Estrategia de Defensa para Bases Militares en Colombia: Protección ante Ataques con Aeronaves No Tripuladas (Drones) por Actores Armados Ilegales

Mayor (EJC) Edier Gustavo Manrique Coronado

Artículo para optar al título profesional:

Magister en Seguridad y Defensa Nacionales

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

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

DATOS GENERALES		
Nombre del estudiante	**:**	Mayor (EJC) Edier Gustavo Manrique Coronado
Identificación	**:**	6.663.476
Programa académico	**:**	Maestría en Seguridad y Defensa Nacionales
Tutor metodológico	**:**	Henry Mauricio Acosta Guzmán
Tutor temático	**:**	Nelson Enrique Carvajal Chisco
Fecha de entrega	**:**	26 de agostó de 2025
Extensión	**:**	

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

El autor declara que este artículo fue escrito de acuerdo con la normatividad de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) y no existe ningún potencial conflicto de interés relacionado con este. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representan la posición oficial ni institucional de la ESDEG, las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.

Este artículo es enteramente mi propio trabajo y no ha sido presentado para la obtención de un título en esta u otra Institución de Educación Superior. Se han referenciado todos los trabajos y puntos de vista de otros autores, así como los datos de otras fuentes utilizadas. No se emplearon herramientas de generación de contenido por Inteligencia Artificial para su elaboración.

El autor acepta ceder los derechos de publicación en favor de la ESDEG y su Sello Editorial de acuerdo con los términos de la licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.

AUTORIZACIÓN DE PUBLICACIÓN

El autor autoriza que este articulo sea publicado por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto.

Estrategia de Defensa para Bases Militares en Colombia: Protección ante Ataques con Aeronaves No Tripuladas (Drones) por Actores Armados Ilegales.

Defense Strategy for Military Bases in Colombia: Protection against Unmanned Aircraft (Drone) Attacks by Illegal Armed Actors.

Edier Gustavo Manrique Coronado[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El uso militar de aeronaves no tripuladas se remonta a 1849 y ha evolucionado significativamente desde la Segunda Guerra Mundial hasta convertirse en una herramienta clave en los conflictos asimétricos actuales. En Colombia, las disidencias de las FARC han comenzado a emplear drones modificados para realizar ataques, lo que representa una amenaza creciente para la seguridad nacional. Esta tecnología, accesible y difícil de detectar, ha transformado la naturaleza del combate, obligando a los Estados a adaptar sus estrategias defensivas. Aunque el Derecho Internacional Humanitario regula el uso de armamento en conflictos, no existe aún una normatividad específica sobre drones. La expansión de esta tecnología, impulsada por avances en mecatrónica, informática y telecomunicaciones, plantea desafíos legales, éticos y operativos. Ante este panorama, la presente investigación busca proponer una estrategia de defensa para las bases militares de Colombia frente a ataques con drones, mediante un enfoque cualitativo y exploratorio, apoyado en análisis documental de fuentes relevantes.

Palabras clave: Actores Armados Ilegales Drones, Defensa Nacional, Estrategia, Seguridad Nacional

[1] Mayor del Ejército Nacional de Colombia. Estudiante de Maestría en Seguridad y Defensa Nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. https://orcid.org/0009-0006-8980-3265- Contacto: Edier.Manrique@esdeg.edu.co.

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

Abstract: The military use of unmanned aircraft dates back to 1849 and has evolved significantly since World War II to become a key tool in today's asymmetric conflicts. In Colombia, FARC dissidents have begun using modified drones to carry out attacks, posing a growing threat to national security. This accessible and difficult-to-detect technology has transformed the nature of combat, forcing states to adapt their defensive strategies. Although international humanitarian law regulates the use of weapons in conflict, there are still no specific regulations on drones. The expansion of this technology, driven by advances in mechatronics, information technology, and telecommunications, poses legal, ethical, and operational challenges. Given this scenario, this research seeks to propose a defense strategy for Colombian military bases against drone attacks, using a qualitative and exploratory approach, supported by documentary analysis of relevant sources.

Keywords: Illegal Armed Actors, Drones, National Defense, Strategy, National Security

Introducción

El uso de aeronaves no tripuladas en el ámbito bélico tiene una historia que se remonta a mediados del siglo XIX. En 1849, el Imperio Austriaco lanzó globos aerostáticos cargados con explosivos sobre Venecia, marcando uno de los primeros intentos documentados de emplear tecnología aérea no tripulada con fines militares (Gregory, 2011). Desde entonces, los conflictos armados han impulsado el desarrollo de estas tecnologías. Durante la Segunda Guerra Mundial, los aliados y el Eje trabajaron en prototipos de aviones no tripulados, y en la Guerra de Vietnam, EE. UU. empleó drones Firebee para reconocimiento y misiones de señuelo (Singer, 2009).

El concepto de aeronaves no tripuladas (VANT) tiene sus raíces en desarrollos militares del siglo XIX, comenzando con el uso de globos aerostáticos por el ejército austrohúngaro en 1849. A lo largo del siglo XX, los drones evolucionaron a partir de plataformas rudimentarias de reconocimiento a sistemas altamente sofisticados. Durante la Guerra de Vietnam, Estados Unidos empleó los drones Firebee como señuelos y dispositivos de reconocimiento (Singer, 2009). El desarrollo de la informática, la inteligencia artificial y las telecomunicaciones en las décadas de 1990 y 2000 impulsó la "segunda era de los drones", caracterizada por su capacidad autónoma, precisión quirúrgica y expansión de uso civil y militar (ONU, 2020).

La evolución tecnológica ha permitido que tanto Estados como grupos armados ilegales accedan a drones con capacidad ofensiva, esta transformación ha sido impulsada por una reducción en los costos de producción, la comercialización de partes en mercados

abiertos, y la falta de regulaciones internacionales específicas que limiten su venta (UNODA, 2019).

Es de resaltar que los drones armados han sido incorporados a doctrinas militares en conflictos asimétricos donde se busca reducir el riesgo para las tropas propias y aumentar la precisión de los ataques, ejemplo de ello es que países como Estados Unidos, Israel, Rusia, Irán y Turquía han liderado su uso en operaciones antiterroristas y enfrentamientos interestatales, sin embargo, su proliferación también ha facilitado su empleo por parte de grupos insurgentes y criminales.

En Colombia, grupos armados organizados como disidencias de las FARC y el ELN han adaptado drones comerciales para lanzar explosivos, ejecutar vigilancia y evadir los sistemas de defensa tradicionales (Noticias Caracol, 2024). Este fenómeno es parte de una tendencia global, como se ha observado en el uso de drones por parte de ISIS en Irak y Siria, inclusive en la guerra entre Ucrania y Rusia, donde han sido esenciales para ataques de precisión de bajo costo (RAND, 2023).

En el ámbito civil, su uso abarca desde la entrega de medicamentos en zonas rurales hasta la vigilancia de cultivos. No obstante, también han sido adoptados por actores no estatales, incluidos grupos narcotraficantes y organizaciones armadas ilegales. El grupo Estado Islámico (ISIS), por ejemplo, ha empleado drones modificados para lanzar explosivos en conflictos en Irak y Siria (BBC, 2017). En América Latina, Colombia ha sido uno de los países donde el uso no convencional de drones por parte de grupos armados organizados ha encendido alarmas.

Según *The Global Intelligence Files* de WikiLeaks, desde el año 2006 Colombia utilizó drones ScanEagle, provistos por Estados Unidos, para operaciones de vigilancia contra grupos armados ilegales (WikiLeaks, 2013). Recientemente, informes del año 2024 documentan el uso de drones armados por disidencias de las FARC y otros grupos armados organizados, que han adaptado drones comerciales para lanzar granadas y otros explosivos, como se evidenció en ataques en los departamentos del Cauca y Arauca (Noticias Caracol, 2024).

Esta situación plantea desafíos muy importantes para la seguridad nacional, pues expertos como Erich Saumeth y el Coronel retirado Jaime Ariza han resaltado que estos ataques representan un cambio en la dinámica del conflicto armado colombiano, en el que las organizaciones ilegales están recurriendo a tácticas cada vez más asimétricas y sofisticadas (Semana, 2024).

En complemento de lo anterior, el uso de drones como ya se dijo genera una preocupación, debido a la capacidad y habilidades de los grupos armados organizados para adaptar técnicas modernas de combate con recursos de bajo costo y alto impacto estratégico. Estas organizaciones han avanzado en una fase de modernización tecnológica, adoptando el uso de aeronaves no tripuladas como armas de guerra, al tiempo que el aparato estatal ha enfrentado limitaciones presupuestarias que han reducido su capacidad operativa, debilitado la inteligencia militar y dejado fuera de servicio parte importante de su flota aérea.

Durante el periodo del cese al fuego bilateral ordenado por el gobierno nacional, las organizaciones criminales aprovecharon la suspensión de operaciones ofensivas para reorganizarse y fortalecer su estructura. Según informes de inteligencia, este contexto fue utilizado por grupos como el Estado Mayor Central, la Segunda Marquetalia, el ELN y el Clan del Golfo para aumentar su capacidad armamentística, expandir su presencia territorial y adoptar nuevas tácticas de combate, entre ellas el uso de drones armados. En mayo de 2023, se documentó una reunión en zona rural de Cartagena del Chaira (Caquetá), liderada por Iván Mordisco, donde participaron cabecillas de varias estructuras armadas ilegales con el objetivo de incorporar el uso ofensivo de drones en sus operaciones (Semana, 2024).

Durante esta reunión, técnicos procedentes de la frontera con Venezuela entrenaron a combatientes seleccionados en el uso de drones comerciales modificados con fines bélicos. Se utilizaron ocho dispositivos básicos para instruir a los integrantes en el pilotaje, carga de explosivos y liberación remota de artefactos mediante sistemas diseñados en 3D. Esta transferencia de conocimiento sentó las bases para expandir el uso de drones entre los distintos frentes armados, replicando tácticas similares a las observadas en el conflicto entre Ucrania y Rusia.

