Revista Inteligencia Estratégica
(Revista Científica en Ciencias Sociales e Interdisciplinaria)
Volumen 2, Número 2, julio - diciembre de 2025
ISSN: 3073-0139 (en línea)
Página Web: https://revista.esici.edu.co/index.php/inest/index
Bogotá, D.C., Colombia

Desafíos de seguridad y defensa de Colombia ante UAV en conflictos modernos

Autor(es):

Diego Alejandro Prieto-Méndez
https://orcid.org/0009-0009-4787-7890
simprix20@gmail.com
Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano", Colombia

Pamela Pirateque-Perdomo
https://orcid.org/0000-0002-5993-3484
pamela.pirateque@esici.edu.co
Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano", Colombia

Citación APA: Prieto-Méndez, D. A. y Pirateque-Perdomo, P. (2025). Desafíos de seguridad y defensa de Colombia ante UAV en conflictos modernos. *Inteligencia Estratégica*, *2*(2), 137-155. https://revista.esici.edu.co/index.php/inest/article/view/26

Publicado en línea: 2025

Revista Científica INTELIGENCIA ESTRATÉGICA

Desafíos de seguridad y defensa de Colombia ante UAV en conflictos modernos

Colombia's security and defense challenges posed by UAVs in modern conflicts

Diego Alejandro Prieto-Méndez* | **Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano", Bogotá, D. C., Colombia**

Pamela Pirateque-Perdomo | **Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano", Bogotá, D. C., Colombia**

Volumen 2, Número 2, julio - diciembre de 2025, pp. 137-155
e-ISSN (3073-0139). Bogotá, D. C., Colombia
*Autor a quien se dirige la correspondencia

Resumen

La tecnología que se ha integrado en los entornos de conflictos ha dejado en claro que ofrece ventajas reales para quienes logren adaptarse con rapidez. Bajo este contexto, en el presente artículo se realizó un proceso analítico sobre los principales desafíos dentro de un enfoque de seguridad y defensa que enfrenta Colombia ante la creciente implementación de vehículos aéreos no tripulados (UAV) en escenarios de combate, tanto por actores estatales regionales como por los Grupos Armados Organizados (GAO) en el territorio nacional. De igual manera, la investigación se desarrolló mediante un enfoque cualitativo de análisis documental, basado en una revisión exhaustiva de fuentes académicas e informes técnicos. Se identificaron tres dimensiones clave: primero, el impacto geopolítico regional derivado del avance UAV en América Latina, con énfasis en la cooperación militar entre Venezuela e Irán; segundo, la caracterización de las capacidades actuales de defensa aérea colombiana frente a amenazas no convencionales; y tercero, la identificación de amenazas tecnológicas emergentes asociadas a la inteligencia artificial, la guerra electrónica y la ciberguerra.

Los resultados evidenciaron que la proliferación de estas tecnologías ha modificado el equilibrio estratégico regional y revelan limitaciones significativas en los sistemas de detección, neutralización y doctrina operativa nacional. Adicionalmente, se proyecta un escenario de alto riesgo hacia 2030 o antes, en el que grupos armados organizados podrían incorporar drones tipo Vista de Primera Persona (FPV) con capacidad

Fecha de recepción: 15/11/2025 | Fecha de aprobación: 16/02/2026

kamikaze, emulando patrones del conflicto entre Rusia y Ucrania. Este escenario, sumado al riesgo de posible transferencia tecnológica desde Venezuela, plantea una amenaza multidimensional que requiere una respuesta anticipada por parte del Estado colombiano, incluyendo inversión en capacidades antidrón, ciberdefensa, marcos normativos actualizados y control del espectro electromagnético.

Palabras clave: Vehículos aéreos no tripulados; seguridad y defensa; grupos armados organizados; conflictos asimétricos; guerra electrónica.

Clasificación JEL: O32, Q55.

Abstract

The integration of technology into conflict environments has clearly demonstrated real advantages for those capable of adapting quickly. Within this context, the present article conducted an analytical assessment of the main challenges facing Colombia in the fields of security and defense, due to the increasing deployment of Unmanned Aerial Vehicles (UAVs) in combat scenarios by both regional state actors and Organized Armed Groups operating within national territory. The research followed a qualitative approach through documentary analysis, based on an exhaustive review of academic sources and technical defense reports. Three key dimensions were identified: first, the regional geopolitical impact of UAV proliferation in Latin America, with emphasis on military cooperation between Venezuela and Iran; second, the characterization of Colombia's current air defense capabilities in response to non-conventional threats; and third, the identification of emerging technological threats related to artificial intelligence, electronic warfare, and cyberwarfare.

The findings revealed that the spread of these technologies has shifted the regional strategic balance and exposed significant limitations in Colombia's detection systems, neutralization capabilities, and operational doctrine. Additionally, a high-risk scenario is projected for 2030 or earlier, in which Organized Armed Groups could incorporate first-person view (FPV) kamikaze drones, emulating tactics observed in the Russia–Ukraine conflict. This scenario, combined with the risk of potential technological transfer from Venezuela, constitutes a multidimensional threat that demands a proactive response from the Colombian state, including investments in anti-drone capabilities, cyber defense, updated legal frameworks, and electromagnetic spectrum control.

***Keywords*:** Unmanned aerial vehicles; Security and defense; Organized armed groups; Asymmetric conflicts; Electronic warfare.

Introducción

La implementación de vehículos aéreos no tripulados (UAV) hace evolucionar la manera en que se presentan los conflictos armados del siglo XXI, al combinar tareas de reconocimiento, inteligencia y ataques de precisión. Este cambio emerge con fuerza en escenarios convencionales, como la guerra entre Rusia y Ucrania, en los que drones FPV y sistemas Bayraktar TB2 (Montoya-Roldan y Massa-Rueda, 2024), prueban su eficacia

táctica y se extiende rápidamente a América Latina. Allí, la cooperación militar entre Venezuela e Irán (Mokhtar, 2024) da origen a un programa nacional de producción de drones armados en Maracay (Bermúdez, 2022), mientras que en Colombia los Grupos Armados Organizados (GAO) adquieren drones comerciales, algunos modificados artesanalmente para la realización de actividades terroristas, lo que evidencia la magnitud y vulnerabilidad de las defensas aéreas colombianas ante amenazas asimétricas.

El objetivo de este artículo es analizar los desafíos en seguridad y defensa que enfrenta Colombia ante la implementación de UAV en escenarios de combate, tanto por parte de actores estatales regionales como por estructuras de los diferentes grupos armados organizados en el territorio nacional. La pregunta que orienta esta investigación plantea: ¿Cuáles son los principales desafíos en seguridad y defensa de Colombia ante la implementación de UAV en escenarios de combate? Al responderla, se podrá caracterizar las capacidades y vulnerabilidades en seguridad y defensa en la detección y neutralización contra UAV. Asimismo, se busca identificar otras amenazas tecnológicas emergentes y determinar el impacto geopolítico regional derivado de la proliferación de UAV. Para ello, se propone un análisis documental de fuentes académicas, informes de defensa e investigaciones, a fin de identificar el estado actual de las capacidades nacionales, las amenazas emergentes y los escenarios prospectivos al año 2030.

Diversos estudios destacan ya el carácter disruptivo de los UAV en conflictos híbridos y asimétricos (Montoya-Roldan y Massa-Rueda, 2024). Sin embargo, dentro de las investigaciones evidenciadas no se encontró información que involucra este fenómeno desde un escenario regional y nacional para Colombia. En consecuencia a lo anterior, el presente estudio se divide en tres fases: en la primera se investiga el empleo táctico de UAV en conflictos actuales; en la segunda se evalúa su penetración estratégica en América Latina con Venezuela como foco; y en la tercera se identifican los principales retos de Colombia en defensa aérea, inteligencia de señales y mitigación de amenazas internas, proyectando riesgos hasta 2030.

