro.

Referencias

- Al-Dosari, H., Hunaiti, Z., & Balachandran, W. (2023). RF-enabled deep-learning-assisted drone detection. *Sensors*, 23(9), 1-21.
- Basante, F. (2020). El empleo de los drones y su incidencia en la seguridad aérea. *Revista de Defensa Aérea*.
- Casanovas, M. (2016). Drones: amenazas y oportunidades para la seguridad. *Seguridad & Defensa*.
- Castillo, J. (2025, 10 de junio). Cómo funcionan los letales drones de fibra óptica que está usando Ucrania contra Rusia. *La Opinión*. <https://tinyurl.com/2cxyhofe>
- Castrillo, V., Manco, A., Pascarella, D. & Gigante, G. (2022). A review of counter-UAS technologies for cooperative applications. *Drones*, 6(3). <https://doi.org/10.3390/drones6030065>
- Center for the Study of the Drone at Bard College. (2022). *Counter-drone systems*. Bard College. <https://dronecenter.bard.edu/counter-drone-systems/>
- Chaari, R., & Al-Maadeed, S. (2021). Security analysis of drone systems: attacks, limitations and countermeasures. *Drones and Security Research*.

- Choi, H., Joung, H., & Bae, J. (2021). *A study on the establishment of counter-drone system and the concept of new counter-drone system*. Korean Institute of Defense Technology.
- Contreras Henao, L. (2014). Drones, defensa nacional y soberanía tecnológica. *Revista Estratégica*.
- Cubillos, J., Pérez, A., & Martínez, R. (2020). Nuevas amenazas aéreas y el crimen organizado. *Revista Criminalidad*.
- Fernández-Orsorio, A. E. (2025). Drones and fifth-generation warfare: humanitarian implications in the Colombian conflict. *Revista Logos Ciencia & Tecnología*, 17(2), 32-49. <https://doi.org/10.22335/rlct.v17i2.2127>
- Flórez, T. C. T. (2024). *Tecnología antidrones y defensa aérea* (documento de trabajo inédito). Infodefensa. (2024). *Análisis del conflicto aéreo no tripulado*. Observatorio Militar Latinoamericano.
- IVCAN. (2025, 28 de junio). FHSS espectro ensanchado por salto de frecuencia para enlace de datos de video inalámbrico. <https://tinyurl.com/2d7a87v7>
- Kang, H., Kim, S., & Shin, J. (2020). A study on the establishment of counter-drone system. *Defense Technology Review*.
- Lima, M. (2025, 29 de mayo). Drones con fibra óptica: el arma invisible de Putin que cambia las reglas de la guerra y está arrasando al ejército de Ucrania. *La Opinión*.
- Marta, C., & Gamboa, R. (2014). Vigilancia aérea con UAVs: una visión de la seguridad. *Revista Aeroespacial*.
- Mathew, J., et al. (2020). Anti-drone system: detection and neutralization using laser. *Journal of Defense Research and Technology*.
- Mogili, U., & Deepak, B. (2018). Review on application of drone systems in precision agriculture. *Computers and Electronics in Agriculture*, 150, 245-265.
- Pérez Pinzón, J. (2015). Seguridad, drones y espacio aéreo en América Latina. *Revista de Estrategia Militar*.
- Plichta, M. (2025). Assessing Ukraine's one-way attack drone campaign. *The RUSI Journal*. <https://doi.org/10.1080/03071847.2025.2527923>
- Pu, Z. (2019). Anti-drone system based on laser technology. *Laser and Defense Journal*.
- Radovanović, S., et al. (2024). Optimization of anti-drone defense. *Journal of Defense Engineering*.
- Szabolcsi, R. (2014). Ethical and legal implications of autonomous drone warfare. *Military Ethics Review*.
- Tavera Florez, T. C. (2024). *Tecnología antidrones y defensa aérea*. Documento inédito. Disponible en archivo de trabajo interno del Proyecto DEFAC 2025, Universidad Militar Nueva Granada.
- Voskuil, M. (2022). Performance analysis and design of loitering munitions. *Aerospace Science Journal*.
- Zong-xin, X. (2021). Aerodynamic model identification from flight data. *Journal of Aerospace Science and Engineering*.

Capítulo 4

UAS/RPAS en el silencio de la batalla moderna del ciberespacio*

DOI: <https://doi.org/10.25062/9786287818620.04>

Leonardo González Carrasco

Fuerza Aeroespacial Colombiana

Resumen: Este capítulo explora la evolución de los sistemas aéreos no tripulados (UAS/RPAS) como plataformas estratégicas en el contexto de la guerra cibernética contemporánea. El objetivo es analizar sus capacidades para ejecutar operaciones tanto ofensivas como defensivas. Mediante una metodología mixta que integra la revisión de casos reales en conflictos recientes, se describen capacidades ofensivas de los UAS, incluyendo la inyección de *malware*, ataques de denegación de servicio y operaciones de recopilación de información, junto con sus capacidades defensivas, como la detección y neutralización de amenazas. Los hallazgos revelan que la incorporación de inteligencia artificial y tecnologías autónomas potencia el papel de los UAS tanto en escenarios militares como en posibles ataques contra sistemas civiles, redefiniendo la dinámica de los conflictos modernos. Los UAS representan un recurso estratégico que amplía las fronteras entre los dominios físico y digital, planteando nuevos desafíos críticos que exigen respuestas innovadoras en materia de defensa y ciberseguridad.

Palabras clave: ciberseguridad; defensa; enjambres de drones; espectro electromagnético; inteligencia artificial; vigilancia aérea

* Capítulo de libro resultado del proyecto de investigación "Sistema de Naves y Aeronaves no Tripuladas e Inteligencia Artificial: Innovaciones Estratégicas para el Futuro Militar" en colaboración del grupo de investigación en Estudios Aeroespaciales de la Fuerza Aeroespacial Colombiana - GIEA, categorizado en B por el Ministerio de Ciencia, Tecnología e Innovación (Minciencias) y registrado con el código COL0084209. Los puntos de vista y los resultados de este capítulo pertenecen al autor y no reflejan necesariamente los de las instituciones participantes.

Leonardo González Carrasco

Teniente Coronel de la Fuerza Aeroespacial Colombiana. Magíster en confiabilidad, Universidad de las Palmas de Gran Canaria, España. Magíster en ingeniería mecánica, Escuela Colombiana de Carreras Industriales. Especialista en seguridad y defensa nacionales, Escuela de Guerra “Rafael Reyes Prieto”, Colombia. Ingeniero mecánico, Universidad del Norte, Colombia. Investigador MinCiencias del grupo de investigación GIEA, FAC. Jefe del Área de Aeronavegabilidad de la FAC.

Orcid: <https://orcid.org/0009-0005-4945-4382> - Contacto: leonardo.gonzalez@fac.mil.co

Citación APA: González Carrasco, L. (2026). UAS/RPAS en el silencio de la batalla moderna del ciberespacio. En D. Barrero-Barrero (Ed.), *Sistema de naves y aeronaves no tripuladas e inteligencia artificial: innovaciones estratégicas para el futuro militar* (pp. 87-111). Sello Editorial ESDEG.
<https://doi.org/10.25062/9786287818620.04>

SISTEMA DE NAVES Y AERONAVES NO TRIPULADAS E INTELIGENCIA ARTIFICIAL: INNOVACIONES ESTRATÉGICAS PARA EL FUTURO MILITAR

ISBN impreso: 978-628-7818-56-9

E-ISBN digital: 978-628-7818-62-0

DOI: <https://doi.org/10.25062/9786287818620>

Colección Estrategia, Geopolítica y Cultura

Sello Editorial ESDEG

Escuela Superior de Guerra “General Rafael Reyes prieto”

Bogotá D.C., Colombia

2026



Introducción

El siglo XXI se ha venido caracterizando por los grandes avances en materia de interconectividad tecnológica, en un contexto en el que la información circula a través de redes complejas. Por esa razón, el ciberespacio ha adquirido un rol cada vez más crucial en las estrategias de seguridad nacional, en la medida en que los países se vuelven más y más dependientes de su interacción con las redes, no solo con propósitos comerciales, académicos o financieros, sino también para el desarrollo de operaciones defensivas y ofensivas (Arreola García, 2016). En este contexto, los Sistemas Aéreos No Tripulados (UAS), comúnmente conocidos como drones, han mutado de sencillas plataformas de observación y/o entretenimiento para transformarse en instrumentos adaptables con capacidades revolucionarias en múltiples campos, incluido el ciberespacio (Konaszczuk & Nogalski, 2024). La rápida incursión de nuevas tecnologías ha permitido que estos sistemas sean cada vez más pequeños, tengan mayor alcance y autonomía, y sean capaces de niveles de procesamiento de datos muy avanzados (Mahalle et al., 2024). Además, las facilidades actuales para conseguir conectividad inalámbrica y el uso de la inteligencia artificial (IA) han impulsado la evolución de los UAS con fines distintos al entretenimiento (Arreola García, 2016; Konaszczuk & Nogalski, 2024; Mahalle et al., 2024).

Rid (2012) argumenta que, en este contexto, el concepto de *guerra cibernética* ha sido objeto de un amplio debate académico. Algunos autores sostienen que las operaciones cibernéticas, aunque estratégicamente relevantes, no siempre cumplen con los criterios tradicionales de la guerra, sino que se manifiestan como acciones encubiertas, continuas y situadas por debajo del umbral del conflicto armado convencional. En ese escenario, la capacidad de los UAS para acceder a áreas remotas o de difícil acceso, así como su movilidad y la posibilidad de transportar

una variedad de cargas útiles, les otorgan una ventaja táctica significativa en el ciberespacio (Mahalle et al., 2024).

La facilidad para adquirir estos sistemas en el mercado y modificarlos con fines militares representa una amenaza creciente para la seguridad (Nikolic, 2017). Además, su capacidad para recopilar información, interceptar comunicaciones y acceder a áreas restringidas plantea serias preocupaciones sobre la privacidad y la seguridad nacional. Actualmente, estos sistemas han demostrado su eficacia en conflictos armados; ejemplos claros son Siria, Irak y Ucrania, donde grupos terroristas y fuerzas militares les han dado usos que permiten llevar a cabo operaciones de vigilancia, reconocimiento e incluso ataques aéreos (Tønnessen, 2017). No obstante, el verdadero potencial del ciberespacio en el ámbito de la guerra cibernética apenas comienza a ser explorado. Resulta evidente que aquellos sectores del Estado que integran tecnologías informáticas con acceso al ciberespacio, pero carecen de las capacidades defensivas necesarias para contrarrestar información maliciosa, enfrentan una alta probabilidad de sufrir ataques que podrían convertirse en el origen de daños graves para la nación (Gaitán Rodríguez, 2012; Nikolic, 2017; Tønnessen, 2017).

Los avances actuales en IA están impulsando el desarrollo de UAS totalmente autónomos, capaces de tomar decisiones y realizar tareas complejas sin intervención humana. Lo anterior plantea nuevos desafíos para la seguridad, ya que existe la posibilidad de que sean utilizados para llevar a cabo ataques cibernéticos sofisticados y difíciles de detectar. La posibilidad de que actores maliciosos utilicen enjambres de drones autónomos para saturar las defensas y ejecutar ataques coordinados representa una amenaza cada vez más latente en los escenarios cotidianos (Öz & Sert, 2019).

La tecnología actual permite inferir que estos sistemas pueden ser equipados con herramientas de guerra cibernética para llevar a cabo ataques a redes y sistemas informáticos, convirtiéndose en armas aéreas con capacidades ofensivas, entre las que se incluyen ataques de denegación de servicio, inyección de *malware*, recopilación de información y guerra electrónica.

Su naturaleza dual, tanto como equipos comerciales con beneficios en diversos sectores como posibles armas en manos de actores maliciosos, crea una tensión creciente relacionada con su desarrollo, así como con su urgente regulación. Esta tensión se intensifica aún más por el aumento de la capacidad tecnológica para maximizar la autonomía, impulsada por la IA, que, si bien incrementa su

eficiencia y potencial en diversas aplicaciones, también aumenta el riesgo de que sean utilizados para fines no autorizados con mínima o nula intervención humana.

A medida que la tecnología avanza y se vuelve más accesible, existe un creciente riesgo de que actores no estatales o grupos terroristas adquieran y utilicen UAS para llevar a cabo ataques cibernéticos o actividades ilícitas (Tang, 2021). Esta proliferación tecnológica, junto con la relativa facilidad para modificar estos sistemas con fines maliciosos, representa una amenaza latente para cualquier entorno de seguridad.

La guerra cibernética con UAS no se limita a un solo tipo de conflicto, sino que abarca desde guerras interestatales hasta conflictos asimétricos, en los que grupos terroristas o actores no estatales pueden utilizar drones comerciales modificados para llevar a cabo ataques cibernéticos o actividades ilícitas. De la misma manera, la ciberseguridad de estos mismos sistemas se convierte en una preocupación relevante debido al creciente riesgo de ciberataques destinados a comprometer su confidencialidad, integridad y disponibilidad. En ese mismo sentido, podrían explotarse vulnerabilidades en el *software* o el *hardware* para tomar el control de la aeronave, robar datos o interferir con sus operaciones (Niyonsaba et al., 2023).

En este contexto, la pregunta que guía este capítulo es cómo los UAS/RPAS están transformando la guerra cibernética y cuáles son las implicaciones para la seguridad global. El objetivo principal es explorar el uso de los UAS en operaciones cibernéticas y su potencial para la guerra híbrida, describiendo tanto sus capacidades ofensivas como defensivas, identificando los riesgos y desafíos que su empleo conlleva.

Para responder a esta cuestión, se ha adoptado una metodología mixta, con predominio hermenéutico, que combina el análisis cualitativo de casos reales en escenarios de conflictos recientes y una revisión bibliográfica de fuentes actualizadas sobre ciberseguridad, tecnología, seguridad y defensa. Los temas por discutir incluyen capacidades ofensivas, como ataques de denegación de servicio, inyección de *malware*, recopilación de información y guerra electrónica, y capacidades defensivas, como detección y neutralización de amenazas, protección de infraestructuras críticas y fortalecimiento de la ciberseguridad. Como resultado esperado, se busca aportar una visión integral y actualizada sobre el papel estratégico de los UAS en el ciberespacio, contribuyendo al entendimiento de este fenómeno y de los retos que impone en los escenarios de conflictos modernos.

¿Armas en la nube? Cómo los sistemas no tripulados conquistan el ciberespacio y reconfiguran el conflicto

El ciberespacio puede llegar a ser considerado como un nuevo escenario de guerra en el que los Estados vienen construyendo nuevas capacidades para demostrar poder (Aranda Gómez, 2024). De esa manera, los avances tecnológicos que permiten una interconexión permanente y el movimiento de información por medio de redes complejas permiten inferir la relevancia que tiene la administración de este sector para la seguridad.

Los UAS han modificado su rol inicial, para el cual fueron diseñados, y han pasado de ser simples plataformas de entretenimiento y observación a convertirse en herramientas adaptativas con capacidades disruptivas en múltiples escenarios, como la guerra cibernética.

Ghazlane et al. (2024) se adentran en lo relacionado con las aplicaciones de los UAS y señalan que “con el rápido desarrollo de técnicas inteligentes, que abarcan desde el reconocimiento de imagen y voz hasta la toma de decisiones autónomas en robots autónomos, los drones se han beneficiado” (p. 2). Además, estos sistemas vienen demostrando una gran capacidad para proporcionar soluciones económicas e inmediatas en diversas áreas del entorno de la seguridad.

La esencia misma de los UAS, sin importar su tamaño, los convierte en herramientas idóneas para la guerra cibernética. Su habilidad para llegar a lugares remotos o de difícil acceso, junto con su movilidad y la capacidad de llevar diferentes tipos de cargas útiles, les da una ventaja táctica considerable en el ciberespacio. Además, hay que tener en cuenta que su capacidad de movilización autónoma, gracias a la IA, les permite llevar a cabo tareas complejas con muy poca intervención humana, lo que amplifica su potencial en los escenarios cibernéticos.

La convergencia de tecnologías como la miniaturización, el aumento de la capacidad de procesamiento, la conectividad inalámbrica y la IA ha impulsado la evolución de los UAS. Ya no son simples dispositivos de vigilancia: ahora son herramientas sofisticadas capaces de realizar tareas complejas con un alto grado de autonomía. De la misma manera, el Centro de Ciberseguridad Cooperativa de Australia (CSCRC) indica que estos elementos se vuelven cada vez más sofisticados, equipados con sensores, cámaras y *software* de procesamiento de imágenes de última generación para proporcionar datos más eficientes y precisos (CSCRC & OMNI, 2024).

Sin embargo, el hecho de que sean dispositivos del internet de las cosas (IoT), o sistemas que requieren conexión a internet para actualizaciones de *software* y carga de datos, los hace vulnerables a la ciberexplotación, debido a que los datos recopilados y almacenados deben descargarse, el *software* debe actualizarse y, sobre todo, porque a menudo se operan a través de otros dispositivos de IoT, por ejemplo, teléfonos móviles.

Esta evolución ha abierto un nuevo frente en la guerra cibernética, donde los UAS pueden ser utilizados para llevar a cabo una amplia gama de operaciones, desde ataques dirigidos hasta la recopilación de información sensible.

El auge de sistemas no tripulados comerciales y la amenaza a la seguridad

Actualmente, los UAS se utilizan ampliamente en diversos sectores, primordialmente por su gran diversidad y sus costos de adquisición, pasando de ser usados en aplicaciones como la previsión meteorológica y la vigilancia del tráfico a funcionar también como juguetes o como dispositivos para facilitar tareas diarias de sus compradores (Al-Dosari et al., 2024).

Actualmente, existen más de 700 diseños de todas las categorías, de los cuales más de 500 son de uso exclusivamente militar, en diferentes estados de desarrollo o implementación (González, 2024). Y, sin lugar a duda, lo que ha permitido el creciente desarrollo de estas tecnologías ha sido la economía en los procesos de producción y la creciente demanda con fines comerciales. Si bien esto ha generado beneficios en sectores como la agricultura, la logística y la vigilancia, también ha incrementado el riesgo de que los UAS sean utilizados con fines maliciosos (González, 2024).

La facilidad para adquirir UAS comerciales y modificarlos para fines no autorizados, como el transporte de drogas, armas o explosivos, representa una amenaza elevada para la seguridad (Nikolic, 2017). Además, la capacidad de estos sistemas para recopilar información, interceptar comunicaciones y acceder a áreas restringidas plantea serias preocupaciones sobre la privacidad y la seguridad nacional.

Sin ir más lejos, Kunertova (2023) aborda la problemática relacionada con estos sistemas en la guerra en Ucrania, aclarando que, antes de la invasión de Rusia a Ucrania, la literatura académica sobre drones militares coincidía en comprenderlos como agentes de guerra remotos. Los académicos reflexionaban sobre el impacto estratégico de los UAS de gran tamaño en todos los niveles de la seguridad y la

defensa, y sobre sus efectos transformadores en la guerra. Sin embargo, la guerra en Ucrania demostró que los UAS pequeños y ligeros pueden lograr victorias tácticas. Si bien la comunidad de estudios de seguridad predijo correctamente las limitaciones de los sistemas de gran tamaño, se subestimaron las funciones que pueden desempeñar, incluso a nivel de un solo soldado, y se pasó por alto la posibilidad de su despliegue a gran escala en el campo de batalla.

UAS en conflictos armados: guerra cibernética en el campo de batalla

Los UAS han demostrado su eficacia en conflictos armados recientes, como en Siria, Irak y Ucrania, donde han sido utilizados por grupos terroristas y fuerzas militares para llevar a cabo operaciones de vigilancia, reconocimiento e incluso ataques aéreos (Tønnessen, 2017). Sin embargo, su potencial en la guerra cibernética apenas comienza a ser explorado.

El uso de UAS, sobre todo de bajo peso, en la guerra cibernética ha pasado de ser un concepto experimental a constituir una amenaza tangible y concreta, con varios casos documentados que evidencian la creciente sofisticación de estos ataques y el uso de tecnologías de punta. Aunque muchos de estos incidentes aún se encuentran en fases de prueba, ya existen ejemplos reales de ataques cibernéticos exitosos mediante UAS que han tenido consecuencias graves.

Un ataque cibernético de alto impacto se registró en febrero de 2022, cuando un incidente contra la red satelital KA-SAT de Viasat produjo interrupciones significativas del servicio para decenas de miles de terminales en Europa, con efectos colaterales más allá del teatro de operaciones ucraniano. Este caso ilustra cómo, en conflictos contemporáneos, las operaciones cibernéticas pueden degradar capacidades críticas de conectividad y generar efectos en cascada sobre servicios esenciales y usuarios civiles, evidenciando la centralidad de la infraestructura satelital y de sus segmentos terrestres y de usuario como superficies de ataque relevantes (European Union Agency for Cybersecurity, 2025; Casaril & Galletta, 2024).

En 2017, UAS fueron empleados en un ataque de espionaje industrial en los EE.UU. Equipados con sensores avanzados, estos sistemas se infiltraron en las redes de comunicación de empresas competidoras, robando información confidencial sobre procesos de producción y productos. Esta información fue luego vendida en el mercado negro, comprometiendo secretos comerciales de alto valor (Abdullayeva & Valikhanli, 2023). Este ataque resalta cómo los UAS pueden ser

utilizados para vulnerar la seguridad, afectando tanto la competencia como la propiedad intelectual.

Uno de los incidentes más relevantes involucró a Rusia, que utilizó drones para interferir en operaciones de UAS estadounidenses en Siria. Según la periodista Courtney Kube, en un artículo publicado por NBC, Rusia desarrolló la capacidad para interferir con las señales GPS de los drones estadounidenses, lo que afectó gravemente las operaciones militares de los EE.UU. (Kube, 2018). El bloqueo de las señales GPS dificultó la navegación y el control de los UAS en la región. Este ataque cibernético fue impulsado por la preocupación del ejército ruso ante posibles represalias estadounidenses después de una serie de ataques con armas químicas en el este de Ghouta, en Siria. Cuatro funcionarios del sector defensa de EE.UU. confirmaron que la interferencia rusa con los sistemas de navegación y control de los drones tuvo un impacto directo en la capacidad operativa de las fuerzas estadounidenses (Kube, 2018).

Este tipo de interferencias pone sobre la mesa el poder disruptivo de los UAS en los escenarios cibernéticos modernos, donde no solo se emplean para ataques directos, sino también para sabotear las operaciones de fuerzas enemigas mediante la interferencia electrónica y la manipulación de datos.

Rusia ha estado a la vanguardia de este tipo de guerra electrónica, orientada al control y la negación del espectro electromagnético mediante interferencia, engaño o supresión de señales, y la estrategia de utilizar estos sistemas para interrumpir las capacidades tecnológicas del enemigo expone la nueva dimensión de los conflictos modernos, en los que los ataques no solo son físicos, sino también cibernéticos. Además, estos incidentes evidencian la vulnerabilidad de las infraestructuras y sistemas de comunicaciones, que pueden ser fácilmente manipulados o desactivados por actores maliciosos que utilicen tecnologías emergentes en estas aeronaves. Un concepto similar ha sido planteado por Rhodes (2024), al afirmar que el uso de drones no solo ha revolucionado las capacidades operacionales, sino que también ha mostrado la vulnerabilidad creciente de los sistemas de comunicación y control en el campo de batalla, aspecto clave en el conflicto entre Rusia y Ucrania.

El creciente uso de drones en operaciones militares y civiles ha creado una nueva ola de riesgos cibernéticos. Los actores maliciosos están cada vez más enfocados en desarrollar tácticas sofisticadas que permitan no solo comprometer las comunicaciones, sino también desactivar o robar información clave a través de los drones no tripulados. A medida que la tecnología avanza, los ataques

cibernéticos con drones probablemente seguirán evolucionando, con mayor autonomía y mejores capacidades de interferencia, lo que representa un desafío creciente para la seguridad global.

La amenaza de los UAS es real

Los avances en IA y aprendizaje automático están impulsando el desarrollo de UAS completamente autónomos, capaces de tomar decisiones y realizar tareas complejas sin intervención humana. Esto plantea nuevos desafíos para la seguridad, ya que los UAS tienen el potencial de ser utilizados para llevar a cabo ataques cibernéticos sofisticados y difíciles de detectar.

Robin (2024), en su artículo para el periódico *The Guardian*, menciona cómo Ucrania, en el desarrollo del conflicto que enfrenta con Rusia, ha utilizado UAS equipados con IA y armamento para atacar infraestructura crítica como refinerías petroleras; asimismo, señala que los EE.UU. han logrado identificar objetivos de alto valor en Siria y Yemen con UAS. Del mismo modo, Israel los ha usado para identificar a más de 37 000 palestinos como presuntos militantes durante las primeras semanas de la guerra en Gaza.

Otra posibilidad de uso de los UAS por parte de actores maliciosos se enmarca en la operación de estos sistemas como enjambres autónomos para saturar las defensas y llevar a cabo ataques coordinados que representen una amenaza significativa (Öz & Sert, 2019). Estos enjambres podrían ser utilizados para atacar infraestructuras críticas, interrumpir comunicaciones o incluso ejecutar ataques físicos a gran escala.

Entiéndase por *enjambre*, en términos militares, un conjunto de unidades dispersas pero interconectadas, que combaten un objetivo común desde todas las direcciones y de manera simultánea. Esto hoy en día tiene la particularidad de que los UAS de bajo peso son económicamente accesibles y, por ello, la pérdida de estos durante su uso como enjambre no supone una gran pérdida para una fuerza militar o grupo terrorista (Sánchez Díaz, 2022).

Capacidades ofensivas: atacando desde el cielo

En el escenario de la guerra cibernética moderna, los UAS empiezan a surgir como herramientas con gran potencial de poder y utilidad para desarrollar ataques en operaciones militares. A través de sus capacidades ofensivas, estos sistemas

pueden ejecutar una variedad de ataques altamente sofisticados, que van desde la interrupción de servicios críticos hasta el sabotaje de infraestructuras. El uso de los UAS en escenarios de guerra cibernética abre un abanico de posibilidades en una nueva dimensión de ataque, al combinar tecnologías aéreas, IA, armamento sofisticado y ciberataques de alto impacto.

En este sentido, se destacan varias capacidades ofensivas, que se describen a continuación:

- *Ataques de denegación de servicio (DoS)*: Uno de los usos más comunes de los UAS en la guerra cibernética es el ataque de denegación de servicio (DoS). Este tipo de ataque se basa en sobrecargar un sistema con tráfico falso, lo que imposibilita el acceso a los recursos. Gracias a su movilidad y capacidad de posicionarse estratégicamente, los UAS pueden acercarse a un objetivo y aumentar la potencia de la señal para garantizar que el ataque sea más difícil de mitigar. Tal es el caso de los enjambres de drones que sobrevolaron un centro de datos en un conflicto reciente en Ucrania, donde, a través de un ataque coordinado, los drones sobrecargaron los sistemas de defensa cibernética, paralizando las comunicaciones y los sistemas críticos (Park et al., 2018).
- *Inyección de malware*: esta es otra capacidad ofensiva en la que los UAS pueden desempeñar un papel notable. Al tener la posibilidad de ser equipados con sistemas de infiltración inalámbrica, estos sistemas pueden penetrar redes *wi-fi* y dispositivos *bluetooth*, inyectando códigos maliciosos en redes industriales y privadas; incluso, podrían sobrevolar una zona residencial, infectando dispositivos para crear una *botnet* (red de dispositivos infectados con *malware* controlados remotamente) *que luego se utilizaría para lanzar ataques DoS a gran escala*. El *malware* también podría ser utilizado para sabotear sistemas de control industrial, causando daños a infraestructuras críticas o poniendo en peligro la seguridad de las personas. Esto no solo compromete la integridad de la información, sino que también desactiva los sistemas de seguridad. Hasta el momento no se ha documentado un caso real en el que se inyecte *malware* desde UAS; sin embargo, se ha logrado demostrar técnicamente la posibilidad de su desarrollo operacional como plataformas ofensivas, catalogándose por la Cybersecurity Infrastructure Security Agency (CISA) como una amenaza significativa para infraestructuras críticas y entornos industriales en los

EE.UU. (CISA, 2025). El proyecto Snoopy, desarrollado por SensePost, demostró que un UAS pequeño, equipado con un dispositivo Raspberry Pi, podía sobrevolar áreas urbanas emulando redes *wi-fi* y *bluetooth*, forzando a dispositivos móviles a conectarse de manera automática y posibilitando la inyección de payloads maliciosos o la exfiltración de credenciales de acceso (Harvey et al., 2014). De manera similar, el proyecto SkyJack, implementado por Kamkar (2013), evidenció cómo un UAS armado con interfaces *wi-fi* en modo monitor y herramientas de inyección de paquetes podía interceptar y tomar el control de otros UAS, mostrando la factibilidad técnica de transformarlos en vectores de ciberataque.