Adicionalmente, se evidenció que estos grupos han desarrollado manuales internos donde se especifican tres finalidades principales para el uso de drones:

1. Realizar vigilancia aérea para recolectar información sobre movimientos y ubicación de tropas
2. Ejecutar ataques aéreos precisos mediante la liberación de explosivos

3. Proteger sus áreas de control anticipando las maniobras del Ejército.

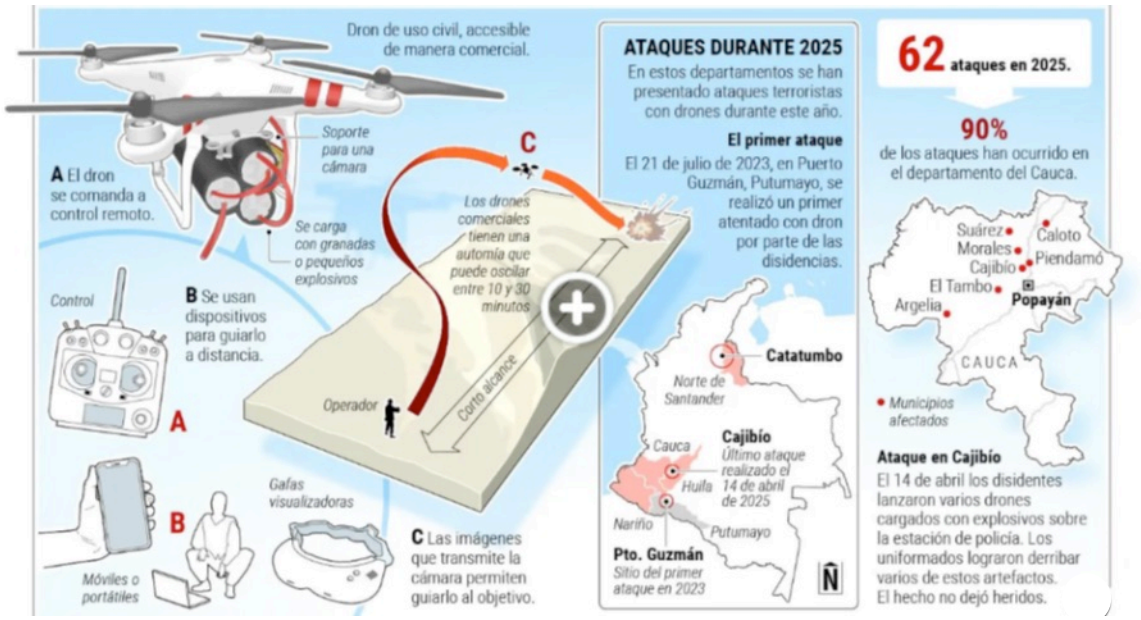
Esta nueva táctica ha permitido a las disidencias realizar exploración táctica de sus enemigos, optimizando tiempo y recursos, y mejorando su capacidad de respuesta y defensa territorial. Los informes de inteligencia revelan que las disidencias han desarrollado dispositivos caseros explosivos adaptados a drones, utilizando cilindros con metralla (tornillos, balines, tuercas, etc.), suspendidos por ganchos metálicos y liberados mediante controles remotos. Estas armas han sido empleadas especialmente en el departamento del Cauca, una de las zonas con mayor presencia de estos grupos (Semana, 2024). Entre mayo y junio de 2024, se registraron al menos 16 ataques con drones en esta región, resultando en varios militares heridos en municipios como Argelia y Suárez.

En paralelo, se ha constatado que otras estructuras criminales, como la Segunda Marquetalia, también han incorporado drones en sus operaciones, incluso para actividades de extorsión. En un operativo realizado en Belén de los Andaquíes (Caquetá) en febrero de 2024, se incautaron tres drones con estas características, asociados a alias "John Tiempos", cabecilla financiero de esta organización.

Estos hallazgos indican que el uso de drones se ha consolidado como una herramienta táctica clave entre los grupos armados ilegales en Colombia, lo que representa un desafío urgente para las capacidades de defensa del Estado. La ausencia de medidas efectivas de contrainteligencia y detección de estas amenazas ha facilitado su expansión, particularmente en zonas donde la presencia del Estado es limitada. La experiencia reciente evidencia la necesidad de actualizar las doctrinas de seguridad y desarrollar estrategias

defensivas tecnológicas capaces de neutralizar estas nuevas formas de agresión (Semana, 2024). https://www.semana.com/nacion/justicia/articulo/los-drones-de-la-muerte-semana-revela-los-secretos-de-la-nueva-y-peligrosa-estrategia-de-guerra-de-las-disidencias-de-las-farc-hay-alarma-por-la-seguridad-nacional/202443/

Figura 1. *Operación de drones terroristas en el territorio nacional*



Nota: Operación de drones terroristas (El Colombiano, 2024) https://www.semana.com/nacion/justicia/articulo/los-drones-de-la-muerte-semana-revela-los-secretos-de-la-nueva-y-peligrosa-estrategia-de-guerra-de-las-disidencias-de-las-farc-hay-alarma-por-la-seguridad-nacional/202443/

Ahora bien, es de resaltar que, en el plano normativo, el Derecho Internacional Humanitario (DIH) aún no regula de manera específica el uso de drones, aunque los principios generales de distinción, proporcionalidad y precaución siguen siendo aplicables (CICR, 2021). Los artículos 35 y 36 del Protocolo Adicional I de 1977 a los Convenios de

Ginebra establecen criterios sobre los medios y métodos de combate, lo cual incluye indirectamente a los drones.

Frente a esta amenaza creciente, las Fuerzas Militares de Colombia enfrentan el reto de diseñar estrategias de defensa antiaérea y ciberdefensa adaptadas a este nuevo tipo de riesgo. Esto implica desarrollar capacidades para detectar, interceptar y neutralizar drones de bajo costo, con perfiles de vuelo bajos y comportamiento errático, lo cual no es tarea sencilla. Se requiere la integración de tecnologías como radares de corto alcance, inhibidores de señal (jammers), sistemas de interferencia electromagnética, y dispositivos de captura como redes aéreas (RAND, 2023).

Teniendo en cuenta lo anterior, como referente teórico, se toma a Ortiz (2023) y su documento titulado "Análisis del Estado de ciberseguridad en las organizaciones colombianas y la efectividad de las políticas gubernamentales de seguridad digital" donde resalta que la ciberseguridad se constituye como una rama de la seguridad informática que se enfoca específicamente en la protección del ciberespacio. Su objetivo principal es disminuir los riesgos asociados a la información manejada en diversas plataformas y dispositivos, concentrándose en su procesamiento, almacenamiento y transmisión. Además de salvaguardar los datos, la ciberseguridad permite cumplir con normativas legales aplicables a distintos sectores, siendo esencial para mantener la continuidad operativa de las organizaciones al mitigar amenazas cibernéticas. Como señala Manrique, los principios fundamentales para proteger los activos informáticos incluyen la disponibilidad**,** que garantiza el acceso solo a usuarios autorizados; la integridad**,** que busca evitar alteraciones o daños a la información; y la confidencialidad**,** que previene su divulgación no autorizada

(Ortiz, 2023). A continuación, se referencian los mecanismos de seguridad ciber y su respectiva descripción:

Tabla 1. *Mecanismos Ciber*

Mecanismo	Descripción
Seguridad de la información	• Confidencialidad • Integridad • Disponibilidad
Seguridad de las aplicaciones	• Procesos • Componentes • Software • Resultados • Datos
Seguridad de la red	• Diseño • Implementación • Operación
Seguridad de Internet	• Servicios en internet seguro • Redes • Disponibilidad de servicios • Fiabilidad de servicios
Seguridad en la infraestructura	• Datacenter • Condiciones ambientales • Acceso Físico • Sitios Alternos

Nota: Mecanismos ciber. Tomado de Ortíz (2023).

Por lo anterior la tesis de la presente investigación sostiene que el uso de drones armados por parte de grupos armados organizados en Colombia representa una amenaza emergente y en rápida evolución para la seguridad nacional, debido a su bajo costo, accesibilidad tecnológica y capacidad de causar daño significativo con alta precisión. Este fenómeno, facilitado por vacíos normativos, limitaciones operativas del Estado y la creciente sofisticación de actores ilegales, requiere una respuesta integral del Estado

colombiano que articule estrategias de defensa, ciberseguridad, actualización normativa y cooperación internacional para contrarrestar eficazmente este nuevo método de guerra asimétrica.

Teniendo en cuenta lo anterior, se ha propuesto la siguiente pregunta de investigación

¿Cuál debe ser la principal estrategia de defensa que debe implementar las bases militares de las Fuerzas Militares de Colombia para la protección de ataques de Aeronaves No Tripuladas (Dron) que están siendo implementadas por actores armados ilegales? Para responder a este interrogante, inicialmente se realizará una categorización de medidas preventivas y reactivas para la protección de las bases militares frente a ataques con aeronaves no tripuladas (drones) teniendo en cuenta tecnologías y tácticas, seguido de ello se determinará el impacto de las normativas internacionales y locales sobre el uso de drones en el ámbito militar, analizando el empleo para a la de bases militares y finalmente se diseñará una estrategia para la protección de las bases militares contra los ataques con aeronaves no tripuladas (drones).

Metodología

La investigación se desarrolló bajo un enfoque cualitativo, ya que se buscó comprender e interpretar el fenómeno del uso de drones por parte de las disidencias de las FARC y su impacto en las estrategias de seguridad y defensa implementadas por las Fuerzas Militares de Colombia. Este enfoque permitió analizar un fenómeno complejo en

su contexto natural, proporcionando una visión profunda desde una perspectiva contextual y flexible (Hernández, Fernández & Baptista, 2014).

El diseño metodológico adoptado fue de tipo exploratorio y descriptivo. La exploración resultó esencial debido a la escasa investigación existente sobre el empleo de drones por parte de grupos armados ilegales en el contexto colombiano. Por su parte, el enfoque descriptivo permitió caracterizar las tácticas asociadas a este tipo de ataques, así como sus consecuencias operativas y estratégicas para la seguridad nacional (Sampieri, Collado & Lucio, 2018).