Metodología

Para el desarrollo de este estudio se adoptó un diseño metodológico no experimental de tipo descriptivo, en el que no se manipularon variables sino que se observó y analizó la información tal como se presentó en las fuentes documentales. Se aplicó un enfoque cualitativo, orientado a comprender en profundidad las dinámicas emergentes vinculadas al uso de UAV en escenarios de conflicto, así como sus implicaciones en la seguridad y defensa de Colombia. En primer lugar, se emplearon palabras clave como: (“UAV Colombia defensa aérea”, “drones híbridos América Latina”, “ciberguerra UAV”, etc.) para ubicar fuentes en bases de datos académicas como (Scopus, Web of Science, Google Académico), repositorios institucionales (Universidad Externado, Mindefensa) e informes periodísticos relevantes, como El Colombiano e Infodefensa, a fin de tener una visión integral y contemporánea para posteriormente realizar una revisión que integra los textos pertinentes, los cuales se organizaron para discernir y extraer la información relevante que permitió establecer el impacto geopolítico, las capacidades de defensa nacionales y las amenazas tecnológicas emergentes.

ISSN 3073-0139 (En línea)

Por otra parte, se consideraron ciertos criterios de inclusión:

1. **Tipo de Fuente:** Se tomaron bases de datos como: Google Académico; bases de datos como Scielo y Dialnet; repositorios institucionales como Universidad Externado y artículos de Mindefensa; por último, artículos periodísticos para recolectar información reciente.

2. **Idioma:** Se incluyeron documentos de investigación, tanto en español como en inglés, considerando que algunos eventos analizados ocurrieron en regiones cuyo idioma oficial no es el español.

3. **Ubicación Geográfica:** La recopilación del material académico se enfocó en publicaciones e investigaciones, tanto internacionales como nacionales, concordando con el tema en desarrollo.

4. **Nivel de acceso:** Las fuentes bibliográficas utilizadas son todas de acceso libre en línea y permiten dotar a la investigación de un carácter abierto hacia los lectores.

Marco Teórico

La óptica investigativa de Hernández-Mantilla (2021) nos dice que el término “drone” se deriva del ámbito militar, y que desde la década de 1940 estas aeronaves no tripuladas se han utilizado como plataformas de observación, ataque o apoyo logístico. Estas capacidades han evolucionado y, debido a sus características de bajo costo, movilidad, versatilidad y acceso comercial, han facilitado su expansión a conflictos convencionales y asimétricos, convirtiéndolos en una amenaza real para la seguridad estatal. Según Fernández-Chiclano et al. (2024), estos sistemas han modificado la lógica operacional tradicional al permitir acciones de inteligencia, adquisición de blancos y destrucción con bajo costo y riesgo humano. Estudios en el ámbito de la seguridad y defensa coinciden en que los UAV representan una forma de ampliar la proyección táctica sin recurrir a despliegues masivos, favoreciendo tanto a Estados como a actores irregulares (Edmonds y Bendett, 2023).

Los conflictos híbridos plantean diversos dinamismos en las guerras contemporáneas combinando variedad de tácticas convencionales, irregulares, cibernéticas y de desinformación, todo ello bajo una lógica flexible y no lineal. El término fue desarrollado ampliamente por (Hoffman, 2007), quien expresa que la guerra híbrida se define por el empleo simultáneo de múltiples métodos de enfrentamientos convencionales, insurgentes y criminales articulados por actores estatales o no estatales. En consecuencia, los UAV se convierten en capacidades diferenciales y funcionales para estos modelos de confrontación, al permitir acciones selectivas, vigilancia táctica, ataques de precisión y disrupción psicológica.

En el mismo sentido, la perspectiva de (Biddle, 2004) manifiesta que la evolución tecnológica en el ámbito militar, incluyendo el uso de capacidades aéreas no tripuladas, obliga a replantear la forma en que los ejércitos realizan sus procesos de planificación y desarrollo de operaciones. Estos conflictos no solo dependen de la superioridad

armamentista sino de la capacidad de adaptación doctrinal frente a entornos asimétricos en los que pequeños actores armados pueden ocasionar daños con impactos estratégicos y con recursos limitados.

Por otra parte, Vergara y Trama (2018) señalan que el desarrollo de estos sistemas, junto con la evolución de sensores e inteligencia artificial, ha modificado sustancialmente las capacidades del instrumento militar, especialmente en los campos de la guerra electrónica, el reconocimiento táctico y la saturación de blancos. Esta transformación convierte estos dispositivos UAV en una plataforma clave para las nuevas formas de proyección de poder, incluso en manos de actores no estatales que pueden replicar tácticas de saturación o evasión electrónica sin contar con superioridad tecnológica convencional.

Introducción al nuevo paradigma bélico y el rol de los UAV

Los vehículos aéreos no tripulados han generado una evolución en los conflictos modernos demarcando ventajas significativas de acuerdo con sus capacidades de vigilancia, ataque e impacto psicológico. Asimismo, la evolución tecnológica ha permitido que modelos comerciales sean usados en diferentes actividades militares en misiones de reconocimiento para ataques de gran precisión. En conflictos internacionales, como el de Ucrania, los UAV han ido denotando la gran capacidad para redefinir las estrategias militares, brindando ventajas en el campo de combate; no obstante, esta evolución ha puesto en evidencia las diferentes falencias en los sistemas de defensa, los cuales no están diseñados para estas amenazas emergentes (Montoya-Roldan y Massa-Rueda, 2024). Esta transición sistémica pone en evidencia la necesidad de adaptabilidad por parte de los estados en diferentes aspectos, como su doctrina militar y sistemas de defensa, para sortear con estas nuevas amenazas tecnológicas.

En el panorama actual se puede evidenciar que la evolución tecnológica en sistemas de UAV ha ganado un protagonismo hegemónico en medio del desarrollo de los conflictos armados. De acuerdo con (Fernández-Chiclano et al., 2024):

> *La reciente invasión de Rusia a Ucrania ha marcado un punto de inflexión en las formas de conflicto conocidas hasta la fecha. Se puede hablar de una nueva modalidad de guerra caracterizada por el predominio de tecnologías emergentes, donde los drones han adquirido un papel preponderante* (p. 287).

Esto indica que los países tienen la necesidad de realizar una evolución adaptativa en el uso de tecnologías disruptivas, que no sólo redefinen el combate, sino que también plantean nuevos desafíos estratégicos y éticos.

El conflicto Rusia-Ucrania

La invasión rusa a Ucrania se convirtió en el primer conflicto convencional en el que los UAV determinaron resultados tácticos. Ucrania empleó drones FPV (First Person View) modificados con cargas explosivas para atacar blindados rusos, logrando una relación costo-eficiencia de 1:140 frente a sistemas tradicionales (Mary, 2024). Los Bayraktar TB2 demostraron su utilidad en la destrucción de columnas logísticas; estos sistemas, según

Montoya-Roldan y Massa-Rueda (2024), son "un dron turco de combate que se convirtió en un elemento fundamental para realizar ataques precisos contra objetivos estratégicos rusos" (p. 11). En consecuencia, las afectaciones tuvieron un daño significativo en capacidades y además realizaron un impacto psicológico en las fuerzas invasoras.