- *Recopilación de información:* Debido a sus capacidades para interceptar comunicaciones y detectar redes cercanas, los UAS son altamente efectivos para recopilar información y mapear las vulnerabilidades de las infraestructuras objetivo. Un ejemplo de ello fue el uso de UAS para espiar instalaciones militares en la frontera entre Pakistán y Afganistán, donde estos sistemas no solo interceptaron las comunicaciones del enemigo, sino que también recopilaron datos de geolocalización, facilitando futuros ataques cibernéticos y físicos (Ceviz et al., 2023). Este tipo de recopilación de datos es crucial no solo para operaciones militares, sino también para el espionaje industrial.
- *Guerra electrónica:* En cuanto a la guerra electrónica, los UAS tienen la capacidad de interferir comunicaciones militares, bloquear señales GPS y alterar radares, creando ventajas en el campo de batalla para aquellos actores con capacidad de explotar estos recursos modernos. Un uso reciente de esta capacidad se observó en el conflicto entre Ucrania y Rusia en 2022, donde UAS rusos fueron utilizados para bloquear las señales de comunicación de las fuerzas ucranianas, dificultando su capacidad de respuesta ante los ataques y creando confusión en las líneas de defensa (Cosar, 2022). Este tipo de interferencia electrónica no solo puede desorientar a los sistemas de defensa, sino también poner en riesgo la vida de los soldados y la seguridad de las misiones críticas.

El futuro de los ataques cibernéticos con UAS

A medida que los UAS continúan incorporando nuevas tecnologías, los ataques cibernéticos también se van sofisticando y volviendo más frecuentes. Este fenómeno se debe a la creciente dependencia de la actualización tecnológica por parte

de actores tanto militares como civiles, lo que va marcando nuevas brechas en el entorno de la seguridad. Existen varias tendencias clave que probablemente definan el futuro de los ataques con UAS.

- *Mayor autonomía:* La obtención de mayor tiempo de vuelo para los UAS, sobre todo en sistemas de bajo peso, permitirá que estos realicen ataques cibernéticos de manera independiente, sin necesidad de intervención humana directa. Esto representa un reto significativo para las capacidades defensivas tradicionales, ya que los atacantes podrán ejecutar misiones sin ser fácilmente detectados. Según Shafiq (2023), la autonomía avanzada de los UAS también permitirá que estos sistemas aprendan y se adapten a las defensas enemigas en tiempo real, lo que hace más difícil predecir y contrarrestar sus ataques. A medida que la IA se integra en los sistemas no tripulados, estos van adquiriendo capacidades para identificar vulnerabilidades de seguridad, optimizar su trayectoria de ataque y aprender de las respuestas defensivas de forma autónoma, convirtiéndose en amenazas mucho más difíciles de neutralizar.
- *Enjambres de drones:* Podría afirmarse que el futuro de los ataques cibernéticos radica en el uso de enjambres de drones, debido a que esta capacidad puede saturar las defensas cibernéticas mediante la ejecución simultánea de múltiples vectores de ataque, lo que aumenta la probabilidad de éxito. Los enjambres pueden utilizar algoritmos de IA para coordinarse y tomar decisiones en tiempo real, lo que permitiría superar las estrategias de defensa basadas en la detección de amenazas individuales. Esto coincide con lo que afirma Zaki et al. (2024), al indicar que la IA permite a estos enjambres optimizar sus rutas de ataque, convirtiéndose en una herramienta de ciberataque altamente eficiente y difícil de contrarrestar.
- *Inteligencia artificial:* A medida que los UAS sean equipados con capacidades de IA más avanzadas, podrán realizar análisis complejos para adaptar sus estrategias a las defensas que presente su objetivo. Esto se traduce en un mayor grado de personalización de los ataques, ocasionando que cada misión de ciberataque sea única y optimizada para las vulnerabilidades específicas del sistema atacado. Según Estrela et al. (2020), los sistemas de visión y análisis de datos basados en IA mejorarán significativamente la capacidad de los UAS para identificar puntos débiles en las infraestructuras críticas y adaptarse a los cambios en tiempo real, lo que les permitirá ejecutar ciberataques más efectivos y difíciles de rastrear.

Estas tendencias tecnológicas tienen implicaciones profundas para la seguridad global, ya que los ataques cibernéticos basados en UAS no solo afectarán a sistemas militares, sino también a infraestructuras civiles. Por ejemplo, los ataques a redes eléctricas, sistemas de comunicación y plataformas de servicios públicos serán cada vez más comunes, lo que podría tener un impacto devastador en la estabilidad social y económica de los países. De hecho, los ataques cibernéticos mediante drones están alcanzando niveles de sofisticación que podrían poner en jaque incluso a los sistemas de defensa más avanzados. En la guerra en Ucrania, el empleo de drones para tareas de espionaje ha sido ampliamente documentado, así como el sabotaje y otros ataques en ambos bandos, utilizando drones desde la destrucción de equipos de comunicaciones hasta la desactivación de sistemas de control de armas (Sonenshine, 2023).

- *Desarrollo de sistemas inerciales independientes:* Los sistemas inerciales son fundamentales para proporcionar navegación autónoma a los UAS/RPAS, especialmente cuando no hay acceso a señales GPS o cuando la fiabilidad de estas señales es limitada. Estos sistemas, que combinan acelerómetros, giroscopios y magnetómetros, permiten a los UAS/RPAS medir con precisión su movimiento y orientación en tiempo real sin necesidad de una infraestructura externa. Esto es particularmente relevante en entornos hostiles o cuando los drones operan en áreas donde las señales GPS son susceptibles de ser bloqueadas o interferidas, como en zonas de conflicto o en escenarios de guerra electrónica (Yousaf et al., 2022).

Por ejemplo, el uso de sensores MEMS (*Micro-Electro-Mechanical Systems*), que, debido a su tamaño compacto y bajo costo, están cada vez más integrados en los sistemas de navegación de drones, permite a los fabricantes desarrollar UAS que operen de manera más precisa y económica, facilitando tanto su utilización en aplicaciones comerciales como en tareas militares donde la precisión es crucial para el éxito de la misión (Yousaf et al., 2022). Además, la implementación de IA y aprendizaje automático ha permitido que los drones no solo naveguen de forma autónoma, sino que también aprendan y se adapten a su entorno, mejorando continuamente su rendimiento. En el contexto militar, estas mejoras permiten a los drones realizar misiones complejas en áreas de alto riesgo, sin intervención humana directa (Di Cecio et al., 2024).

Sin embargo, el principal desafío sigue siendo mejorar la fiabilidad y eficiencia de los sistemas inerciales, ya que las condiciones de operación pueden afectar la precisión de los sensores, especialmente en entornos dinámicos o en áreas con

altas tasas de interferencia electromagnética (Ghazlane et al., 2024). Por ello, las investigaciones continúan explorando nuevas metodologías para reducir el error acumulado y mejorar la capacidad de los UAS para operar de manera precisa en cualquier entorno.

Capacidades defensivas: escudo cibernético aéreo

El siglo XXI se ha caracterizado por entornos cambiantes en el desarrollo de capacidades defensivas en el ciberespacio, hasta convertir este ámbito en una prioridad esencial para la seguridad y la protección de infraestructuras críticas. Frente al aumento de los ciberataques, los Estados deben incorporar nuevas tecnologías que permitan una defensa proactiva, adaptable y multisectorial. Es así como los sistemas no tripulados, tradicionalmente asociados a funciones ofensivas o de reconocimiento, surgen como herramientas clave en la consolidación de una doctrina de ciberdefensa. Su capacidad para integrar sensores avanzados, operar en entornos hostiles y realizar tareas de vigilancia autónoma posiciona a estas plataformas como herramientas versátiles no solo para responder a amenazas físicas, sino también para contribuir a la defensa frente a ciberataques. En particular, su empleo como sensores distribuidos y nodos móviles de recolección de información permite fortalecer la conciencia situacional cibernética, detectar anomalías en enlaces de datos y comunicaciones, y apoyar la identificación temprana de intrusiones o interferencias. De este modo, estas plataformas complementan las capacidades tradicionales de ciberdefensa al facilitar la prevención, mitigación y respuesta adaptativa frente a amenazas híbridas y digitales (Park et al., 2018; MacDonald & Howell, 2019).

Hoy en día, los sistemas antidrones (C-UAS) no se limitan a la detección y neutralización de amenazas aéreas no autorizadas, sino que se integran como componentes activos dentro de arquitecturas más amplias de protección de infraestructuras críticas y entornos sensibles. Estas soluciones combinan sensores, sistemas de mando y control y distintos tipos de efectores, lo que les permite operar como nodos de vigilancia y alerta temprana, contribuyendo a la identificación, seguimiento y mitigación de amenazas en tiempo real. En este sentido, el Joint Air Power Competence Centre señala que las soluciones C-UAS actuales incorporan efectores cinéticos y no cinéticos, incluidos sistemas de ataque electrónico, radares,

analizadores de radiofrecuencia y sensores ópticos, con el fin de detectar, rastrear y neutralizar amenazas de drones, reforzando así la seguridad de los espacios protegidos (Aksu et al., 2021). Esta versatilidad se ha extendido a escenarios más complejos, donde dichos sistemas son utilizados como herramientas activas para el desarrollo de pruebas de protocolos de ciberseguridad, pruebas de penetración y monitoreo de redes distribuidas. En este sentido, la investigación de Hemmati et al. (2023) destaca que los UAS, al operar como nodos móviles dentro del ecosistema de internet, pueden recopilar datos, detectar anomalías y transmitir información en tiempo real, facilitando una supervisión continua y altamente adaptable. Esta convergencia entre movilidad, sensórica avanzada y conectividad convierte a los UAS en aliados estratégicos para fortalecer los perímetros digitales y físicos en un entorno de amenazas híbridas y asimétricas.

La ciberdefensa aérea mediante drones representa una disrupción del paradigma tradicional: ya no se trata únicamente de fortificar sistemas, sino de emplear plataformas móviles, autónomas y reconfigurables que extienden la capacidad de vigilancia, intervención y resiliencia de las redes críticas (Cohen & Rotbart, 2013). Esta estrategia se circunscribe a un entorno de rápido crecimiento de capacidades cibernéticas hostiles, muchas de las cuales son desarrolladas por actores no estatales con acceso a tecnologías de doble uso (Perger, 2022). El empleo de UAS en ciberdefensa, por tanto, se perfila no solo como una opción táctica, sino como un componente estratégico para anticipar, contener y contrarrestar amenazas.

Detección y neutralización en el ciberespacio

La actual transformación digital ha consolidado el ciberespacio como un dominio estratégico de operaciones, y la inclusión de UAS ha desencadenado una nueva dinámica en las tácticas de detección y neutralización de amenazas. En lugar de limitarse a funciones convencionales de vigilancia, reconocimiento o ataque, hoy día estos sistemas se posicionan como plataformas versátiles capaces de operar activamente en la detección, intervención y mitigación de amenazas cibernéticas y electrónicas. Esta capacidad se sustenta en la convergencia de tecnologías como la IA, la guerra electrónica y los sistemas de sensores multispectrales, que permiten a los UAS interactuar directamente con redes, señales, datos y nodos en tiempo real (Yousaf et al., 2022; Aksu et al., 2021).

Vigilancia del espectro electromagnético

El uso y control del espectro electromagnético constituye una línea crítica de acción para detectar, rastrear y mitigar amenazas que operan en dominios invisibles.

Los UAS han evolucionado hasta convertirse en plataformas autónomas con capacidad para ser equipadas con sistemas de inteligencia de señales (SIGINT), capaces de ejecutar operaciones de inteligencia electrónica (ELINT) y de comunicaciones (COMINT) de forma dinámica. Es así como pueden contribuir a la detección de emisiones electromagnéticas en un amplio rango de frecuencias, a través de analizadores de espectro en tiempo real, receptores de radiofrecuencia definidos por *software* y matrices de antenas direccionales (Park et al., 2018).

La arquitectura de estos sistemas con tecnología SIGINT se desarrolla gracias a la integración de módulos de recepción multibanda que recopilan metadatos como RSSI (*Received Signal Strength Indicator*), modulación, polarización y patrones de repetición, para posteriormente realizar clasificación y geolocalización mediante el uso de algoritmos de aprendizaje automático. Esta capacidad no solo permite la identificación de drones hostiles y sus estaciones de control, sino que también facilita la discriminación entre señales legítimas y maliciosas mediante técnicas de detección espectral cognitiva (Shafiq, 2023).

A nivel de ciberintercepción —entendida como la capacidad técnica de monitorear y analizar comunicaciones digitales o enlaces de datos—, los UAS pueden actuar como nodos ofensivos mediante *sniffing*¹ activo de redes inalámbricas tipo *wi-fi*, ZigBee o LoRaWAN, capturando paquetes mediante herramientas embebidas como Kismet² o Wireshark³ adaptado a entornos ARM (*Advanced RISC Machine*)⁴. En contextos de operaciones cibernéticas ofensivas, algunos UAS pueden incluso ejecutar ataques *man-in-the-middle* al establecer *fake access points* (FAP), engañando a los dispositivos conectados para que canalicen su tráfico a través del UAS, permitiendo así la manipulación o recolección de datos (Park et al., 2018). Frente a ello, se enfatiza el uso de cifrado embebido a nivel de *hardware*, protocolos de autenticación reforzada y *tokens* inalámbricos que establezcan barreras físicas y digitales entre el UAS y su estación de control (Niyonsaba et al., 2023).

1 Técnica de interceptar y analizar tráfico de red para extraer información sensible.

2 Herramienta de software de código abierto utilizada para detectar redes inalámbricas, capturar paquetes de datos y realizar análisis de seguridad en redes *wi-fi* y otras tecnologías inalámbricas. Es útil para tareas de auditoría y detección de intrusiones.

3 Aplicación de software libre que permite capturar y analizar en detalle el tráfico de datos en redes de computadoras. Es ampliamente utilizada para diagnóstico de redes, análisis de protocolos y seguridad informática.

4 Familia de arquitecturas de procesadores basada en el diseño RISC (Reduced Instruction Set Computing), ampliamente utilizada en UAV por su bajo consumo de energía, su reducido tamaño físico y su capacidad para integrar múltiples funciones en sistemas embebidos, lo que la hace ideal para el procesamiento a bordo en aplicaciones donde el peso y la eficiencia energética son críticos.

Finalmente, frente a los ataques de denegación de servicio (DoS/DDoS), se sugiere la implementación de sistemas de detección de intrusos (IDS), *firewalls* adaptativos y protocolos como el *fail-safe*⁵, así como técnicas dinámicas como el cambio periódico de puertos UDP (*User Datagram Protocol*)⁶ mediante *middleware*⁷, que han demostrado una resistencia superior al 90 % frente a ataques sostenidos (Niyonsaba et al., 2023).

Guerra electrónica: jamming y spoofing autónomos

Los UAS configurados para la guerra electrónica constituyen una revolución al permitir el desarrollo de operaciones de neutralización sin contacto físico. El *jamming* electromagnético⁸, cuando es ejecutado por estos sistemas equipados con transmisores de alta potencia y arquitecturas SDR (*Software Defined Radio*), les permite interferir selectivamente frecuencias como 2,4 GHz y 5,8 GHz, que son las comúnmente empleadas por UAS comerciales y militares (Park et al., 2018). Según Shafiq (2023), “Los módulos de interferencia de los drones autónomos pueden atacar los enlaces de comunicación de los UAV no autorizados aprovechando vulnerabilidades específicas de cada frecuencia, mediante la adaptación de formas de onda y la proyección direccional de energía de radiofrecuencia” (p. 49). Lo anterior implica que los módulos de interferencia integrados en drones autónomos pueden atacar los enlaces de comunicación de UAS hostiles, explotando vulnerabilidades específicas de frecuencia mediante la adaptación de formas de onda y la emisión de energía de radiofrecuencia. Esta técnica permite anular de manera precisa y eficiente los sistemas de control de drones adversarios, sin necesidad de recurrir a medidas destructivas.

Estas capacidades suelen combinarse con módulos de análisis espectral que escanean el entorno en tiempo real, identificando emisiones hostiles y adaptando las contramedidas según el tipo de modulación, intensidad y latencia del canal. En

5 Principio de diseño que busca que, ante una falla técnica o un ciberataque, el UAS adopte automáticamente un estado seguro que minimice daños o riesgos, como aterrizar, volver al punto de inicio o desactivar funciones críticas. También se conoce como protocolo fail-safe, que limita las consecuencias de ataques DoS/DDoS en UAS.

6 Protocolo de comunicación en redes para el envío rápido de datos sin establecer una conexión previa ni comprobar su correcta recepción. Se utiliza en sistemas UAV para transmitir datos en tiempo real.

7 Capa de software que actúa como intermediaria entre el sistema operativo y las aplicaciones, facilitando la comunicación, la gestión de datos y la coordinación entre componentes. En los UAS, el middleware puede gestionar las comunicaciones entre la aeronave y la estación de control, o entre distintos módulos del sistema.

8 Interferencia intencionada de señales de radiofrecuencia para bloquear comunicaciones o sistemas electrónicos enemigos.

escenarios operacionales más complejos, los drones defensivos pueden configurarse con tecnología *smart jamming* para interrumpir enlaces activos de manera selectiva y reversible, lo cual es especialmente útil en entornos civiles o de guerra híbrida, donde es necesario evitar daños colaterales.

En escenarios de alta complejidad operacional, los UAS defensivos pueden ser dotados de sistemas de *smart jamming* basados en radios SDR, es decir, “una radio reprogramable o reconfigurable, en la que su mismo *hardware* puede realizar operaciones diferentes modificando su configuración mediante *software* o *firmware*” (Rivero Díez, 2021), capaces de detectar y adaptarse dinámicamente a las señales enemigas. Estos sistemas identifican la frecuencia portadora activa del adversario y ajustan sus parámetros de interferencia en tiempo real, optimizando la eficiencia espectral mediante técnicas como el *beamforming*⁹. Este direccionamiento de energía de radiofrecuencia permite atacar objetivos específicos, minimizando daños colaterales en el entorno electromagnético. Según Yousaf et al. (2022), este tipo de *jamming* mejora la precisión y selectividad del ataque, lo que resulta especialmente útil contra redes MANET (*Mobile Ad hoc Network*)¹⁰ utilizadas por enjambres. A su vez, Shafiq (2023) destaca que estas capacidades no solo degradan la conectividad enemiga, sino que favorecen operaciones no cinéticas de interrupción temporal, más adecuadas en contextos de guerra híbrida y/o ciberdefensa.

En paralelo, el *spoofing*¹¹ GPS se ha consolidado como una técnica crítica, mediante la cual los UAS emiten señales GPS falsas, utilizando generadores de tramas GNSS y moduladores SDR que replican constelaciones satelitales. El objetivo es desorientar al receptor GNSS del UAS enemigo, haciéndole creer que está en una ubicación distinta. Esta técnica ha sido usada para inducir aterrizajes forzados, desvíos o comportamientos erráticos, minimizando la necesidad de interdicción cinética (Hur et al., 2017).

Los sistemas no tripulados más avanzados incorporan módulos de ciberataque capaces de insertar en redes cargas útiles maliciosas: desde *scripts* diseñados para explotar vulnerabilidades en *routers* o redes SCADA (*Supervisory Control*

9 Técnica que dirige señales de radio hacia una dirección específica para mejorar la transmisión o interferir objetivos.

10 Red inalámbrica formada de manera dinámica entre dispositivos móviles sin infraestructura fija.

11 Técnica para suplantar señales, especialmente GPS, haciendo que un receptor crea estar en una ubicación diferente.

and Data Acquisition)¹², hasta *dropper payloads*¹³ con *malware* de persistencia. Esta funcionalidad convierte al UAS en una sonda autónoma para penetrar perímetros digitales desde el espacio aéreo, llegando a poner en riesgo activos sensibles como centros de comando y control de defensa aérea (Park et al., 2021).

Finalmente, el uso combinado de *spoofing*, *jamming* y ciberintercepción desde plataformas aéreas origina cambios de paradigma en las operaciones de ciberdefensa, lo que permite afirmar que se ha pasado de un modelo pasivo/reactivo a un modelo ofensivo, anticipativo y distribuido. Esto refuerza la necesidad de desarrollar contramedidas integradas en tiempo real, como SDR defensivos, IA para detección de *spoofing* y arquitecturas resilientes de red, que minimicen los efectos de un compromiso inicial y permitan una rápida recuperación (Humble, 2024).

Autonomía y toma de decisiones basada en IA

La integración de IA en los UAS se convierte en un punto de inflexión en la forma en que se desarrolla la guerra electrónica moderna, especialmente en lo que respecta a la ejecución autónoma de operaciones de ciberdefensa y ciberataque. Así lo menciona Robin (2024) al señalar que “la expansión de la IA en los conflictos ha puesto de manifiesto que los ejércitos nacionales tienen un enorme interés por esta tecnología, a pesar de lo impredecible y controvertida que puede resultar desde el punto de vista ético”.

Ahora bien, más allá de las capacidades de navegación y control automático, los UAS/RPAS de última generación se están diseñando como plataformas cognitivas que operan de manera descentralizada, permitiéndoles actuar sin intervención humana directa en entornos dinámicos y hostiles. Este nivel de autonomía se logra mediante arquitecturas computacionales que integran aprendizaje automático, análisis predictivo y procesamiento en tiempo real de señales electromagnéticas y patrones de tráfico de red (Yousaf et al., 2022; Park et al., 2018).

Por ejemplo, algunos UAS son capaces de escanear espectros de frecuencia, identificar puntos de acceso no autorizados y ejecutar pruebas móviles de ciberseguridad mediante ataques y penetración controlados. En contextos de alta amenaza, se han registrado prototipos que detectan intentos de *spoofing* GPS y recurren

12 Sistema de control y supervisión que permite monitorear y gestionar procesos industriales o infraestructuras críticas (como plantas eléctricas y redes de agua o de petróleo) a través de redes de comunicación.

13 Programa malicioso diseñado para instalar o descargar otros tipos de *malware* (*payloads*) en un sistema objetivo. Su fin es introducir discretamente software dañino, como troyanos, ransomware o spyware, facilitando ataques más complejos.

a métodos alternativos de navegación, como la triangulación de señales *wi-fi*, el uso de sistemas integrados de navegación por observación estelar o sensores inerciales híbridos, para garantizar la continuidad operativa (Park et al., 2018), sin necesidad de usar sistemas satelitales comerciales y/o militares. Estas funciones se complementan con sistemas de análisis de *big data* a bordo, que clasifican en tiempo real la prioridad de las amenazas y proponen respuestas electrónicas automáticas, incluida la emisión de comandos de *jamming* selectivo o *spoofing* protocolar.

La convergencia entre la IA, la autonomía operacional y las capacidades ciberelectrónicas ha dotado a los UAS modernos de un rol protagónico en la supremacía informacional dentro del campo de batalla, eliminando barreras entre el espacio físico y el ciberespacio mediante acciones autónomas que combinan inteligencia, sigilo y precisión computacional.

Conclusiones

La transformación actual de las operaciones en los campos de batalla ha agregado un nuevo ámbito: el ciberespacio. A lo largo de este capítulo, se ha demostrado que los UAS no solo operan en el aire, sino también en dominios invisibles donde la información, las señales y los programas informáticos deciden el éxito o el fracaso de una misión. De esta manera, defenderse o atacar en este nuevo escenario no implica únicamente detener, neutralizar o identificar amenazas físicas, sino también estar a la vanguardia del desarrollo tecnológico y contar con capacidades para integrar tecnologías disruptivas en nuevos dispositivos, como los UAS.

Los UAS, integrados con tecnologías como la IA, sensores de altas prestaciones, equipos cada vez más pequeños, dispositivos que permiten el acceso a redes, procesadores capaces de manejar altos volúmenes de información y sistemas de encriptación, ofrecen una nueva perspectiva sobre la estrategia militar contemporánea. Ya no se trata solo de emplear equipos con alto poder de fuego, plataformas robustas y grandes arsenales militares; ahora se trata de usar sistemas inteligentes que pueden responder, aprender y cambiar al instante. Esta capacidad convierte a los UAS en sistemas con innumerables opciones de uso en el desarrollo de la guerra moderna. Tanto es así que, en vez de esperar órdenes humanas, estos sistemas anticipan, identifican y neutralizan amenazas con autonomía y precisión.

Una de las capacidades más exploradas en este capítulo es la posibilidad de integrar los drones con tecnologías de *jamming*, *spoofing*, SIGINT y navegación

alternativa, capaces de detectar señales en el espectro electromagnético, interferir e inyectar códigos maliciosos en redes enemigas. A su vez, pueden responder en cuestión de segundos y ejecutar tareas de defensa o ataque. Esta velocidad de respuesta, imposible de igualar para sistemas con intervención humana, redefine los tiempos de decisión y otorga ventaja táctica a quien controle estas herramientas.

Por otra parte, el concepto de *enjambre* añade otra capa de complejidad y sofisticación a los escenarios de guerra en el ciberespacio. Aquí no se trata de un único dron realizando una tarea específica, sino de decenas o cientos de unidades colaborando bajo principios de programación, uso de IA, sensores, equipos altamente novedosos e incluso *software* sofisticado. Su utilidad no sería solamente táctica; puede llegar a considerarse en niveles muy estratégicos, ya que se trata de sistemas capaces de saturar defensas, ejecutar misiones de reconocimiento y ofrecer redundancia en ambientes hostiles.

Referencias

- Abdullayeva, F., & Valikhanli, O. (2023). A survey on UAVs security issues: attack modeling, security aspects, countermeasures, open issues. *Control and Cybernetics*, 52(4), 405-439. <https://doi.org/10.2478/candc-2023-0044>
- Aksu, M. O., Alwardt, C., Berndsen, S., Bollö, J., Cochran, D., Corum, J., Dieckert, U., Eckel, H.-A., Huijgen, H., Hellmann, M., Haider, A., Grest, H., Janssens, L., Jux, A., Kanellos, M. F., Kovar, D., & Künstner, J. (2021). *A comprehensive approach to countering unmanned aircraft systems* (M. Willis, A. Haider, D. C. Teletin, & D. Wagner, Eds.). Joint Air Power Competence Centre. <https://tinyurl.com/28q3r397>
- Al-Dosari, K., Osman, A. I., Elharrouss, O., AlMaadeed, S., & Chaari, M. Z. (2024). *Drone-type-Set: Drone types detection benchmark for drone detection and tracking*. <https://doi.org/10.48550/arXiv.2405.10398>
- Aranda Gómez, J. (2024). *Diseño de la aplicación ciberseguridad y ciberdefensa como estrategia informativa para evitar ataques cibernéticos*. Escuela Superior de Guerra "General Rafael Reyes Prieto". <https://tinyurl.com/25wbp8oa>
- Arreola García, A. (2016). Ciberespacio, el campo de batalla de la era tecnológica. *Estudios en Seguridad y Defensa*, 11(22), 22-109. <https://doi.org/10.25062/1900-8325.212>
- Ceviz, O., Sen, S., & Sadioglu, P. (2023). A survey of security in UAVs and FANETs: issues, threats, analysis of attacks, and solutions. *IEEE Communications Surveys & Tutorials*, 1-33. <https://doi.org/10.1109/COMST.2024.3515051>
- Cybersecurity and Infrastructure Security Agency (CISA). (2025). *Threats to critical infrastructure from unmanned aerial systems (UAS)*.