Para la recolección de información, se utilizó la técnica del análisis documental, mediante el cual se revisaron diversas fuentes secundarias. Estas incluyeron informes oficiales del Ministerio de Defensa y la Policía Nacional, comunicados de prensa de las Fuerzas Militares, artículos académicos especializados, reportes de organismos multilaterales y think tanks como la Fundación Ideas para la Paz (FIP) e Insight Crime, además de notas periodísticas de medios reconocidos como Noticias Caracol y El Espectador. Esta técnica permitió recopilar evidencia empírica y discursiva relevante, sin incurrir en riesgos propios del trabajo de campo en contextos de conflicto (Flick, 2015).

La selección documental se llevó a cabo a través de un muestreo no probabilístico por conveniencia, basado en la disponibilidad, actualidad y pertinencia temática de los documentos. Se priorizaron fuentes publicadas entre 2015 y 2024, de carácter institucional o académico, que aportaran información detallada sobre el uso de vehículos aéreos no

tripulados (UAV) por parte de actores armados y su impacto en las operaciones militares del Estado colombiano (Patton, 2002).

Lo anterior, permitió construir una comprensión crítica sobre la evolución del conflicto armado en Colombia y la adaptación de los grupos ilegales al entorno tecnológico global. Esta investigación pretende contribuir al análisis académico del fenómeno, así como también ofrecer insumos para la formulación de políticas públicas orientadas a la protección de instalaciones estratégicas y a la actualización doctrinal de la defensa nacional.

Medidas preventivas y reactivas para la protección de las bases militares frente a ataques con aeronaves no tripuladas (drones) teniendo en cuenta tecnologías y tácticas

Para abordar esta parte, importante resaltar que el Gobierno de Colombia ha implementado un plan integral para contrarrestar amenazas de ataques con drones, con el objetivo de salvaguardar infraestructuras críticas y espacios estratégicos como instalaciones militares, redes de energía y centros poblados. Lo anterior con una inversión superior a los 20.000 millones de pesos, que el Ministerio de Defensa Nacional ha destinado para fortalecer las capacidades operativas de las Fuerzas Militares y de Policía mediante sistemas diseñados para detectar y neutralizar drones utilizados ilegalmente por grupos criminales (Presidencia de la República, 2024)

En 2024 se registraron 115 incidentes de ataques con drones, principalmente perpetrados por organizaciones armadas ilegales y terroristas, afectando tanto a

uniformados como a infraestructuras estratégicas. Bajo este panorama, el Gobierno ha diseñado una estrategia que posiciona a Colombia como pionera en la región en el uso de tecnologías anti-drones. Al respecto, la Fuerza Aeroespacial Colombiana lidera la implementación de una hoja de ruta especializada que garantiza el despliegue eficiente y sostenible de estos sistemas, con un enfoque de economías de escala, transferencia tecnológica y proyectos de uso dual que también benefician sectores civiles como la agricultura, el medio ambiente y la gestión de desastres (Red Noticias, 2024).

El ex ministro de Defensa Iván Velásquez se ha referido a lo anterior como que "El sistema anti-drones es una muestra del compromiso del Gobierno nacional con la innovación tecnológica y la defensa de la soberanía. Esta inversión no solo refuerza nuestra seguridad nacional, sino que posiciona a Colombia como referente regional en la lucha contra amenazas emergentes". Con esta iniciativa, el Gobierno busca responder de manera efectiva a los desafíos globales y asegurar un entorno más seguro, optimizando los recursos disponibles y reforzando la seguridad de las infraestructuras más sensibles del país.

Además de lo anterior, hay que decir que el Ejército Nacional de Colombia ha desarrollado un programa de capacitación especializado para fortalecer las capacidades operativas de oficiales, suboficiales y soldados en la detección, identificación, neutralización y mitigación de amenazas provenientes de sistemas de aeronaves no tripuladas (UAS). Esta iniciativa responde al creciente uso de drones por parte de grupos armados ilegales para realizar ataques y labores de inteligencia contra la fuerza pública y la población civil.

Otra iniciativa corresponde a la formación liderada por el Comando de Educación y Doctrina del Ejército Nacional, en este aspecto se ha buscado capacitar al personal en identificación, uso de drones, y el objetivo es que el personal se convierta en multiplicadores del conocimiento adquirido, capacitando a otros miembros de la institución en todo el país (Matta, 2025).

Además, el Ministerio de Defensa Nacional ha implementado una estrategia integral para contrarrestar las amenazas de ataques con drones, incluyendo la adquisición de sistemas avanzados de defensa contra estos dispositivos. Estos sistemas están diseñados para detectar y neutralizar drones utilizados ilegalmente por grupos criminales, con el fin de salvaguardar infraestructuras críticas y espacios estratégicos como instalaciones militares, redes de energía y centros poblados (Ministerio de Defensa Nacional, 2024)

En complemento de lo anterior, hay que mencionar que la Dirección de Proyección de Capacidades e Innovación del Ministerio de Defensa desempeña un papel crucial en la modernización y fortalecimiento de las capacidades de la Fuerza Pública, coordinando la implementación de un modelo de planeación y desarrollo de capacidades, y trabajando estrechamente con las Fuerzas Militares y la Policía Nacional para elaborar conceptos operacionales adaptados a las amenazas actuales (Política de Ciencia y Tecnología, 2024).

En este contexto, la Fuerza Aeroespacial Colombiana también ha fortalecido su capacidad operativa mediante la formación de operadores de drones tácticos, en virtud de ello. la Escuela Básica de Aeronaves Remotamente Piloteadas ha desarrollado cursos especializados para capacitar a sus integrantes en el uso de drones para el desarrollo de misiones de seguridad e inteligencia. Como ya se ha mencionado anteriormente, estas

acciones reflejan el compromiso del Gobierno Nacional con la innovación tecnológica y la defensa de la soberanía, posicionando a Colombia como referente regional en la lucha contra amenazas emergentes (FAC, 2025).

Ahora, pese a que el gobierno ha tomado medidas como las que ya se mencionaron anteriormente, hay que hacer hincapié en que el uso de drones por parte de Grupos Armados Organizados representa una transformación táctica en el conflicto interno colombiano, generando riesgos más complejos para las Fuerzas Militares. Estos vehículos aéreos no tripulados (VANT) han pasado de ser herramientas tecnológicas de uso comercial o recreativo a convertirse en plataformas de ataque aéreo improvisado. Las disidencias de las FARC, el ELN y otras estructuras criminales los han adaptado para lanzar explosivos sobre instalaciones militares y patrullas, lo que representa una amenaza asimétrica altamente preocupante.

El principal riesgo del uso de estos artefactos, radica en la capacidad para evadir sistemas de defensa tradicionales pues a diferencia de ataques convencionales, los drones pueden operar de forma remota, silenciosa y a baja altura, lo que dificulta su detección con radares militares convencionales (Saumeth, 2023).

Además, estos dispositivos son económicos y de fácil adquisición en el mercado, lo cual reduce la necesidad de grandes recursos logísticos por parte de los grupos armados, en este sentido, la adaptabilidad de la tecnología civil para fines militares genera un desafío adicional para las Fuerzas Armadas, que requieren altos niveles de innovación para contrarrestar amenazas de bajo costo pero alto impacto (Schneider, 2020).

Ahora bien, desde un enfoque estratégico, los drones usados por los GAO alteran la dinámica del enfrentamiento territorial toda vez que permiten extender el radio de acción ofensivo de estos grupos sin exponer a sus integrantes, lo cual incrementa su capacidad de intimidación. Este tipo de ataques compromete no solo a las unidades militares en terreno, sino también a la infraestructura crítica del Estado (puestos policiales, bases militares, y redes eléctricas), afectando la gobernabilidad en zonas de presencia limitada del Estado.

En resumen de lo anterior, el uso de drones por parte de los Grupos Armados Organizados representa una transformación significativa en las dinámicas del conflicto armado, especialmente para las Fuerzas Militares que tradicionalmente han enfrentado amenazas más convencionales. En la actualidad, estos dispositivos han sido adaptados como armas de ataque directo o de reconocimiento, lo que ha alterado los esquemas de seguridad, vigilancia y defensa, generando nuevos desafíos operacionales y estratégicos.

En complemento, es importante mencionar los riesgos a los que se enfrentan las Fuerzas Militares y uno de ellos es el elemento sorpresa y la capacidad de evadir detección, pues los drones comerciales, fácilmente adaptables para uso ofensivo, pueden volar a baja altura y con escasa firma térmica o sonora, dificultando su detección mediante radares tradicionales. Esto permite ataques precisos y repentinos sobre puestos militares, patrullas o infraestructura crítica. Tal como lo señala el *Centro de Estudios Estratégicos Internacionales* (CSIS, 2022), "los drones armados están permitiendo a grupos insurgentes cambiar las reglas del combate al acceder a capacidades antes reservadas a fuerzas estatales" (CSIS, 2022).

Además, los ataques con drones fragmentan la seguridad del personal militar, ya que pueden ocurrir inclusive en zonas donde se presumía estabilidad territorial, por ejemplo, el ataque con drones a unidades militares en el departamento del Cauca en 2024, que dejó varios soldados heridos, revela una clara capacidad de penetración por parte de estos grupos criminales. Esta capacidad genera una presión adicional sobre las operaciones militares, ya que deben reforzar la defensa de múltiples instalaciones de forma permanente, incrementando los costos logísticos y el desgaste de tropas.

Otro riesgo importante es la asimetría tecnológica inversa, tradicionalmente el Estado ha sido quien posee ventaja tecnológica; sin embargo, la masificación y bajo costo de los drones ha democratizado su acceso, permitiendo que actores no estatales los adquieran y los modifiquen fácilmente. Investigaciones como la de Boulanin et al. (2020) del *Stockholm International Peace Research Institute* (SIPRI), alertan que "los drones comerciales armados representan un reto creciente para las fuerzas militares, no solo por su uso ofensivo, sino por su capacidad de vigilancia, lo que compromete la seguridad táctica y estratégica de las tropas" (SIPRI, 2020).

Por último, el uso de drones implica una amenaza simbólica y psicológica, en este aspecto los GAO emplean esta tecnología para mostrar poder, sofisticación y capacidad de causar daño sin necesidad de combate directo. Esto puede erosionar la moral de las tropas, generar temor en las poblaciones y afectar la percepción de control por parte del Estado. El impacto psicológico de estos ataques es similar al efecto de las minas antipersona o los francotiradores: inhiben el movimiento, restringen la operación y aumentan el estrés operativo.