En el conflicto ruso-ucraniano la modernización de la guerra se ha denotado como un factor determinante para obtener ventajas tanto tácticas como estratégicas, debido al rol de los vehículos aéreos no tripulados (UAV), donde estos pasaron de adoptar un papel de observadores para erigirse en elementos disruptivos con un impacto decisivo en el desarrollo del conflicto, "lo que comenzó con drones comerciales adaptados para misiones de reconocimiento y ataque, evolucionó rápidamente hacia un programa organizado con apoyo gubernamental y colaboración internacional", derivando la conformación del proyecto "Ejército de Drones" (Barón, 2025, párr. 1-2). Este conflicto ilustra de manera palpable las significativas ventajas tácticas y estratégicas que el despliegue ingenioso de los UAV puede conferir a una nación en estado de guerra, generando afectaciones estratégicas a bajo costo.

La adaptación ucraniana de drones FPV con cargas explosivas ejemplificó una innovación táctica trascendental. Según Singer y Brooking (2018), la proliferación de tecnologías de bajo costo con capacidad de causar daños significativos redefine la guerra asimétrica. En el contexto ucraniano, la relación costo-eficiencia de 1:140 frente a sistemas de armas convencionales permitió a una nación con recursos limitados infligir pérdidas sustanciales al adversario, contrarrestando la superioridad numérica rusa en blindados (Mary, 2024).

Los sistemas *Bayraktar TB2* de fabricación turca se consolidaron como herramientas tácticas de gran valor para Ucrania. Su capacidad para ejecutar ataques con alto grado de exactitud contra objetivos de gran valor estratégico rusos, como señalan Bendett y Edmonds (2022) en un análisis para el Center for Naval Analyses (CNA), desarticuló nodos logísticos esenciales, interrumpió líneas de suministro y neutralizó puestos de mando cruciales. Esta precisión minimizó los daños colaterales y maximizó el impacto operativo, erosionando la capacidad rusa para mantener su ofensiva.

La difusión mediática de imágenes y videos de ataques exitosos con drones desde ambos frentes tuvo un impacto significativo en la percepción pública a nivel mundial. Esto no solo demostró la resistencia y la capacidad de adaptación entre las partes, sino que también logró impulsar el apoyo militar, financiero y político por parte de la comunidad internacional (Nye, 2004).

El despliegue de capacidades de los UAV obligó a ambas partes a redefinir sus estrategias y la disposición de sus fuerzas. Las capacidades de reconocimiento aéreo y ataques certeros desde el aire requirieron la implementación de medidas de dispersión, camuflaje y el desarrollo de defensas aéreas específicas. Esta necesidad de adaptación estratégica impactó en la velocidad y la naturaleza de las operaciones militares de ambos bandos. Biddle (2004) argumenta cómo las innovaciones tecnológicas, incluida la vigilancia aérea (un precursor de las capacidades de los UAV), pueden alterar fundamentalmente la forma en que se planifican y ejecutan las operaciones militares,

obligando a los actores a reconsiderar sus doctrinas y tácticas.

Regionalización de la Amenaza, el avance de los UAV en América Latina

En Latinoamérica, el entorno geopolítico regional en el que países como "Argentina, Chile, República Dominicana, Ecuador, Perú, Uruguay y Venezuela, todos poseen aviones no tripulados y se encuentran trabajando en el desarrollo de su propia tecnología" (Cawley, 2014, párr. 4). Por consiguiente, se revela un interés cada vez mayor en desarrollo y compra de UAV con capacidades progresivamente más avanzadas, esto ha permitido evidenciar que "la inversión en tecnología de drones se vuelve más relevante en América Latina. Las áreas de mayor crecimiento están relacionadas con la protección fronteriza, sistemas tácticos de vigilancia y sistemas inhibidores de drones" (Vasconez, 2024, párr. 14). Esta demanda abre las puertas a una carrera en capacidades tecnológicas con fines en seguridad y defensa que, en algunos casos, los diferentes Estados han contado con el respaldo de potencias extranjeras.

Lipin (2022) menciona que Venezuela ha establecido una asociación militar significativa con Irán, que incluye la creación de una instalación de producción de drones y la formación de personal venezolano en técnicas de ensamblaje y operación de UAV. Esta alianza estratégica en tecnología de estos dispositivos, desde el año 2007 (párr. 5), ha permitido que Venezuela se posesione como el primer país latinoamericano en desplegar drones armados que han sido utilizados incluso en operaciones contra el GAO residual en el área de la frontera colombo-venezolana (Bermúdez, 2022). Lo anterior ha despertado preocupaciones legítimas en materia de equilibrio estratégico y proyección de amenazas transfronterizas por la ubicación geoestratégica de Venezuela, su capacidad de producción y el historial de cooperación con actores irregulares.

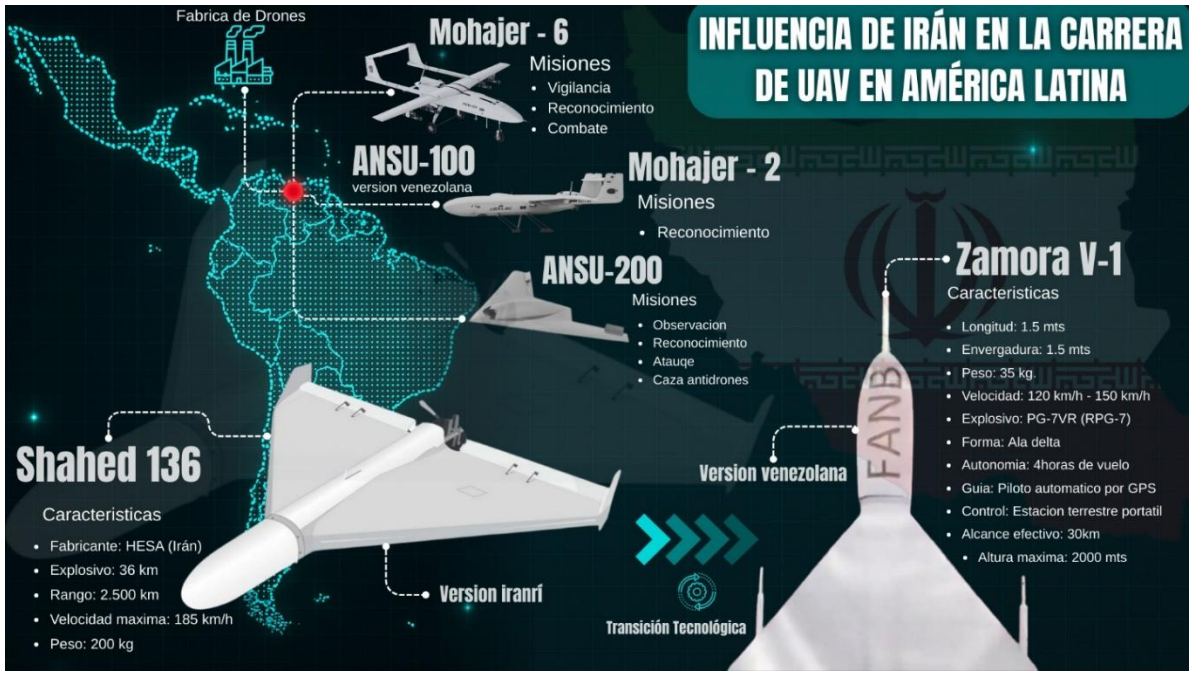
> *En una entrevista concedida al diario The New York Times, y publicada el 21 de febrero de 2019 -poco después de hacer público su respaldo el presidente encargado de Venezuela, Juan Guaidó- el mayor general del Ejército Hugo Carvajal Barrios, conocido con el alias de "El Pollo", relató algunos episodios sobre narcotráfico, terrorismo y actividades con la guerrilla en Venezuela* (InSight Crime, 2019, párr. 2).