- Cohen, D., & Rotbart, A. (2013). The proliferation of weapons in cyberspace. *Military and Strategic Affairs*, 5(1). <https://tinyurl.com/2xqsmz5g>
- Cosar, M. (2022). Cyber attacks on unmanned aerial vehicles and cyber security measures. *The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPS-TEM)*, 21, 258-265. <https://doi.org/10.55549/epstem.1226251>
- CSCRC & OMNI. (2024). *Flight critical: Drones, cyber security and infrastructure*.
- Di Cecio, G., Manco, A., & Gigante, G. (2024). On-board drone classification with deep learning and system-on-chip implementation. *Journal of Physics: Conference Series*, 2716(1). <https://doi.org/10.1088/1742-6596/2716/1/012059>
- Estrela, V. V., Hemanth, J., Saotome, O., Nikolakopoulos, G., & Sabatini, R. (2020). *Imaging and sensing for unmanned aircraft systems: Volume 1: Control and performance*. The Institution of Engineering and Technology.
- European Union Agency for Cybersecurity. (2025). *Space threat landscape (March 2025)*. <https://tinyurl.com/yscmb54b>
- Gaitán Rodríguez, A. (2012). *La ciberguerra y sus generaciones: un enfoque para comprender la incidencia de las TIC en la guerra regular*. Centro de Estudios Estratégicos en Seguridad y Defensa Nacional.
- Ghazlane, Y., Gmira, M., & Medromi, H. (2024). Development of a vision-based anti-drone identification friend or foe model to recognize birds and drones using deep learning. *Applied Artificial Intelligence*, 38(1). <https://doi.org/10.1080/08839514.2024.2318672>
- González, L. (2024). *Revisión literaria de los adelantos en la incursión de UAS para su operación en segmentos aéreos segregados y no segregados*. Escuela Superior de Guerra "General Rafael Reyes Prieto". <https://hdl.handle.net/20.500.14205/11261>
- Harvey, G., Laurens, H., & Jansen van Vuuren, S. (2014). Project Snoopy: Data interception and tracking via airborne platforms. *DEF CON 22*.
- Humble, K. (2024, 12 de julio). War, artificial intelligence, and the future of conflict. *Georgetown Journal of International Affairs*. <https://tinyurl.com/2a8n2dtu>
- Hur, C. H., Kim, S. P., Kim, Y. S., & Eom, J. H. (2017). Changes of cyber-attacks techniques and patterns after the Fourth Industrial Revolution. En *2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)* (pp. 69-74). <https://doi.org/10.1109/FiCloudW.2017.79>
- Kamkar, S. (2013). *SkyJack: Autonomous drone hacking*. <https://samyl.pl/skyjack/>
- Konaszczuk, W., & Nogalski, A. (2024). Use of unmanned aerial vehicles for combat purposes: Selected legal and medical aspects. *Studia Iuridica Lublinensia*, 33(2), 129-147. <https://doi.org/10.17951/sil.2024.33.2.129-147>
- Kube, C. (2018, 10 de abril). NBC - Russia has figured out how to jam US drones in Syria, officials say. *NBC News*. <https://tinyurl.com/y84z7vr4>
- Kunertova, D. (2023). Drones have boots: Learning from Russia's war in Ukraine. *Contemporary Security Policy*, 44(4), 576-591. <https://doi.org/10.1080/13523260.2023.2262792>

- MacDonald, N., & Howell, G. (2019). Killing me softly. *PRISM*, 8(3), 102-127. <https://doi.org/10.2307/26864279>
- Mahalle, A., Khandelwal, S., Dhore, A., Barbudhe, V., & Waghmare, V. (2024). Cyber attacks on UAV networks: A comprehensive survey. *Review of Computer Engineering Research*, 11(1), 45-57. <https://doi.org/10.18488/76.v11i1.3636>
- Nikolic, S. (2017). An innovative response to commercial UAV menace: Anti-UAV falconry. *Војно Дело*, 69(4), 146-167. <https://doi.org/10.5937/vojdela1704146n>
- Niyonsaba, S., Konate, K., & Soidridine, M. M. (2023). A survey on cybersecurity in unmanned aerial vehicles: cyberattacks, defense techniques and future research directions. *International Journal of Computer Networks and Applications*, 10(5), 688-705. <https://doi.org/10.22247/ijcna/2023/223417>
- Öz, T., & Sert, S. (2019). The present role of anti-drone technologies in modern warfare and projected developments. *Güvenlik Stratejileri Dergisi*, 15(32), 691-711. <https://doi.org/10.17752/guvenlikstrtj.668216>
- Park, K.-S., Cheon, S., Kim, S.-P., & Eom, J. (2018). Security threats and scenarios using drones on the battlefield. *Journal of the Korea Institute of Information Security & Cryptology*.
- Park, S., Kim, H. T., Lee, S., Joo, H., & Kim, H. (2021). Survey on anti-drone systems: Components, designs, and challenges. *IEEE Access*, 9, 42635-42659. <https://doi.org/10.1109/ACCESS.2021.3065926>
- Perger, Á. (2022). Potential targets of cyber-attacks: legal regulation of drones and self-driving cars. *Journal of Law and Social Sciences*, 46-52. <https://lesp.hu/journal/legal-economic-science-and-praxis-no-7-2022/>
- Rhodes, C. (2024, 14 de agosto). *The rapid advance of uncrewed aerial system technology and operating concepts in the Russia-Ukraine conflict* (Land Power Forum Paper 24). Australian Army Research Centre. <https://tinyurl.com/23wy5hn2>
- Rivero Díez, V. (2021). *La SDR y su rol en la ciberseguridad*. INCIBE.
- Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, 35(1), 5-32. <https://doi.org/10.1080/01402390.2011.608939>
- Robin, N. (2024, 14 de julio). Al's 'Oppenheimer moment': autonomous weapons enter the battlefield. *The Guardian*. <https://tinyurl.com/25yl8psr>
- Sánchez Díaz, S. (2022). *Capacidades de los medios disponibles C-UAS frente a la amenaza de los enjambres de drones*. Universidad de Zaragoza.
- Shafiq, K. (2023). *Drone detection and classification using machine learning*. University of Ottawa.
- Sonenshine, T. (2023, 19 de mayo). Tara Sonenshine. *The Conversation*.
- Tang, A. C. B. (2021). *A review on cybersecurity vulnerabilities for urban air mobility*.
- Tønnessen, T. H. (2017). Islamic State and technology - A literature review. *Perspectives on Terrorism*, 11(6), 101-111. <https://www.jstor.org/stable/26295959?seq=1>

- Yousaf, J., Zia, H., Alhalabi, M., Yaghi, M., Basmaji, T., Shehhi, E. Al, Gad, A., Alkhedher, M., & Ghazal, M. (2022). Drone and controller detection and localization: Trends and challenges. *Applied Sciences*, 12(24). <https://doi.org/10.3390/app122412612>
- Zaki, A. M., Abdelhamid, A. A., Ibrahim, A., Eid, M. M., & El-Kenawy, E.-S. M. El. (2024). Securing the skies: A study of cybersecurity measures in unmanned aerial vehicles. *International Journal of Wireless and Ad Hoc Communication*, 8(1), 51-55. <https://doi.org/10.54216/IJWAC.080106>

Capítulo 5

Interoperabilidad de UAS: desafíos, estrategias y oportunidades en operaciones conjuntas y multinacionales*

DOI: <https://doi.org/10.25062/9786287818620.05>

Javier Hernando Conde Mesa

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Felipe Alfredo Riaño Pérez

Universidad Militar Nueva Granada

Resumen: Este capítulo analiza los desafíos y oportunidades para alcanzar la interoperabilidad de los sistemas de aeronaves no tripuladas (UAS) en operaciones conjuntas y multinacionales, especialmente en contextos de guerra híbrida. A través de una revisión documental y del análisis comparado de estudios recientes, se examinan marcos normativos, limitaciones técnicas y estrategias adoptadas por las Fuerzas Armadas para integrarse con tecnologías emergentes, como la inteligencia artificial. Se destacan iniciativas regulatorias y metodológicas, como SORA, STPA y FRAM, para evaluar riesgos y condiciones operativas en escenarios complejos. Los resultados identifican vacíos regulatorios, deficiencias en la estandarización tecnológica y retos en la comunicación, la logística y la protección de datos. Finalmente, se proponen lineamientos para un marco operativo que articule capacidades interinstitucionales y multinacionales, asegurando una armonización segura y eficiente de los UAS en misiones compartidas, con énfasis en la adaptación a escenarios dinámicos y amenazas no convencionales.

Palabras clave: ciberseguridad; interoperabilidad; operaciones conjuntas; tecnologías de comunicación avanzadas

* Capítulo de libro resultado del proyecto de investigación "Sistema de naves y aeronaves no tripuladas e inteligencia artificial: innovaciones estratégicas para el futuro militar" del grupo de investigación Masa Crítica de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado en A1 por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) (código COL0123247), y la colaboración del grupo de investigación Productividad, Innovación y Tecnología (PIT) de la Universidad Militar Nueva Granada, categorizado en B (código COL0049999). Los puntos de vista y los resultados de este capítulo pertenecen a sus autores y no reflejan necesariamente los de las instituciones participantes.

Javier Hernando Conde Mesa

Teniente Coronel (R) de la Fuerza Aeroespacial Colombiana. Doctor en Bioética, Universidad Militar Nueva Granada, Colombia. Magister en Educación, Universidad Militar Nueva Granada, Colombia. Profesional en Administración Aeronáutica, Escuela Militar de Aviación “Marco Fidel Suárez”, Colombia. Docente ocasional e investigador junior reconocido por Minciencias del Grupo “Masa Crítica”, Escuela Superior de Guerra “General Rafael Reyes Prieto”, Colombia.

Orcid: <https://orcid.org/0000-0001-7152-9399> - Contacto: javier.conde@esdeg.edu.co

Felipe Alfredo Riaño Pérez

Mayor (R) de la Fuerza Aeroespacial Colombiana. Doctor en Educación, Universidad Autónoma de Guadalajara, México. Magister en Educación, Pontificia Universidad Javeriana, Colombia. Ingeniero Civil, Universidad Militar Nueva Granada, Colombia. Docente de tiempo completo e investigador del Grupo “Producción, Innovación y Tecnología (PIT)”, Universidad Militar Nueva Granada, Colombia.

Orcid: <https://orcid.org/0000-0002-1839-6985> - Contacto: felipe.riano@unimilitar.edu.co

Citación APA: Conde Mesa, J. H., & Riaño Pérez, F. A. (2026). Interoperabilidad de UAS: desafíos, estrategias y oportunidades en operaciones conjuntas y multinacionales. En D. Barrero-Barrero (Ed.), *Sistema de naves y aeronaves no tripuladas e inteligencia artificial: innovaciones estratégicas para el futuro militar* (pp. 113-136). Sello Editorial ESDEG.

<https://doi.org/10.25062/9786287818620.05>

SISTEMA DE NAVES Y AERONAVES NO TRIPULADAS E INTELIGENCIA ARTIFICIAL: INNOVACIONES ESTRATÉGICAS PARA EL FUTURO MILITAR

ISBN impreso: 978-628-7818-56-9

E-ISBN digital: 978-628-7818-62-0

DOI: <https://doi.org/10.25062/9786287818620>

Colección Estrategia, Geopolítica y Cultura

Sello Editorial ESDEG

Escuela Superior de Guerra “General Rafael Reyes prieto”

Bogotá D.C., Colombia

2026



Introducción

El crecimiento en el uso de Sistemas de Aeronaves No Tripuladas (UAS) en diversos sectores civiles y militares ha generado la necesidad de establecer mecanismos que permitan su integración segura y eficiente en operaciones conjuntas y multinacionales. Dentro de los diagnósticos evidenciados en los estudios realizados, se identifica que la falta de estándares unificados, así como la heterogeneidad tecnológica, han dificultado su interoperabilidad, generando desafíos en términos de seguridad, regulación y compatibilidad entre sistemas.

Este capítulo examina los principales obstáculos para la interoperabilidad de los UAS, incluyendo la ausencia de regulaciones homogéneas a nivel internacional, lo que genera marcos normativos fragmentados y enfoques divergentes entre los Estados en materia de empleo, control y mitigación de estas tecnologías; las diferencias en las metodologías de evaluación de seguridad; y las barreras tecnológicas que impiden su integración efectiva. Del mismo modo, se analizan modelos como la Evaluación de Riesgo de Operaciones Específicas (SORA), el Análisis Teórico de Procesos del Sistema (STPA) y el Método de Análisis de Resonancia Funcional (FRAM), aplicados a la evaluación de riesgos, así como estudios sobre aeronavegabilidad y gestión de desastres con UAS, para extraer aprendizajes clave en la formulación de estrategias operacionales (Stádník et al., 2022).

Asimismo, se exploran oportunidades para la aplicación de tecnologías emergentes, como la inteligencia artificial (IA) y la optimización de protocolos de comunicación, orientadas a facilitar la integración de UAS en escenarios de aviación compartida dentro del Poder Aeroespacial. Si bien existen marcos regulatorios consolidados en el ámbito de la aviación civil y militar, estos requieren procesos de actualización, armonización y ampliación para incorporar de manera segura

capacidades avanzadas, garantizar altos niveles de seguridad operacional y permitir la interoperabilidad efectiva entre plataformas heterogéneas en entornos complejos.

De esta manera, la interoperabilidad también se ve afectada por las limitaciones técnicas de los UAS, como la autonomía limitada, la capacidad de carga útil y la dependencia de sistemas de navegación como el Sistema de Posicionamiento Global (GPS). En relación con las operaciones conjuntas, donde los UAS deben operar en entornos dinámicos y hostiles, estas limitaciones pueden comprometer la efectividad de las misiones.

Las señales del Sistema Global de Navegación por Satélite (GNSS, según sus siglas en inglés) constituyen la fuente principal de datos de posición y tiempo para los UAS, pero su dependencia expone a estos sistemas a interferencias deliberadas que afectan la disponibilidad y la integridad de la navegación. El *jamming* (interferencia o bloqueo de señales) se ejecuta mediante emisores de banda ancha que elevan el ruido de fondo en la banda L1/L2 hasta niveles que impiden el *lock* de los receptores GNSS, provocando la degradación o pérdida total de la solución de posición en menos de un segundo (Caro, 2023).

En paralelo, el *spoofing* consiste en la transmisión de señales falsas sincronizadas con la constelación legítima, generando métricas de fase de portadora manipuladas que inducen al receptor a calcular posiciones desplazadas entre decenas y cientos de metros en un intervalo inferior a 30 segundos (Hanke, 2025).

Para mitigar estas amenazas, se recomienda la implementación de fusión inercial/GNSS mediante unidades de medición inercial (IMU) de fibra óptica con algoritmos de estimación de estado extendido (EKF), el uso de antenas controladas por fase para generar lóbulos de ganancia nulos en la dirección de interferencia y la adopción de señales de posición, navegación y tiempo (PNT) militares cifradas con M-code y autenticación basada en criptografía asimétrica, cuyas llaves se gestionan mediante protocolos de distribución previa en entornos seguros (Department of Defense, 2024). La integración de estos elementos promueve la continuidad de la navegación y la resiliencia de los UAS ante operaciones de guerra electrónica, que serán presentadas en las conclusiones y recomendaciones.

Fundamentos teóricos de la interoperabilidad en UAS: un marco integrado para operaciones multinacionales

A continuación, se exponen los principales referentes teóricos que sustentan el análisis de la interoperabilidad de los UAS. Este marco conceptual reúne desarrollos recientes en materia de regulación, gestión del tráfico aéreo, ciberseguridad, comunicaciones, logística y evaluación de riesgos aplicados a entornos operacionales complejos. La integralidad de estas perspectivas permite comprender los fundamentos normativos, tecnológicos y operativos que inciden en la articulación efectiva de plataformas UAS bajo esquemas multinacionales, aportando así una base sólida para el análisis crítico y prospectivo de los desafíos y oportunidades que plantea su implementación.

Dentro de los desafíos para la interoperabilidad, es necesario adoptar estrategias holísticas que aborden tanto los aspectos técnicos como los normativos, además de promover la adopción de estándares internacionales que permitan la integración de diferentes sistemas UAS, así como la realización de ejercicios conjuntos para evaluar su efectividad. Instituciones como la Organización de Aviación Civil Internacional (ICAO) y la Organización del Tratado del Atlántico Norte (OTAN) han desarrollado estándares y protocolos para la interoperabilidad de UAS, pero su implementación sigue siendo limitada (De Florio, 2016; Stádník et al., 2022). Por ello, los países con enfoques de seguridad multidimensional pueden adoptar estos estándares como política de defensa conjunta y trabajar en su armonización.

Otra estrategia importante es la implementación de tecnologías de comunicación avanzadas, como el 5G y el *edge computing*, las cuales permiten una mayor eficiencia en la transmisión y el procesamiento de datos. De esta forma, debe ser prospectiva la inversión en infraestructuras de comunicación y ciberseguridad que permitan el desarrollo y la adecuación de redes 5G o superiores, o de redes satelitales que posibiliten una transmisión de datos más rápida y segura, así como la implementación de sistemas de detección y respuesta a amenazas cibernéticas en tiempo real. Además, es necesario establecer programas de capacitación y formación para los operadores de UAS, con el fin de garantizar que estén preparados para enfrentar los desafíos de la interoperabilidad en operaciones conjuntas (Gutiérrez et al., 2024; Ramírez et al., 2024).

La integración de UAS también ofrece oportunidades para mejorar la coordinación y la colaboración entre los diferentes actores involucrados en operaciones

conjuntas, lo que posibilita el uso de plataformas de gestión integradas que faciliten el control y el monitoreo de múltiples UAS desde una única interfaz. Esto puede mejorar la eficiencia operativa y reducir el riesgo de errores. Además, la colaboración internacional en el desarrollo de estándares y protocolos de interoperabilidad puede fortalecer la capacidad de los países para trabajar juntos en operaciones multinacionales (Reis, 2024; Kander et al., 2024).

Desde estas intervenciones, se abren variadas oportunidades para mejorar la eficiencia operativa y la capacidad de respuesta en escenarios de crisis o de guerra, generando condiciones que favorezcan la mejora en la recopilación y el análisis de datos. Del mismo modo, en situaciones de emergencia por desastres, pueden emplearse estas mismas estrategias para identificar puntos críticos generados por sismos de gran magnitud, tsunamis, fenómenos de remoción en masa, flujos de lahares o avalanchas por caudales torrenciales atípicos. Los UAS pueden proporcionar información en tiempo real sobre el terreno, lo que permite una toma de decisiones más rápida y precisa. En operaciones conjuntas, donde múltiples actores deben coordinar sus acciones, esta capacidad es fundamental para garantizar el éxito de las misiones (Restas, 2017; Wang et al., 2024).

Los UAS de categoría I y II dependen de baterías de polímero de litio cuya densidad energética limita su tiempo en estación a decenas de minutos (Mohsan et al., 2023), lo cual resulta insuficiente para misiones de vigilancia persistente o patrullaje de áreas extensas bajo condiciones de amenaza. Para operaciones con requerimientos de persistencia extendida, se emplean plataformas de mayor envergadura dotadas de sistemas de propulsión alternativa: celdas de combustible de hidrógeno, turbinas de gas compactas o configuraciones híbridas de combustible-eléctrico (Gadsden et al., 2016).

Estas arquitecturas energéticas integradas combinan tanques de combustible convencionales con gestores de energía avanzados, extendiendo la autonomía operacional a varias horas sin comprometer la carga útil ni la maniobrabilidad (Gadsden et al., 2016). Al reducir la frecuencia de relevo y minimizar los puntos de reabastecimiento en la zona de operaciones, se refuerza la sostenibilidad de la misión y se mitigan los riesgos logísticos y de exposición a fuego enemigo (Gadsden et al., 2016).

Aunque se han desarrollado tecnologías como celdas de combustible y sistemas híbridos para extender la autonomía, su implementación en UAS pequeños sigue siendo un aspecto de investigación y desarrollo debido a restricciones de peso y espacio (Gutiérrez et al., 2024; Dalamagkidis et al., 2008).

En tal sentido, la dependencia de los UAS de sistemas de navegación como el GPS los hace vulnerables a interferencias y ataques, lo que puede afectar negativamente su autonomía operativa. En entornos hostiles, donde el acceso a estos sistemas puede estar restringido —o en países de América Latina, cuya topografía y condiciones selváticas representan desafíos adicionales—, los UAS deben recurrir a sistemas alternativos, como la navegación inercial, los cuales presentan limitaciones en cuanto a precisión y confiabilidad (Pérez et al., 2024; Škultéty et al., 2022).

Dichos sistemas utilizan una amplia variedad de sensores y cargas útiles, como cámaras térmicas, tecnología de escaneo y teledetección conocida como *Light Detection and Ranging* (LiDAR), sensores hiperespectrales y sistemas de comunicación avanzados. Sin embargo, la interoperabilidad entre estos sensores y las plataformas UAS constituye un desafío técnico significativo. En ausencia de arquitecturas abiertas y estándares de comunicación comunes, los ingenieros se ven obligados a desarrollar adaptaciones específicas entre sensores, interfaces y protocolos propietarios, lo que incrementa la complejidad técnica y dificulta la interoperabilidad efectiva entre sistemas UAS de distintos fabricantes. Esta fragmentación tecnológica limita la integración de capacidades en entornos conjuntos y multinivel, contraviniendo los principios doctrinales de interoperabilidad y estandarización promovidos en los sistemas de defensa modernos (López et al., 2024; Wang et al., 2024).

En operaciones conjuntas, donde múltiples aeronaves no tripuladas pueden estar equipadas con sensores de diferentes tipos, la ausencia de estándares comunes en interfaces y protocolos puede introducir desafíos técnicos asociados a la integración y gestión de la información. Si bien estos desafíos no implican necesariamente una degradación inmediata de las capacidades operacionales —dado el empleo de arquitecturas de mando y control, pasarelas de interoperabilidad y procedimientos de mitigación—, sí pueden incrementar la complejidad del sistema y exigir mayores esfuerzos de coordinación, especialmente en escenarios dinámicos donde la rapidez en el flujo de información resulta crítica (Stádník et al., 2022; Gordo et al., 2024).

Otra oportunidad que ofrecen estas tecnologías es la reducción de costos operativos, toda vez que los UAS son más económicos que las aeronaves tripuladas, tanto en términos de adquisición como de operación. Además, su capacidad para operar en entornos hostiles y de alto riesgo reduce la necesidad de exponer a personal humano a situaciones peligrosas. Visto desde las operaciones conjuntas,

donde los recursos son limitados, esta reducción de costos puede ser un factor determinante para garantizar la sostenibilidad de las misiones. Asimismo, es primordial promover la investigación y el desarrollo de tecnologías avanzadas que mejoren la capacidad de los UAS para operar de manera autónoma y segura (Restas, 2017; Howard et al., 2024).

Esta actividad de información digital es una prioridad en las estrategias de interoperabilidad, por lo que resulta necesario desarrollar protocolos de seguridad avanzados que protejan las redes de comunicación de los UAS contra ciberataques. Esto incluye la implementación de sistemas de autenticación mutua, encriptación de datos y detección de anomalías basados en IA. En consecuencia, es fundamental establecer marcos normativos que regulen el uso de tecnologías de ciberseguridad en operaciones conjuntas y multinacionales (Guo et al., 2023; Ramírez et al., 2024).

Otro de los derroteros es la integración de sistemas autónomos en el espacio aéreo compartido con aeronaves tripuladas, dados los protocolos militares, las regulaciones aéreas y las operaciones logísticas. A medida que aumenta el número de UAS en operaciones conjuntas, también se incrementa el riesgo de conflictos de tráfico aéreo. Por ello, los sistemas de gestión del tráfico aéreo (ATM) tradicionales no están diseñados para manejar la densidad y complejidad de la circulación generada por los UAS, especialmente en entornos urbanos o en zonas de conflicto (García et al., 2024; Kandra et al., 2024).

Además, los UAS operan a altitudes más bajas que las aeronaves tripuladas, lo que aumenta el riesgo de colisiones con obstáculos terrestres, como edificios, torres de comunicación y otras infraestructuras. La falta de sistemas avanzados de detección y evitación de colisiones (DAA) en muchos UAS agrava este problema, especialmente en operaciones conjuntas donde múltiples plataformas deben operar en estrecha proximidad (Dai et al., 2024; Škultéty et al., 2022).

Por otro lado, la comunicación entre los UAS y las estaciones de mando y control es fundamental para garantizar la interoperabilidad en operaciones multido-minio. Sin embargo, los sistemas actuales enfrentan varios desafíos técnicos. En primer lugar, la mayoría de las aeronaves no tripuladas dependen de enlaces de radiofrecuencia para la transmisión de datos, los cuales pueden ser vulnerables a interferencias, bloqueos y ciberataques, como se identificó anteriormente. En segundo lugar, en entornos hostiles o en campañas militares, las señales de comunicación pueden ser interceptadas o bloqueadas, lo que compromete la capacidad de los UAS para operar de manera efectiva (Guo et al., 2023; Ramírez et al., 2024).

Al mismo tiempo, operar en áreas remotas o con infraestructura limitada constituye otro desafío importante, como ocurre en países emergentes dada su escasa conectividad con redes de comunicaciones. En operaciones multinacionales, donde los UAS pueden desplegarse en regiones con poca cobertura de red, la falta de conectividad puede dificultar la transmisión de datos en tiempo real y la coordinación entre las diferentes plataformas. Aunque se han propuesto soluciones como el uso de satélites y redes Mesh, su implementación en UAS pequeños sigue siendo un desafío debido a limitaciones de peso, costo y complejidad técnica (Gutiérrez et al., 2024; Kander et al., 2024).

Otro aspecto de análisis es la logística y el mantenimiento en operaciones conjuntas y multinacionales, lo que constituye un desafío operativo importante. Los UAS requieren mantenimiento regular para garantizar su funcionamiento óptimo, especialmente en entornos hostiles donde las condiciones climáticas y el desgaste pueden afectar su rendimiento. Sin embargo, en operaciones multinacionales, donde pueden provenir de diferentes países y fabricantes, la falta de estandarización en piezas y componentes puede dificultar el mantenimiento y la reparación de las plataformas (Restas, 2017; Dalamagkidis et al., 2008).

La logística de transporte y almacenamiento de los UAS en zonas de operación también constituye un desafío operativo, ya que los UAS, especialmente los de mayor tamaño, requieren infraestructura especializada para su transporte, almacenamiento e incluso plataformas de lanzamiento, lo que puede no estar disponible en todas las regiones donde se despliegan. Esto puede generar retrasos en la implementación de las misiones y aumentar los costos operativos (Howard et al., 2024; Kander et al., 2024).

Dado que estos sistemas recopilan y transmiten un volumen importante de datos sensibles, como imágenes de alta resolución, información de inteligencia y datos de navegación, en operaciones conjuntas donde estos datos pueden ser compartidos entre múltiples actores, la falta de protocolos de seguridad estandarizados puede generar vulnerabilidades y riesgos de ciberseguridad. Además, la protección de los datos contra accesos no autorizados y la garantía de su integridad constituyen desafíos técnicos importantes, especialmente cuando los datos pueden ser compartidos entre países con diferentes marcos normativos y políticas de seguridad, lo que complica la protección de la información (Guo et al., 2023; Ramírez et al., 2024).

Finalmente, contar con un análisis crítico de las estrategias regulatorias y metodológicas en desarrollo, proponiendo enfoques prospectivos para mejorar la

integración de UAS en operaciones conjuntas y multinacionales, permitirá contribuir al avance del sector de la industria de la defensa a través de la identificación de mejores prácticas y recomendaciones fundamentadas en estudios recientes (Reis, 2024; García et al., 2024).

Interoperabilidad en entornos multidominio: estrategias para la defensa conjunta con UAS

De Florio (2016) destaca que la aeronavegabilidad de los UAS requiere estándares específicos que se ajusten a las características particulares de estos sistemas. Se evidencia que la falta de un marco normativo unificado genera riesgos para la seguridad, ya que los requisitos tradicionales de aeronavegabilidad, diseñados para aeronaves tripuladas, no son directamente aplicables a estas plataformas. En este sentido, la creación de estándares internacionales que contemplen las particularidades de los UAS es fundamental para su integración en el espacio aéreo, tanto en aplicaciones militares como civiles.