En concordancia con lo anterior, hay que hacer precisión en que los Grupos Armados Organizados han evolucionado en sus tácticas mediante el uso de nuevas tecnologías que les permiten expandir su accionar sin depender exclusivamente de métodos tradicionales. Entre estas tecnologías se destacan los drones, sistemas de comunicaciones cifradas, redes sociales y mecanismos de geolocalización, lo que ha permitido transformar el conflicto armado hacia una dimensión híbrida donde confluyen lo militar, lo informático y lo psicológico.

Esta transformación tecnológica responde a una racionalidad estratégica: maximizar el impacto operativo con los menores riesgos posibles. El acceso a drones, por ejemplo, no requiere de una industria propia ni del apoyo de estados externos, como sí ocurre en otros conflictos internacionales. En Colombia, estas tecnologías se adquieren a través del mercado informal, contrabando o incluso donaciones indirectas canalizadas desde redes transnacionales (Ariza, 2024).

El uso de redes sociales y plataformas digitales también se ha intensificado por parte de estos grupos, no solo como mecanismo de propaganda sino como herramienta para inteligencia de fuente abierta (OSINT). Analizan movimientos de las Fuerzas Armadas, identifican actores vulnerables y divulgan mensajes de intimidación para generar desestabilización.

Además, la integración de sistemas GPS y softwares de planificación ha sido reportada en operaciones de narcotráfico y minería ilegal. Estas tecnologías permiten a los GAO coordinar rutas seguras, anticiparse a operativos militares y asegurar territorios

estratégicos sin necesidad de enfrentamientos constantes, lo que representa una ventaja considerable frente a los métodos tradicionales de guerra de guerrillas.

Respecto a lo anterior, es importante mencionar también que la innovación en medios de comunicación interna también ha sido significativa, pues el uso de aplicaciones como Zello o Signal permite mantener la confidencialidad de las comunicaciones y reduce el riesgo de interceptación por parte de la inteligencia militar. Este ecosistema tecnológico crea una estructura más robusta y descentralizada, que dificulta su desmantelamiento y facilita su reorganización. Por tanto, se requiere un enfoque multidimensional en la respuesta estatal. La acción militar debe ir acompañada de estrategias de ciberdefensa, regulación tecnológica y control fronterizo, así como de programas de desarticulación de redes logísticas ilegales.

Tabla 2

Matriz de medidas preventivas y reactivas del Ejército Nacional ante ataques con drones

Categoría	Medidas Preventivas	Medidas Reactivas
Tecnologías de detección	- Instalación de sistemas de detección de drones (radar portátil, RF scanners, acústicos e infrarrojos). - Integración de sensores y cámaras térmicas para vigilancia aérea. - Coordinación con plataformas de inteligencia para monitoreo de espacio aéreo no controlado.	- Activación de protocolos de bloqueo de señal (jammers) en zonas críticas. - Uso de drones interceptores (UAVs defensivos). - Registro y análisis forense del patrón de vuelo para neutralizar futuras amenazas.
Defensa física de bases	- Refuerzo estructural de techos y cubiertas con materiales anti-explosivos. - Implementación de redes o mallas anti-drones sobre instalaciones sensibles.	- Cierre inmediato del espacio aéreo sobre la base afectada. - Evacuación táctica de áreas vulnerables. - Activación de planes de

	- Diseño de perímetros de seguridad con sistemas antiaéreos de bajo alcance (tipo C-UAS).	contingencia y protocolos de primeros auxilios para lesionados.
Inteligencia y ciberseguridad	- Fortalecimiento de capacidades SIGINT y HUMINT para detectar adquisición o modificación de drones por parte de los GAO. - Seguimiento a redes ilegales de comercio de componentes electrónicos. - Desarrollo de ciberinteligencia para detectar programación maliciosa en UAVs.	- Análisis post-ataque de componentes capturados (drones derribados o recuperados). - Recolección de inteligencia táctica y estratégica para contraataques dirigidos. - Ajuste de protocolos de ciberdefensa.
Capacitación y entrenamiento	- Entrenamiento especializado en guerra asimétrica con drones para tropas en terreno. - Simulacros periódicos de respuesta ante ataques con aeronaves no tripuladas. - Cursos de identificación y neutralización de amenazas aéreas no convencionales.	- Despliegue de equipos de respuesta rápida con formación específica en manejo de ataques UAV. - Evaluación posterior al ataque con retroalimentación operativa para mejorar procesos.
Relaciones interinstitucionales	- Coordinación con la Fuerza Aérea Colombiana y Policía Nacional para compartir inteligencia sobre uso criminal de drones. - Alianzas con sector privado y universidades para el desarrollo de sistemas anti-UAV.	- Activación de redes de apoyo interinstitucional para asistencia médica, técnica y logística. - Difusión de alertas tempranas a otras unidades militares y autoridades locales.

Nota: Elaboración propia

Estas acciones permiten anticiparse y mitigar los impactos que este tipo de artefactos pueden causar en bases militares. Según un informe del *Center for Strategic and International Studies (CSIS)* (2024), los drones no solo representan una amenaza cinética, sino también una vía de recolección de inteligencia y desestabilización psicológica. Asimismo, el informe de *NATO Review* (2023) sobre "Countering the Drone Threat"

sugiere adoptar un enfoque mixto que combine detección temprana, disuasión electrónica y respuesta táctica coordinada.

Bajo este contexto, la doctrina militar requiere adaptarse al concepto de guerra híbrida y conflictividad asimétrica, donde la innovación tecnológica se convierte en herramienta de poder irregular. Las Fuerzas Armadas deben responder con sistemas anti-drones, medidas de inteligencia electrónica, y protocolos preventivos actualizados.

En suma, el uso de drones por parte de los GAO constituye una amenaza creciente y multifacética para las Fuerzas Militares colombianas, se requiere de una adaptación doctrinal, inversiones en tecnología antidron y fortalecimiento de capacidades de inteligencia técnica y electrónica para contrarrestar esta tendencia.

Impacto de las normativas internacionales y locales sobre el uso de drones en el ámbito militar, analizando el empleo para a la de bases militares

En el contexto de la lucha contra el terrorismo, se ha evidenciado el uso de drones armados con explosivos por parte de grupos como el Estado Islámico, lo cual ha representado una amenaza directa para las fuerzas militares de los Estados Unidos desplegadas en el Medio Oriente (Schmidt & Schmitt, 2016). En respuesta a esta situación, la empresa fabricante de drones DJI, en coordinación con el gobierno estadounidense, implementó una actualización de su sistema de navegación que restringe el vuelo de sus dispositivos sobre extensas zonas de Irak y Siria. Estas áreas fueron catalogadas como zonas de exclusión aérea, y se suman a las ya existentes No-Fly Zones (NFZ), tradicionalmente establecidas alrededor de aeropuertos y bases militares (Corfield, 2017).

En el caso colombiano, la Unidad Administrativa Especial de Aeronáutica Civil (UAEAC), a través de la Resolución No. 04201 de 2018, estableció los lineamientos operativos y de seguridad para el uso de sistemas de aeronaves no tripuladas (UAS). Dicha normativa define las zonas prohibidas como espacios aéreos de dimensiones específicas en los cuales está completamente prohibido el vuelo de aeronaves, mientras que las zonas restringidas son áreas con limitaciones de vuelo sujetas a condiciones particulares (UAEAC, 2018, p. 11).

La misma resolución también impone restricciones operativas de acuerdo con la clasificación del dron (categorías A, B o C), prohibiendo expresamente el transporte de materiales peligrosos como explosivos, armas o sustancias corrosivas, salvo las baterías necesarias para su funcionamiento. Asimismo, se prohíben las operaciones en un radio de 2 km alrededor del lugar donde se encuentre el Presidente de la República u otros jefes de Estado, y en un radio de 1 km en torno a instalaciones militares, penitenciarias, infraestructura crítica o aeronaves tripuladas en operación (UAEAC, 2018, pp. 18–19).

Como resultado de estas regulaciones, las empresas fabricantes de drones configuran las NFZ conforme a las disposiciones legales de cada país. En ese sentido, las No-Fly Zones son límites virtuales que los drones no pueden cruzar gracias al uso del sistema de posicionamiento global (GPS), el cual permite ubicar al dispositivo en un mapa digital que contiene una capa con dichas zonas. Si un dron se encuentra o se aproxima a una de estas áreas, el sistema interno detecta la ubicación y evita el encendido de los motores o emite alertas al operador para evitar el ingreso a la zona restringida (PePinair, 2019).

La empresa DJI, que concentra aproximadamente el 70 % del mercado mundial de drones (Moreno, 2020), ha implementado el sistema GEO (Geospatial Environment Online) o geocercado, el cual emplea tecnología GPS y otras señales satelitales para impedir automáticamente el vuelo de drones en áreas sensibles como aeropuertos, prisiones, centrales nucleares o eventos especiales. En determinadas zonas, los dispositivos DJI no pueden despegar ni volar sin una autorización previa. Los operadores registrados en la plataforma de DJI pueden solicitar el desbloqueo de algunas áreas justificando su necesidad y presentando los permisos requeridos. En el caso de las zonas más críticas, se exigen medidas adicionales por parte de la empresa para aprobar el desbloqueo. DJI ha optimizado este proceso, permitiendo que los pilotos con autorización legal reciban un código de activación en un lapso de hasta 30 minutos tras presentar su solicitud en línea (RPASDrones, 2019).