Lo anterior, aunado a la presencia del GAO Ejército de Liberación Nacional (ELN) en la frontera colombo-venezolana y su expansión en territorio venezolano (InSight Crime, 2025), configura un posible puente facilitador de tecnología UAV hacia estos grupos en territorio colombiano. Esta hipótesis adquiere mayor fuerza si se considera la creciente evidencia de que estos grupos ya han utilizado drones de tipo comercial para labores de inteligencia delictiva y materialización de acciones terroristas. Dado el bajo costo, la facilidad de adaptación y el uso creciente de drones FPV y kamikaze en conflictos como el de Ucrania, se proyecta como altamente plausible que hacia el año 2030 estas estructuras criminales puedan integrar drones de ataque en sus operaciones contra unidades de la Fuerza Pública e infraestructura crítica. La convergencia de intereses geopolíticos, el avance tecnológico regional y la evolución táctica de los GAO configuran un escenario de riesgo que requiere atención inmediata desde la planeación de defensa nacional.

ISSN 3073-0139 (En línea)

En consecuencia, desde la perspectiva geopolítica regional se evidenció que diferentes países en la región Latinoamericana han fortalecido sus capacidades militares mediante la adquisición y producción de UAV, en algunos casos con el respaldo de potencias extrarregionales como Irán, con especial énfasis en el caso venezolano, estableciendo una fábrica de drones armados en Maracay, Estado Aragua, lo que configura un cambio en el equilibrio estratégico regional y plantea un riesgo potencial para la seguridad fronteriza de Colombia (Bermúdez, 2022; Mokhtar, 2024). Lo anterior se puede evidenciar de la siguiente forma:

Figura 1. Infografía influencia extrarregional de Irán



Fuente: elaboración propia, con datos tomados de (Bermúdez, 2022; Luchetta, 2024)

De este modo se logra observar la transferencia tecnológica materializada en la fabricación local de sistemas como el Mohajer-2, Mohajer-6 y su adaptación nacional ANSU-100, todos con capacidades de vigilancia y reconocimiento. Esta cooperación ha permitido a Venezuela no solo adquirir plataformas avanzadas como el Shahed 136, sino también desarrollar modelos propios como el ANSU-200 y el Zamora V-1, con misiones orientadas al ataque y la interdicción aérea.

Teniendo en cuenta lo anterior, la presencia iraní no solo puede representar un factor de rearme tecnológico, sino también un cambio en el equilibrio estratégico regional, al facilitar la proyección de capacidades ofensivas que podrían emplearse en escenarios de presión geopolítica o disuasión regional. Para Colombia, esta evolución supone una amenaza latente sobre su frontera oriental, particularmente en términos de vigilancia aérea, superioridad táctica local y potenciales escenarios de conflicto asimétrico con medios de origen no convencional.

Vulnerabilidades y capacidades de Colombia ante amenazas aéreas no convencionales

En consecuencia, la carrera evolutiva por parte de los diferentes países de la región en estas capacidades plantea una preocupación legítima para la defensa nacional como resultado de la propagación de estas tecnologías que también podrían alterar los equilibrios de poder de los Estados y exponer vulnerabilidades en el sistema de defensa aérea del país. Colombia ha buscado tener un enfoque adaptativo en cuanto a defensa aérea en el que las amenazas no convencionales, como los vehículos aéreos no tripulados (UAV), han comenzado a adquirir un rol cada vez más protagónico, donde el conflicto interno ha obligado la implementación de dispositivos denominados antidrones, especialmente en el departamento del Cauca (Semana.com, 2024); esto ha permitido minimizar las afectaciones de las tropas, principalmente en las bases fijas o bases semimóviles.

Habitualmente, las capacidades de vigilancia aérea del país han centrado su enfoque más al monitoreo del espacio aéreo con el fin de detectar vuelos irregulares vinculados al narcotráfico y el contrabando, implementando el uso de radares convencionales y control aéreo. Sin embargo, estas herramientas presentan limitaciones significativas frente a los drones, "debido a que estos módulos son pequeños y pueden volar a baja altura resultando difíciles de detectar, pudiendo atacar los costosos Sistemas de Defensa Aérea que quedarían anulados ante la imposibilidad de advertir un ataque" (Allende, 2017, p. 197). De modo que el bajo perfil térmico y la reducida firma de radar, características comunes en UAV de pequeño y mediano tamaño, tanto comerciales como modificados para uso militar representan una amenaza que permite replantear las capacidades en Defensa Aérea colombiana.

La Tabla 1 presenta la caracterización de los radares actualmente operativos en Colombia que permite comprender las fortalezas y vacíos existentes frente a amenazas aéreas emergentes, como el uso de UAV por parte de actores estatales y no estatales. En la siguiente tabla se resumen los principales sistemas radar desplegados tanto en el ámbito militar como civil, diferenciando sus capacidades, limitaciones técnicas y tipo de cobertura, lo cual resulta clave para evaluar el nivel de preparación del país ante escenarios de conflicto asimétrico y de defensa aérea.

Tabla 1. Caracterización de radares en Colombia

Nombre del radar o sistema	Tipo / Categoría	Principales capacidades	Limitaciones (frente a UAV)
AN/TPS-78	Radar 3D táctico móvil de largo alcance.	Cobertura de ~450 km; detección 3D de aeronaves; resistente a interferencias electrónicas.	Limitada eficacia contra UAV pequeños de baja cota y firma radar reducida.
AN/TPS-70	Radar 3D móvil de largo alcance.	Cobertura ~440 km; rastreo de ~500 objetivos; incluye sistema IFF.	Dificultad para detectar drones de bajo perfil y vuelo rasante.
AN/TPS-43	Radar 3D móvil (generación anterior).	Cobertura ~400 km; detección tridimensional de largo alcance.	Tecnología más antigua, menor capacidad frente a drones modernos.
TADER	Radar 3D táctico móvil (fabricación nacional).	Detección de aeronaves a baja altura; alcance ~40–75 km; movilidad táctica.	Alcance limitado; requiere despliegue puntual; no diseñado para enjambres.

ISSN 3073-0139 (En línea)

Radar Primario (PSR) - Aerocivil	Radar primario fijo de vigilancia aérea civil.	Detección de objetos no cooperativos en áreas terminales (~60–150 km).	Cobertura parcial en vuelos bajos; vulnerable a objetos pequeños no detectables.
Radar Secundario (SSR) - Aerocivil	Radar secundario fijo de control aéreo (modo S).	Identificación y seguimiento de vuelos con transpondedor hasta ~450 km.	Depende de respuesta del transpondedor; ineficaz ante UAV no cooperativos.

Fuente: Elaboración propia, con datos tomados de (Aeronáutica Civil de Colombia, 2023; Fuerza Aeroespacial colombiana, 2015; Saumeth, 2017)

En los últimos años, los Grupos Armados Organizados (GAO), como el ELN, GAO residual y Clan del Golfo, han implementado drones comerciales a su accionar (Rodríguez-Álvarez, 2024). Estos drones son empleados tanto para la realización de actividades de inteligencia delictiva (vigilancia y reconocimiento) como de ataque y terrorismo, representando una nueva dimensión en el conflicto armado. "Para Jorge Restrepo, investigador del Centro de Recursos para el Análisis de Conflictos, el uso masificado de drones por parte de los GAO significaría un salto de capacidad militar enorme para estos grupos ilegales" (Swissinfo.ch, 2024, párr. 21).