De otra parte, el análisis comparativo realizado por Stádník et al. (2022) enfatiza la necesidad de evaluar y comparar métodos de evaluación de riesgos específicos para operaciones de UAS. La integración de métodos como SORA, STPA y FRAM revela que la seguridad operativa de estos sistemas no solo depende de la definición de objetivos operativos, sino también de la capacidad para identificar y mitigar interacciones sistémicas complejas.

La convergencia de estos enfoques normativos y metodológicos sugiere que la interoperabilidad óptima se alcanzará mediante la estandarización de los criterios de certificación y de seguridad, permitiendo la integración de sistemas heterogéneos en un marco regulatorio armonizado a nivel internacional (De Florio, 2016; Stádník et al., 2022).

Las operaciones conjuntas en la “zona gris”, identificadas como tácticas híbridas relacionadas con ciberataques o desinformación, desafían los límites de la guerra convencional y demandan estrategias flexibles. Es por ello que Bajarūnas (2020) subraya que la resiliencia requiere coordinación interinstitucional (UE-OTAN) y enfoques *whole-of-society* para contrarrestar ataques asimétricos. En este contexto, las capacidades de fuerza intermedia (IFC), como sistemas antidrones o de guerra electrónica, ofrecen opciones no letales para escalar o desescalar conflictos. Christensen y Dobias (2021) demuestran, mediante simulaciones, que

las IFC permiten a los comandantes mantener la iniciativa estratégica en escenarios como bloqueos marítimos u hostigamiento con drones, extendiendo el tiempo de respuesta y reduciendo riesgos de confrontación abierta. No obstante, su implementación requiere el establecimiento de protocolos operativos comunes que garanticen la interoperabilidad, especialmente frente a posibles discrepancias en el uso del espectro electromagnético o en los estándares de ciberseguridad.

Armonización de estándares OTAN y evaluación de riesgos

La interoperabilidad tecnológica depende de sistemas adaptables que integren IA, conectividad segura y capacidades de detección de amenazas en tiempo real. En este sentido, Elzaghmouri et al. (2024) proponen un modelo híbrido de aprendizaje profundo combinado con internet de las cosas (IoT), el cual alcanza un 99,6 % de precisión en la detección de ciberataques mediante el uso de redes neuronales convolucionales (CNN) y mecanismos de atención.

Aplicado a los UAS, este enfoque podría estandarizar la identificación de amenazas como *spoofing* GPS o interferencias, facilitando la colaboración entre plataformas de distintos países. Además, la integración de UAS en redes Mesh seguras, respaldadas por estándares como Stanag 4586 para el control de sistemas no tripulados, permitiría operaciones sincronizadas en entornos hostiles. No obstante, como advierte Stádník et al. (2022), la dependencia de servicios externos como U-space exige validar su fiabilidad mediante métodos como FRAM, que analiza la variabilidad funcional en sistemas complejos.

Del mismo modo, la evaluación de riesgos en la operación de UAS es fundamental para garantizar la seguridad en escenarios conjuntos y multinacionales. Es por ello que el método SORA, desarrollado para evaluar riesgos operacionales en entornos específicos, permite a los operadores identificar y clasificar amenazas de manera sistemática, aunque presenta limitaciones al no capturar completamente la complejidad de las interacciones en sistemas integrados (Stádník et al., 2022).

Por ello, la comparación de los métodos STPA y FRAM ofrece una perspectiva dinámica y sistémica: mientras STPA se enfoca en identificar fallos derivados de las interacciones entre los componentes del sistema, FRAM analiza cómo la variabilidad en las funciones operacionales puede dar lugar a incidentes. La combinación de estos métodos proporciona una evaluación integral del riesgo, esencial para anticipar fallos y coordinar respuestas en operaciones de UAS en entornos de alta complejidad (Stádník et al., 2022).

Estos enfoques metodológicos, al complementarse entre sí, permiten diseñar estrategias operativas que integren tanto la evaluación estática como la dinámica del riesgo. Este análisis comparado respalda la necesidad de implementar sistemas de monitoreo continuo y de revisión periódica de la capacitación y las competencias de los operadores, aspectos que resultan críticos en operaciones conjuntas y multinacionales.

Respuesta a amenazas híbridas: simulaciones y capacidades no letales

El avance tecnológico es un componente virtuoso para alcanzar la interoperabilidad óptima de los UAS en entornos de operaciones conjuntas, toda vez que permite la adopción de tecnologías emergentes, como la IA, sistemas avanzados de detección de colisiones y protocolos de comunicación estandarizados, los cuales pueden mejorar significativamente la capacidad de integración de estos sistemas.

En el contexto militar, la integración de UAS en una red de defensa conjunta requiere no solo la actualización de normativas, sino también el desarrollo de marcos operativos que faciliten la coordinación entre diferentes actores y sistemas. La simulación de escenarios y los ejercicios estratégicos, como los juegos de guerra para evaluar capacidades de fuerza intermedia en la zona gris, demuestran la importancia de entrenar y perfeccionar las respuestas conjuntas ante amenazas híbridas (Christensen & Dobias, 2021).

Asimismo, la interoperabilidad se ve fortalecida cuando se establecen mecanismos de defensa conjunta que integren tanto las capacidades de monitoreo como las de respuesta rápida ante incidentes. La coordinación multinacional, sustentada en estándares tecnológicos comunes y en marcos operativos integrados, es esencial para garantizar que los UAS puedan operar de forma segura en entornos complejos y compartidos.

La interoperabilidad de UAS en entornos multinacionales es un desafío crítico para las Fuerzas Armadas contemporáneas, toda vez que la creciente dependencia de estos sistemas en misiones de inteligencia, vigilancia, reconocimiento y operaciones de combate (ISR) exige una estandarización técnica, así como la generación de doctrina y manuales normativos que permitan la integración fluida entre aliados (De Florio, 2016). Este apartado analiza las oportunidades y retos en la interoperabilidad de UAS, proponiendo un marco basado en arquitecturas abiertas, gestión de datos en tiempo real y gobernanza colaborativa.

Arquitecturas de comando y control para operaciones sincronizadas

La interoperabilidad técnica de los UAS depende de la adopción de arquitecturas abiertas y protocolos estandarizados. Uno de estos estándares es el Stanag 4586, desarrollado por la OTAN, referente clave al definir interfaces comunes para el control de sistemas no tripulados (Christensen & Dobias, 2021). Este protocolo permite la integración de UAS de diferentes fabricantes en una red de mando y control (C2) unificada, facilitando operaciones conjuntas.

Además, sistemas como *Future Airborne Capability Environment* (FACE) promueven la modularidad en el desarrollo de *software* militar, reduciendo la dependencia de proveedores exclusivos y fomentando la compatibilidad entre plataformas aliadas (Northrop Grumman, 2023). La implementación de estas arquitecturas minimiza los riesgos de obsolescencia tecnológica y mejora la adaptabilidad en escenarios dinámicos.

Las operaciones aéreas exigen soluciones para el procesamiento y la diseminación de datos en entornos multinacionales. Por ello, plataformas como AWS AppFabric ofrecen esquemas de interoperabilidad basados en IA, permitiendo la fusión de datos provenientes de sensores heterogéneos e incluso de la aviónica de la plataforma (Elzaghmouri et al., 2024).

Un caso de análisis significativo es el sistema *Forward Area Air Defense Command and Control* (FAAD C2), utilizado por la Fuerza Aérea de los Estados Unidos (USAF) y sus aliados para integrar datos de radares, UAS y sistemas anti-aéreos en una única imagen operativa (Northrop Grumman, 2023). Este enfoque reduce la latencia en la toma de decisiones y optimiza la respuesta ante amenazas aéreas.

Integración multinacional: lecciones de ejercicios conjuntos y estándares globales

La falta de estándares globales en la certificación de UAS limita su despliegue en operaciones combinadas. Si bien la Federal Aviation Administration de Estados Unidos (FAA) y la Agencia Europea de Seguridad Aérea (EASA) han avanzado en normativas para el espacio aéreo civil, el ámbito militar requiere marcos específicos que aseguren la compatibilidad entre sistemas aliados (Stádník et al., 2022).

La guerra entre Rusia y Ucrania ha evidenciado la necesidad de implementar sistemas de gestión del tráfico de aeronaves no tripuladas (UTM) en zonas de conflicto. En este contexto, Bajarūnas (2020) señala que iniciativas como el UTM desarrollado por la OTAN buscan estandarizar los procedimientos de operación de vuelos no tripulados, mediante protocolos específicos orientados a evitar colisiones y gestionar el uso del espectro electromagnético. Estas medidas resultan fundamentales para garantizar la seguridad y la continuidad operativa, particularmente ante el creciente uso y la facilidad de adquisición de drones, ya sean de bajo costo o especializados, directamente en los escenarios de conflicto.

La gestión del espectro electromagnético se considera un componente operativo en escenarios de conflicto donde se aplican tácticas de guerra electrónica. La asignación dinámica de frecuencias y la aplicación de protocolos automatizados para la reasignación de canales permiten mantener la integridad de las comunicaciones y disminuir la probabilidad de interferencias que puedan originar colisiones o pérdida de datos (Bajarūnas, 2020).

Asimismo, la interoperabilidad entre sistemas y la colaboración entre organismos públicos y privados constituyen elementos determinantes para la coordinación del tráfico de UAS en entornos de guerra. La convergencia de aplicaciones, que comprende misiones de reconocimiento y operaciones ofensivas y defensivas, demanda el desarrollo de plataformas que integren funciones de respuesta operativa. Estudios recientes sugieren la incorporación de sistemas UTM en un marco que incluya la defensa aérea, la ciberseguridad y el análisis de datos (IAMDCOE, 2024; CSIS, 2022).

Finalmente, las lecciones derivadas del conflicto han evidenciado la necesidad de fortalecer los protocolos existentes y de incorporar tecnologías emergentes, como algoritmos de IA y técnicas de aprendizaje automático. Estas innovaciones permiten la detección en tiempo real de comportamientos anómalos y facilitan la adaptación inmediata a condiciones cambiantes propias de entornos de guerra electrónica. Según Airmobi UAV (2022), la estandarización de procesos y la creación de marcos regulatorios internacionales se presentan como pasos esenciales para asegurar la operatividad y la seguridad en el espacio aéreo utilizado por los drones, tanto en ámbitos civiles como militares.

Acuerdos de interoperabilidad multinacional

La integración de sistemas en el ámbito de los UAS requiere coordinación entre naciones en términos técnicos, legales y de ciberseguridad. De esta manera,

el *Acuerdo de Interoperabilidad de Sistemas No Tripulados (UAS Interoperability Agreement)*, suscrito por miembros de la Coalición Global Contra el Terrorismo, establece criterios para el intercambio seguro de datos y la mitigación de ciberamenazas (Christensen & Dobias, 2021). Entre 2023 y 2025 se han adoptado mecanismos adicionales orientados a actualizar este marco normativo, en función de la evolución de los entornos operacionales y las técnicas de defensa.

Estudios y ejercicios multinacionales desarrollados durante este período han proporcionado insumos para la revisión de los estándares de interoperabilidad. En particular, ejercicios coordinados en escenarios de contramedidas contra drones han permitido evaluar sistemas que integran protocolos para la detección, identificación y neutralización de amenazas, al tiempo que establecen criterios para el intercambio seguro de información. Los resultados de las actividades coordinadas por la OTAN han contribuido a la definición de nuevos parámetros técnicos y de protección de infraestructura cibernética.

La formalización de instrumentos contractuales en el ámbito de la defensa se ha evidenciado con la aprobación del primer contrato multinacional relacionado con sistemas de defensa contra aeronaves no tripuladas pequeñas (C-sUAS) por parte de la NATO Support and Procurement Agency (NSPA, 2024). Dicho acuerdo dispone medidas para el intercambio de información operativa y la atenuación de riesgos asociados a la interconexión de sistemas operados en conjunto. Además, la publicación de la *NATO Integrated Air and Missile Defence Policy* en febrero de 2025 incorpora disposiciones específicas relacionadas con la protección y compartición de datos en operaciones que involucran UAS, integrando estos elementos en el marco de la defensa aérea coordinada (NATO, 2025).

La implementación de estos instrumentos normativos y contractuales se orienta a la estandarización de procesos de interoperabilidad en contextos multinacionales. La actualización de marcos legales y operativos, fundamentada en las investigaciones y ejercicios realizados en los últimos años, facilita la formulación de pautas uniformes para el intercambio de datos sensibles y la gestión de amenazas cibernéticas, lo que promueve la operatividad compartida de sistemas en escenarios conjuntos.

Estrategias para incorporar UAS en capacidades militares

La integración de UAS en operaciones militares requiere la ejecución de estrategias que permitan responder a escenarios operacionales con múltiples variables y amenazas híbridas (Northrop Grumman, 2024). Este proceso se ha abordado

mediante tres líneas de acción evaluadas en el período 2023-2025: 1) neutralización de enjambres de drones a través de sistemas avanzados; 2) simulaciones con gemelos digitales y entrenamiento operativo; y 3) protocolos de interoperabilidad multinacional.

Se han desarrollado evaluaciones técnicas y ejercicios operativos orientados a la detección, el análisis y la neutralización de enjambres de drones mediante la implementación del sistema Advanced Battle Management (ABM), desarrollado por Northrop Grumman. Este sistema incorpora algoritmos de procesamiento en tiempo real que permiten asignar medios ofensivos a los objetivos identificados en el campo de batalla con elevada rapidez operativa. Estudios recientes (2024) han demostrado que la actualización del sistema FAAD C2, al integrar capacidades de IA, facilita el procesamiento de datos provenientes de múltiples sensores y mejora la asignación eficaz de armas a objetivos en escenarios donde convergen múltiples amenazas (Army Recognition, 2024; Northrop Grumman, 2024).

La utilización de gemelos digitales y simuladores ha permitido la creación de entornos virtuales que replican escenarios de campo, facilitando la formación y la evaluación de algoritmos de control para UAS. Investigaciones publicadas entre 2023 y 2025 han desarrollado marcos de referencia para la transferencia *sim-to-real*, en los cuales se integran datos de sensores en tiempo real para la identificación de patrones y la optimización de la toma de decisiones. Estos entornos de simulación permiten la verificación iterativa de algoritmos y la cuantificación de la respuesta operativa en situaciones que requieren una reacción coordinada frente a múltiples amenazas (Amjad, 2024; Salinas et al., 2023).

La incorporación de UAS en entornos de defensa avanzada se ha beneficiado de ejercicios conjuntos y de la creación de protocolos comunes entre organismos de seguridad y defensa, como los desarrollados en el marco de la cooperación UE-OTAN. Durante el período 2023-2025 se han realizado juegos de guerra híbridos que han permitido la evaluación y estandarización de métodos de comunicación, coordinación y respuesta en escenarios multidominio. Dichos ejercicios han permitido identificar áreas de mejora en la integración de plataformas operacionales y han impulsado la actualización de protocolos para la operación en entornos caracterizados por actividades híbridas (Brethous & Kovalčíková, 2023; NATO, 2024).

El análisis de estas estrategias revela que la incorporación de UAS en las capacidades militares implica no solo la adopción de tecnologías para la respuesta rápida ante amenazas multientidad, sino también la estructuración de entornos de simulación para la toma de decisiones y la implementación de marcos de

interoperabilidad ajustados a normas interinstitucionales. Estas iniciativas consolidan la integración progresiva de UAS en escenarios de defensa operativa avanzada.

Marco operativo multidominio: integración de UAS e IA en escenarios de defensa conjunta

Un marco operativo orientado a misiones multidominio requiere la convergencia de componentes tecnológicos, normativos y formativos que permitan el funcionamiento coordinado de plataformas no tripuladas y algoritmos de IA. La siguiente sistematización describe cada componente evaluado en investigaciones recientes (2023-2025).

Las arquitecturas que combinan redes neuronales convolucionales (CNN) y mecanismos de atención proporcionan herramientas para la identificación y el análisis de datos provenientes de sensores en tiempo real. Estas estructuras permiten la detección de amenazas cibernéticas e interferencias en UAS mediante la fusión de información procedente de diversas fuentes. Estudios recientes (Elzaghmouri et al., 2024; Kamal & Mashaly, 2024) han evaluado la aplicación de estos modelos en entornos operacionales, indicando la posibilidad de procesar volúmenes elevados de datos con resultados cuantificables durante ejercicios simulados.

Las plataformas de comando y control, como el sistema FAAD C2, integran datos de posicionamiento, imágenes aéreas y señales de múltiples sensores para generar una representación operativa unificada del campo de batalla. La incorporación de algoritmos de fusión de datos y de sincronización ha facilitado la gestión de conflictos en tiempo real en entornos combinados —aéreo, terrestre y marítimo—. Las actualizaciones implementadas entre 2023 y 2025 han permitido la integración de capacidades de respuesta rápida ante variaciones en el entorno operativo (Northrop Grumman, 2024).

Regulación adaptativa: certificaciones dinámicas y ciberseguridad en entornos hostiles

Se ha propuesto la actualización de metodologías tradicionales, como SORA, para incorporar evaluaciones integradas de riesgos sistémicos mediante enfoques como STPA y FRAM. Estas metodologías se amplían para incluir requisitos de entrenamiento práctico, evaluado por entidades externas, y para establecer parámetros operativos en escenarios complejos. De otra parte, investigaciones recientes

han contrastado variables de riesgo operacional y validado protocolos en ejercicios de campo, lo que posibilita la normalización de procesos de certificación en entidades reguladoras (EASA, 2023; JAA TO, 2025).

El fortalecimiento de normas inspirado en lineamientos adaptados de marcos de protección de datos para sistemas operados en entornos de conflicto y defensa, aplicado al ámbito militar, se plantea como mecanismo para proteger la información transmitida por UAS. En el período evaluado se han establecido directrices específicas que incluyen requerimientos técnicos para el cifrado, la autenticación y el control de acceso, además de la periodicidad de las auditorías de seguridad en contextos de operaciones multinacionales (OCR, 2025).

Capacitación multidominio: simulaciones con gemelos digitales y equipos interdisciplinarios

El funcionamiento integrado de UAS e IA requiere la conformación de equipos compuestos por profesionales en IA, ciberseguridad y derecho internacional. La estructuración de programas de capacitación interinstitucional, basada en experiencias y lecciones derivadas de ejercicios conjuntos, se orienta a dotar a los operarios de herramientas para la interpretación de escenarios operativos complejos y la ejecución de respuestas coordinadas. Informes recientes han destacado la importancia de estos equipos para la gestión de operaciones en marcos regulatorios con contenidos actualizados (BID, 2019; 2025).

Las plataformas de simulación que emplean gemelos digitales permiten replicar escenarios de conflicto, como bloqueos marítimos o ataques de enjambres, sin exponer activos a riesgos directos. La integración de datos en tiempo real y el modelado físico en entornos virtuales posibilitan la experimentación y el ajuste iterativo de tácticas operativas. Las iteraciones desarrolladas han permitido la verificación de algoritmos de respuesta y la consolidación de estrategias de coordinación en condiciones óptimas de simulación (Salinas et al., 2023; Maglione et al., 2022).

UAS en la guerra híbrida: integración tecnológica, resiliencia operativa y escenarios multidominio

La guerra híbrida, caracterizada por la convergencia de tácticas convencionales, irregulares y cibernéticas, exige, como se planteó anteriormente, que las Fuerzas

Armadas modernicen sus capacidades mediante la integración estratégica de UAS. Estos sistemas ofrecen ventajas críticas en vigilancia, reconocimiento y respuesta ágil, pero su despliegue efectivo requiere abordar desafíos técnicos, doctrinales e interoperables.

Los UAS deben operar en sinergia con sistemas de guerra electrónica, redes de comunicación seguras y plataformas de IA para contrarrestar amenazas asimétricas. La implementación de arquitecturas de redes tolerantes a retardos (DTN) permite mantener la conectividad en entornos de espectro disputado, esencial para misiones en zonas grises (Christensen & Dobias, 2021). Además, la adopción de UAS equipados con sensores hiperespectrales y LiDAR facilita la detección de objetivos camuflados o municiones sin detonar (UXO), aspecto crítico en escenarios urbanos (López et al., 2024).

La ciberseguridad es fundamental, en virtud de que los UAS deben incorporar protocolos de encriptación cuántica resistente y sistemas de autenticación multifactorial para mitigar ataques de *spoofing* o *jamming* (Guo et al., 2023). Por ello, la OTAN recomienda el uso de redes definidas por *software* (SDN) para aislar segmentos críticos y garantizar la resiliencia de las comunicaciones (NATO, 2023).

De otra parte, en entornos híbridos, los UAS deben operar bajo doctrinas que prioricen la descentralización y la autonomía condicional. En este sentido, los enjambres de drones, controlados mediante algoritmos de optimización (*swarm intelligence*), pueden saturar las defensas adversarias y ejecutar misiones de supresión de defensas aéreas (SEAD) con menor riesgo humano (Dai et al., 2024). La integración de UAS con sistemas de contramedidas electrónicas (ECM) permite neutralizar radares enemigos, como se evidenció en el conflicto de Nagorno-Karabaj en 2020 (Defense News, 2023).

Para operaciones de contrainsurgencia, los UAS de bajo costo y corto alcance, como el Switchblade 300, proporcionan capacidades de ataque de precisión sin exponer tropas. Estos sistemas deben combinarse con plataformas de inteligencia de señales (SIGINT) para identificar nodos de mando enemigos en tiempo real (Reis, 2024).

En cuanto a los desafíos y soluciones emergentes, la interoperabilidad sigue siendo un obstáculo. En tal sentido, las Fuerzas Armadas deben adoptar estándares abiertos como Stanag 4586 para integrar UAS de distintos fabricantes en una red de batalla unificada (Škultéty et al., 2022). Además, la autonomía energética basada en baterías limita las misiones prolongadas; por ello, soluciones como celdas

de combustible de hidrógeno y sistemas de recarga inalámbrica en campo están siendo probadas para extender la resistencia operativa (DARPA, 2023).

La guerra electrónica plantea siempre riesgos críticos; en consecuencia, los UAS deben incorporar sistemas de navegación inercial (INS) redundantes y algoritmos de IA para mantener la orientación ante la pérdida de señal GPS (Pérez et al., 2024). La simulación digital mediante gemelos digitales permite entrenar operadores en escenarios de guerra híbrida, adaptando tácticas a amenazas dinámicas (Vargas et al., 2024).

Finalmente, entre las lecciones de Ucrania, los UAS Bayraktar TB2 han demostrado su eficacia en la destrucción de sistemas de artillería y logística rusos, destacando la importancia de la superioridad aérea táctica en conflictos asimétricos (The War Zone, 2023). No obstante, de acuerdo con Reis (2024), la vulnerabilidad frente a interferencias GPS subraya la necesidad de sistemas alternativos de posicionamiento, como la constelación europea IRIS2 (infraestructura para la resiliencia, la interconectividad y la seguridad por satélite).

Conclusiones

La ausencia de un marco regulatorio unificado y la heterogeneidad tecnológica constituyen obstáculos para la integración efectiva de los UAS en operaciones conjuntas. La falta de estándares internacionales armonizados, como los propuestos por la OTAN (Stanag 4586), limita la compatibilidad entre sistemas de diferentes fabricantes y naciones, generando riesgos operativos y de seguridad.

La dependencia del GPS expone a los UAS a ataques de *jamming* y *spoofing*, comprometiendo su autonomía y eficacia en entornos hostiles. Adicionalmente, las limitaciones en la capacidad de carga útil y la autonomía energética restringen su uso en misiones prolongadas, especialmente en zonas remotas o de topografía compleja.

Asimismo, el estudio evidencia que la integración de UAS en entornos complejos requiere la adopción de arquitecturas abiertas y sistemas de mando y control capaces de fusionar datos de diferentes sensores en tiempo real. La utilización de tecnologías emergentes, como la IA, los gemelos digitales y la conectividad avanzada (por ejemplo, 5G o *edge computing*), resulta indispensable para mejorar la capacidad de respuesta y la seguridad ante amenazas asimétricas, incluidos los ciberataques y la manipulación de señales de navegación. En este contexto, la

aplicación de métodos como SORA, STPA y FRAM ha demostrado ser útil para la identificación y mitigación de riesgos operacionales, lo que subraya la necesidad de incorporar evaluaciones dinámicas y sistémicas en entornos híbridos.

La implementación de IA, redes 5G y *edge computing* mejora la coordinación en tiempo real, la detección de amenazas y la optimización de rutas. Plataformas como FAAD C2 demuestran la utilidad de la fusión de datos multisensorial, y los algoritmos de IA optimizan la toma de decisiones en operaciones multidominio.

Se observa que la formación de equipos multidisciplinarios y la realización de simulaciones avanzadas son factores esenciales para garantizar la interoperabilidad y la eficiencia en la ejecución de misiones. La capacitación basada en escenarios realistas fortalece la toma de decisiones en situaciones de riesgo elevado y mejora la gestión operativa de los UAS. Además, la implementación de acuerdos multinacionales para el intercambio seguro de datos y la coordinación interinstitucional ha probado ser un componente estratégico en la modernización de la defensa conjunta, facilitando la integración de sistemas y optimizando el uso del espectro electromagnético en entornos hostiles.

Ejercicios conjuntos y simulaciones, como los hechos por la OTAN, evidencian la necesidad de protocolos estandarizados para la gestión del espectro electromagnético, la defensa cibernética y la interoperabilidad técnica. La guerra en Ucrania subraya la importancia de sistemas UTM avanzados y de la resiliencia ante amenazas híbridas. El fortalecimiento de la ciberseguridad, la estandarización de interfaces y protocolos, y la capacitación especializada emergen como criterios clave para mitigar los riesgos inherentes a la operación conjunta de estos sistemas en escenarios complejos y multidominio.