Para ampliar la información sobre las estrategias y normativas relacionadas con el uso de drones y las medidas de seguridad implementadas, se consultaron los siguientes documentos oficiales:

- Resolución No. 04201 de 2018 de la Unidad Administrativa Especial de Aeronáutica Civil (UAEAC), que establece los requisitos y medidas de seguridad para la operación de sistemas UAS (drones) en Colombia.
- Guía de Sistemas Contra UAS (C-UAS) 2024 de la Fuerza Aeroespacial Colombiana, que proporciona directrices sobre la detección y neutralización de amenazas aéreas no tripuladas. (aaaes.fac.mil.co)

- Plan de Acción FAC 2024 de la Fuerza Aeroespacial Colombiana, que detalla las estrategias y actividades planificadas para fortalecer la defensa aérea del país. fac.mil.co

Estos documentos ofrecen un marco normativo y estratégico muestran las acciones del Gobierno en materia de seguridad y defensa frente a las amenazas emergentes asociadas al uso indebido de drones. A continuación se presenta un normograma que permite entender mejor la normatividad internacional:

Tabla 3

Normograma del uso y control de sistemas UAS en Colombia

Nivel Normativo	**Nombre de la Norma o Documento**	**Entidad Responsable**	**Contenido Relevante**	**Aplicabilidad al Ejército Nacional**
Norma Técnica y Reglamentaria Nacional	Resolución No. 04201 de 2018	Unidad Administrativa Especial de Aeronáutica Civil (UAEAC)	Regula el uso de drones en el espacio aéreo colombiano. Establece categorías de operación, zonas restringidas, y requisitos para operadores civiles y estatales.	Define zonas de exclusión aérea y protocolos que deben ser conocidos por unidades militares para evitar interferencias operativas y establecer acciones de control ante vuelos no autorizados.
Guía Institucional	Guía de Sistemas Contra UAS (C-UAS) 2024	Fuerza Aeroespacial Colombiana (FAC)	Proporciona criterios técnicos y tácticos para la detección, identificación, seguimiento y} neutralización de drones hostiles mediante sensores,	Es base doctrinal para la implementación de estrategias de defensa activa y pasiva del Ejército Nacional en zonas de combate y protección de instalaciones

			inhibidores y medios cinéticos o electrónicos.	estratégicas. Aplica a unidades militares desplegadas y a comandos conjuntos.
Plan Estratégico Operacional	Plan de Acción FAC 2024	Fuerza Aeroespacial Colombiana (FAC)	Detalla actividades y estrategias para la protección del espacio aéreo nacional frente a amenazas asimétricas, incluyendo el uso hostil de UAS por parte de actores no estatales. Incluye proyectos de radarización, sensores multidominio y fortalecimiento de capacidades C-UAS.	Sirve como hoja de ruta para la interoperabilidad entre Fuerza Aérea y Ejército Nacional en misiones de seguridad, defensa territorial y protección de infraestructura crítica frente a ataques con drones.

Nota: Elaboración propia

En un escenario de creciente complejidad operativa, el Ejército Nacional de Colombia enfrenta un desafío significativo: la protección de sus instalaciones, personal y operaciones frente al uso hostil de aeronaves no tripuladas por parte de grupos armados organizados. Este fenómeno, propio de las guerras asimétricas contemporáneas, ha exigido una respuesta coordinada entre instituciones civiles y militares.

El normograma presentado articula tres niveles normativos fundamentales que orientan el accionar institucional:

1. La Resolución No. 04201 de 2018, expedida por la Unidad Administrativa Especial de Aeronáutica Civil (UAEAC), constituye la norma técnica que regula el uso de

drones en Colombia. Aunque fue diseñada principalmente para operadores civiles y comerciales, esta resolución establece los límites legales sobre zonas restringidas de vuelo, alturas máximas, y requisitos de registro, lo cual es relevante para el Ejército, ya que muchas de sus bases y zonas operativas están en áreas de especial protección o exclusión aérea. Conocer esta normatividad permite al personal militar identificar cuándo un UAS infringe el espacio aéreo autorizado, facilitando la toma de decisiones sobre neutralización o reporte a autoridades (UAEAC, 2018).

2. La Guía de Sistemas Contra UAS (C-UAS) 2024, elaborada por la Fuerza Aeroespacial Colombiana, ofrece directrices operativas y tecnológicas para enfrentar drones hostiles. Esta guía reconoce la urgencia de dotar a las unidades militares con sensores, inhibidores de señal y medios electrónicos o cinéticos capaces de detectar, identificar y neutralizar UAS no autorizados o con fines delictivos. Para el Ejército Nacional, esta guía representa una herramienta doctrinal clave para planificar acciones preventivas y reactivas, especialmente en zonas rurales donde los GAO operan con mayor libertad aérea (Fuerza Aeroespacial Colombiana, 2024).
3. Finalmente, el Plan de Acción FAC 2024 detalla una visión estratégica a nivel nacional para fortalecer la defensa aérea, integrando capacidades de radarización, control del espectro electromagnético e interoperabilidad entre fuerzas. Este plan, aunque formulado desde la FAC, requiere que el Ejército Nacional articule sus capacidades terrestres con las aéreas, reconociendo que los drones no solo

representan una amenaza táctica, sino también estratégica y psicológica, al vulnerar la seguridad percibida en zonas militares.

En conjunto, estas normas y lineamientos permiten construir una respuesta integral, técnica y humana a una amenaza real. Desde la perspectiva humana, es fundamental proteger la vida del personal militar, así como la seguridad de la población civil que rodea las instalaciones castrenses. Implementar estas normas con sensibilidad también implica respetar el uso legítimo de la tecnología por parte de la sociedad, evitando excesos y fortaleciendo la confianza institucional.

Como lo indica el Centro de Estudios Estratégicos e Internacionales (CSIS), los drones no solo modifican el campo de batalla, sino que democratizan el acceso a capacidades ofensivas antes exclusivas de los Estados, lo cual exige una respuesta normativa y operativa innovadora (Bendett, 2023). Así mismo, la NATO Review advierte que el desarrollo de capacidades antidrón debe ser flexible, escalable y multidisciplinario, integrando inteligencia, ciberseguridad y tecnología de punta (NATO, 2023).

Desde que los drones armados comenzaron a redefine el campo de batalla en los primeros años del siglo XXI, el mundo ha enfrentado un desafío inesperado y es cómo regular su uso de manera que se respete el Derecho Internacional Humanitario (DIH) y la soberanía de los Estados; al respecto hay que decir que los tratados internacionales no han creado aún normas específicas para dron armado, pero sí existe un consenso firme y es que estas aeronaves no están prohibidas en sí mismas, pero su uso viene condicionado por los principios de distinción, proporcionalidad y precaución (Comité Internacional de la Cruz Roja, 2023). En otras palabras, pueden ser usadas siempre que se distingan claramente los

objetivos militares de los civiles, se evite daño excesivo colateral y se adopten todas las medidas posibles para minimizar víctimas.

Observadores internacionales como PAX[*] han advertido que, sin normas claras de transparencia y rendición de cuentas, el uso de drones podría convertirse en una herramienta usada indiscriminadamente (PAX, 2022). En el escenario global, potencias como Estados Unidos han llevado a cabo ataques aéreos con drones en países como Pakistán, Yemen o Somalia, generando tensiones sobre soberanía estatal y víctimas civiles. La responsabilidad del Estado que facilita una base como al de Ramstein en Alemania, para que operaciones con drones fuera debatida recientemente en tribunales; se concluyó que internacionalmente no hay obligación automática de garantizar que las operaciones cumplan la interpretación de otro país del derecho internacional, aunque sí existe un compromiso general con la protección de derechos básicos incluso en territorio extranjero (Reuters, 2025).

En conflictos no internacionales, como el colombiano, las normas del DIH siguen siendo aplicables, la Comisión Internacional de la Cruz Roja ha reiterado que ataques con drones, incluso en operativos internos, deben regirse por las mismas reglas que otros métodos de guerra: distinción, proporcionalidad y precaución (CICR, 2023). Por ejemplo, un dron que lance un artefacto explosivo sobre una base militar debe asegurar que el personal objetivo es legítimo, que el daño civil no supera el beneficio militar y que se han minimizado los riesgos mediante buen planeamiento.

[*] Es una organización no gubernamental (ONG) con sede en los Países Bajos que trabaja en temas de paz, desarme y protección de civiles en zonas de conflicto armado.

En Colombia, las normas locales complementan este marco internacional con reglas específicas, la Resolución No. 04201 de 2018 de la UAEAC (mencionada en el normograma) regula el uso de drones dentro del espacio aéreo nacional, estableciendo zonas prohibidas y restringidas, áreas de exclusión alrededor de bases militares, y limitaciones para transportar materiales peligrosos (UAEAC, 2018). Por ejemplo, los operadores de drones civiles no pueden sobrevolar a menos de un (01) kilómetro de una base militar o infraestructura crítica, y transportar explosivos o armas está prohibido. Estas restricciones se reflejan también en tecnologías comerciales, los fabricantes como DJI integran geocercas digitales que impiden despejar dentro de zonas No-Fly predeterminadas, lo cual añade una capa preventiva tecnológica (PePinair, 2019).

La implementación de estas normas tiene un impacto tangible en las bases militares y su defensa aérea, en principio, legitima el uso de sistemas contra drones (radar portátil, inhibidores de señal, drones interceptores) siempre y cuando la acción militar sea proporcional y necesitada. Si un dron no autorizado se aproxima a una base, puede ser neutralizado, registrando su posición, tipo y origen para enfrentar futuras amenazas dentro del marco legal nacional.

En la práctica, normas como la Guía C-UAS 2024, de la Fuerza Aeroespacial Colombiana, ofrecen directrices operacionales para detectar y neutralizar drones hostiles; la guía incluye procedimientos para identificación visual y radar, criterios de uso de inhibidores electromagnéticos, y opciones de respuesta cinéticas o electrónicas (FAC, 2024, p. 16). Todo ello se basa también en estándares internacionales adoptados por organismos

como la OACI o las fuerzas armadas de Estados Unidos, lo que fortalece la interoperabilidad y aporta coherencia jurídica y técnica (FAC, 2024).

El Plan de Acción FAC 2024, por su parte, organiza el despliegue nacional de capacidades antidrón: desde la ampliación de redes de radarización hasta la formación de operadores y coordinación con el Ejército Nacional en defensa territorial. Este plan reconoce que proteger bases militares ya no es solo cuestión de defensa terrestre, sino de asegurar el espacio aéreo frente a actores que pueden realizar ataques a distancia (FAC, 2024).