Los GAO vienen implementando principalmente drones comerciales de tipo quadcóptero disponibles en el mercado; estos dispositivos, relativamente pequeños (generalmente de menos de 2 kg) y de fácil adquisición, han facilitado su incorporación a las acciones terroristas. Algunos modelos específicos identificados en incautaciones y ataques incluyen:

Tabla 2. Caracterización de drones empleados por los GAO en Colombia

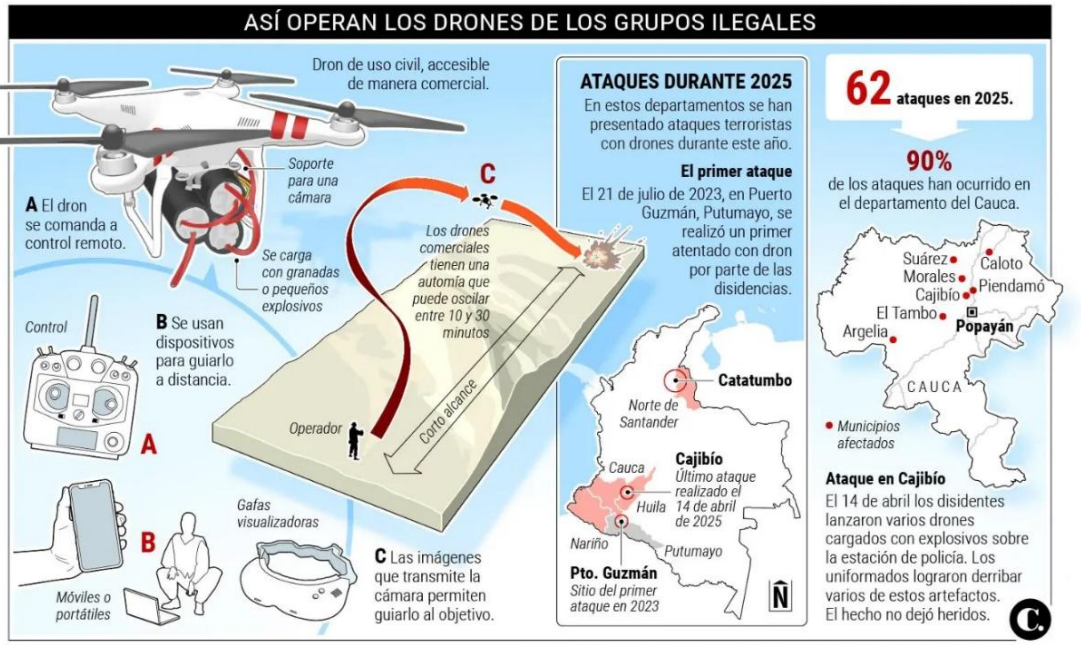
Nombre del dron	Tipo de uso	Origen / Fabricación	Capacidades	Limitaciones
DJI Mavic 3 Thermal	Reconocimiento / Ataque nocturno.	Comercial (China).	Cámara térmica y diurna, vuelo nocturno, precisión media.	Costoso, vulnerable a interferencias.
DJI Mini 4 Pro	Reconocimiento / Ataques con carga ligera.	Comercial (China).	Ultracompacto, portátil, carga útil moderada.	Alcance limitado, baja resistencia al viento.
DJI Phantom / Mavic (otros)	Vigilancia / Ataque artesanal.	Comercial (China).	Cámaras HD, GPS, fácil adquisición.	Fácilmente detectables, modificables artesanalmente.
Drones adaptados con explosivos	Terrorismo / Sabotaje.	Comercial modificado.	Carga útil de hasta 4 kg, alcance corto.	Imprecisos, vulnerables a contramedidas.

Fuente: Elaboración propia, con datos tomados de (Patiño, 2025b; Saumeth, 2024)

En el mismo sentido se logra evidenciar que el uso de drones comerciales por parte de los GAO, además de ser de fácil adquisición y manipulación, representa una herramienta de alta efectividad para realizar ataques a corta y media distancia. Su capacidad para transportar cargas explosivas y realizar vigilancia en tiempo real ha

incrementado significativamente el impacto en el accionar de estos grupos (Patiño, 2025b). Esta tecnología les permite ejecutar ataques con mayor precisión, sorpresa y alcance, como se evidencia en la siguiente ilustración:

Figura 2. Accionar delictivo de los GAO mediante el uso de drones comerciales



Fuente: Tomado de Patiño (2025b)

Esta modalidad refleja una evolución preocupante en las capacidades ofensivas por parte de los GAO, que aprovechan vacíos tecnológicos y doctrinales del Estado para desarrollar métodos asimétricos de alto impacto. La creciente frecuencia, adaptabilidad y precisión de estos ataques convierte a los drones en una herramienta efectiva de afectación, terror y sabotaje, y exige una respuesta urgente desde los niveles de defensa, inteligencia y regulación.

Si bien la mayoría de casos evidenciados en Colombia han involucrado drones convencionales que suelen soltar una carga explosiva sobre el objetivo, existe no obstante preocupación por una eventual evolución o implementación en el uso de drones de tipo vista de primera persona, o conocidos por su sigla en inglés FPV (First Person View), adaptados con explosivos. En conflictos como Ucrania se han visto drones FPV cargados de explosivos impactando objetivos a alta velocidad (drones suicidas o Kamikaze) (Cervantes-Zárate, 2024). Hasta el momento, los GAO aún están mayormente usando drones de tipo comercial estándar con adaptaciones artesanales, no sistemas FPV sofisticados. Sin embargo, no se descarta que estén explorando esta modalidad en razón a interceptaciones de comunicaciones que denotan su interés por adquirir drones de distintos precios y características (Patiño, 2025b).

En consecuencia, las Fuerzas Militares colombianas han incorporado ciertos

ISSN 3073-0139 (En línea)

sistemas de vigilancia y neutralización de UAV; sin embargo, persisten limitaciones técnicas significativas, especialmente frente a drones de bajo perfil térmico, vuelo rasante y difícil detección. Informes institucionales han documentado la insuficiencia de los radares convencionales para rastrear estos dispositivos, así como la necesidad urgente de expandir la cobertura antidrón en zonas críticas, como el departamento del Cauca, donde la actividad de los Grupos Armados Organizados (GAO) ha estado acompañada del uso de plataformas no tripuladas (Allende, 2017; Cuesta, 2024).

Estas limitaciones evidencian que, si bien existen avances puntuales, la defensa aérea colombiana aún enfrenta restricciones estructurales y tecnológicas para adaptarse a amenazas no convencionales. La carencia de sistemas multidominio que integren sensores pasivos, inhibidores electrónicos y cobertura automatizada representa un obstáculo para responder eficazmente a entornos asimétricos y dinámicos. En este sentido, caracterizar las capacidades actuales permite visualizar el grado de preparación y los ajustes necesarios para proyectar una defensa aérea adaptable y eficaz hacia el año 2030.

Identificación de amenazas tecnológicas emergentes vinculadas a UAV en Colombia

En el dominio de la ciberguerra, los UAV representan tanto un medio de ataque susceptible a hackers como posibles plataformas de intrusión empleadas por actores delictivos. Por un lado, los drones modernos dependen de sistemas de control remoto, enlaces inalámbricos (radiofrecuencia, Wi-Fi) y navegación GPS; todos estos componentes pueden ser vulnerados vía ciberataques. Expertos en seguridad advierten que la "piratería con drones" o la piratería de proximidad pretende un uso más allá de la vigilancia o apoyo militar; ahora, más que nunca, los drones comerciales se ciernen como una de las grandes amenazas cibernéticas; ya es una realidad con el alcance, capacidades y precios de los drones comerciales actuales (Castro-Valencia, 2022; Peña Suárez, 2023).