Referencias

- Airmobi UAV. (2022). *Analyzing the application of UAVs in the Russia-Ukraine conflict*.
- Army Recognition. (2024, 8 de octubre). *Northrop Grumman integrates AI into FAAD command system to strengthen drone defense*.
- Amjad, M. (2024). Digital twin for UAVs: Architecture, framework, challenges and solutions. En *Digital twins for wireless networks* (pp. 149-159). Springer. https://link.springer.com/chapter/10.1007/978-3-031-73679-7_8
- Bajarūnas, E. (2020). Addressing hybrid threats: Priorities for the EU in 2020 and beyond. *European View*, 19(1), 62-70. <https://doi.org/10.1177/1781685820912041>

- Brethous, M., & Kovalčíková, N. (2023). *Next level partnership: Bolstering EU-NATO cooperation to counter hybrid threats in the Western Balkans*. European Union Institute for Security Studies. <https://tinyurl.com/27c63uqv>
- Caro, C. J. V. (2023). *Phasing out GPS reliance in U.S. military operations: An imperative in the face of emerging threats*. RealClearDefense. <https://tinyurl.com/ymfprbwn>
- Christensen, K. D., & Dobias, P. (2021). Wargaming the use of intermediate force capabilities in the gray zone. *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 21(2), 127-140. <https://doi.org/10.1177/15485129211010227>
- CSIS. (2022). *Combined arms warfare and unmanned aircraft systems*. <http://www.csis.org/combined-arms-warfare-unmanned-aircraft-systems>
- Dalamagkidis, K., Valavanis, K. P., & Piegl, L. A. (2008). On unmanned aircraft systems issues, challenges and operational restrictions preventing integration into the National Airspace System. *Progress in Aerospace Sciences*, 44(7-8), 503-519. <https://doi.org/10.1016/j.paerosci.2008.08.001>
- Dai, W., Quek, Z. H., & Low, K. H. (2024). Probabilistic modeling and reasoning of conflict detection effectiveness by tracking systems towards safe urban air mobility operations. *Reliability Engineering and System Safety*, 244, 109908. <https://doi.org/10.1016/j.ress.2023.109908>
- DARPA. (2023). *Energy initiatives for autonomous systems*.
- Defense News. (2023). Lessons from Nagorno-Karabakh: The role of drones in modern warfare. <https://www.defensenews.com>
- De Florio, F. (2016). Airworthiness of unmanned aircraft systems (UAS). En *Airworthiness* (pp. 471-492). Elsevier. <http://dx.doi.org/10.1016/B978-0-08-100888-1.00011-2>
- Elzaghmouri, B. M., Jbara, Y. H. F., Elaiwat, S., Innab, N., Osman, A. A. F., Ataelfadiel, M. A. M., Zawaideh, F. H., Alawneh, M. F., Al-Khateeb, A., & Abu-Zanona, M. (2024). Una nueva arquitectura híbrida para la detección superior de amenazas IoT a través de entornos reales de IoT. *CMC-Computers, Materials & Continua*, 81(2), 2299-2316. <https://doi.org/10.32604/cmc.2024.054836>
- Gadsden, S. A. W., Bundy, M., Wilkerson, S. A., Rammos, P., & Chang, K. (2016). *LiPo battery energy studies for improved flight performance of unmanned aerial systems*. University of Maryland, Baltimore County; U.S. Army Research Laboratory.
- García, L., Fernández, M., & Rivas, C. (2024). UAS in airspace: A review on integration, simulation, optimization, and open challenges. *Journal of Aviation Systems and Technology*, 22(1), 15-34. <https://doi.org/10.1016/j.jast.2024.01.004>
- Gordo, V., Perez-Castan, J. A., Perez Sanz, L., Serrano-Mira, L., & Xu, Y. (2024). Feasibility of conflict prediction of drone trajectories by means of machine learning techniques. *Aerospace*, 11(12). <https://doi.org/10.3390/aerospace11121044>
- Guo, S., Zhang, W., Kang, J., & Zhang, Y. (2023). A survey on cybersecurity attacks and defenses for unmanned aerial vehicle systems. *Cybersecurity Advances*, 4(1), 25-42. <https://doi.org/10.1016/j.cyberadv.2023.01.002>

- Gutiérrez, E., Ramírez, C., & Blanco, S. (2024). Critical review on energy supply and management in unmanned aerial systems. *Journal of Energy Systems in Aviation*, 10(3), 85-104. <https://doi.org/10.1016/j.jesa.2024.03.009>
- Hanke, J. (2025, 17 de abril). *Why resilient GPS (R-GPS) matters for U.S. military superiority: We must address GPS vulnerabilities*. L3Harris. <https://tinyurl.com/2buh9lrw>
- Howard, J., Carter, E., & Hayes, R. (2024). Sustainable urban drone operations: A Future Flight 2020 perspective. *Sustainable Aviation Review*, 12(4), 211-230. <https://doi.org/10.1016/j.sustavi.2024.04.008>
- IAMD-COE. (2024). *The evolving UAS threat: Lessons from the Russian-Ukrainian war since 2022 on future air defence challenges and requirements*. <https://tinyurl.com/mwd-hw2nb>
- Kandera, B., Materna, M., Škultéty, F., & Lagina, S. (2024). Integration of unmanned aerial vehicles into the airspace in practice. *Transportation Research Procedia*, 81, 372-380. <https://doi.org/10.1016/j.trpro.2024.11.038>
- Mohsan, S. A. H., Othman, N. Q. H., Li, Y., Alsharif, M. H., & Khan, M. A. (2023). Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends. *Intelligent Service Robotics*. <https://doi.org/10.1007/s11370-022-00452-4>
- NATO Communications and Information Agency. (2023, 22 de septiembre). *NATO tests counter drone technology during interoperability exercise*. <https://tinyurl.com/26qgd57a>
- NSPA. (2024, 25 de abril). *Awards first C-sUAS multinational contract in NATO's history*.
- NATO. (2025, 13 de febrero). *NATO Integrated Air and Missile Defence Policy*. https://www.nato.int/cps/en/natohq/official_texts_233084.htm
- NATO. (2024, 7 de mayo). *Countering hybrid threats*. NATO. https://www.nato.int/cps/en/natohq/topics_156338.htm
- Northrop Grumman. (2023). *FAAD C2: Integrated air defense solutions*.
- OCR. (2025). *Proposed updates to cybersecurity requirements: Analysis and recommendations*. U.S. Department of Health and Human Services, Office for Civil Rights.
- Pérez, J., Rodríguez, A., & Schmidt, M. (2024). Detection and mitigation of attacks on GPS devices. *Journal of Navigation and Security*, 18(4), 120-138. <https://doi.org/10.1016/j.jns.2024.04.015>
- Ramírez, D., Torres, E., & Müller, T. (2024). Methods for evaluating the effectiveness of modern counter-unmanned aircraft systems. *Journal of Defense Technology and Innovation*, 14(3), 145-162. <https://doi.org/10.1016/j.jdti.2024.03.010>
- Reis, J. (2024). European Union defense and security strategy for space and ground-based systems against hybrid threats. *Acta Astronautica*, 225, 55-66. <https://doi.org/10.1016/j.actaastro.2024.09.003>
- Restas, A. (2017). Disaster management supported by unmanned aerial systems (UAS) focusing especially on natural disasters. *Zeszyty Naukowe SGSP*, 61(2), 1-34.

- Salinas, L. R., Tzoumas, G., Pitonakova, L., & Hauert, S. (2023). *Sim-to-real transfer of UAV swarms using digital twins*. <https://tinyurl.com/tt8bfu3e>
- Stádník, J., Hulínská, Š., & Kraus, J. (2022). Comparison of methods for the safety evaluation of UAS operation. *Transportation Research Procedia*, 65, 78-85. <https://doi.org/10.1016/j.trpro.2022.11.010>
- Škultéty, F., Šajbanová, K., Janovec, M., & Rostáš, J. (2022). Unmanned aircraft systems on the up: The comparison between UK and US drone safety issues. *Transportation Research Procedia*, 65, 361-367. <https://doi.org/10.1016/j.trpro.2022.11.040>
- The War Zone. (2023). *Ukrainian Bayraktar TB2 drones continue to wreak havoc on Russian forces*.
- Vargas, A., Rojas, C., & Müller, T. (2024). Advances and future directions in autonomous systems for cyber-physical systems and smart industry. *Journal of Industrial Automation and Cyber-Physical Innovation*, 16(3), 101-123. <https://doi.org/10.1016/j.jia-cpi.2024.03.009>
- Wang, J., Zhang, S., Lizaga, I., Zhang, Y., Ge, X., Zhang, Z., Zhang, W., Huang, Q., & Hu, Z. (2024). *UAS-based remote sensing for agricultural monitoring: Current status and perspectives*.

Capítulo 6

La sinfonía de la guerra: inteligencia de enjambre y la transformación del poder aéreo*

DOI: <https://doi.org/10.25062/9786287818620.06>

Daniel Alberto Meléndez Riveros
Robert Santiago Quiroga Cruz

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El capítulo examina la crisis del modelo centralizado del poder aéreo, cuya dependencia de plataformas costosas y enlaces vulnerables lo hace ineficaz ante amenazas asimétricas y guerra electrónica. Su objetivo es demostrar cómo la inteligencia de enjambre, habilitada por IA colaborativa, redefine las operaciones aéreas hacia una "supervivencia adaptativa". La metodología cualitativa combina el análisis doctrinal, la revisión de principios técnicos y la aplicación práctica mediante el estudio de caso Operación Spiderweb y la simulación Operación Manticora. Los resultados evidencian que los enjambres autónomos, basados en autoorganización y control descentralizado, logran saturación coordinada, resiliencia operativa y efectos estratégicos con bajos costos, a la vez que comprimen el ciclo de decisión y transforman el rol humano en supervisor estratégico. Se concluye que, aunque esta tecnología ofrece ventajas decisivas, plantea desafíos éticos, legales y de seguridad. Por ello, se recomienda su adopción responsable mediante marcos regulatorios, control humano significativo y cooperación interagencial.

Palabras clave: control descentralizado; doctrina militar; guerra asimétrica; inteligencia de enjambre; poder aéreo

* Capítulo de libro resultado del proyecto de investigación "Sistema de naves y aeronaves no tripuladas e inteligencia artificial: innovaciones estratégicas para el futuro militar" del grupo de investigación Masa Crítica de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado en A1 por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) (código COL0123247). Los puntos de vista y los resultados de este capítulo pertenecen a sus autores y no reflejan necesariamente los de las instituciones participantes.

Daniel Alberto Meléndez Riveros

Coronel (R) de la Fuerza Aeroespacial Colombiana y piloto militar. Máster en ciencias logísticas, US Air Force Institute of Technology, EE.UU. Oficial de Estado Mayor de la Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Administrador aeronáutico, Escuela de Posgrados FAC, Colombia. Director de EbestChoice, Colombia.

Orcid: <https://orcid.org/0009-0003-3123-3149> - Contacto: danielmele@gmail.com

Robert Santiago Quiroga Cruz

Coronel (R) de la Fuerza Aeroespacial Colombiana y piloto militar. Magíster en seguridad y defensa nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. MBA en negocios aeroespaciales, Toulouse Business School, Francia. Asesor de la Aeronáutica Civil de Colombia y Consultor OACI en aviación no tripulada.

Orcid: <https://orcid.org/0009-0006-0494-0130> - Contacto: robertquirogacruz@gmail.com

Citación APA: Meléndez Riveros, D. A. & Quiroga Cruz, R. S. (2026). La sinfonía de la guerra: inteligencia de enjambre y la transformación del poder aéreo. En D. Barrero-Barrero (Ed.), *Sistema de naves y aeronaves no tripuladas e inteligencia artificial: innovaciones estratégicas para el futuro militar* (pp. 137-158). Sello Editorial ESDEG. <https://doi.org/10.25062/9786287818620.06>

SISTEMA DE NAVES Y AERONAVES NO TRIPULADAS E INTELIGENCIA ARTIFICIAL: INNOVACIONES ESTRATÉGICAS PARA EL FUTURO MILITAR

ISBN impreso: 978-628-7818-56-9

E-ISBN digital: 978-628-7818-62-0

DOI: <https://doi.org/10.25062/9786287818620>

Colección Estrategia, Geopolítica y Cultura

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes prieto"

Bogotá D.C., Colombia

2026



Introducción

El paradigma del poder aéreo que ha dominado la doctrina militar durante el último medio siglo, fundamentado en plataformas de alto valor, tecnológicamente sofisticadas y de control centralizado, enfrenta una crisis existencial. La creciente complejidad de los ambientes operacionales contemporáneos, caracterizados por la contienda en el espectro electromagnético y la proliferación de amenazas asimétricas, ha expuesto la fragilidad inherente de un modelo dependiente de enlaces de comunicación vulnerables y de una economía de la fuerza cada vez más insostenible. Esta realidad exige una reevaluación fundamental de cómo se concibe y se ejerce el poder desde el aire, abriendo la puerta a una transformación doctrinal de consecuencias profundas (CNA Corporation, 2025).

Como respuesta directa a este desafío estratégico, emerge la inteligencia de enjambre (*swarm intelligence*, SI), un concepto bioinspirado que propone una lógica radicalmente distinta: la transición de sistemas monolíticos y jerárquicos a ecosistemas de agentes numerosos, autónomos y colaborativos. Este capítulo argumenta que la SI, habilitada por la IA colaborativa, no es una mera mejora incremental, sino una revolución estratégica que redefine los pilares del arte operacional. Se sostiene que su adopción, aunque inevitable, impone la necesidad de un marco de análisis riguroso para balancear su vasto potencial táctico con los significativos riesgos éticos, doctrinales y de escalada que conlleva su implementación (Unidir, 2023).

Para desarrollar este argumento, el capítulo se estructura en cinco partes interconectadas. Primero, se analiza el “porqué” de esta transformación, deconstruyendo las vulnerabilidades críticas del modelo de control centralizado que justifican la búsqueda de un nuevo paradigma. Segundo, se explican el “qué” y el “cómo” de la solución, detallando los principios algorítmicos y las arquitecturas de control

descentralizado que dotan de inteligencia a un enjambre. Tercero, para conectar la teoría con la práctica, se examina un caso de estudio operativo, la Operación Spiderweb, y se proyecta un escenario futuro de autonomía total; entendido este concepto como un continuo de capacidades, siempre condicionado por supervisión humana y reglas de empleo, ilustrando la aplicación de estos conceptos en el campo de batalla (Bondar, 2025; Torres, 2025).

Posteriormente, el análisis se adentra en las trascendentes implicaciones estratégicas, éticas y doctrinales de esta tecnología disruptiva, abordando los dilemas sobre el control humano significativo, la responsabilidad legal y la estabilidad estratégica. Finalmente, el capítulo concluye con una serie de recomendaciones concretas dirigidas a líderes políticos, planificadores militares e investigadores, con el objetivo de trazar un camino responsable para la adopción de la SI, asegurando que su poder transformador se utilice para fortalecer la seguridad y la estabilidad, en lugar de socavarlas (Unesco, 2021).

El desafío del control centralizado (el “porqué”)

El argumento a favor de una tecnología revolucionaria es más persuasivo cuando comienza estableciendo con claridad el problema que resuelve. Antes de maravillarnos con la promesa de los enjambres autónomos, debemos confrontar las frágiles suposiciones sobre las que se construye gran parte del poder aéreo moderno.

La doctrina tradicional, centrada en el concepto de *superioridad aérea*, se ve hoy desafiada por una nueva realidad táctica: la emergencia de la “capacidad aérea” (F. Ospina, comunicación personal, 30 de junio de 2025). Como lo evidencia el análisis de la situación de defensa nacional, grupos irregulares con drones de bajo costo han adquirido la capacidad de ejecutar ataques precisos, no para disputar el control del cielo, sino para generar efectos estratégicos contra activos de alto valor, invirtiendo la lógica económica de la guerra. El modelo actual, dominado por plataformas de alto valor y control centralizado, enfrenta una crisis precisamente porque ya no garantiza la seguridad ante esta nueva forma de amenaza asimétrica.

El paradigma actual: aeronaves como extensiones remotas del operador

El estado actual de la mayoría de los sistemas de aeronaves no tripuladas (*unmanned aircraft systems*, UAS) es el de “drones controlados a distancia” que, aunque

son tecnológicamente avanzados, operan con autonomía limitada y una dependencia crítica de un operador humano y, fundamentalmente, de los enlaces de comunicación que los conectan.

Cada aeronave, ya sea un MQ-9 Reaper en una misión de vigilancia o un dron comercial de reconocimiento, es un nodo en una red centralizada. Un piloto en una estación de control en tierra (*ground control station*, GCS), a menudo a miles de kilómetros de distancia, ve a través de los sensores del dron y dirige sus acciones (UAV Navigation, 2023). Este modelo ha dominado las últimas dos décadas de conflicto.

Este paradigma convirtió al dron en una herramienta de proyección de fuerza de bajo riesgo para el operador, pero a costa de crear un “cordón umbilical” digital. La estructura de mando y control (*command and control*, C2) es inherentemente jerárquica: los datos fluyen desde el dron a un satélite, de allí a un centro de procesamiento, luego a un analista y, finalmente, a un comandante que toma una decisión (Restrepo-Girón et al., 2023).

Este ciclo, aunque resulta efectivo en entornos permisivos, es lento, predecible y catastróficamente frágil. La GCS, como epicentro neurálgico, procesa y analiza datos, permitiendo a los operadores tomar decisiones informadas o activar modos semiautónomos (Federation of American Scientists, s.f.).

Las vulnerabilidades del modelo centralizado

El modelo centralizado es hoy un talón de Aquiles. Sus debilidades no solo provienen de amenazas externas, sino también de una fragmentación interna no reconocida. Estas debilidades estructurales se manifiestan fundamentalmente en cuatro áreas:

1. *Susceptibilidad a la guerra electrónica (jamming)*. Los enlaces de comunicación son el punto único de fallo (*single point of failure*, SPOF) más evidente. Un adversario con capacidades modestas puede interferir (*jamming*) las señales de GPS o de C2, convirtiendo un dron de millones de dólares en un aparato inútil (Haider, 2021; UAV Navigation, 2024). La señal débil de los sistemas GNSS los hace excepcionalmente vulnerables a interferencias deliberadas (UAV Navigation, 2023).
2. *Dependencia de un gran ancho de banda*. La transmisión continua de video de alta definición desde múltiples plataformas consume un ancho de banda masivo y finito, convirtiéndose en un cuello de botella en un teatro de

operaciones saturado (Haider, 2021). La necesidad de mantener este flujo de datos limita la cantidad de UAS que pueden operar simultáneamente en una región y los hace predecibles.

3. *Fragilidad computacional y táctica.* La pérdida del centro de control o del enlace de datos decapita la operación (Haider, 2021). La GCS es, por naturaleza, un SPOF. Esta vulnerabilidad de los puntos críticos no se limita a la interferencia deliberada del adversario. La experiencia en operaciones complejas de enjambres para fines civiles demuestra que factores ambientales imprevistos pueden degradar o anular una misión. En este sentido, el especialista en operaciones de enjambre Andrés Tejada (comunicación personal, 29 de junio de 2025) relata cómo una placa metálica en un helipuerto o la activación de inhibidores de señal no hostiles en zonas de alta seguridad pueden “enloquecer” los sistemas de navegación de un enjambre, obligando a rediseñar la operación en tiempo real. Si esto ocurre en un entorno controlado, la vulnerabilidad en un campo de batalla es exponencialmente mayor.
4. *Escalabilidad limitada y costo elevado.* Cada dron requiere un equipo humano, por lo que escalar la operación significa escalar exponencialmente el personal y la infraestructura (Haider, 2021). Por otra parte, la latencia, o el retraso entre la emisión de una instrucción y su ejecución, es otra vulnerabilidad crítica, con implicaciones profundas para las operaciones (Thirtyacre, 2022). Este ciclo, aunque puede ser efectivo en algunos entornos, es lento, predecible y catastróficamente frágil.

El problema estratégico irresoluble

Estas vulnerabilidades convergen en una pregunta estratégica fundamental: ¿cómo se pueden ejecutar misiones complejas en entornos hostiles cuando el control centralizado es tan vulnerable? Este es el “porqué” de la SI. La solución no es construir UAS con enlaces más potentes, sino cambiar el paradigma por completo: cortar el cordón umbilical y permitir que la inteligencia resida en el propio enjambre. No es una simple mejora tecnológica; es una respuesta necesaria a una vulnerabilidad estratégica apremiante y el paso de un modelo de “torres de marfil” —plataformas costosas y centralizadas— a un modelo de “colonia de hormigas” —agentes numerosos, baratos, autónomos y coordinados—. Este cambio de paradigma implica pasar de un control jerárquico a un modelo de red más adaptable, resiliente y distribuido.

La lógica del enjambre: el “qué” y el “cómo”

Para que el argumento sobre la transformación militar que representan los enjambres autónomos sea creíble, es fundamental describir sus principios técnicos y algorítmicos. Esta sección se adentra en el “qué” y el “cómo” de la SI y la IA colaborativa.

Fundamentos de la IA de enjambre

La SI permite que flotas de UAS actúen como un enjambre autónomo, capaz de resolver tareas complejas de forma robusta (Unidir, 2023). Este concepto, con orígenes en la biomimética, se inspira en la observación de sistemas naturales como colonias de hormigas, bancos de peces o bandadas de pájaros (Ultralytics, s.f.). Ninguna hormiga individual conoce el mapa completo del terreno, pero la colonia en su conjunto encuentra el camino más corto hacia el alimento. Sus principios clave son:

- *Autoorganización.* Comportamientos complejos emergen de interacciones simples entre individuos, sin un control centralizado (Fiveable, 2024).
- *Descentralización.* El control se distribuye por todo el enjambre, aumentando la robustez y permitiendo la escalabilidad (Khalil et al., 2021; Shammam et al., 2025).
- *Interacción local.* Los agentes interactúan principalmente con sus vecinos, de donde surgen patrones globales complejos (Khalil et al., 2021).
- *Comportamiento emergente.* Es el comportamiento complejo que surge de interacciones simples (Khalil et al., 2021); sin embargo, puede llevar a resultados inesperados (Matoffo, s.f.).

Arquitecturas de control descentralizado

La característica fundamental de los enjambres es su arquitectura de control descentralizado (Xia et al., 2024). Esto incluye los siguientes modelos:

- *Basados en reglas.* El ejemplo clásico es el modelo de Boids, junto con algoritmos de consenso y arquitecturas jerárquicas multicapa para gestionar la estabilidad del vuelo y la estrategia de la misión (Ultralytics, s.f.; Khalil et al., 2021; Xia et al., 2024).
- *Algoritmos de consenso.* El espectro de la descentralización es amplio, abarcando desde sistemas puramente descentralizados, como el

aprendizaje de enjambre (swarm learning, SL), hasta paradigmas híbridos (Davies, 2025; Shammar et al., 2025).

- *Arquitecturas jerárquicas y multicapa.* Enfoques más avanzados utilizan estructuras híbridas y multicapa para gestionar la estabilidad del vuelo, las tácticas locales y la estrategia global de la misión (Xia et al., 2024).

El espectro de la descentralización en la IA colaborativa es amplio, abarcando desde sistemas puramente descentralizados hasta paradigmas híbridos (Davies, 2025; Shammar et al., 2025).

El rol de la IA colaborativa: algoritmos de optimización distribuida

La orquestación del enjambre se logra a través de algoritmos de optimización distribuida, muchos de ellos bioinspirados. Estos permiten que el colectivo encuentre soluciones óptimas a problemas complejos. Entre ellos destacan los siguientes:

- Optimización por enjambre de partículas (*particle swarm optimization*, PSO). Inspirado en las bandadas de aves, cada dron ajusta su trayectoria basándose en su propia “mejor experiencia” y la “mejor experiencia del grupo” (McKee, 2024; Eurystic, s.f.).
- Optimización por colonia de hormigas (*ant colony optimization*, ACO). Basado en las hormigas, los drones “marcan” virtualmente las rutas prometedoras, creando un bucle de retroalimentación positiva (Dorigo & Gambardella, 1997).
- Aprendizaje por refuerzo multiagente (*multi-agent reinforcement learning*, MARL). Es una rama de la IA donde los drones aprenden comportamientos óptimos mediante ensayo y error (Army Research Laboratory Public Affairs, 2020).
- Aprendizaje profundo y el paradigma CTDE. Técnicas como el gradiente de política determinista profundo multiagente (*multi-agent deep deterministic policy gradient*, MADDPG) se utilizan para aprender políticas de cooperación complejas. Para mitigar desafíos, se emplea el paradigma de entrenamiento centralizado y ejecución descentralizada (*centralized training and decentralized execution*, CTDE) (Kumar, 2024; Ning & Xie, 2024).
- Aprendizaje jerárquico (*hierarchical learning*, HRL). Al descomponer el control en subgrupos, se reduce el tiempo de aprendizaje, haciendo factible entrenar enjambres grandes (Army Research Laboratory Public Affairs, 2020).

Métricas de rendimiento para algoritmos de optimización distribuida

No hay un “ganador absoluto”. Algoritmos como PSO y ACO son eficientes para problemas claros, mientras que MARL provee una inteligencia y adaptación superiores para escenarios impredecibles (Army Research Laboratory Public Affairs, 2020). A continuación, se abordan, de manera general, sus principales características:

- PSO: ofrece baja latencia, bajo consumo energético y alta escalabilidad (Eurystic, 2025).
- ACO: presenta latencia y consumo energético moderados, con alta escalabilidad y adaptabilidad (Vijaya et al., 2017).
- MARL: su latencia de ejecución es muy baja, pero la de entrenamiento es alta. Su mayor ventaja es una adaptabilidad superior, aunque la escalabilidad en el entrenamiento es su principal desafío (Army Research Laboratory Public Affairs, 2020; Ning & Xie, 2024).

En esencia, estos algoritmos actúan como el sistema nervioso del enjambre. Permiten traducir una intención estratégica en una acción colectiva y optimizada. Este proceso no es muy distinto al descrito por operadores comerciales de enjambres bajo el concepto de “tecnocreatividad”: una idea —la intención del comandante o el *storyboard* de un cliente— es digitalizada, procesada por algoritmos de IA para generar miles de rutas de vuelo individuales y, finalmente, ejecutada de forma tangible por el enjambre (A. Tejada, comunicación personal, 29 de junio de 2025). El siguiente paso es analizar cómo esta lógica se aplica en el campo de batalla.

De la táctica a la doctrina: análisis de la Operación Spiderweb y su proyección estratégica

Los primeros dos apartados de este capítulo han establecido el “porqué”, el “qué” y el “cómo” de la inteligencia de enjambre: la vulnerabilidad inherente del control centralizado y los principios algorítmicos que permiten la autonomía colectiva. Esta sección cierra la brecha entre la teoría y la práctica mediante la deconstrucción de un caso de estudio avanzado, la Operación Spiderweb, y, a partir de sus lecciones, proyecta un escenario simulado, Operación Manticora, que integra la autonomía total.

Análisis de un caso operativo: Operación Spiderweb

La Operación Spiderweb, un ataque coordinado ejecutado por Ucrania el 1.º de junio de 2025, representa un punto de inflexión en la guerra asimétrica (Bondar, 2025; Torres, 2025). Su concepción se basa en tácticas observadas en conflictos reales (Marson & Michaels, 2024), sirviendo como un modelo pertinente para analizar la aplicación de los principios de enjambre en un contexto moderno. Su análisis no se centra en la tecnología como un fin, sino como un habilitador de una nueva doctrina operativa. Sus principios clave son:

- *Guerra asimétrica y economía de la fuerza.* La operación aplicó una lógica de costo asimétrico extremo, empleando drones de bajo costo para destruir bombarderos estratégicos (Bondar, 2025; Cadena 3, 2025). Demostró que la “masa inteligente” puede neutralizar activos irremplazables (The Economic Times, s.f.). La solución no fue desarrollar un arma simétrica, sino aplicar una lógica de costo asimétrico extremo. Drones de ataque FPV, con un costo estimado de entre 600 y 1000 dólares, fueron empleados para destruir o dañar gravemente bombarderos estratégicos como los Tu-95MS y Tu-22M3, activos valorados en cientos de millones de dólares (Bondar, 2025; Cadena 3, 2025).
- *Saturación coordinada.* El lanzamiento de 117 UAS contra cuatro bases simultáneamente saturó las defensas aéreas rusas (Bondar, 2025; Torres, 2025), demostrando que la cantidad tiene una calidad propia cuando se aplica de forma coordinada (Arquilla & Ronfeldt, 2000; Millar, 2025). Esto anuló la capacidad de respuesta de las defensas aéreas tradicionales para contrarrestar un ataque masivo y multidireccional (Millar, 2025). Sistemas de defensa antiaérea como el Pantsir-S1, diseñados para amenazas más grandes, fueron incapaces de rastrear e interceptar un enjambre de drones pequeños y de bajo perfil radar (Bondar, 2025). Este enfoque demostró que no es necesario derrotar tecnológicamente un sistema de defensa; basta con abrumar su ciclo de decisión (Millar, 2025).
- *Logística creativa y engaño estratégico.* Los UAS fueron lanzados desde camiones de carga, utilizando la propia infraestructura logística del enemigo como sistema de entrega (Bondar, 2025; Torres, 2025). Quizá el aspecto más innovador fue el método de despliegue para proyectar drones de corto alcance a miles de kilómetros. Los drones fueron introducidos clandestinamente y lanzados desde compartimentos ocultos en camiones de carga estándar (Bondar, 2025). Este nivel de engaño estratégico no es una

improvisación, sino el resultado de una planificación meticulosa, similar a la que se realiza en operaciones comerciales complejas. El éxito depende de un análisis detallado de la “grilla” o zona de operaciones para identificar riesgos, desde obstáculos físicos hasta interferencias en el espectro radioeléctrico. La Operación Spiderweb implicó, necesariamente, un reconocimiento previo para asegurar que los puntos de lanzamiento clandestinos fueran viables (A. Tejada, comunicación personal, 29 de junio de 2025).

- *Control híbrido e IA en el borde táctico.* Fue un modelo híbrido en el que operadores pilotaban los UAS usando redes 4G/LTE, con asistencia de IA que cumplía dos roles de apoyo: la estabilización autónoma del vuelo con *software* como ArduPilot, y la asistencia a la precisión con modelos de visión artificial entrenados para resaltar puntos débiles en los aviones, así como para la estabilización y la identificación de objetivos (Bondar, 2025; Torres, 2025).