Este marco legal e institucional brinda varias ventajas concretas. Permite una defensa preventiva y democrática: las autoridades pueden notificar incursiones ilegales al operador civil o identificar drones comerciales usados con fines delictivos. Asimismo, regula el uso de tecnologías duales (civil y defensiva) para que incluso empresas como DJI o proveedores locales configuren las zonas No-Fly de acuerdo con la normativa colombiana.

Pero también plantea retos significativos. Mientras las normas nacionales como la resolución 04201 y los planes de la FAC crean una base sólida, no existe un tratado internacional vinculante sobre drones armados. El vacío legal permite que actores no estatales como los grupos armados organizados para el caso colombiano o grupos terroristas en otras regiones, usen drones sin control, aumentando la vulnerabilidad de las bases militares y de la población civil (PAX, 2022). Además, en conflictos internacionales recientes como Ucrania, se han desplegado drones autónomos en enjambres capaces de

actuar sin control humano directo, lo cual complica aún más la rendición de cuentas y crea riesgos de violaciones de derechos (The Guardian, 2025).

Incluso dentro de Colombia, si bien las normas civiles funcionan, pueden existir brechas en zonas apartadas donde los operadores no estén capacitados o no cuenten con autorización legal. Esto refuerza la necesidad de fortalecer la vigilancia y control gubernamental, entrenando a operadores militares y civiles, y promoviendo mecanismos de reporte transparente.

En definitiva, las normativas internacionales y locales convergen en una concepción de guerra responsable y legal, en la cual el uso de drones armados está sujeto a límites claros. Para las bases militares colombianas, estas normas ofrecen legitimidad jurídica y herramientas técnicas para detectar, disuadir y responder ante ataques dron hostiles. Cualquier acción defensiva puede justificarse con base en el DIH y las reglas nacionales. Pero para que esta convergencia reglamentaria sea efectiva, se deben superar desafíos como el desarrollo de normas internacionales vinculantes, la proliferación no regulada de drones, y la necesidad de formación continua para operadores y autoridades.

Por ultimo, es importante destacar que el impacto de estas normativas depende no solo de su formulación, sino de su implementación consciente y humana que entre otras cosas debe protegerse a las personas y resguardarse la soberanía sin sacrificar los derechos fundamentales ni dar cabida a abusos bajo la premisa de la seguridad.

Estrategia para la protección de las bases militares contra los ataques con aeronaves no tripuladas (drones)

En este apartado, hay que destacar que en el marco de las amenazas híbridas que caracterizan el escenario de seguridad contemporáneo, la incorporación de los drones como herramienta ofensiva por parte de actores armados ilegales representa un desafío sin precedentes para la defensa de las bases militares en Colombia. El DRIL de combate, como célula táctica mínima con capacidad de maniobra independiente, surge como un elemento central en la adaptación de las Fuerzas Militares a este nuevo tipo de confrontación. Más allá de su función tradicional en combate terrestre, el DRIL debe integrarse a sistemas de defensa aérea y ciberdefensa que permitan la detección, seguimiento y neutralización de aeronaves no tripuladas hostiles. Esto refiere una evolución doctrinal en la que el soldado de infantería ya no solo responde a amenazas visibles y terrestres, sino también a aquellas que operan en un espacio aéreo reducido, silencioso y tecnológicamente sofisticado.

En operaciones recientes a nivel internacional, se ha evidenciado que la clave para contrarrestar amenazas de drones no reside únicamente en la adquisición de sistemas costosos de neutralización, sino en la creación de protocolos combinados que integren capacidades humanas y tecnológicas. El caso ucraniano es un ejemplo relevante, pues pequeñas unidades móviles equipadas con inhibidores de señal portátiles y rifles antidron han demostrado que, con un entrenamiento intensivo y coordinación con sistemas de radar y sensores, es posible interceptar drones incluso en condiciones de baja visibilidad (Hybrid CoE, 2025). Esta experiencia puede extrapolarse a los DRIL en Colombia, configurándolos

como nodos de reacción rápida que complementen los sistemas anti-UAS ya instalados en bases estratégicas.

El despliegue de estas unidades tácticas en el entorno colombiano debe considerar la geografía y el patrón de amenazas propias del conflicto interno, en regiones como el Catatumbo, Cauca y Arauca, donde la presencia de grupos armados ilegales es persistente, pues ofrecen condiciones propicias para el uso de drones debido a la dispersión de las fuerzas y a la cercanía de zonas no controladas por el Estado. En este escenario, el DRIL puede cumplir un papel en doble línea: actuar como elemento de disuasión en el perímetro inmediato de la base y proyectar su capacidad a entornos cercanos, identificando posibles zonas de lanzamiento o tránsito de drones hostiles antes de que se aproximen al objetivo.

La necesidad de esta adaptación es reforzada por la tendencia creciente en el uso de drones en conflictos asimétricos, en virtud de lo anterior, un informe del *Center for the Study of the Drone* (2024) destaca que en los últimos cinco años se ha registrado un aumento del 500% en ataques con drones armados contra instalaciones militares y policiales en contextos de insurgencia y terrorismo. Este patrón se replica en Colombia, donde entre 2023 y 2025 los ataques con drones pasaron de ser incidentes esporádicos a convertirse en una amenaza recurrente, con más de un centenar de reportes confirmados por el Ministerio de Defensa (Ministerio de Defensa Nacional, 2025). Estos datos justifican la necesidad de que los DRIL estén permanentemente adiestrados y equipados con sistemas de detección y neutralización portátiles, capaces de operar de forma autónoma y con rapidez.

Otra dimensión relevante es la inteligencia, en este aspecto, los drones empleados por grupos armados ilegales no siempre portan explosivos; en muchos casos, son utilizados

para el reconocimiento aéreo, lo que les permite obtener imágenes en tiempo real de movimientos de tropas, posiciones defensivas y rutinas de patrullaje (West Point CTC, 2024). Esto representa una amenaza estratégica que va más allá del daño físico, ya que erosiona la seguridad operativa y permite al enemigo planificar ataques con mayor precisión. En este sentido, el DRIL, como unidad con movilidad y flexibilidad, puede desempeñar un papel clave en la detección temprana de estos vuelos de reconocimiento, ya sea mediante observación visual, uso de equipos ópticos avanzados o integración con sistemas de alerta temprana.

Ahora bien, la experiencia de las Fuerzas Armadas estadounidenses en Irak y Siria ha mostrado que las respuestas efectivas ante amenazas de drones requieren un sistema escalonado que combine defensas tecnológicas, tácticas de camuflaje, dispersión de recursos y contramedidas electrónicas (Schmidt & Schmitt, 2016). La doctrina C-UAS (Counter-Unmanned Aircraft Systems) sugiere que las unidades pequeñas como el DRIL no deben limitarse a la defensa reactiva, sino que deben participar en operaciones ofensivas para eliminar la capacidad del adversario antes de que pueda desplegar sus drones. Esto incluye la identificación y neutralización de talleres de ensamblaje, almacenes de repuestos y redes de distribución de estos dispositivos.

Desde una perspectiva tecnológica, la cooperación con la industria civil y la academia puede fortalecer las capacidades del DRIL, universidades con programas en ingeniería electrónica y telecomunicaciones podrían desarrollar, en colaboración con el Ejército Nacional, sistemas portátiles de detección y bloqueo adaptados a las necesidades de estas unidades. Estos dispositivos podrían incluir sensores multispectrales, cámaras

térmicas y software de análisis de patrones de vuelo, elementos que han demostrado ser eficaces en teatros de operaciones como el de Nagorno-Karabaj (PAX, 2022).

En el plano normativo, la Resolución 04201 de 2018 de la UAEAC ya establece restricciones de vuelo sobre instalaciones militares, pero su cumplimiento en zonas de conflicto requiere un enfoque operativo y no solo legal. El DRIL, con su despliegue en campo, puede actuar como garante físico de estas disposiciones, reforzando las zonas de exclusión aérea mediante patrullajes y puntos de observación estratégicos. Esto se alinea con el principio de control territorial que históricamente ha guiado las operaciones del Ejército Nacional, pero adaptado ahora a un entorno tridimensional que incluye el espacio aéreo cercano.

La articulación interinstitucional es otro factor determinante, el Ministerio de Defensa, la Fuerza Aeroespacial Colombiana y la Policía Nacional ya han comenzado a trabajar en conjunto para establecer protocolos comunes frente a ataques con drones. No obstante, la inserción del DRIL en este esquema podría mejorar la capacidad de respuesta en el nivel táctico. Su proximidad al terreno le permite actuar como enlace entre las capacidades tecnológicas centralizadas (radares, sistemas anti-dron fijos) y la realidad dinámica del campo de batalla, donde las decisiones deben tomarse en segundos.

En concordancia, es imprescindible reconocer el factor humano en la ecuación. La tecnología por sí sola no garantiza el éxito; requiere operadores capacitados, disciplinados y con criterio táctico para adaptarse a las condiciones cambiantes. La formación continua, los ejercicios de simulación realista y el intercambio de experiencias con fuerzas extranjeras que enfrentan amenazas similares son pasos esenciales para que los DRIL puedan cumplir

eficazmente su misión. Como señalan Young y Kott (2016), la interacción entre unidades pequeñas y tecnologías emergentes es más efectiva cuando existe un entrenamiento conjunto que fomenta la confianza en el equipo y en el material.