De igual forma, desde 2022 empresas de ciberseguridad alertan sobre casos de drones usados para hackear redes Wi-Fi corporativas, capturando datos sensibles tras superar barreras físicas mediante sobrevuelo remoto, convirtiendo una especie de ciberamenaza aérea (Scoblete, 2022). Laboratorios como Kaspersky han pronosticado que esta técnica de intrusión crecerá, permitiendo a delincuentes desplegar dispositivos para interceptar comunicaciones o inyectar malware, sin necesidad de contacto físico con la red víctima (Castro-Valencia, 2022), de esta manera incrementan el nivel evolutivo en las amenazas emergentes que pueden ser empleadas por actores estatales y no estatales hacia organizaciones militares o infraestructura crítica del Estado, como se ha podido evidenciar en Ucrania y Estados Unidos (Moreland, 2025).

En Colombia, la ciberdelincuencia por medio de drones aún no ha protagonizado incidentes de alto perfil conocidos públicamente, pero las Fuerzas Militares y de seguridad anticipan el riesgo. En particular, el aumento en el uso de drones por los diferentes grupos armados obliga a considerar escenarios de interferencia remota o sabotaje cibernético. Por otra parte, la proliferación de drones hostiles ha convertido al espectro electromagnético en un campo de batalla crucial en Colombia. La guerra electrónica (EW), entendida como el uso ofensivo/defensivo del electromagnetismo para negar ventajas al adversario (Cataldo-Soto, 2023; Nieto, 2023), es en la actualidad un eje central para enfrentar a los

UAV de grupos armados. Neutralizar un dron en pleno vuelo suele requerir técnicas de interferencia de señal (jamming) o incluso engaño (spoofing). Las Fuerzas Militares colombianas han tenido que adaptarse rápidamente ante los ataques con drones; soldados en el terreno improvisaron disparándoles para derribarlos, sin embargo, este método es poco fiable contra dispositivos pequeños y maniobrables y por ello, en el año 2024, se aceleró la adquisición de sistemas antidrón electrónicos. A finales de ese año, la Gobernación del Cauca entregó al Ejército los primeros ocho inhibidores de drones (jammers) adquiridos con una inversión de 7.500 millones de pesos (Cuesta, 2024), permitiendo de esta manera contrarrestar algunos ataques con drones principalmente en bases fijas.

No obstante, la guerra electrónica contra drones presenta desafíos significativos dentro del contexto colombiano. Gran parte de las acciones ocurren en entornos rurales y selváticos, donde el componente militar carece a veces de cobertura tecnológica robusta, dada la falta de infraestructura; esto representa un desafío operativo de gran envergadura para las Fuerzas Militares. Los inhibidores o radares antidrón suelen ser costosos y requieren energía, mantenimiento y personal capacitado. En áreas aisladas dentro de un entorno rural, su despliegue logístico puede ser limitado, lo que deja lagunas de vulnerabilidad aprovechables por los grupos armados. Además, integrantes del GAO residual han hecho volar estos dispositivos a mayor altura para salir del rango efectivo de los inhibidores terrestres, eligiendo el modelo de dron comercial DJI Mini 4 Pro, siendo este el más utilizado por este grupo debido a sus características técnicas (Patiño, 2025a). Aparte de emplear estos dispositivos a gran altura, también pueden recurrir a navegación preprogramada (waypoints GPS) para que el dron siga su ruta aun si se bloquea la señal de radio desde el operador, permitiendo incrementar el grado de dificultad ante la superioridad en guerra electrónica de la Fuerza Pública.

Por último, la integración de inteligencia artificial en vehículos aéreos no tripulados (UAV) se pensó desde el inicio como una herramienta la cual facilitara el análisis de información o la automatización de sistemas en actividades de vigilancia; sin embargo, ha evolucionado hacia aplicaciones más complejas, incluyendo la autonomía operacional, el reconocimiento de patrones en tiempo real y la toma de decisiones sin intervención humana. Herrera (2025), señala que estos dispositivos han sido desplazados hacia roles estratégicos que incluyen la conducción de operaciones militares de forma autónoma, lo que posiblemente representa riesgos significativos en términos de control y responsabilidad operativa.

Del mismo modo, Pinzón (2025) destaca que los drones modernos, como el Northrop Grumman MQ-4C Tritón, ya se despliegan con capacidad para ejecutar tareas previamente programadas de Vigilancia, Inteligencia y Reconocimiento (ISR). De igual forma, Matiz-Rojas y Fernández-Camargo (2023) explican que los avances actuales permiten a estos sistemas no solo identificar objetivos, sino también tomar decisiones tácticas autónomas, lo que implica una nueva reconfiguración de los medios y métodos de confrontación tecnológica en escenarios bélicos demarcando una ventaja táctica y estratégica a los Estados al reducir la dependencia de factores humanos en el uso de estos dispositivos, lo que representa una amenaza latente en términos de guerra electrónica y ciberguerra ofensiva (Cano-Cuevas, 2023; Herrera, 2025).

Conclusiones

De forma general, los resultados de esta investigación evidencian que la proliferación y adaptación de sistemas UAV en la región representan una amenaza creciente y multidimensional para la seguridad y defensa colombiana. Estas amenazas no solo responden a desarrollos tecnológicos acelerados, sino también a nuevas configuraciones geopolíticas, vacíos doctrinales y la capacidad de actores híbridos para apropiarse de tecnologías avanzadas. El estudio permitió observar cómo el fenómeno de los drones ya no es exclusivo de potencias militares, sino que se ha descentralizado, afectando directamente la seguridad del Estado desde múltiples flancos.

En cumplimiento del primer objetivo, se determinó que el impacto geopolítico regional derivado de la proliferación de UAV se materializa en un cambio progresivo del equilibrio estratégico en América Latina. La cooperación entre Venezuela e Irán en materia de transferencia tecnológica, ensamblaje local y despliegue de drones armados configura un escenario de presión regional que trasciende lo convencional. Esta alianza ha dotado a Venezuela de una capacidad diferencial en la región, lo que incrementa la vulnerabilidad de Colombia, especialmente en su frontera oriental, al facilitar condiciones para escenarios de disuasión, vigilancia avanzada o conflicto asimétrico.

Respecto al segundo objetivo, se caracterizó el estado actual de las capacidades de defensa aérea colombiana, evidenciándose limitaciones técnicas importantes en la detección y neutralización de UAV, particularmente de bajo perfil térmico y vuelo rasante. Aunque existen esfuerzos institucionales para mejorar la vigilancia aérea y la adquisición de sistemas antidrón, aún persisten vacíos estructurales que impiden una respuesta integral frente a amenazas dinámicas y de naturaleza híbrida. Esto exige el fortalecimiento de la interoperabilidad tecnológica, la ampliación de coberturas y la actualización doctrinal orientada al enfrentamiento de estos medios no convencionales.

En cuanto al tercer objetivo, se identificaron amenazas tecnológicas emergentes vinculadas a la inteligencia artificial, la guerra electrónica y la ciberguerra, todas con alto potencial de ser explotadas tanto por actores estatales regionales como por estructuras armadas híbridas presentes en Colombia. Se observó que los UAV comerciales pueden ser modificados con software autónomo, sensores avanzados y funciones evasivas para evadir radares y contramedidas electrónicas. Además, la ausencia de una regulación clara sobre el uso ofensivo de IA en sistemas militares y el rezago en capacidades de ciberdefensa refuerzan la necesidad de diseñar un marco normativo y operativo adaptado a estas amenazas. La creciente capacidad de los GAO para incorporar estos desarrollos plantea un riesgo que trasciende lo táctico y entra en la dimensión estratégica de la seguridad nacional.