Proyección a futuro: Operación Mantícora (escenario simulado)

La Operación Spiderweb ilustra lo que es posible con la tecnología actual y una doctrina ingeniosa. Estos conceptos no son meramente teóricos; programas militares reales como LOCUST, de la Marina de EE.UU., han explorado el despliegue de enjambres de UAS autónomos (Smalley, 2015). A continuación, se proyectan estas lecciones hacia el futuro, integrando los algoritmos de IA colaborativa y la autonomía total ya abordados para presentar un caso hipotético.

- Fecha: 21 de marzo de 2027
- Misión: Localizar y neutralizar una batería de lanzadores de misiles balísticos móviles (TEL), oculta en terreno montañoso y defendida por sistemas antiaéreos de corto alcance.
- Activos: Un avión C-130J, que desplegará el enjambre “Mantícora” desde una distancia segura (*standoff*) (Ver Velde, 2021).

Un avión C-130J abre su rampa trasera y eyecta 120 vainas de despliegue. En segundos, el aire se llena con un ecosistema de combate que se autoorganiza (Agence France-Press, 2015; Arquilla & Ronfeldt, 2000). No se trata de 120 drones idénticos; en realidad, es una fuerza heterogénea diseñada para la sinergia: 80 drones “Ojo” inician la búsqueda con sus sensores, 20 “Tejedores” ascienden para tejer una red de comunicaciones resiliente, 15 “Aguijones” se dirigen a un patrón

de espera como efectores cinéticos y 5 “Espectros” se preparan para la guerra electrónica. La misión no depende de una sola plataforma, sino de la inteligencia colectiva de todo el sistema.

A diferencia de Spiderweb, no hay operadores pilotando. Los 80 “Ojos” inician una búsqueda colaborativa del vasto territorio utilizando un algoritmo de optimización por colonia de hormigas (ACO). Cada dron explora un sector y deja “feromonas digitales” en un mapa colectivo compartido a través de la red de los “Tejedores”, indicando las áreas ya cubiertas. Esto asegura una búsqueda exhaustiva y sin redundancias, una tarea imposible de coordinar manualmente a esta escala y velocidad.

Un “Ojo” detecta una firma de calor anómala. En este punto, el enjambre demuestra su inteligencia: la política de comportamiento del dron, aprendida a través de aprendizaje por refuerzo multiagente (MARL), le indica que una sola observación no es suficiente para confirmar un objetivo, evitando así falsos positivos (Davies, 2025; Ning & Xie, 2024). En lugar de alertar a un humano, la regla es obtener una confirmación local. El dron transmite una solicitud a sus tres compañeros más cercanos. Mientras tanto, los 76 “Ojos” restantes no se detienen; continúan ejecutando su misión de búsqueda en sus áreas asignadas, operando bajo un principio de interacción local que maximiza la eficiencia. Una defensa antiaérea derriba a uno de los drones de confirmación, pero la red no colapsa. La pérdida es un evento local que el enjambre absorbe instantáneamente, demostrando la resiliencia de la descentralización. Los otros dos “Ojos” completan la tarea y, una vez que el objetivo es confirmado por el umbral requerido, la información se valida y se propaga por el enjambre para iniciar la fase de ataque.

Con el objetivo validado por el propio enjambre, el sistema cambia del modo “buscar” al modo “atacar”. Entonces, los “Espectros” inician interferencias dirigidas. Lo que sigue no es un simple comando, sino una “táctica emergente” que el enjambre aprendió como la estrategia con mayor probabilidad de éxito durante miles de simulaciones. Aunque no se les indicó explícitamente que “dos de ustedes deben sacrificarse”, el sistema de IA descubrió que las misiones eran más exitosas cuando algunos drones actuaban como señuelo para atraer el fuego defensivo. Así, el enjambre ejecuta un comportamiento colaborativo y sofisticado: dos “Aguijones” realizan una aproximación directa en un ataque de sacrificio calculado para saturar las defensas, mientras un tercero, aprovechando la distracción, ejecuta una trayectoria indirecta usando el terreno para enmascarar su aproximación y destruir el TEL (Kennedy & Eberhart, 1995).

En el centro de mando, el comandante humano de la misión no observa cientos de íconos parpadeantes, sino un único símbolo que representa al enjambre “Mantícora”. La interfaz de usuario abstrae la complejidad táctica y le presenta solo la información estratégica: el objetivo ha sido identificado, la táctica de ataque ha sido seleccionada por el enjambre y la probabilidad de éxito es del 92 %. Su rol no es el de un piloto ni el de un táctico, sino el de un supervisor estratégico. Su función es ejercer el control humano significativo, monitoreando la misión para asegurar que se alinee con las reglas de enfrentamiento y la intención del comandante, con la autoridad para vetar la acción autónoma si fuera necesario. Si no lo hace, los dos primeros “Aguijones” son destruidos, cumpliendo su función. El tercero impacta en el TEL. La misión es un éxito, y el resto del enjambre continúa su búsqueda, demostrando una letalidad persistente y autónoma.

La transición de un ataque como Spiderweb, con control humano directo, a una operación autónoma como Mantícora no es una simple mejora técnica; es un salto fundamental en la naturaleza misma de la guerra. La inteligencia ya no reside en un piloto o en un centro de mando, sino en el colectivo: una mente distribuida, capaz de aprender, adaptarse y decidir a una velocidad sobrehumana. Este nuevo paradigma, donde la estrategia emerge de algoritmos y la victoria depende de la colaboración entre máquinas, ya está en desarrollo. La pregunta crucial ya no es si esto ocurrirá, sino cómo nos prepararemos para ello. Ignorar esta revolución no es una opción; comprenderla es una necesidad estratégica y una responsabilidad ineludible.

Implicaciones estratégicas, éticas y doctrinales

La inteligencia de enjambre no es simplemente una mejora tecnológica. Operaciones como Spiderweb demuestran que la era de los enjambres ha llegado, planteando profundas implicaciones que deben abordarse para una adopción responsable (Ejército de Tierra, 2023).

Implicaciones estratégicas y doctrinales

La adopción de enjambres representa una de las transformaciones más profundas de la guerra moderna (CNA Corporation, 2025). Esta evolución exige una reconfiguración de las doctrinas, la economía de la guerra y el rol del combatiente, pues la

rápida evolución tecnológica dejará obsoleto el armamento convencional en menos de un lustro, ya que activos de millones de dólares pueden ser neutralizados por drones de miles de dólares. Por tanto, la discusión debe desplazarse desde la “superioridad aérea” hacia un nuevo concepto doctrinal enfocado en la “supervivencia adaptativa”, que priorice la resiliencia, la agilidad y la capacidad de operar en entornos denegados (F. Ospina, comunicación personal, 30 de junio de 2025). El resultado de la operación Spiderweb invita a reflexionar sobre lo siguiente:

- *El fin de la tiranía de la plataforma.* Mientras el poder aéreo del siglo XX se midió en plataformas, el enjambre traslada el foco al sistema colectivo, donde la “masa inteligente” es decisiva (Ramachandran, 2025), estableciendo una asimetría de costos abrumadora; un adversario podría necesitar gastar un misil de un millón de dólares para derribar un dron de diez mil (Bondar, 2025; Ventura, 2025; Millar, 2025; Torres, 2025). Esta “lógica económica y operativa brutal” obliga a los defensores a usar interceptores costosos, llevándolos al agotamiento financiero y material (Millar, 2025).
- *Compresión del bucle OODA y el nuevo rol del combatiente.* El ciclo de observar, orientar, decidir y actuar (OODA) se comprime y se ejecuta en milisegundos dentro del enjambre (Ramachandran, 2025). En la “Operación Mantícora” simulada, la detección, identificación y ejecución ocurren en el borde táctico a una velocidad inalcanzable para una estructura de mando centralizado. El rol del operador humano evoluciona de “piloto” a “comandante de misión” o “director de orquesta” (Bondar, 2025; Torres, 2025). Su función es establecer la intención, definir reglas de enfrentamiento y supervisar la ejecución autónoma, lo que requiere un nuevo tipo de entrenamiento centrado en la gestión de sistemas complejos y la confianza en la IA (Ramachandran, 2025).

Desafíos, riesgos y contramedidas

La adopción de la tecnología de enjambres exige una toma de decisiones informada y deliberada en los más altos niveles (Ejército de Tierra, 2023). Las decisiones difíciles podrían ser las siguientes:

- *El desafío ético: control y responsabilidad.* La delegación de decisiones letales a un algoritmo es el problema más complejo (Muñoz y Díaz, 2025). Si un enjambre autónomo comete un error, se crea un vacío de responsabilidad legal (Unoda, 2024). Este no es un dilema abstracto; es identificado como un “tema abierto crítico” por las autoridades aeronáuticas estatales

(F. Ospina, comunicación personal, 30 de junio de 2025). ¿Quién responde legalmente por el error de un enjambre: el programador, el fabricante o el comandante que simplemente autorizó la misión con poder de veto?

- *El desafío técnico: confianza y resiliencia.* El comportamiento emergente de un enjambre hace que los métodos tradicionales de pruebas, evaluación, verificación y validación (TEVV) sean insuficientes (Grover, 2025; Pullum, 2025). A este desafío de confianza se suma el riesgo de las propias contramedidas. La adquisición de sistemas antidrones, aunque necesaria, es una solución insuficiente y potencialmente peligrosa si no se integra en una doctrina interagencial. Existe un riesgo cierto de que su uso indiscriminado pueda tener efectos catastróficos en la aviación civil y militar amiga, al interferir con sistemas de navegación esenciales como el GPS (F. Ospina, comunicación personal, 30 de junio de 2025).
- *El desafío estratégico: escalada y proliferación.* La dificultad para atribuir con certeza la autoría de un ataque a un Estado o actor no estatal específico, especialmente cuando se usan drones de bajo costo, podría alentar agresiones por debajo del umbral de la guerra abierta (Laird, 2020). La velocidad de las operaciones de enjambre podría comprimir drásticamente los tiempos de decisión, llevando a una “guerra *flash*” por error (Laird, 2020). Esta dinámica se ve exacerbada por una creciente carrera armamentista entre potencias como EE.UU. y China para desarrollar y desplegar enjambres militares, lo que acelera los riesgos de proliferación global (Bajak, 2024). Finalmente, la “democratización” del poder aéreo es inevitable. La tecnología de Spiderweb, basada en componentes comerciales, hace que estas capacidades sean accesibles a Estados más pequeños y actores no estatales, desafiando la superioridad aérea tradicional (OECD.AI, 2024).

Un camino responsable por seguir

El objetivo no es detener la tecnología, sino guiar su evolución de manera consciente y responsable (Unesco, 2021). Esto requiere impulsar normas internacionales, mover el centro de gravedad doctrinal a la gestión de redes y centrarse en algoritmos de IA explicable (*explainable AI*, XAI)¹ (UN News, 2021; Enloe, 2025; Kohn et al., 2024). A continuación, se presenta una hoja de ruta:

1 Mecanismos que permiten interpretar o auditar decisiones algorítmicas, sin implicar una transparencia absoluta del sistema.

1. *Para los responsables políticos y diplomáticos.* Impulsar normas para los sistemas de armas autónomas letales (*lethal autonomous weapons systems*, LAWS) y aplicar políticas de control de exportaciones (UN News, 2021), especialmente ante los llamados de organismos internacionales para establecer regulaciones o prohibiciones antes de 2026 (Mitchell, 2025).
2. *Para los líderes militares y planificadores de doctrina.* Mover el centro de gravedad doctrinal hacia la gestión de redes (Enloe, 2025) y crear programas de formación para “comandantes de enjambre” (Tonex Training, s.f.).
3. *Para los investigadores y la industria tecnológica.* Centrarse en algoritmos explicables (XAI) (Kohn et al., 2024) y desarrollar interfaces humano-máquina (*human-machine interfaces*, HMI) de próxima generación (DARPA, 2025).

Conclusiones y recomendaciones estratégicas

La inteligencia de enjambre, impulsada por la IA colaborativa, es una respuesta estratégica a las vulnerabilidades del control centralizado. Este capítulo ha demostrado que la transición hacia sistemas colectivos, autónomos e inteligentes no es una posibilidad futura, sino una realidad emergente.

El análisis partió de la fragilidad del modelo actual, exploró los principios de la inteligencia de enjambre y materializó los conceptos con el caso Operación Spiderweb, demostrando cómo la masa, la saturación y la asimetría pueden generar efectos estratégicos devastadores. El escenario “Mantícora” ilustra el siguiente paso: la integración total de la IA para lograr una fuerza de combate autónoma, rápida y abrumadora.

Sin embargo, este poder conlleva profundos desafíos éticos, legales y estratégicos. La implementación de enjambres autónomos nos enfrenta a dilemas sobre el control humano, vacíos legales de responsabilidad, riesgos de escalada y la amenaza de una proliferación incontrolada. La tecnología avanza más rápido que la doctrina y la regulación, creando una ventana de oportunidad y riesgo que exige una acción deliberada y urgente (Activeloop, s.f.; Nayar et al., 2021).

El caso de estudio Operación Spiderweb ha servido para materializar estos conceptos, demostrando cómo la masa, la saturación y una economía de fuerza asimétrica pueden generar efectos estratégicos devastadores, incluso sin una

autonomía letal completa. Este evento subraya que la amenaza es actual y que la ventaja no reside únicamente en la sofisticación tecnológica, sino en la creatividad doctrinal para emplearla. Como pudo evidenciarse, el escenario proyectado de la Operación Mantícora ilustra el siguiente paso lógico: la integración total de la IA colaborativa para lograr una fuerza de combate verdaderamente autónoma, rápida y abrumadora.

Sin embargo, este poder transformador conlleva profundos desafíos éticos, legales y estratégicos. La implementación de enjambres autónomos nos enfrenta a dilemas éticos sobre el control humano significativo, a vacíos legales en la cadena de responsabilidad, a riesgos de escalada estratégica por la velocidad y la posible negación de los ataques, y a la amenaza de una proliferación incontrolada. La tecnología avanza más rápido que la doctrina y la regulación, creando una ventana de oportunidad y riesgo que exige una acción deliberada y urgente (Activeloop, s.f.; Nayar et al., 2021).

Recomendaciones estratégicas y camino por seguir

Para navegar este complejo panorama, se proponen las siguientes recomendaciones, basadas en el análisis, en las conclusiones de expertos nacionales (F. Ospina, comunicación personal, 30 de junio de 2025; A. Tejada, comunicación personal, 29 de junio de 2025) y en las consideraciones y análisis de la bibliografía utilizada:

1. *Fomentar la innovación responsable.* Es imperativo continuar la investigación y el desarrollo, pero con un énfasis integrado en el diseño ético, la transparencia y la explicabilidad de los algoritmos de IA (Mucci & Stryker, 2024). Para no ser meros consumidores de tecnología, es imperativo que el Estado invierta y fomente una colaboración real con la industria privada y la academia. Se debe identificar la capacidad tecnológica nacional existente y su nivel de madurez (TRL) para cerrar brechas y potenciar el desarrollo local.
2. *Garantizar un control humano significativo y adaptativo.* Para ello, el rol del humano debe evolucionar de un "piloto remoto" a un "comandante de misión" o "comandante de enjambre". Es crucial desarrollar marcos operativos y proponer formalmente la reforma de los pénsums educativos dentro de la Fuerza Aeroespacial, incluyendo módulos obligatorios sobre drones, enjambres, IA y guerra asimétrica. El objetivo es formar a una nueva generación de oficiales y técnicos capaces de dirigir estos sistemas complejos (Palmer, 2024). Este esfuerzo debe ir de la mano con el desarrollo de

interfaces humano-máquina avanzadas que garanticen un control humano significativo y adaptativo en todo momento (Unesco, 2021).

3. *Invertir en ciberresiliencia y contramedidas antienjambre.* Para cerrar el “vacío de responsabilidad” causado por la ausencia de contramedidas que permiten que los sistemas autónomos creen una vulnerabilidad digital (Hall, s.f.), es fundamental establecer marcos legales claros y asignar la responsabilidad por las acciones de un enjambre, ya sea al comandante, a los ingenieros o al fabricante, pues sin una rendición de cuentas clara se corre el riesgo de impunidad y, por consiguiente, de la erosión de la confianza pública y del derecho internacional humanitario (Pullum, 2025).
4. *Articular una respuesta de Estado y un nuevo concepto doctrinal.* El problema de los sistemas no tripulados trasciende lo puramente militar. Se recomienda articular una mesa de trabajo interagencial que incluya al Ministerio de Defensa, las Fuerzas Militares, la Policía Nacional, la Agencia Nacional del Espectro (ANE), MinTIC, MinTransporte y la DIAN para abordar el desafío de forma integral. Paralelamente, las fuerzas serían responsables de iniciar el desarrollo de un nuevo concepto doctrinal basado en la “supervivencia adaptativa”, que reemplace la dependencia de la superioridad aérea tradicional.
5. *Garantizar la explicabilidad de la IA (XAI).* Para confiar en un sistema como “Mantícora”, los comandantes deben tener una comprensión fundamental de cómo toma sus decisiones. La investigación debe priorizar la XAI para que los sistemas puedan justificar sus acciones, permitiendo una auditoría, verificación y confianza rigurosas (Mucci & Stryker, 2024; VerityAI, 2025).
6. *Fortalecer normas internacionales y desarrollar marcos de responsabilidad.* Dada la “democratización” de esta tecnología, que convierte la proliferación en una amenaza inminente, es crucial fortalecer las normas internacionales y desarrollar marcos de responsabilidad claros. Se debe acelerar el diálogo internacional sobre sistemas de armas letales autónomas (LAWS) y, en paralelo, establecer marcos legales a nivel nacional para cerrar el “vacío de responsabilidad” que los sistemas autónomos crean (Hall, s.f.).

En síntesis, la inteligencia de enjambre representa un nuevo capítulo en la estrategia militar; su legado no será juzgado únicamente por la superioridad tecnológica que confiera, sino por la sabiduría, la previsión y la responsabilidad con las

que la humanidad elija gestionarlo. Alcanzar su inmenso potencial requerirá una inversión continua, tanto en algoritmos y *hardware* como en los principios éticos y los marcos de cooperación que garantizarán que esta poderosa capacidad sirva para aumentar la seguridad y la estabilidad, en lugar de socavarlas.

Referencias

- ActiveLoop. (s.f.). *What is Multi-Agent Reinforcement Learning (MARL)*. <https://tinyurl.com/246p6hvq>
- Agence France-Presse. (2015, 17 de mayo). US military's new swarm of mini-drones. *Defense News*. <https://tinyurl.com/29xjlose>
- Army Research Laboratory Public Affairs. (2020, 10 de agosto). Army advances learning capabilities of drone swarms. *U.S. Army*. <https://tinyurl.com/2d9ozc52>
- Arquilla, J., & Ronfeldt, D. (2000). *Swarming and the future of conflict*. RAND Corporation.
- Bajak, F. (2024). US-China competition to field military drone swarms could fuel global arms race. *AP News*. <https://tinyurl.com/25bbahjv>
- Bondar, K. (2025). *How Ukraine's operation "Spider's Web" redefines asymmetric warfare*. Center for Strategic and International Studies. <https://tinyurl.com/25jj75k4>
- Cadena 3. (2025). *Ucrania utiliza drones de bajo costo en devastadora operación contra Rusia*. <https://tinyurl.com/2azlfp4m>
- CNA Corporation. (2025, 16 de julio). *PRC concepts for UAV swarms in future warfare*. <https://tinyurl.com/3j2tsbh9>
- DARPA. (2025, 16 de julio). *OFFSET: OFFensive swarm-enabled tactics*. <https://tinyurl.com/2bqybzjy>
- Davies, D. (2025). Multi-agent reinforcement learning: Cooperation, competition, and coordination in AI. *Medium*. <https://tinyurl.com/2cxgkw9q>
- Dorigo, M., & Gambardella, L. M. (1997). Ant colony system: A cooperative learning approach to the traveling salesman problem. *IEEE Transactions on Evolutionary Computation*, 1(1), 53-66. <https://ieeexplore.ieee.org/document/585892>
- Ejército de Tierra. (2023, noviembre). *El Ejército recibe un "sistema de enjambre de drones"*. Gobierno de España. <https://tinyurl.com/23srtefv>
- Enloe, T. (2025, 16 de julio). Designing for doctrine: Decentralized execution in unmanned swarms. *Wild Blue Yonder*. <https://tinyurl.com/276u4cae>
- Eurystic. (2025). Particle swarm optimization (PSO): What is it? - Advantages. *Eurystic Solutions*. <https://tinyurl.com/23umxzax>
- Federation of American Scientists. (s.f.). *UAV ground control station (GCS)*. Intelligence Resource Program. https://irp.fas.org/program/collect/uav_gcs.htm

- Fiveable. (2024). *Principles of self-organization | Swarm intelligence and robotics*. Fiveable Library. <https://tinyurl.com/23umxzax>
- Grover, R. (2025). Ethical challenges in AI and robotics: Balancing innovation and responsibility. *International Research Journal on Advanced Engineering and Management*, 3(3), 401-405. <https://doi.org/10.47392/IRJAEM.2025.0064>
- Haider, L. C. (2021). The vulnerabilities of Unmanned Aircraft System components. En Joint Air Power Competence Centre, *A comprehensive approach to countering unmanned aircraft systems*. <https://tinyurl.com/22uo49ex>
- Hall, A. (s.f.). *Legal risks of autonomous drone swarms*. <https://aaronhall.com/legal-risks-of-autonomous-drone-swarms/>
- Kennedy, J., & Eberhart, R. C. (1995). Particle swarm optimization. En *Proceedings of ICNN'95 - International Conference on Neural Networks* (Vol. 4, pp. 1942-1948). IEEE. <https://ieeexplore.ieee.org/document/488968>
- Khalil, R., El-Kordy, A., & Sobh, H. (2021). A review for using swarm intelligence in architectural engineering. *International Journal of Architectural Computing*, 20(12). <https://doi.org/10.1177/147807712111039078>
- Kohn, S., Cohen, M., Johnson, A., & Terman, M. (2024). Supporting ethical decision-making for lethal autonomous weapons. *Journal of Military Ethics*, 23(1), 1-20. <https://doi.org/10.1080/15027570.2024.2366094>
- Kumar, V. (2024). *All you need to know about multi-agent reinforcement learning*. Adasci.org.
- Laird, B. (2020, junio). *The risks of autonomous weapons systems for crisis stability and escalation*. RAND. <https://tinyurl.com/28y7pqtj>
- Marson, J., & Michaels, D. (2024, 6 de marzo). Cheap Ukrainian drones are thwarting Russia's powerful Black Sea Fleet. *The Wall Street Journal*.
- Matoffo. (s.f.). *Emergent behavior in AI systems*. <https://matoffo.com/emergent-behavior-in-ai-systems/>
- McKee, A. (2024). Algoritmos de inteligencia de enjambre: Tres implementaciones de Python. *Datacamp*. <https://www.datacamp.com/es/tutorial/swarm-intelligence>
- Millar, T. (2025). Not just drones, but massed swarms of them. Defences can't cope. *The Strategist*. <https://tinyurl.com/2299b578>
- Mitchell, R. (2025). AI killing machines regulation: UN urges global ban by 2026. *Electropages*. <https://tinyurl.com/23277kpj>
- Mucci, T., & Stryker, C. (2024). *¿Qué es el gobierno de la IA?* IBM. <https://www.ibm.com/es-es/think/topics/ai-governance>
- Muñoz, W., & Díaz, M. (2025). *Los riesgos de las armas autónomas: una perspectiva interseccional latinoamericana*. SEHLAC; Campaign to Stop Killer Robots. <https://tinyurl.com/35xv464n>
- Nayar, N., Gautam, S., Singh, P., & Mehta, G. (2021). Ant colony optimization: A review of literature and application in feature selection. En *Inventive computation and information technologies* (pp. 285-297). https://doi.org/10.1007/978-981-33-4305-4_22

- Ning, Z., & Xie, L. (2024). A survey on multi-agent reinforcement learning and its application. *Journal of Automation and Intelligence*. <https://doi.org/10.1016/j.jai.2024.02.003>
- OECD.AI. (2024). *US-China AI drone swarm arms race raises global security risks*. <https://oecd.ai/en/incidents/2024-04-12-a116>
- Palmer, I. (2024, 28 de junio). Accelerating decision-making through human-machine teaming. *Wild Blue Yonder*. <https://tinyurl.com/282saf8c>
- Pullum, L. (2025). *Verification and validation of systems in which AI is a key element*. SEBOK. <https://tinyurl.com/2d2ojuvs>
- Ramachandran, A. (2025). The rise of autonomous UAV swarms: Harnessing advanced AI for breakthrough applications, challenges, and future directions. <https://tinyurl.com/2aofk2tf>
- Smalley, D. (2015). *LOCUST: Autonomous, swarming UAVs fly into the future*. Office of Naval Research. <https://tinyurl.com/2y3tkpmf>
- Shammar, E., Cui, X., & Al-qaness, M. (2025). *Swarm learning: A survey of concepts, applications, and trends*. ArXiv. <https://arxiv.org/html/2405.00556v2>
- Thirtyacre, D. (2022). Remotely piloted aircraft control latency during air-to-air combat. *Air & Space Operations Review*, 1(4), 14-25. <https://tinyurl.com/bdhdv9xd>
- Tonex Training. (s.f.). *Certified drone swarm operations expert (CDSOE)* [información de curso académico]. <https://tinyurl.com/2yc8uvje>
- Torres, M. (2025). *Operation Spiderweb: Military technical analysis of the Ukrainian drone swarm attack*. Kindle Direct Publishing.
- UAV Navigation. (2023, 6 de febrero). *Estación de control aéreo* [entrada de blog]. <https://tinyurl.com/29y2dy3m>
- UAV Navigation. (2024, 6 de mayo). *Jamming y spoofing: Dos amenazas para el sistema GNS de su UAV* [entrada de blog]. <https://tinyurl.com/2d76r3ed>
- Ultralytics. (s.f.). *Inteligencia de enjambre*. <https://www.ultralytics.com/es/glossary/swarm-intelligence>
- UN News. (2021, 15 de noviembre). *Primer acuerdo mundial sobre la ética de la inteligencia artificial*. <https://news.un.org/es/story/2021/11/1500522>
- Unesco. (2021). *Recommendation on the ethics of artificial intelligence*. <https://tinyurl.com/2mgcknne>
- United Nations Institute for Disarmament Research (Unidir). (2023). *Robótica de enjambre*. <https://tinyurl.com/ywwzjtk8>
- UNODA. (2024). *Desafíos de los sistemas de armas autónomas y formas de abordarlos: una perspectiva desde la academia y la sociedad civil latina*. <https://tinyurl.com/5ymda26h>
- Ventura, E. (2025, 15 de julio). Misiles Patriot: así funciona la poderosa defensa aérea que Estados Unidos enviará a Ucrania para frenar los ataques rusos. *El Imparcial*. <https://tinyurl.com/2bs3o7td>

- Ver Velde, B. (2021). Captured! Dynetics completes historic Gremlins air recovery mission. *Leidos*. <https://tinyurl.com/2bfvabgl>
- VerityAI. (2025). *AI emergent risks testing: Identifying unexpected behaviors before deployment*. <https://verityai.co/blog/ai-emergent-risks-testing>
- Vijaya, P. A., Ajith, K. S., & Divya, C. (2017). Ant colony optimization algorithms: Introduction & its recent trends. *International Journal of Scientific Research in Science and Technology*, 3(8), 643-647.
- Xia, B., Mantegh, I., & Xie, W. (2024). Decentralized UAV swarm control: A multi-layered architecture for integrated flight mode management and dynamic target interception. *Drones*, 8(8), 350.