En síntesis, el DRIL de combate, fortalecido con capacidades tecnológicas, doctrinales y normativas específicas contra UAS hostiles, representa una herramienta esencial para la defensa de bases militares en Colombia. Su versatilidad, movilidad y capacidad de operar de manera autónoma lo convierten en un actor privilegiado para enfrentar una amenaza que seguirá evolucionando en complejidad y alcance. La integración de estos elementos en una estrategia nacional coherente permitirá no solo proteger las instalaciones críticas, sino también garantizar la seguridad de quienes las defienden y de las comunidades circundantes. En la siguiente tabla se muestra un comparativo de las capacidades del DRIL de Combate en Función Anti-Dron

Tabla 4

Comparativo capacidades del DRIL

Dimensión	**Capacidades Actuales del DRIL**	**Capacidades Propuestas para la Función Anti-Dron**	**Justificación**
Movilidad y despliegue	Alta movilidad terrestre en entornos rurales y urbanos; capacidad de desplazamiento rápido en distancias cortas.	Movilidad combinada con equipos portátiles anti-dron y sistemas ligeros de inhibición de señal.	Permite interceptar y neutralizar drones antes de que alcancen el perímetro de la base.
Armamento	Fusiles de asalto, ametralladoras ligeras, granadas de mano.	Rifles antidron, sistemas portátiles de interferencia de frecuencia (RF Jammer), drones interceptores.	Amplía el espectro de defensa más allá del enfrentamiento terrestre convencional.
Vigilancia y reconocimiento	Observación directa, binoculares, cámaras térmicas.	Sensores multispectrales, radares portátiles de baja cota,	Aumenta la capacidad de detección temprana

		integración con sistemas C-UAS fijos.	de amenazas aéreas de bajo perfil.
Comunicación y coordinación	Radios convencionales VHF/UHF, comunicación con unidades cercanas.	Integración con redes de mando y control C4ISR, enlace en tiempo real con operadores de sistemas anti-dron.	Garantiza respuesta coordinada y oportuna con otras unidades y centros de comando.
Entrenamiento	Instrucción básica en combate terrestre, patrullaje y seguridad perimetral.	Entrenamiento especializado en reconocimiento aéreo, protocolos de respuesta ante drones, análisis forense post-impacto.	Prepara al personal para actuar eficazmente ante amenazas tecnológicas y no convencionales.
Inteligencia	Recopilación de información en terreno, observación de actividades enemigas.	Identificación de rutas de vuelo, localización de puntos de lanzamiento, análisis de patrones de ataque con drones.	Mejora el ciclo de inteligencia para anticiparse a las amenazas.
Intervención post-impacto	Aseguramiento del área, evacuación de heridos.	Recuperación de restos de drones, análisis técnico, recolección de datos para inteligencia militar.	Contribuye a la retroalimentación de sistemas defensivos y desarrollo doctrinal.

Nota: Elaboración propia con base en FAC (2025), Ministerio de Defensa Nacional (2024), UAEAC (2018), y experiencias internacionales (Hybrid CoE, 2025; West Point CTC, 2024).

Complementando lo anterior, hay que mencionar que el *Boletín Doctrinal N.º 003 – DRIL de Combate* ofrece una base táctica valiosa que se alinea con los objetivos de la estrategia nacional para la protección de instalaciones críticas frente al uso hostil de aeronaves no tripuladas (UAS, por sus siglas en inglés).

El DRIL de combate, entendido como la unidad mínima de maniobra con alto nivel de movilidad, letalidad y capacidad de respuesta autónoma, se convierte en un actor clave en la detección, contención y neutralización de amenazas aéreas no convencionales, como las que representan los drones armados. Esta célula táctica, compuesta entre 3 y 5 hombres, puede desempeñar funciones preventivas y reactivas alrededor de bases militares, actuando

como fuerza de reconocimiento, vigilancia y reacción rápida ante la detección de UAS hostiles.

Hay que agregar que el boletín doctrinal refuerza el principio de descentralización del mando, lo cual permite a los DRIL operar con autonomía en situaciones críticas, como la irrupción de drones en el espacio aéreo restringido. Este nivel de maniobra táctica es esencial cuando se requiere interceptar o neutralizar un dron antes de que alcance zonas sensibles dentro de la base. Por lo anterior, en el marco de una estrategia integral anti-UAS, los DRIL podrían formar parte de anillos de defensa terrestre complementarios a los sistemas electrónicos y cinéticos de neutralización.

Así mismo, el enfoque de entrenamiento intensivo planteado en el documento doctrinal responde directamente a la necesidad de contar con personal altamente capacitados para operar en un entorno tecnológico cambiante. Ahora bien, hay que resaltar que la incorporación de herramientas de geolocalización, sensores portátiles, sistemas de alerta temprana y protocolos de reacción ante amenazas aéreas podría integrarse de manera eficiente a las tareas del DRIL, lo cual fortalece la sinergia entre los componentes tecnológicos y humanos en las unidades de combate.

En paralelo, dentro del componente preventivo de la estrategia anti-dron, la vigilancia permanente del perímetro de las bases es una necesidad, pues los DRIL pueden rotar en patrullajes periféricos, identificar posibles zonas de despegue clandestinas cercanas, establecer puntos de observación con binoculares o estaciones portátiles de radar terrestre y articularse con operadores de sistemas anti-UAS para ofrecer una respuesta eficaz, rápida y precisa.

Por último, cabe resaltar que el DRIL puede desempeñar funciones de intervención post-impacto, siendo la primera unidad en responder al lugar del ataque, asegurar el área, evacuar heridos, y recolectar evidencias para el análisis forense del dispositivo aéreo utilizado, fortaleciendo así el ciclo de inteligencia y retroalimentación para la mejora continua de los sistemas de protección.

La doctrina del DRIL de combate por lo descrito anteriormente, no solo refuerza las capacidades tácticas del Ejército Nacional, sino que también representa un componente vital en la estrategia integral para proteger las bases militares contra ataques con drones. Su implementación coordinada con las tecnologías de defensa anti-UAS, el entrenamiento especializado y el fortalecimiento del mando táctico, permite a las Fuerzas Militares de Colombia posicionarse con ventaja ante una amenaza creciente, adaptable y de alto impacto como es el uso de aeronaves no tripuladas por parte de actores armados ilegales.

Complementando lo anterior, es importante decir que la doctrina militar en Colombia, reflejada en el *Boletín Doctrinal No. 002 del Ejército Nacional* (2025), destaca la urgencia de abordar de manera estratégica y diferenciada la amenaza que representan las aeronaves no tripuladas en escenarios de combate y seguridad. Esta perspectiva doctrinal complementa y fortalece los lineamientos de la estrategia nacional presentada anteriormente, al advertir que los drones han dejado de ser herramientas exclusivamente tecnológicas para convertirse en vectores de agresión asimétrica utilizados por actores armados ilegales.

El boletín en mención enfatiza que los UAS no solo facilitan el transporte de artefactos explosivos, sino que, por su bajo costo, tamaño reducido, baja huella sonora y

capacidad de operar a distintas altitudes, se convierten en herramientas de difícil detección, representando una amenaza latente para las bases militares. Esta capacidad de pasar desapercibidos exige de las Fuerzas Militares una respuesta que trascienda la reacción tradicional y que se base en sistemas integrados de alerta temprana, vigilancia constante y protocolos de respuesta ante incursiones aéreas no autorizadas.

Lo anterior conecta directamente con los esfuerzos institucionales ya implementados, como la adquisición de sistemas anti-drones, el desarrollo de capacidades operativas especializadas y la creación de zonas de exclusión aérea a través del sistema GEO de geocercado (UAEAC, 2018; FAC, 2025). La doctrina propone que los comandantes aborden esta amenaza con un enfoque adaptativo y diferencial, ajustado al carácter cambiante del conflicto moderno. Es decir, la estrategia de protección de las bases militares no puede limitarse a medidas defensivas pasivas, sino que debe contemplar acciones preventivas, reactivas y de inteligencia proactiva.

Además, el boletín plantea la necesidad de asumir que las unidades desplegadas podrían estar bajo observación constante del enemigo, incluso en zonas aparentemente seguras, lo cual resalta la importancia de establecer zonas restringidas de vuelo, como lo estipula la Resolución No. 04201 de 2018 de la Aeronáutica Civil. Esta medida, en combinación con los sistemas de detección y neutralización, busca cerrar brechas de vulnerabilidad en las instalaciones militares, haciendo más difícil que actores no estatales puedan recopilar inteligencia o ejecutar ataques a través de UAS.

En este sentido, el pensamiento militar debe replantearse, tal como se expone en el Plan de Acción FAC 2024 y en la Guía de Sistemas Contra UAS 2024, no se trata

únicamente de adquirir tecnología, sino de adaptar las doctrinas operativas, capacitar al personal y articular los marcos legales existentes con la práctica cotidiana del despliegue militar. Esta sinergia entre doctrina, estrategia institucional y normatividad nacional configura el fundamento de una respuesta efectiva ante el uso criminal de drones, alineando al país con los estándares internacionales de defensa y anticipación tecnológica.

En resumen, el boletín doctrinal no solo valida la estrategia nacional, sino que la complementa desde el componente táctico y formativo, brindando directrices concretas sobre cómo deben prepararse y actuar los comandantes frente a esta amenaza. Esta conexión entre lo normativo, lo estratégico y lo operacional permite construir una estrategia de defensa integral, indispensable para garantizar la seguridad de las bases militares frente a una amenaza que ha redefinido las reglas del combate contemporáneo.

Tabla 5.

Estrategias para la protección de las bases militares contra los ataques con aeronaves no tripuladas

Nombre de la Estrategia	Descripción
1. Estrategia de Inversión en Tecnología Anti-Drones	El Gobierno Nacional, a través del Ministerio de Defensa, invirtió más de 20.000 millones de pesos en la adquisición de sistemas de detección y neutralización de drones para proteger instalaciones estratégicas como bases militares, plantas de energía y centros urbanos vulnerables (Presidencia de la República, 2024).
2. Estrategia de Desarrollo de una Hoja de Ruta Tecnológica (FAC)	La Fuerza Aeroespacial Colombiana lidera la implementación de una hoja de ruta para el desarrollo de capacidades anti-drones basada en economías de escala, transferencia tecnológica y proyectos de uso dual (FAC, 2025).
3. Estrategia de Capacitación y Formación Militar Especializada	El Comando de Educación y Doctrina del Ejército Nacional capacita a oficiales,

	suboficiales y soldados para detectar, identificar, neutralizar y mitigar amenazas con drones. Estos militares formarán a sus compañeros a nivel nacional (Matta, 2025).
4. Estrategia Normativa Nacional (Resolución 04201 de 2018)	Reglamenta el uso de UAS en Colombia, estableciendo zonas prohibidas, restricciones operativas, y clasificaciones de drones en categorías A, B y C (UAEAC,2018).
5. Estrategia de Implementación de Geocercas (GEO) en drones comerciales	Empresas como DJI han incorporado el sistema GEO para impedir vuelos no autorizados en zonas críticas usando GPS. Adaptaciones también aplican para Colombia, Moreno (2020).
6. Estrategia de Articulación Interinstitucional Ciencia-Tecnología-Seguridad	La Dirección de Proyección de Capacidades e Innovación del Ministerio de Defensa articula estrategias operativas con el desarrollo científico y tecnológico para responder a amenazas emergentes como los drones armados (Ministerio de Defensa Nacional, 2024).