A modo de cierre estratégico, la revisión permitió establecer que uno de los escenarios de mayor riesgo para Colombia es la posible adopción de drones FPV, incluidos modelos kamikaze por parte de los Grupos Armados Organizados, siguiendo patrones observados en el conflicto entre Rusia y Ucrania. Esta evolución táctica, altamente probable hacia el año 2030 o antes, podría otorgar a los GAO una capacidad ofensiva sin

precedentes a bajo costo, afectando infraestructura crítica y posiciones militares en zonas de difícil acceso o incluso en áreas urbanas. A esto se suma el riesgo de posible transferencia tecnológica en territorio venezolano, país que con apoyo de Irán ha desarrollado una capacidad local de ensamblaje y producción de UAV armados. Esta combinación de factores configura una amenaza de carácter asimétrico, regionalizada y tecnológicamente avanzada, que exige del Estado colombiano una anticipación estratégica sostenida, inversión en capacidades antidrón, ciberdefensa y control del espectro electromagnético.

Referencias

Aeronáutica Civil de Colombia. (10 de mayo de 2023). *La Aeronáutica Civil publica los pliegos definitivos para la adquisición de siete nuevos sistemas de vigilancia aeronáutica.* www.aerocivil.gov.co. https://aerobarranquilla.aerocivil.gov.co/publicaciones/4206/la-aeronautica-civil-publica-los-pliegos-definitivos-para-la-adquisicion-de-siete-nuevos-sistemas-de-vigilancia-aeronautica/

Allende, W. (2017). Drones. La siguiente guerra en Escuela Superior Técnica - Centro de Estudios de Prospectiva Tecnológica Militar Gral. Enrique Mosconi (CEPTM) (Eds.), *TEC1000 2017: estudios de vigilancia y prospectiva tecnológica en el Área de Defensa y Seguridad* (1a ed. Ampliada, pp. 193-212). Centro de Estudios de Prospectiva Tecnológica Militar de Argentina. https://cefadigital.edu.ar/handle/1847939/1673

Barón, D. (1 de marzo de 2025). *Drones e inteligencia artificial: cómo fue la estrategia de Ucrania utilizada en el conflicto con Rusia*. Defonline.com.ar. https://defonline.com.ar/ciencia-tecnologia/drones-e-inteligencia-artificial-como-fue-la-estrategia-de-ucrania-utilizada-en-el-conflicto-con-rusia/

Bendett, S. y Edmonds, J. (7 de junio de 2022). *Russian military autonomy in Ukraine: four months in*. Centro de Análisis Navales (CAN). https://www.cna.org/analyses/2022/07/russian-military-autonomy-in-ukraine-four-months-in

Bermúdez, Á. (30 de noviembre de 2022). *Cómo Venezuela se convirtió con la ayuda de Irán en el "único país latinoamericano que cuenta con drones armados"*. British Broadcasting Corporation (BBC) - BBC News Mundo. https://www.bbc.com/mundo/noticias-america-latina-63670715

Biddle, S. (2004). *Military power: explaining victory and defeat in modern battle*. Princeton University Press. https://doi.org/10.1515/9781400837823

Cano-Cuevas, D. F. (2023). *La inteligencia artificial en el postacuerdo colombiano : el caso de los drones de combate para operaciones sostenidas contra grupos armados organizados* [Tesis de maestría, Universidad Externado de Colombia]. Repositorio institucional.

Castro-Valencia, V. (15 de noviembre de 2022). *Hackeo con drones y ataques satelitales, nuevas amenazas cibernéticas en 2023*. Eltiempo.com. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/hackeo-con-drones-y-ataques-satelitales-nuevas-amenazas-ciberneticas-717726#:~:text=Pirater%C3%ADa%20con%20drones

Cataldo-Soto, C. (2023). Análisis de la Función de Combate Guerra Electrónica en (Centro de Estudios Estratégicos CEEAG) (Eds.), *Dimensión terrestre del conflicto ruso-ucraniano 2022, perspectiva rusa* (pp. 313-348). Centro de estudios estratégicos de la Academia de Guerra Ejército de Chile. https://publicacionesacague.cl/index.php/tica/issue/view/35

Cawley, M. (18 de abril de 2014). *El uso de drones en Latinoamérica: riesgos y oportunidades*. Insightcrime.org. https://insightcrime.org/es/noticias/analisis/el-uso-de-drones-en-latinoamerica-riesgos-y-oportunidades/

Cervantes-Zárate, S. (2024). Leyes internacionales de guerra en materia de drones, mercenarios y plantas nucleares, en la guerra ruso-ucraniana. *Revista de Ciencia e Investigación en Defensa -CAEN*, *5*(3), 41-65. https://doi.org/10.58211/2q8wew81

Cuesta, A. M. (27 de diciembre de 2024). *Entregan primeros inhibidores de drones en el Cauca para enfrentar ataques de grupos armados*. Eltiempo.com. https://www.eltiempo.com/justicia/conflicto-y-narcotrafico/entregan-primeros-inhibidores-de-drones-en-el-cauca-para-enfrentar-ataques-de-grupos-armados-3412737

Edmonds, J. A. y Bendett, S. (2023). *Russia's Use of Uncrewed Systems in Ukraine*. Centro de Análisis Navales (CNA). https://www.cna.org/analyses/2023/05/russias-use-of-drones-in-ukraine

Fernández-Chiclano, R., Giner-Alegría, C. A. y Durán-Rodríguez, R. A. (2024). Unmanned aerial vehicles: factor decisivo en el conflicto bélico de Ucrania. *Estudios en Seguridad y Defensa*, *19*(38), 285-302. https://doi.org/10.25062/1900-8325.4875

Fuerza Aeroespacial colombiana. (20 de agosto de 2015). *Comandante de la FAC anunció adquisición de nuevos radares para regiones estratégicas del país*. Webinfomil – fac.mil.co. https://www.fac.mil.co/es/noticias/comandante-de-la-fac-anuncio-adquisicion-de-nuevos-radares-para-regiones-estrategicas-del

Hernández-Mantilla, H. S. (2021). Seguridad aérea de las unidades militares: prevención frente a drones utilizados con fines terroristas. *Revista Pensamiento estratégico y seguridad CISDE*, *6*(1), 11-24. https://uajournals.com/ojs/index.php/cisdejournal/article/view/791

Herrera, M. (2025). La intersección entre inteligencia artificial y armas nucleares: riesgos, beneficios, y recomendaciones. *Revista UNISCI,* (67), 87-109.

https://dialnet.unirioja.es/servlet/articulo?codigo=10017704
https://doi.org/10.31439/UNISCI-221

Hoffman, F. G. (2007). *Conflict in the 21st Century: the rise of hybrid wars*. Potomac Institute for Policy Studies.

InSight Crime. (22 de febrero de 2019). *Exjefe de inteligencia de Venezuela revela vínculos con el crimen organizado*. Insightcrime.org. https://insightcrime.org/es/noticias/analisis/exjefe-de-inteligencia-de-venezuela-revela-vinculos-con-el-crimen-organizado/

InSight Crime. (2025). *Ejército de Liberación Nacional (ELN) en Venezuela*. Insightcrime.org. https://insightcrime.org/es/noticias-crimen-organizado-venezuela/eln-en-venezuela/

Lipin, M. (25 de abril de 2022). *Aparente suministro de drones de combate de Irán a Venezuela destaca riesgos del terrorismo*. Dialogo-americas.com. https://dialogo-americas.com/es/articles/aparente-suministro-de-drones-de-combate-de-iran-a-venezuela-destaca-riesgos-del-terrorismo/

Luchetta, J. (13 de abril de 2024). *Las Fuerzas Armadas Bolivarianas de Venezuela apuestan a la producción de un dron de ataque copia del iraní Shahed 131/136*. zona-militar.com. https://www.zona-militar.com/2024/04/13/las-fuerzas-armadas-bolivarianas-de-venezuela-apuestan-a-la-produccion-de-un-dron-de-ataque-copia-del-dron-irani-shahed-131-136/