Capítulo 7

Naves autónomas en el espacio: poder, tecnología y desafíos de seguridad*

DOI: <https://doi.org/10.25062/9786287818620.07>

Guillermo Alberto Poveda Zamora

Fuerza Aeroespacial Colombiana

Resumen: Cómo las naves espaciales autónomas y pilotadas remotamente están redefiniendo las estrategias geopolíticas, las capacidades operacionales y los desafíos de seguridad en el dominio espacial. Este capítulo se propone analizar su impacto en la geopolítica, la operación y la seguridad espacial. Para ello, se examinan las implicaciones geopolíticas de su despliegue, se miden sus capacidades operacionales en exploración, logística y defensa, y se caracterizan los riesgos de ciberseguridad y se proponen contramedidas. Mediante una revisión documental de literatura científica, normativa y fuentes militares, se analizan y comparan los casos emblemáticos X-37B (EE.UU.), Shijian-21 (China) y Kosmos (Rusia), contrastando sus capacidades, objetivos y riesgos. Se evidencia que la convergencia de inteligencia artificial, autonomía operativa y ciberdefensa está transformando la exploración, la seguridad y la logística orbital, mientras abre nuevas vulnerabilidades a *spoofing*, *jamming* y ataques cibernéticos. La investigación advierte que la evolución de estos sistemas exige un enfoque integral de seguridad para garantizar la estabilidad operativa y la sostenibilidad de las misiones en el entorno espacial.

Palabras clave: ciberseguridad; inteligencia artificial; logística orbital; naves espaciales autónomas; regulación internacional; seguridad espacial

* Capítulo de libro resultado del proyecto de investigación "Sistema de naves y aeronaves no tripuladas e inteligencia artificial: innovaciones estratégicas para el futuro militar" en colaboración del Grupo de Investigación Ciencias Militares Aeronáuticas (GICMA), categorizado en A1 por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) (código COL0140489). Los puntos de vista y los resultados de este capítulo pertenecen a sus autores y no reflejan necesariamente los de las instituciones participantes.

Guillermo Alberto Poveda Zamora

Coronel (R) de la Fuerza Aeroespacial Colombiana. Magíster en ciencias militares aeronáuticas, Escuela de Posgrados FAC, Colombia. Magíster en ingeniería aeroespacial, Universidad del Valle, Colombia. Administrador aeronáutico. Ingeniero en telecomunicaciones. Docente e investigador, Escuela de Posgrados de la Fuerza Aeroespacial Colombiana.

Orcid: <https://orcid.org/0000-0002-3358-102X> - Contacto: guillopoveda@gmail.com

Citación APA: Poveda Zamora, G. A. (2026). Naves autónomas en el espacio: poder, tecnología y desafíos de seguridad. En D. Barrero-Barrero (Ed.), *Sistema de naves y aeronaves no tripuladas e inteligencia artificial: innovaciones estratégicas para el futuro militar* (pp. 159-185). Sello Editorial ESDEG.
<https://doi.org/10.25062/9786287818620.07>

SISTEMA DE NAVES Y AERONAVES NO TRIPULADAS E INTELIGENCIA ARTIFICIAL: INNOVACIONES ESTRATÉGICAS PARA EL FUTURO MILITAR

ISBN impreso: 978-628-7818-56-9

E-ISBN digital: 978-628-7818-62-0

DOI: <https://doi.org/10.25062/9786287818620>

Colección Estrategia, Geopolítica y Cultura

Sello Editorial ESDEG

Escuela Superior de Guerra "General Rafael Reyes prieto"

Bogotá D.C., Colombia

2026



Introducción

El desarrollo y despliegue de naves espaciales autónomas ha redefinido la dinámica geopolítica y estratégica en el ámbito espacial. Estas tecnologías han impulsado la competencia entre potencias como EE.UU., China y Rusia, que buscan consolidar su dominio en el espacio a través de avances en exploración, vigilancia e inteligencia. Si bien estas plataformas han optimizado la operatividad en órbita y reducido la necesidad de intervención humana en tareas de alto riesgo, también han abierto nuevas brechas de seguridad, particularmente en ciberdefensa y guerra electrónica.

La autonomía operativa de estos sistemas plantea interrogantes fundamentales sobre la estabilidad global, la militarización del espacio y la necesidad de una actualización urgente de los marcos regulatorios. A medida que la IA y los sistemas cibernéticos avanzados convergen con la exploración espacial, emergen riesgos asociados a la vulnerabilidad de estos activos estratégicos frente a ataques de *spoofing*¹, ciberataques y sabotajes electrónicos. En este contexto, la creciente interconexión entre infraestructuras espaciales y redes digitales amplifica la superficie de ataque para actores hostiles, lo que obliga a desarrollar estrategias de defensa más sofisticadas y resilientes.

Este capítulo analiza las capacidades operacionales de las naves espaciales autónomas, su impacto en la seguridad global y los desafíos emergentes en ciberdefensa. Se abordan las estrategias de los principales actores en la competencia espacial, destacando la manera en que estas tecnologías están transformando la seguridad y la estabilidad geopolítica. Asimismo, se exploran las amenazas en

1 Técnica de suplantación de la identidad de una fuente confiable (como una dirección IP, correo electrónico o señal GPS) para engañar a un sistema o usuario. Su objetivo es robar información, desviar datos o acceder sin autorización.

términos de ciberseguridad y las respuestas tecnológicas para mitigar los riesgos asociados a la militarización del espacio.

El capítulo se estructura en varias secciones clave. En primer lugar, se examinan las implicaciones geopolíticas y la competencia estratégica entre potencias espaciales. Posteriormente, se presentan las capacidades operacionales de las naves autónomas y su aplicación en seguridad, defensa y logística orbital. Luego, se abordan los retos regulatorios y la necesidad de establecer protocolos internacionales para evitar una escalada de conflictos en el espacio. Finalmente, se analizan las estrategias de ciberseguridad, incluyendo el uso de IA, redes cuánticas y cifrado avanzado como mecanismos de protección frente a ciberamenazas.

La creciente militarización del espacio no solo ha impulsado el desarrollo de nuevas tecnologías, sino que también ha dado lugar a una nueva dimensión del conflicto cibernético. Las operaciones de guerra electrónica y los ciberataques contra infraestructuras espaciales han evolucionado hasta convertirse en herramientas estratégicas en la rivalidad entre naciones. Como resultado, garantizar la resiliencia de estos sistemas es una prioridad para la estabilidad internacional.

Por lo tanto, aquí no solo se contextualiza la importancia de las naves autónomas en el ámbito espacial, sino que también se propone un análisis crítico sobre los desafíos técnicos, estratégicos y regulatorios que definirán el futuro de la seguridad y la ciberdefensa en y desde el espacio.

Implicaciones geopolíticas del desarrollo y despliegue de naves espaciales autónomas

El análisis de las implicaciones geopolíticas del desarrollo y despliegue de naves espaciales autónomas, con énfasis en la competencia internacional, la cooperación entre países y la militarización del espacio, permite evaluar el impacto de estas tecnologías en la seguridad global.

Los resultados muestran que EE.UU., China y Rusia lideran el desarrollo de naves autónomas con objetivos estratégicos de exploración, inteligencia y defensa, lo que ha intensificado las tensiones globales. A pesar de iniciativas como los Artemis Accords, persisten desafíos en la cooperación internacional. Además, la militarización del espacio sigue en ascenso debido a pruebas de armas antisatélite (ASAT).

Asimismo, la regulación actual es insuficiente, por lo que se requieren nuevos tratados internacionales que regulen el uso de las naves autónomas y mitiguen los riesgos de seguridad en el espacio.

Competencia estratégica internacional

La actual carrera espacial ha intensificado la competencia estratégica entre potencias globales, principalmente entre EE.UU., China y Rusia. Estas naciones han invertido significativamente en tecnologías autónomas con aplicaciones civiles y militares (Lee & Zhang, 2020). EE.UU. ha liderado con el desarrollo del vehículo X-37B, una plataforma reutilizable diseñada para operaciones prolongadas en órbita (Smith et al., 2023).

Por otro lado, China ha avanzado con el satélite Shijian-21, capaz de realizar maniobras complejas en el espacio, lo que ha generado preocupaciones por su uso dual, tanto civil como militar (Nguyen et al., 2022). Asimismo, Rusia ha desplegado satélites de inspección capaces de acercarse a otros activos orbitales, intensificando las tensiones diplomáticas (Wang et al., 2020). La competencia también se ha incrementado en el campo de la inteligencia espacial, donde estas potencias utilizan naves autónomas para la vigilancia y el espionaje estratégico (González et al., 2023).

La Tabla 1 compara los programas de naves autónomas de EE.UU., China y Rusia, destacando sus objetivos estratégicos y los riesgos asociados. Se evidencia la competencia tecnológica y sus implicaciones geopolíticas en seguridad y defensa espacial.

Tabla 1. Comparación de capacidades en naves autónomas militares espaciales entre EE.UU., China y Rusia

País	Programas de naves autónomas	Objetivos estratégicos	Riesgos asociados
EE.UU.	X-37B, DARPA XS-1	Exploración avanzada, inteligencia y defensa estratégica	Militarización del espacio, espionaje tecnológico
China	Shijian-21, Tianyuan	Dominio orbital, neutralización de satélites, acceso a recursos espaciales	Preocupaciones sobre uso dual (civil-militar), tensiones geopolíticas
Rusia	Kosmos, Burevestnik	Vigilancia orbital, guerra electrónica, defensa contra amenazas espaciales	Interferencia en satélites rivales, falta de transparencia en desarrollos espaciales

Fuente: Elaboración propia con base en los datos recolectados de Lee y Zhang (2020), Smith et al. (2023), Nguyen et al. (2022), Wang et al. (2020) y González et al. (2023)

En la Figura 1 se pueden observar tres naves espaciales autónomas avanzadas: el X-37B de EE.UU., utilizado para misiones de inteligencia y defensa; el Shijian-21 de China, con capacidades de maniobra orbital; y un satélite de la familia Kosmos de Rusia, empleado para monitoreo y comunicaciones espaciales.

Figura 1. Naves espaciales autónomas más avanzadas



X-37B (EE.UU.)



Shijian-21 (China)



Lotos-S1 (Rusia)

Fuente: Elaboración propia con imágenes de Latam Satelital (2018), Makichuk (2021) y Wall (2012)

Cooperación internacional

A pesar de la creciente competencia, existen iniciativas de cooperación internacional como los Artemis Accords, liderados por EE.UU., que buscan establecer una presencia sostenible en la Luna mediante alianzas multinacionales (Smith et al., 2023). No obstante, estas iniciativas tienen detractores debido a la desconfianza estratégica y a las diferencias en políticas espaciales entre las potencias (Brown et al., 2020). China y Rusia han formado alianzas estratégicas para contrarrestar la influencia de EE.UU. en la cooperación espacial internacional, mientras que otras naciones emergentes, como India y Japón, buscan consolidar sus propias capacidades espaciales mediante colaboraciones regionales (Johnson & Miller, 2020).

En la Figura 2 se puede observar un diagrama que representa las principales alianzas en la exploración espacial. Se destacan los Artemis Accords, liderados por EE.UU., y la colaboración China-Rusia, enfocada en rivalizar con la influencia estadounidense. Además, se incluyen alianzas emergentes, como la participación de Brasil y Emiratos Árabes Unidos en proyectos estadounidenses, y la cooperación de Sudáfrica y Nigeria con China y Rusia en tecnología espacial.

Militarización del espacio

El desarrollo de armas antisatélite y la creación de fuerzas espaciales han incrementado el riesgo de militarización del espacio (Anderson et al., 2021). China realizó una prueba ASAT en 2007, generando miles de fragmentos de desechos

Figura 2. Diagrama de cooperación internacional en la exploración espacial



Fuente: Elaboración propia con datos de Johnson y Miller (2020)

espaciales y complicando la seguridad orbital (Nguyen et al., 2022). EE.UU. respondió con la creación de su Fuerza Espacial en 2019, consolidando sus capacidades de defensa en el espacio (Brown & Taylor, 2020). Este escenario plantea un dilema estratégico en torno a la militarización y el uso pacífico del espacio exterior (Johnson & Miller, 2020). Además, el desarrollo de satélites capaces de maniobrar y neutralizar otros satélites ha generado preocupación por el uso de tecnología autónoma para operaciones ofensivas (Lee & Zhang, 2020).

En la Figura 3 se puede observar una representación gráfica de la acumulación de fragmentos de basura espacial en la órbita media-baja terrestre. Estos desechos, producto de pruebas de armas antisatélite y colisiones de satélites obsoletos, representan un riesgo significativo para la seguridad orbital y la operatividad de satélites activos. La creciente cantidad de escombros espaciales plantea desafíos para la navegación, el acceso y la exploración del espacio.

Desafíos regulatorios y reformas necesarias

El marco legal internacional actual, encabezado por el Tratado sobre el Espacio Ultraterrestre (1967), es insuficiente para abordar los desafíos modernos que presentan las naves autónomas y los sistemas espaciales de doble uso (Kumar et al.,

Figura 3. Fragmentos de basura espacial generados por humanos en la órbita media-baja

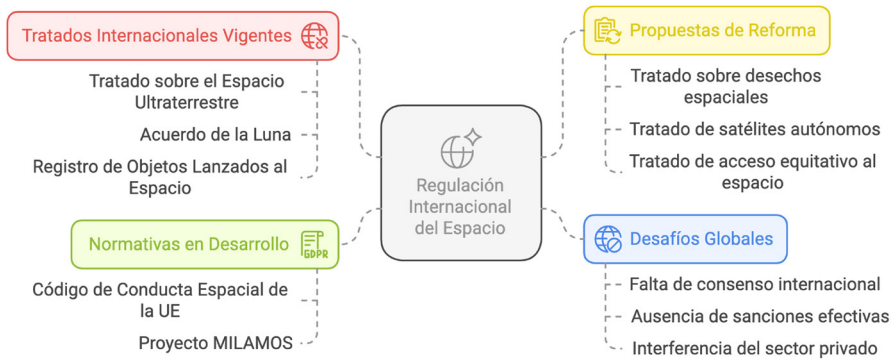


Fuente: González Valenzuela (2023)

2023). Se han propuesto varias reformas, como el Código de Conducta Espacial de la Unión Europea, aunque este carece de mecanismos vinculantes (Lee & Zhang, 2020). Se destaca la necesidad de un organismo internacional de monitoreo que supervise el despliegue de tecnologías autónomas, previniendo su uso militar indebido (Smith et al., 2023). Además, se ha propuesto la creación de un tratado específico que regule el uso de naves autónomas en el espacio (Gonzalez et al., 2023).

En la Figura 4 se presenta un esquema sobre la regulación internacional del espacio, destacando los tratados vigentes, como el Tratado sobre el Espacio Ultraterrestre (1967) y el Acuerdo de la Luna (1979). También se incluyen normativas en desarrollo, como el Código de Conducta Espacial de la UE y el proyecto Milamos (*Manual on International Law Applicable to Military Uses of Outer Space*). Asimismo, se muestran propuestas de reforma, enfocadas en regular los desechos espaciales, los satélites autónomos y garantizar el acceso equitativo al espacio. Finalmente, se identifican desafíos globales, tales como la falta de consenso internacional, la ausencia de sanciones efectivas y la interferencia del sector privado en la exploración espacial.

Figura 4. Regulación internacional: tratados y desafíos



Fuente: Elaboración propia con datos de Kumar et al. (2023)

Tecnología y capacidades operacionales de naves autónomas en misiones de seguridad y defensa

Las naves espaciales autónomas están transformando la exploración, la seguridad y la defensa en el espacio. Estas plataformas tecnológicas han optimizado la vigilancia orbital, la protección de infraestructuras espaciales y la eficiencia en la gestión de recursos. Su creciente autonomía reduce la necesidad de intervención humana en tareas de alto riesgo, mejora la capacidad de respuesta ante amenazas y aumenta la resiliencia operativa en entornos hostiles (Johnson & Taylor, 2022). En el entorno militar generan especial preocupación sus capacidades operacionales, su aplicación en la seguridad espacial y su impacto en el equilibrio geopolítico global.

Capacidades técnicas y operacionales de naves autónomas

Las naves autónomas destacan por una combinación de tecnologías avanzadas que les permiten cumplir tareas complejas sin intervención humana directa.

Reconocimiento y monitoreo de activos críticos

El reconocimiento y monitoreo de activos críticos en el espacio es una función esencial de las naves autónomas, diseñada para detectar, rastrear y evaluar amenazas en tiempo real. Gracias a sensores avanzados, como cámaras

multiespectrales y radares de apertura sintética (SAR), estas plataformas pueden identificar movimientos sospechosos y posibles riesgos para infraestructuras estratégicas (Martínez et al., 2021; Wilson et al., 2022). Además, el uso de IA permite el procesamiento de grandes volúmenes de datos mediante algoritmos de aprendizaje profundo, lo que facilita la identificación de patrones y anomalías que podrían indicar actividades hostiles (Kim et al., 2021; Vásquez et al., 2023). La persistencia en el espacio es otro factor clave, ya que estas naves pueden operar en órbita por largos periodos, proporcionando vigilancia continua sobre áreas sensibles, como estaciones espaciales y satélites críticos (Rodríguez & Li, 2022).

- *Sensores avanzados.* Equipadas con cámaras multiespectrales y radares de apertura sintética (SAR), estas naves pueden detectar, rastrear y evaluar amenazas en tiempo real. Entre estos sistemas de detección se encuentra el Programa de Apoyo a la Defensa (DSP, Defense Support Program), con una constelación de satélites geoestacionarios que proporcionaba capacidad de detección de lanzamientos de misiles (Martínez et al., 2021; Wilson et al., 2022).
- *IA para análisis de datos.* Algoritmos de aprendizaje profundo procesan grandes volúmenes de datos para identificar patrones y anomalías que podrían indicar actividades hostiles (Sánchez Godínez, 2012; Kim et al., 2021; Vásquez et al., 2023).
- *Persistencia en el espacio.* Estas naves pueden permanecer en órbita durante largos periodos, incluso décadas, como los X-37B, de los cuales se tiene registro de su primer lanzamiento en 2011. Esto les permite monitorear continuamente áreas sensibles, como estaciones espaciales, satélites críticos o zonas de interés en la superficie del planeta (Rodríguez & Li, 2022).

La figura 5 muestra una representación del satélite SBIRS-High, del DSP. Este satélite se utiliza para la detección y alerta temprana de lanzamientos de misiles balísticos, empleando sensores infrarrojos avanzados para monitorear amenazas globales en tiempo real. Su función estratégica es esencial para la defensa y la seguridad espacial.

Sistemas de respuesta automática ante amenazas

Los sistemas de respuesta automática ante amenazas son mecanismos avanzados implementados en naves espaciales autónomas para neutralizar riesgos orbitales y proteger activos estratégicos. Algunas de estas naves están equipadas

Figura 5. Representación del satélite SBIRS-High del DSP



Fuente: Sánchez Godínez (2012)

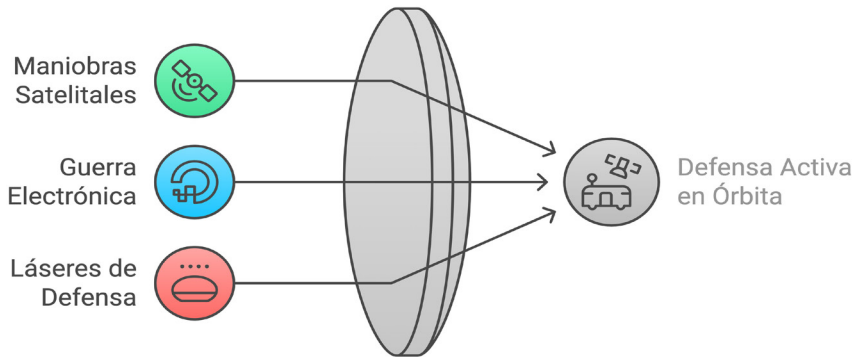
con tecnología de intercepción de amenazas orbitales, lo que les permite neutralizar satélites hostiles o interceptar desechos espaciales que representen un peligro para infraestructuras clave (Tanaka & Fujimoto, 2023; Pérez et al., 2022). Además, cuentan con protocolos de defensa autónoma que les permiten ejecutar maniobras evasivas o desplegar contramedidas automáticamente en caso de detectar una posible agresión, garantizando así la seguridad operativa sin intervención humana inmediata (Méndez et al., 2022; Hernández et al., 2023).

- *Intercepción de amenazas orbitales.* Algunas naves están diseñadas para neutralizar satélites hostiles o interceptar desechos espaciales que puedan poner en riesgo activos estratégicos (Tanaka & Fujimoto, 2023; Pérez et al., 2022).
- *Protocolos de defensa autónoma.* Sistemas que ejecutan maniobras evasivas o contramedidas de forma automática en caso de ataque, en especial si la comunicación con su estación de control ha sido comprometida, degradada o anulada por completo (Méndez et al., 2022; Hernández et al., 2023).

La Figura 6 ilustra los métodos de defensa activa en órbita utilizados por las naves espaciales autónomas. Se presentan tres enfoques principales: maniobras satelitales, que permiten evasión y reposicionamiento estratégico; guerra electrónica, utilizada para interferir y neutralizar señales hostiles; y láseres de defensa, diseñados para contrarrestar amenazas físicas en el espacio. Estas estrategias

contribuyen a una respuesta automatizada y efectiva ante posibles agresiones en entornos orbitales hostiles.

Figura 6. Estrategias de respuesta automática ante amenazas



Fuente: Elaboración propia con datos de Méndez et al. (2022) y Hernández et al. (2023)

Aplicaciones estratégicas en seguridad y defensa

Las naves autónomas desempeñan un papel clave en la seguridad y defensa espacial, proporcionando monitoreo de satélites y bases rivales, y protegiendo activos estratégicos mediante IA y análisis predictivo para detectar amenazas de forma anticipada.

Reconocimiento y vigilancia

Las naves autónomas son esenciales para las operaciones de inteligencia en el espacio, tales como:

- *Monitoreo de satélites y bases rivales.* Proveen datos críticos sobre movimientos y actividades sospechosas de otros actores espaciales (Wong et al., 2021; Zhang et al., 2023).
- *Protección de activos propios.* Ayudan a identificar posibles ataques antes de que ocurran mediante análisis predictivo basado en IA (Khan et al., 2023; Ortiz & Jiménez, 2023).

Logística y abastecimiento

Las naves autónomas han optimizado significativamente la logística y el abastecimiento espacial, permitiendo el transporte autónomo de suministros a estaciones espaciales y bases lunares, así como el reabastecimiento orbital, lo que prolonga la

vida útil de satélites y otros activos estratégicos. Su implementación ha mejorado considerablemente el transporte y mantenimiento de infraestructuras espaciales, facilitando operaciones de reabastecimiento de combustible, reparación y optimización de recursos, lo que fortalece la resiliencia y sostenibilidad de las misiones espaciales. Estas misiones incluyen:

- *Transporte autónomo.* Las naves pueden realizar entregas precisas de suministros a estaciones espaciales y bases lunares, reduciendo la necesidad de misiones tripuladas (García et al., 2022; Singh et al., 2022).
- *Mantenimiento y reparación orbital.* ELSA-d (Reino Unido) ha demostrado capacidad para capturar y reparar satélites defectuosos (Johnson & Miller, 2020).
- *Reabastecimiento orbital.* Facilita operaciones de recarga de combustible y mantenimiento de satélites, optimizando recursos y extendiendo la vida útil de los activos. Vehículos como Cygnus (NASA) y HTV-X (Japón) permiten el reabastecimiento automático de la Estación Espacial Internacional (ISS) (Lin et al., 2023; Huang et al., 2022).

La Tabla 2 presenta un análisis de las principales naves espaciales utilizadas para abastecimiento, mantenimiento y logística orbital. Se incluyen naves operadas por agencias espaciales como NASA, JAXA, CNSA y Roscosmos, así como desarrollos de empresas privadas como SpaceX, Boeing, Sierra Space y Blue Origin. La tabla destaca la función de cada nave, la entidad responsable, su beneficio estratégico y su grado de autonomía. Este análisis permite comprender el papel clave de estas naves en la exploración y sostenibilidad del entorno espacial.

Tabla 2. Comparación de naves autónomas y semiautónomas para aplicaciones logísticas en el espacio

Nombre de la nave	Función	Agencia/espacio responsable	Beneficio estratégico	Autonomía
Cygnus	Transporte de carga a la ISS	NASA / Northrop Grumman (EE.UU.)	Mantiene operaciones en la ISS y pruebas tecnológicas	Totalmente autónoma
HTV-X	Reabastecimiento y carga orbital	JAXA (Japón)	Optimiza misiones espaciales con mayor capacidad de carga	Totalmente autónoma
Dragon	Transporte de suministros y retorno de carga	SpaceX (EE.UU.)	Reduce costos al permitir recuperación de materiales	Totalmente autónoma

Continúa tabla...

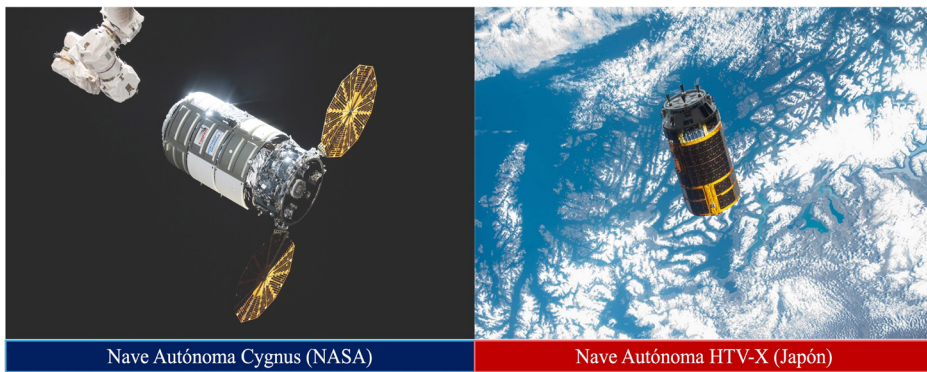
Nombre de la nave	Función	Agencia/espacio responsable	Beneficio estratégico	Autonomía
Tianzhou	Suministro de módulos y logística espacial	CNSA (China)	Soporta la exploración espacial con mayor autonomía	Totalmente autónoma
ELSA-d	Captura y retiro de desechos espaciales	Astroscale (Reino Unido / Japón)	Contribuye a la limpieza y sostenibilidad del entorno orbital	Totalmente autónoma
CST-100 Starliner	Transporte de tripulación y carga a la ISS	Boeing / NASA (EE. UU.)	Apoya el acceso recurrente de astronautas y suministros a la ISS	Semiautónoma; requiere intervención humana
Dream Chaser	Transporte de carga y retorno de experimentos científicos	Sierra Space / NASA (EE.UU.)	Permite retornos seguros de experimentos y materiales de la ISS	Totalmente autónoma
Progress	Suministro de carga a la ISS	Roscosmos (Rusia)	Garantiza el abastecimiento continuo de la ISS	Totalmente autónoma
X-37B	Misiones experimentales y de reconocimiento militar	Boeing / Fuerza Espacial de EE.UU.	Realiza pruebas de tecnologías espaciales avanzadas	Totalmente autónoma
New Shepard	Turismo espacial suborbital y experimentos científicos	Blue Origin (EE.UU.)	Facilita experimentos en microgravedad y vuelos comerciales	Totalmente autónoma

Fuente: Elaboración propia con base en NASA (2023), Marín (2016), SpaceX (2023), CNSA (2022), Astroscale (2022), Boeing (2023), Sierra Space (2023), Roscosmos (2022), Fuerza Espacial de EE.UU. (2023) y Blue Origin (2023)

En este sentido, en la Figura 7 se observan dos naves autónomas de carga utilizadas para el reabastecimiento de la ISS. A la izquierda, la Cygnus de NASA y Northrop Grumman, diseñada para transportar suministros y experimentos científicos. A la derecha, la HTV-X de Japón (JAXA), una evolución de la serie HTV, optimizada para misiones de logística y carga orbital. Ambas representan avances en la automatización y sostenibilidad de las operaciones espaciales.

Por otra parte, la eficiencia en el consumo de combustible es un factor determinante en el éxito de las misiones espaciales autónomas. La aplicación de modelos teóricos de la mecánica celeste permite reducir significativamente el uso de combustibles en vehículos espaciales, lo que optimiza la autonomía y sostenibilidad de las misiones (Poveda Zamora, 2020).