Nota: Elaboración propia

Como conclusión de este capítulo, se evidencia que Colombia ha asumido un papel proactivo y estratégico frente a las amenazas emergentes que representan las aeronaves no tripuladas, particularmente aquellas empleadas por actores armados ilegales. A través de una combinación coherente de inversión tecnológica, desarrollo doctrinal, normativas claras, formación especializada y articulación interinstitucional, el país ha construido una hoja de ruta sólida para la defensa de sus infraestructuras más sensibles, especialmente las bases militares. Esta estrategia no solo posiciona a Colombia como un referente regional en la lucha contra tecnologías empleadas con fines hostiles, sino que también demuestra el compromiso del Estado por anticiparse a los riesgos del conflicto moderno, adaptando sus capacidades a un entorno operativo cada vez más asimétrico y tecnificado. Fortalecer estas

medidas y promover una cultura de innovación y prevención dentro de la Fuerza Pública será clave para garantizar la seguridad nacional en el presente y el futuro inmediato.

[T1] Conclusiones (10% del trabajo aproximadamente)

A lo largo del presente trabajo se ha evidenciado que los ataques con aeronaves no tripuladas, representan una amenaza creciente y real para la seguridad nacional, en especial para las bases militares de las Fuerzas Militares de Colombia. El uso de esta tecnología por parte de actores armados ilegales ha cambiado la naturaleza del conflicto, haciéndolo más asimétrico, impredecible y difícil de contener bajo los esquemas tradicionales de defensa.

En este contexto, el Estado colombiano ha respondido con una estrategia integral que combina innovación tecnológica, inversión en capacidades operativas, normativas claras y formación especializada. Esta respuesta refleja no solo una política pública de seguridad avanzada, sino también el compromiso con la defensa de la vida, la soberanía y la integridad de las fuerzas encargadas del orden.

La investigación permitió identificar medidas preventivas y reactivas que fortalecen la protección de las bases militares frente a estas nuevas amenazas. Entre ellas destacan el uso de sistemas anti-drones, la implementación de zonas de exclusión aérea, el desarrollo de doctrinas operativas adaptadas, y la capacitación de personal especializado. Asimismo, se reconoció el valor de la articulación entre instituciones estatales, la industria tecnológica y la comunidad internacional para lograr una respuesta coherente y sostenible.

Sin embargo, también quedó claro que la tecnología por sí sola no es suficiente. La eficacia de la estrategia de defensa depende del factor humano: de la preparación, el compromiso y la ética de quienes operan estos sistemas y toman decisiones en momentos

críticos. Por ello, es imprescindible seguir promoviendo una cultura de innovación, anticipación y adaptación dentro de las Fuerzas Militares, donde la protección de la vida, la inteligencia operativa y el respeto por el Derecho Internacional Humanitario vayan siempre de la mano.

Finalmente, se concluye que Colombia avanza en el camino correcto al asumir los desafíos del siglo XXI con herramientas modernas, con visión estratégica y con un enfoque integral de seguridad. Aún hay mucho por fortalecer, pero las acciones desarrolladas hasta el momento sientan las bases para una defensa más sólida, eficaz y humana frente a las amenazas tecnológicas que desafían al Estado en el presente y en el futuro.

[T1] Referencias (APA séptima edición)

AllMilitaryOps. (2024). Drones and international law: navigating legal challenges in warfare. https://allmilitaryoperations.com/drones-and-international-law/

Bendett, S. (2023). Drone warfare and asymmetric threats. Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/drone-warfare-and-asymmetric-threats

Cambridge Core. (2025). The international law framework regulating the use of armed drones. International & Comparative Law Quarterly. https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/international-law-framework-regulating-the-use-of-armed-drones/E92C0FCA200F667633B0C3686A9EDE3C

Centre for Strategic and International Studies. (2025). Lessons from the Ukraine conflict: Modern warfare in the age of autonomy, information and resilience. https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience

Comité Internacional de la Cruz Roja. (2023). Ensuring the use of remotely piloted aircraft or armed drones is consistent with international humanitarian law. https://www.icrc.org/en/document/ensuring-use-remotely-piloted-aircraft-or-armed-drones-counterterrorism-and-military

Colmundo Radio. (2024). Colombia refuerza su seguridad con sistemas antidrone para proteger infraestructuras críticas. https://www.colmundoradio.com/noticias/colombia-refuerza-su-seguridad-con-sistemas-antidrone/

Corfield, G. (2017). DJI drones grounded over Iraq and Syria with a software update. The Register. https://www.theregister.com/2017/04/25/dji_drone_geofencing_middle_east/

ECFR (European Council on Foreign Relations). (2025). Drones in Ukraine: Four lessons for the West. https://ecfr.eu/article/drones-in-ukraine-four-lessons-for-the-west/

Ejército Nacional de Colombia. (2024). Fuerza pública se capacita para enfrentar amenazas con drones en zonas críticas. https://www.ejercito.mil.co/?idcategoria=651184

El País. (2025, mayo 22). El aumento del uso de drones con explosivos cambia la dinámica del conflicto armado interno en Colombia. https://elpais.com/america-colombia/2025-05-22/el-aumento-del-uso-de-drones-con-explosivos-cambia-la-dinamica-del-conflicto-en-colombia.html

Fuerza Aeroespacial Colombiana. (2024). Guía de sistemas Contra UAS (C-UAS). Autoridad Aeronáutica de Aviación de Estado. https://www.fac.mil.co/sites/default/files/2024-01/GUIA_C-UAS_FAC.pdf

Fuerza Aeroespacial Colombiana, (2023). Finalizó con éxito el curso de drones tácticos. https://www.fac.mil.co/es/noticias/finalizo-con-exito-el-curso-de-drones-tacticos?utm_

Fuerza Aeroespacial Colombiana. (2024). Plan de Acción FAC 2024. https://www.fac.mil.co

Hybrid Centre of Excellence for Countering Hybrid Threats. (2025). Countering drones in hybrid conflicts: Best practices for defence forces. https://www.hybridcoe.fi/publications/countering-drones-in-hybrid-conflicts

ICCT (International Centre for Counter-Terrorism). (2023). Tower 22: Innovations in drone attacks by non-state actors. https://icct.nl/publication/tower-22-innovations-drone-attacks-non-state-actors

Le Monde. (2024). Yemen: Western armies powerless to halt Houthi attacks. https://www.lemonde.fr/en/international/article/2024/07/26/yemen-western-armies-powerless-to-halt-houthi-attacks_6699126_4.html

Matta, N. (2025). Ejército seleccionó a 35 militares para entrenarlos en la lucha contra drones terroristas. https://www.elcolombiano.com/colombia/ejercito-entrena-militares-contra-ataques-de-drones-PN27191961

Ministerio de Defensa Nacional, (2024). Ministerio de Defensa Nacional, (2024). Colombia refuerza su seguridad con sistemas avanzados de defensa contra drones para proteger a la comunidad, la fuerza pública y el territorio nacional. https://www.mindefensa.gov.co/prensa/noticia-visualizacion/noticias-prensa-colombia-refuerza-su-seguridad?utm_

Moreno, J. (2020). ¿Qué tan seguros son los drones que usamos? El Tiempo. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/seguridad-de-los-drones-en-colombia-521648

NATO Review. (2023). Countering the drone threat: NATO's evolving strategies. https://www.nato.int/docu/review

NextTools. (2025). Drone warfare legality: blurred lines in modern conflict. https://nexttools.net/is-drone-warfare-legal/

ONU (United Nations). (2013). Report of the Special Rapporteur on the use of drones in counter-terrorism operations. https://casebook.icrc.org/case-study/general-assembly-use-drones-counter-terrorism-operations

PAX. (2022). Humanitarian concerns raised by the use of armed drones. https://www.genevacall.org/fr/actualites/humanitarian-concerns-raised-by-the-use-of-armed-drones/

Política de Ciencia y Tecnología, (2024). Proyección de capacidades e innovación. https://www.mindefensa.gov.co/estrategia-y-planeacion/proyeccion-de-capacidades-e-innovacion?utm_

PePinair. (2019). ¿Qué es una zona de exclusión aérea para drones? https://www.pepinair.com/blog/no-fly-zone-drones/

RPASDrones. (2019). Desbloqueo de zonas GEO de DJI. https://rpasdrones.es/desbloqueo-de-zonas-geo-de-dji/

Reuters. (2025). Germany's constitutional court dismisses complaint against U.S. drone missions via Ramstein Air Base on grounds it did not violate international law. https://www.reuters.com/world/germanys-top-court-dismisses-complaint-against-us-drone-missions-via-ramstein-2025-07-15/

Schmidt, M. A., y Schmitt, M. N. (2016). Armed drones and the ethics of war: Military virtue in a post-heroic age. Air & Space Power Journal. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-30_Issue-2/F-Schmitt_Schmidt.pdf

The Guardian. (2025). Killing machines: How Russia and Ukraine's race to perfect deadly pilotless drones could harm us all. https://www.theguardian.com/world/2025/jun/25/ukraine-russia-autonomous-drones-ai

Teleantioquia. (2024). Gobierno de Colombia lanza estrategia para enfrentar amenazas con drones. https://www.teleantioquia.co/noticias/gobierno-de-colombia-lanza-estrategia-antidrones/

Unidad Administrativa Especial de Aeronáutica Civil. (2018). Resolución No. 04201 de 2018. https://www.aerocivil.gov.co

United States Military Academy, Combating Terrorism Center (CTC). (2024). The evolution of drone threats and military countermeasures. https://ctc.westpoint.edu/the-evolution-of-drone-threats

Vision of Humanity. (2023). How drones have shaped the nature of conflict. https://www.visionofhumanity.org/how-drones-have-shaped-the-nature-of-conflict/