Mary, G. (22 de abril de 2024). *El Impacto de los drones en la guerra moderna*. Pucará Defensa. https://www.pucara.org/post/el-impacto-de-los-drones-en-la-guerra-moderna

Matiz-Rojas, A. H. y Fernández-Camargo, J. A. (2023). Sobre el uso de la inteligencia artificial como medios y métodos en los conflictos armados. *Revista Científica General José María Córdova*, *21*(42), 525-549. https://doi.org/10.21830/19006586.1151

Mokhtar, A. (2024). Latin America: A new market for Iranian drones. *Journal for Iranian Studies*, *8*(19), 63-79. https://rasanah-iiis.org/english/wp-content/uploads/sites/2/2024/06/Latin-America-A-New-Market-for-Iranian-Drones.pdf

Montoya-Roldan, D. y Massa-Rueda, D. (24 de julio de 2024). *Drones en la Vanguardia: Tecnologías Avanzadas redefiniendo la Guerra Moderna* [Sesión de conferencia]. XVII Congreso - GT 8.3 La adaptación del sector de la seguridad a los nuevos desarrollos tecnológicos, Asociación española de ciencia política y de administración. https://aecpa.es/es-es/drones-en-la-vanguardia-tecnologias-avanzadas-redefiniendo-la-guerra/congress-papers/4279/

Moreland, S. (2025). Rogues with Robots: Malign Actors and Drones in an Age of Hybrid Conflict. *Global ECCO journal (CTX)*, 22-31. https://nps.edu/web/ecco/-/rogues-with-robots-malign-actors-and-drones-in-an-age-of-hybrid-conflict?utm_source=chatgpt.com

Nieto, Ignacio. (2023). *¿Por qué lo llamas ciber cuando quieres decir guerra electrónica?* Global Strategy. Report, 9/2023. https://global-strategy.org/por-que-lo-llamas-ciber-cuando-quieres-decir-guerra-electronica/

Nye, J. S. (2004). *Soft power: the means to success in world politics*. PublicAffairs.

Patiño, J. P. (17 de abril de 2025a). *Enjambres de drones: la nueva estrategia de guerra de las disidencias de las Farc*. CambioColombia.com. https://cambiocolombia.com/conflicto-armado-en-colombia/articulo/2025/4/conflicto-armado-disidencias-farc-ejercito-cauca-drones-explosivos/

Patiño, J. P. (20 de abril de 2025b). *Así es como las disidencias han perfeccionado los ataques con drones, ¿el Gobierno está preparado?* ElColombiano.com. https://www.elcolombiano.com/colombia/disidencias-han-perfeccionado-los-ataques-con-drones-PC27168575

Peña Suárez, J. S. (2023). Ciberseguridad, un desafío para las Fuerzas Militares colombianas en la era digital. *Perspectivas en Inteligencia, 15*(24), 333-359. https://doi.org/10.47961/2145194X.628

Pinzón, D. E. (9 de diciembre de 2025). *Reportan que imponente dron estadounidense de vigilancia, inteligencia y reconocimiento atravesó el espacio aéreo frente a la costa venezolana.* Ntn24.com. https://www.ntn24.com/noticias-actualidad/reportan-que-imponente-dron-estadounidense-de-vigilancia-inteligencia-y-reconocimiento-atraveso-el-espacio-aereo-frente-a-la-costa-venezolana-594631

Rodríguez-Álvarez, S. (21 de mayo de 2024). *Drones en conflicto colombiano: militares se preparan para nueva amenaza*. La silla vacía. https://www.lasillavacia.com/silla-nacional/drones-en-conflicto-colombiano-militares-se-preparan-para-nueva-amenaza/

Saumeth, E. (23 de marzo de 2017). *La Fuerza Aérea colombiana incorporará el radar Tader de Codaltec el 29 de marzo*. Infodefensa.com. https://www.infodefensa.com/texto-diario/mostrar/3077672/fuerza-aerea-colombiana-incorporara-radar-tader-codaltec-29-marzo

Saumeth, E. (5 de agosto de 2024). *Las FARC emplean drones con cámaras térmicas para atacar al Ejército colombiano*. Infodefensa.com. https://www.infodefensa.com/texto-diario/mostrar/4951519/140-colombia-farc-emplean-drones-camaras-termicas

Scoblete, G. (31 de octubre de 2022). *Wi-Fi Spy Drones Are Hacking Corporate Networks*. core.verisk.com. https://core.verisk.com/Insights/Emerging-Issues/Articles/2022/October/Week-5/Wi-Fi-Spy-Drones-Are-Hacking-Corporate-Networks

Semana.com. (28 de julio de 2024). *Entre 60.000 y 100.000 dólares cuestan los antidrones que busca comprar el Ejército para frenar ataques de las disidencias de las Farc*. https://www.semana.com/nacion/articulo/entre-60000-y-100000-dolares-cuestan-los-antidrones-que-busca-comprar-el-ejercito-para-frenar-ataques-de-las-disidencias-de-las-farc/202403/#google_vignette

Singer, P. W. y Brooking, E. T. (2018). *Likewar: the weaponization of social media*. Houghton Mifflin Harcourt.

Swissinfo.ch. (22 de junio de 2024). *Drones con explosivos, la nueva arma de los disidentes de las FARC en Colombia*. https://www.swissinfo.ch/spa/drones-con-explosivos%2C-la-nueva-arma-de-los-disidentes-de-las-farc-en-colombia/81450792

Vasconez, J. D. (26 de septiembre de 2024). *El mercado de drones en América Latina: dónde invertir*. UAV latam.com. https://uavlatam.com/el-mercado-de-drones-en-america-latina-donde-invertir/

Vergara, E. y Trama, G. A. (2018). *Operaciones militares cibernéticas: Planeamiento y ejecución en el nivel operacional*. Escuela Superior de Guerra Conjunta de las Fuerzas Armadas de Argentina – CEFA Digital. https://cefadigital.edu.ar/handle/1847939/939

ISSN 3073-0139 (En línea)

Revista Inteligencia Estratégica
(Revista Científica en Ciencias Sociales e Interdisciplinaria)
Volumen 2, Número 2, julio - diciembre de 2025
ISSN: 3073-0139 (en línea)
Página Web: https://revista.esici.edu.co/index.php/inest/index
Bogotá, D.C., Colombia

Desafíos de seguridad y defensa de Colombia ante UAV en conflictos modernos

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo.

Financiamiento

Los autores no declaran fuente de financiamiento para la realización de este artículo.

Sobre el/los autor(es)

Diego Alejandro Prieto-Méndez es Estudiante de Gerencia de la Seguridad y Análisis Sociopolítico de la Institución Universitaria Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano" (Colombia), es Tecnólogo en Administración y Análisis de la Seguridad de la Institución Universitaria Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano" (Colombia).
https://orcid.org/0009-0009-4787-7890 - Contacto: simprix20@gmail.com

Pamela Pirateque-Perdomo es Estudiante de Doctorado en Estado de Derecho y Gobernanza Global de la Universidad de Salamanca (España), es Magister en Inteligencia Estratégica de la Institución Universitaria Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano" (Colombia), es profesional en Política y Relaciones Internacionales de la Universidad Sergio Arboleda (Colombia), es investigadora científica del grupo de investigación CIGA categorizada Junior en Minciencias, y asesora del Departamento de Ciencia, Tecnología, Investigación y Doctrina (DECTID) de la Institución Universitaria Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano", es docente universitaria de catedra.
https://orcid.org/0000-0002-5993-3484 - Contacto: pamela.pirateque@esici.edu.co