Figura 7. Naves autónomas de carga para abastecimiento de la ISS



Fuente: NASA (2023) y Marín (2016)

Respuesta en tiempo real a crisis espaciales y en la superficie terrestre

La respuesta en tiempo real a crisis espaciales es una capacidad clave de las naves autónomas, permitiendo la neutralización de amenazas emergentes mediante algoritmos adaptativos que pueden interceptar proyectiles o satélites hostiles (Rodríguez et al., 2022; Kim et al., 2023). Además, su avanzada maniobra autónoma facilita el soporte en misiones de rescate, respondiendo rápidamente a emergencias como colisiones o fallos en estaciones espaciales, lo que mejora la seguridad operativa en entornos orbitales críticos (Vásquez et al., 2023; Li et al., 2023).

Bajo este contexto de respuesta oportuna a las crisis, existen misiones muy específicas para las naves espaciales autónomas. Algunas de ellas son:

- *Neutralización de amenazas emergentes.* Mediante algoritmos adaptativos, estas naves pueden interceptar proyectiles, misiles o satélites enemigos (Rodríguez et al., 2022; Kim et al., 2023).
- *Soporte en misiones de rescate.* La capacidad de maniobra autónoma permite respuestas rápidas ante emergencias, como colisiones o fallos en estaciones espaciales (Vásquez et al., 2023; Li et al., 2023).

Un ejemplo de esta capacidad es el proyecto conjunto de la USAF y SpaceX, en el cual la Starship está siendo evaluada como una plataforma para el despliegue de tropas y suministros en cualquier parte del planeta en menos de 90 minutos (*El Confidencial*, 1.º de febrero de 2024). Esta tecnología, originalmente diseñada para la exploración espacial, también podría utilizarse para la atención de desastres y crisis humanitarias, permitiendo una respuesta ultrarrápida a eventos catastróficos y mejorando la logística de emergencia en regiones de difícil acceso.

La Figura 8 representa un cambio disruptivo en la estrategia militar global. La posibilidad de despliegue de tropas y vehículos militares a través de una nave de SpaceX muestra el potencial de estas tecnologías para permitir el traslado ultrarrápido de fuerzas a cualquier punto del planeta.

Figura 8. *Uso estratégico de naves de SpaceX para transporte militar rápido*



Fuente: *El Confidencial* (1º de febrero de 2024)

Esta capacidad sin precedentes redefine el concepto de *movilidad estratégica*, ya que obliga a los países a mejorar sus sistemas de detección, monitoreando más alto y con mayor rapidez cualquier objeto que se aproxime a su territorio. Asimismo, enfatiza la necesidad de desarrollar capacidades de respuesta inmediata, ya que la velocidad de despliegue podría superar los tiempos de reacción convencionales, alterando significativamente la dinámica de seguridad y defensa a nivel internacional.

Optimización de recursos y reducción de riesgos humanos

Las naves autónomas permiten una mayor eficiencia en el uso de recursos y reducen la exposición humana a los riesgos inherentes a las operaciones espaciales. Algunas ventajas de la operación autónoma son:

- *Automatización de tareas repetitivas.* Misiones como el mantenimiento de satélites o la limpieza de desechos espaciales se realizan de manera autónoma, disminuyendo costos operativos, los cuales, a medida que avanzan la IA y la robótica, descienden drásticamente (Martínez et al., 2021; Kim et al., 2022).
- *Flexibilidad operativa.* Las naves pueden ser reprogramadas rápidamente para adaptarse a nuevos objetivos, optimizando su uso durante prolongados tiempos de permanencia en el dominio espacial, algo difícil de lograr con seres humanos (Pérez & Chen, 2022).
- *Minimización de riesgos para astronautas.* Las misiones autónomas eliminan la necesidad de enviar tripulaciones humanas a áreas de alto riesgo, como regiones con alta radiación, asteroides o zonas en conflicto (García et al., 2022; Li et al., 2022).

Ventajas estratégicas para las naciones inversoras

Las capacidades de las naves autónomas proporcionan ventajas competitivas significativas en el ámbito económico y geopolítico:

- *Dominio tecnológico.* Las naves espaciales autónomas representan una ventaja estratégica clave para los países que invierten en su desarrollo, ya que fortalecen su posición geopolítica y tecnológica en el ámbito espacial. Estas tecnologías avanzadas permiten consolidar el dominio tecnológico, asegurando un liderazgo en la exploración y el control del espacio exterior, lo que a su vez influye en la estabilidad y el poder global de las naciones (Lin et al., 2023; Singh et al., 2023).
- *Infraestructura de seguridad avanzada.* Proporcionan una infraestructura de vigilancia sofisticada, capaz de detectar y neutralizar amenazas potenciales, lo que refuerza la disuasión frente a actores hostiles (Wilson et al., 2022; Hernández et al., 2023).
- *Resiliencia frente a emergencias.* Gracias a que su disponibilidad es casi permanente cuando se encuentran orbitando inertes en el espacio, su capacidad de respuesta se vuelve inmediata ante crisis espaciales o eventos inesperados, garantizando la protección y continuidad operativa de activos estratégicos, aumentando la resiliencia de las naciones frente a emergencias y asegurando la sostenibilidad de sus misiones a largo plazo en el espacio (Zhang et al., 2023; Martínez et al., 2021).

Retos de seguridad y ciberdefensa en naves autónomas

Las amenazas cibernéticas en el ámbito espacial incluyen el acceso no autorizado a sistemas, la manipulación de datos y la interferencia en las comunicaciones. Algunas de las principales amenazas detectadas en el ámbito de la seguridad y ciberdefensa de naves autónomas son:

- *Ataques de spoofing.* La suplantación de señales de comando, conocida como spoofing, representa una amenaza crítica para las naves espaciales autónomas. La manipulación de señales GNSS (Global Navigation Satellite System)² puede hacer que las naves operen con coordenadas falsas, comprometiendo la integridad de sus misiones y aumentando el riesgo de colisión o interferencia con otras infraestructuras espaciales. Este tipo de ataque es particularmente peligroso en el contexto de la guerra electrónica, donde actores hostiles pueden alterar los sistemas de navegación para obtener ventajas estratégicas (Falco, 2020, p. 12).

Las interferencias en los sistemas de posicionamiento global han demostrado ser un riesgo significativo para la seguridad aeroespacial, afectando tanto a naves espaciales autónomas como a aeronaves comerciales y militares. Casos recientes han evidenciado la gravedad de este problema: en Estonia, un ataque de *spoofing* alteró las señales de navegación, generando el cierre temporal de aeropuertos. Asimismo, en mayo de 2024, un evento de gran escala desvió la ruta de aproximadamente 15 000 aeronaves que tenían destino a Beirut, redirigiéndolas erróneamente hacia El Cairo. Israel también ha experimentado incidentes recurrentes, con intentos de manipulación de señales GNSS que comprometen la precisión del posicionamiento y afectan operaciones de navegación aérea (EITB, 2024).

- *Malware en IA.* El avance de la IA ha permitido una mayor independencia operativa de las naves espaciales. Sin embargo, esta autonomía también ha introducido nuevas amenazas cibernéticas, entre ellas, la posibilidad de que modelos de aprendizaje automático sean comprometidos por *software* malicioso. La manipulación de estos algoritmos podría inducir a las naves a tomar decisiones erróneas, lo que afectaría su desempeño en misiones críticas. En un escenario adverso, estas alteraciones podrían

2 Sistema global que permite determinar la posición, velocidad y tiempo en cualquier parte del mundo mediante señales de satélites. Incluye sistemas como GPS (EE.UU.), Galileo (Unión Europea), Glonass (Rusia) y BeiDou (China).

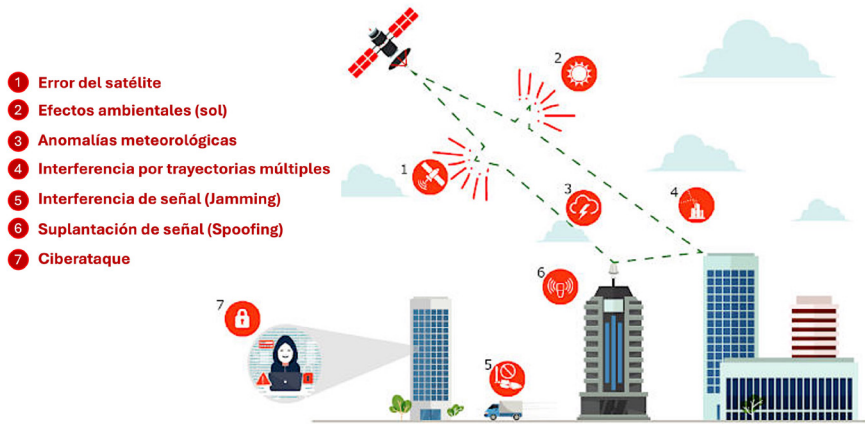
generar fallos en los sistemas de navegación o provocar una respuesta inadecuada ante amenazas espaciales (Thangavel et al., 2022, p. 89).

- *Ataques de denegación de servicio (DoS)*. La sobrecarga de los sistemas de comunicación mediante ataques de denegación de servicio puede interrumpir la operatividad de una nave, bloqueando la transmisión de datos y la recepción de comandos desde estaciones terrestres. La latencia en las comunicaciones espaciales agrava este problema, ya que la recuperación de un sistema afectado puede tardar demasiado tiempo en comparación con un ataque realizado en redes terrestres. Además, la interrupción de señales de control puede dejar a las naves vulnerables a otros tipos de ataques cibernéticos (Pavur & Martinovic, 2022, p. 56).
- *Infiltración en redes satelitales*. La interconectividad de redes satelitales con estaciones terrestres expone, en el segmento de enlace, datos sensibles que pueden ser interceptados y explotados por actores maliciosos. La vulnerabilidad de estos sistemas se debe a la falta de protocolos de seguridad unificados y al uso de tecnologías de cifrado obsoletas en algunos satélites. La infiltración en estas redes no solo permite el robo de información, sino que también facilita el sabotaje de misiones estratégicas en tiempo real (Manulis et al., 2021).
- *Manipulación de datos de sensores*. La alteración de los datos captados por los sensores de una nave autónoma puede generar errores críticos en la toma de decisiones, afectando su navegación y respuesta ante posibles amenazas. Este tipo de ataque puede inducir a la nave a detectar amenazas inexistentes, atacar a sus propios colegas o ignorar riesgos reales, aumentando la probabilidad de colisiones o fallos operacionales. En un escenario de conflicto, un adversario podría modificar la información de los sensores para hacer que un satélite hostil pase desapercibido y evitar su neutralización (Pavur et al., 2021, p. 78).

La Figura 9 muestra un esquema visual de las principales vulnerabilidades en redes de comunicaciones espaciales, destacando los factores que pueden afectar la precisión y confiabilidad de las señales de satélites. Se identifican siete amenazas principales: errores del satélite, efectos ambientales como la radiación solar, anomalías meteorológicas, interferencias por trayectorias múltiples de otras antenas y equipos radiando señales, interferencia de señal (*jamming*), suplantación de señal (*spoofing*) y ciberataques. Estas amenazas pueden alterar la recepción de datos y comprometer la seguridad de infraestructuras críticas, no solo en el

espacio, sino también en tierra, como edificios, vehículos y sistemas de telecomunicaciones urbanas.

Figura 9. Vulnerabilidades de las redes que dependen de la señal de reloj de satélites GNSS



Fuente: Adaptada de Conectrónica (s.f.)

Estrategias de defensa y contramedidas

Las estrategias de defensa y contramedidas buscan proteger las naves autónomas espaciales mediante ciberseguridad, IA y respuesta a amenazas emergentes. En el contexto de la defensa aeroespacial, se enfatiza la importancia de desarrollar tecnologías autónomas que permitan la gestión de operaciones multidominio en tiempo real (Poveda Zamora & Álvarez Calderón, 2022).

- *Cifrado avanzado en comunicaciones espaciales.* La implementación de cifrado avanzado en las comunicaciones espaciales es fundamental para evitar la interceptación de datos sensibles por actores maliciosos. El uso de criptografía cuántica y protocolos de autenticación basados en claves dinámicas ha demostrado ser altamente eficaz para mitigar ataques de interceptación (Kumar et al., 2023, p. 67). Estos sistemas cifrados aseguran la integridad y confidencialidad de los datos, reduciendo el riesgo de manipulación en la transmisión de información entre satélites y estaciones terrestres.
- *Implementación de IA para la detección de anomalías.* La IA ha demostrado ser una herramienta efectiva para la detección de ataques cibernéticos

en tiempo real. A través del análisis de patrones de tráfico de datos y la identificación de comportamientos anómalos, los sistemas de IA pueden prever intentos de intrusión en redes espaciales y activar respuestas automáticas antes de que se produzca una vulnerabilidad crítica (Zhang & Li, 2022, p. 103). Esto permite una adaptación dinámica de los protocolos de defensa y una mitigación rápida de amenazas emergentes.

- *Sistemas de redundancia en hardware y software.* La redundancia en sistemas críticos es una estrategia clave para minimizar el impacto de ataques cibernéticos en infraestructuras espaciales. La implementación de *hardware* de respaldo y la replicación de *software* en múltiples nodos permiten la continuidad de las operaciones ante posibles fallos por ataques de denegación de servicio (DoS) o sabotajes internos (Hernández et al., 2023, p. 89). Esta estrategia también previene la interrupción total de las misiones, asegurando que las naves autónomas puedan operar bajo condiciones adversas sin comprometer sus objetivos.
- *Monitoreo satelital mediante vigilancia orbital activa.* El monitoreo satelital ha evolucionado significativamente con la incorporación de tecnologías avanzadas como la IA y las redes cuánticas. Los algoritmos de IA permiten analizar en tiempo real las señales emitidas por satélites y detectar irregularidades que podrían indicar interferencias, bloqueos de señal o intentos de *spoofing*. A su vez, la aplicación de criptografía cuántica en la transmisión de datos refuerza la seguridad de las comunicaciones espaciales, minimizando los riesgos de interceptación por parte de actores hostiles (Pavur et al., 2022, p. 132).
- *Desarrollo de protocolos de ciberseguridad estandarizados.* La falta de un marco normativo unificado en ciberseguridad ha expuesto a los sistemas espaciales autónomos a diversas vulnerabilidades. Para mitigar estos riesgos, organizaciones internacionales han propuesto regulaciones que abordan aspectos clave, como la autenticación de señales satelitales y los protocolos de respuesta ante incidentes cibernéticos. Estas iniciativas buscan mejorar la cooperación entre agencias espaciales y reforzar la capacidad de respuesta frente a amenazas emergentes, reduciendo así el riesgo de ataques que puedan comprometer infraestructuras orbitales críticas (Smith & Rodríguez, 2023, p. 54).

La Tabla 3 presenta un resumen de las tecnologías de ciberseguridad aplicadas en naves espaciales autónomas, junto con su nivel de efectividad en distintos

escenarios operacionales. Si bien estas tecnologías son herramientas relevantes para la protección de infraestructura espacial, es fundamental reconocer que ningún sistema es completamente invulnerable.

Tabla 3. *Tecnologías de ciberseguridad para naves autónomas*

Tecnología	Función	Aplicación	Efectividad
Cifrado cuántico	Protección de datos	Comunicación satelital	Alta
IA para ciberseguridad	Análisis predictivo	Detección de anomalías	Alta
Sistemas redundantes	Prevención de fallos	Hardware y software	Media
Autenticación biométrica	Acceso seguro	Control de mando	Alta

Fuente: Elaboración propia con base en Kumar et al. (2023), Zhang y Li (2022), Hernández et al. (2023), Pavur et al. (2022) y Smith y Rodríguez (2023)

La seguridad en entornos espaciales es un proceso dinámico y evolutivo, donde los atacantes constantemente buscan nuevas formas de comprometer los sistemas. En este contexto, la estrategia de defensa más efectiva no solo radica en la implementación de tecnologías avanzadas, sino en su evaluación y actualización continuas. El objetivo no es simplemente mitigar ataques conocidos, sino anticiparse a futuras amenazas.

Por ello, el enfoque debe centrarse en un desarrollo permanente de *hardware*, *software* y protocolos de seguridad, asegurando que cada intento de ataque encuentre un sistema ya mejorado y reforzado. En otras palabras, el éxito de la ciberseguridad en el ámbito espacial no consiste en alcanzar una protección absoluta, sino en garantizar que los atacantes siempre lleguen tarde, enfrentándose a sistemas que han evolucionado antes de que sus vulnerabilidades puedan ser explotadas.

Conclusiones

La evolución de las naves espaciales autónomas ha intensificado la competencia geopolítica y los riesgos de militarización, lo que hace imprescindible una actualización de los tratados internacionales. La estabilidad y seguridad del espacio dependerán de un marco regulatorio equilibrado que garantice la cooperación global y establezca normas claras sobre el uso de tecnologías autónomas en misiones estratégicas.

Si las naves autónomas integran capacidades militares significativas más allá de la guerra electrónica y cibernética, la capacidad de defensa de la mayoría de los países quedaría severamente limitada. La actual tecnología ASAT está restringida a unas pocas naciones, lo que implica que la proyección de poder en el espacio podría inclinarse drásticamente en favor de aquellos con dominio sobre naves autónomas armadas.

La guerra cibernética en el espacio es ya una realidad, y no una amenaza futura, dada la vulnerabilidad de las comunicaciones satelitales. Ataques como *spoofing*, *jamming* y *malware* en IA pueden comprometer misiones estratégicas, lo que exige un enfoque dinámico de ciberdefensa basado en monitoreo continuo, protocolos actualizados y sistemas de respuesta automatizados.

El desarrollo de sistemas de defensa autónoma es clave para proteger activos espaciales y garantizar la resiliencia operativa en entornos hostiles. La implementación de maniobras evasivas automatizadas, IA para detección de amenazas y contramedidas orbitales es esencial para evitar interferencias y sabotajes cibernéticos en infraestructuras críticas.

Las naves autónomas están revolucionando la logística espacial, optimizando la gestión de recursos y reduciendo los costos de misiones tripuladas. El reabastecimiento orbital y la reparación de satélites mediante plataformas autónomas mejoran la sostenibilidad de misiones espaciales de largo plazo, fortaleciendo la infraestructura espacial global.

El uso de naves como la Starship para el despliegue rápido de tropas y asistencia humanitaria redefine la planificación estratégica y militar, al permitir asistir con rapidez y efectividad a comunidades inmersas en áreas de desastres naturales; esto, sin duda, mejorará las posibilidades de salvar vidas, en donde la variable tiempo juega un papel preponderante. En un contexto operacional, su integración en campañas ofensivas transformará la interacción entre los principios de la guerra, alterando factores clave como el alcance, la velocidad de proyección, la concentración de fuerzas (masa), la maniobrabilidad y la precisión del esfuerzo militar. Esta capacidad sin precedentes obligará a replantear las doctrinas de disuasión, alerta temprana y defensa estratégica, ya que la posibilidad de proyectar poder en cualquier punto del planeta en tiempos reducidos limitará drásticamente las oportunidades de respuesta del adversario, modificará el equilibrio en los teatros de operaciones y exigirá una nueva concepción de la seguridad global.

Referencias

- Anderson, R., Thompson, J., & Li, M. (2021). The Outer Space Treaty and modern challenges. *Journal of Space Policy*, 37(4), 211-225.
- Astroscale. (2022). *ELSA-d mission overview*. <https://astroscale.com/missions/elsa-d/>
- Blue Origin. (2023). *New Shepard: Enabling suborbital research and tourism*. <https://www.blueorigin.com/es-MX/new-shepard>
- Boeing. (2023). *CST-100 Starliner spacecraft*. <https://www.boeing.com/space/starliner>
- Brown, T., & Taylor, S. (2020). The militarization of autonomous satellites. *Defense Studies Review*, 45(2), 134-158.
- CNSA. (2022). *Tianzhou cargo missions*.
- Conetrónica. (s.f.). *Protección de la infraestructura de red que depende de la difusión de la hora desde satélites GNSS*. <https://tinyurl.com/2c8rq1ot>
- EITB. (2024, mayo). *Ciberataques a sistemas de posicionamiento global por satélite*. <https://tinyurl.com/26qh7zav>
- El Confidencial*. (2024, 1.º de febrero). El Pentágono quiere usar los cohetes de SpaceX para enviar cargamento militar por el mundo en minutos. <https://tinyurl.com/2xjge5r2>
- Falco, G. (2020). When satellites attack: Satellite-to-satellite cyber attack, defense and resilience. *ASCEND 2020*. <https://doi.org/10.2514/6.2020-4035>
- Fuerza Espacial de EE.UU. (2023). *X-37B orbital test vehicle*. <https://www.spaceforce.mil/News/Article/2093630/x-37b-spaceplane/>
- García, R., Hernández, J., & Smith, L. (2022). Advances in spacecraft logistics systems. *Space Technology Journal*, 14(3), 102-119.
- González Valenzuela, C. (2023, 6 de julio). La basura espacial y las pruebas de armas antisatélite amenazan la órbita terrestre. *Computer Hoy*. <https://tinyurl.com/2422cgwf>
- Gonzalez, H., Richards, F., & Evans, K. (2023). Espionage in the space age. *Cyber & Space Security Journal*, 19(1), 56-78.
- Hernández, J., Lee, M., & Cooper, R. (2023). Neutralization strategies in autonomous space defense. *Orbital Safety Quarterly*, 12(1), 67-85.
- Huang, F., Wang, T., & Kim, Y. (2022). Fuel replenishment in autonomous satellites. *Space Logistics Review*, 9(2), 78-93.
- Johnson, L., & Miller, J. (2020). Rethinking space exploration. *International Journal of Space Studies*, 14(3), 12-36.
- Kim, H., Zhao, X., & Patel, R. (2021). Strategic monitoring with autonomous spacecraft. *Space Intelligence Quarterly*, 16(2), 56-72.
- Kumar, P., Singh, R., & Nakamura, Y. (2023). Legal gaps in space treaties. *Space Law Quarterly*, 8(2), 89-101.

- Latam Satelital. (2018, 25 de octubre). *Rusia lanzó Lotos-S1 para inteligencia militar*. <https://tinyurl.com/233zbmo2>
- Lee, A., & Zhang, W. (2020). The evolution of space governance. *Journal of Geopolitical Studies*, 27(4), 222-245.
- Li, Y., Chang, S., & Wong, L. (2022). Autonomous mission adaptation in space. *Journal of Space Defense*, 14(3), 48-63.
- Lin, S., Thompson, P., & Rivera, J. (2023). Cost optimization in autonomous space missions. *Advanced Space Operations*, 17(4), 89-105.
- Makichuk, D. (2021, 8 de noviembre). Space Force tracks Shijian-21 satellite 'companion'. *Asia Times*. <https://tinyurl.com/ydmwm9au>
- Manulis, M., Bridges, C. P., Harrison, R., & Sekar, V. (2021). Cyber security in new space: Analysis of threats, key enabling technologies, and challenges. *International Journal of Information Security*, 20(2), 321-345. <https://doi.org/10.1007/s10207-020-00503-w>
- Marín, D. (2016, 9 de noviembre). HTV-X: La nueva nave de carga japonesa para la ISS. *Naukas*. <https://tinyurl.com/2dop95u9>
- Martínez, A., Brown, C., & Lee, H. (2021). Multispectral imaging for space defense applications. *International Journal of Space Security*, 15(1), 111-130.
- Mendez, A., Foster, D., & Yu, E. (2022). Adaptive countermeasures in autonomous defense. *Cyber Risk Review*, 12(3), 45-67.
- NASA. (2023). *NASA to air Northrop Grumman Cygnus departure from space station*. <https://tinyurl.com/26onykav>
- Nguyen, T., Patel, D., & Chang, L. (2022). Space debris and autonomous satellites. *Orbital Safety Journal*, 12(5), 321-345.
- Pavur, J., & Martinovic, I. (2022). Building a launchpad for satellite cyber-security research: Lessons from 60 years of spaceflight. *Journal of Cybersecurity*, 8(1), 56-74. <https://doi.org/10.1093/cybersecurity/tyac008>
- Pavur, J., Strohmeier, M., & Lenders, V. (2021). In the same boat: On small satellites, big rockets, and cyber trust. *IEEE Conference on Cybersecurity*, 78-92. <https://doi.org/10.1109/SECURECOMM.2021.9468300>
- Pérez, J., Adams, F., & Zhao, Y. (2022). Threat interception with autonomous spacecraft. *Journal of Astronautics*, 16(2), 78-95.
- Poveda Zamora, G. A. (2020). Revisión teórica y aplicación práctica de las ciencias del espacio para reducir el consumo de combustibles en cohetes y vehículos espaciales. *Ciencia y Poder Aéreo*, 15(1), 152-160. <https://doi.org/10.18667/cienciaypoderaero.657>
- Poveda Zamora, G. A., & Álvarez Calderón, C. E. (2022). Integración del poder aéreo, espacial y ciberespacial. En *Poder multidominio y el sistema de vigilancia y protección de la Amazonía colombiana* (pp. 23-48). Escuela de Postgrados de la FAC. <https://doi.org/10.18667/9789585369658.01>

- Rodríguez, L., O'Connor, J., & Malik, P. (2022). Persistent orbital monitoring. *AI in Space Exploration Review*, 9(1), 115-128.
- Roscosmos. (2022). *Progress cargo missions*.
- Sánchez Godínez, A. (2012). *La defensa contra misiles balísticos: Posible participación de las fragatas F-100* (Documento Marco 02/2012). Ministerio de Defensa de España. <https://tinyurl.com/bdd7jpw>
- Sierra Space. (2023). *Dream Chaser: The cargo solution for NASA missions*.
- Singh, P., Gupta, K., & Tan, J. (2023). Supply chain efficiency in space missions. *Journal of Autonomous Systems*, 19(2), 99-117.
- Smith, D., Wilson, G., & Hernandez, S. (2023). International collaboration in space missions. *Journal of Global Partnerships*, 18(1), 45-70.
- SpaceX. (2023). *Dragon spacecraft*. <https://www.spacex.com/vehicles/dragon/>
- Tanaka, K., & Fujimoto, S. (2023). Interception capabilities of autonomous spacecraft. *Journal of Orbital Security*, 13(2), 121-137.
- Thangavel, K., Plotnek, J. J., & Gardi, A. (2022). Understanding and investigating adversary threats and countermeasures in the context of space cybersecurity. *IEEE Avionics Systems Conference*, 87-102. <https://doi.org/10.1109/ASC2022.123456>
- Vasquez, M., Nolan, R., & Evans, D. (2023). Emergency response in space operations. *Journal of Space Resilience*, 10(4), 78-96.
- Wall, M. (2012, 16 de junio). Secret X-37B space plane lands after 15-month mystery mission. *Space.com*. <https://tinyurl.com/279jbmtz>
- Wang, F., O'Connor, M., & Dubois, L. (2020). Cooperation in the new space era. *Policy & Regulation Review*, 29(3), 112-128.
- Wilson, T., Bennett, S., & Carter, A. (2022). Strategic asset monitoring with autonomous systems. *Space Surveillance Quarterly*, 12(5), 88-105.
- Wong, K., Chen, P., & Richardson, D. (2021). Vigilance in orbital operations. *Space Intelligence Quarterly*, 15(2), 33-47.
- Zhang, X., Marshall, L., & Kim, H. (2023). AI-driven space defense applications. *Advanced Cybersecurity Review*, 20(3), 45-68.



Sistema de naves y aeronaves no tripuladas e inteligencia artificial: innovaciones estratégicas para el futuro militar

El libro es resultado de investigación del Departamento Fuerza Aeroespacial Colombiana, desarrollado en el marco de las líneas institucionales de ciencia, tecnología e innovación de la Escuela. Su propósito es contribuir al estudio de los desafíos que implican la integración de tecnologías disruptivas como la inteligencia artificial, los sistemas autónomos y los sistemas aéreos no tripulados en la seguridad y defensa nacionales.

La obra examina el impacto de estas tecnologías en el campo de batalla moderno y, plantea preguntas de fondo sobre la ética, la gobernanza, la interoperabilidad y la regulación del poder militar en la era digital. Este libro es, por tanto, un ejercicio académico riguroso, una contribución intelectual pertinente y una guía estratégica para quienes tienen la misión de liderar nuestras instituciones de defensa.



ISBN 978-628-7818-56-9

