Adaptación de la Contrainteligencia de la Fuerza Aeroespacial Colombiana ante Amenazas Híbridas Emergentes

Mayor (FAC) Julie Andrea Rodríguez Gutiérrez

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 (FAC) Julie Andrea Rodríguez Gutiérrez
Identificación	**:**	1106889614
Programa académico	**:**	Maestría en Seguridad y Defensa Nacionales
Tutor metodológico	**:**	Henry Mauricio Acosta Guzmán
Tutor temático	**:**	Capitán René Alonso Guerra Molina
Fecha de entrega	**:**	25 de agosto de 2025
Extensión	**:**	7.820 palabras

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

Adaptación de la Contrainteligencia de la Fuerza Aeroespacial Colombiana ante Amenazas Híbridas Emergentes

Adaptation of the Colombian Aerospace Force Counterintelligence to Emerging Hybrid Threats

Julie Andrea Rodríguez Gutiérrez [1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El presente artículo analiza cómo la Fuerza Aeroespacial Colombiana (FAC) ha adaptado sus operaciones de contrainteligencia ante la amenaza emergente del uso de drones por actores no estatales, en el marco de las amenazas híbridas. A través de una metodología cualitativa de tipo documental, se examinaron informes oficiales, doctrina institucional y estudios comparativos con las fuerzas aéreas de Israel y España. El análisis se estructuró en torno al ciclo de inteligencia (recolección, procesamiento, análisis y difusión), identificando limitaciones técnicas y doctrinales en la respuesta institucional. Se incorporaron gráficos y una figura ilustrativa sobre zonas vulnerables, complementadas por una tabla comparativa de capacidades operativas. Entre los hallazgos preliminares, se evidenció una débil implementación de contramedidas electrónicas y una respuesta predominantemente reactiva. Se concluye que es necesaria una doctrina robusta, apoyada en tecnologías disruptivas, para fortalecer las capacidades de defensa activa ante incursiones aéreas no tripuladas.

Palabras clave: contrainteligencia; drones; inteligencia militar; seguridad nacional; amenazas híbridas.

Abstract: This article analyzes how the Colombian Aerospace Force (FAC) has adapted its counterintelligence operations in response to the emerging threat posed by drones used by non-state actors, within the framework of hybrid threats. Using a qualitative and documentary methodology, official reports, institutional doctrine, and comparative studies with the air forces of Israel and Spain were examined. The analysis was structured around the intelligence cycle (collection, processing, analysis, and dissemination), identifying technical and doctrinal limitations in the institutional response. Graphs and a figure illustrating vulnerable zones were incorporated, along with a comparative table of operational capabilities. Preliminary findings reveal a weak implementation of electronic countermeasures and a predominantly reactive response. It is concluded that a robust doctrine supported by disruptive technologies is required to strengthen active defense capabilities against unmanned aerial incursions.

Keywords: counterintelligence; drones; military intelligence; national security**,** hybrid threats.

[1] Mayor de la Fuerza Aeroespacial Colombiana. Estudiante Maestría en Seguridad y Defensa Nacionales, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Magister Docencia y Educación, Universidad Tecnológica Latinoamérica en Línea, Profesional en Relaciones Internacionales y Asuntos Políticos, Universidad Militar Nueva Granada, Colombia. Administradora Aeronáutica, Escuela Militar Marco Fidel Suarez, Colombia. https://orcid.org/0009-0006-4851-7828 Contacto: julie.rodriguez@esdeg.edu.co.

Introducción

La evolución tecnológica en el ámbito militar ha dado paso a nuevas formas de amenaza, especialmente aquellas que combinan tácticas convencionales y no convencionales, conocidas como amenazas híbridas. Dentro de ellas, el uso de drones por parte de actores no estatales representa una preocupación creciente para las fuerzas armadas de diversos países. En Colombia, estas tecnologías han sido empleadas para misiones de espionaje, monitoreo de instalaciones militares y transporte de ilícitos, desafiando los esquemas tradicionales de seguridad. Investigaciones recientes (Corredor, 2024; Carrasquilla, 2021) han documentado el aumento de estos incidentes, particularmente en las áreas circunvecinas de las Unidades Militares Aéreas (UMAS), lo que evidencia una necesidad urgente de modernizar las estrategias de contrainteligencia en la FAC.

El presente artículo se enfoca en un problema concreto: la insuficiencia de estrategias de contrainteligencia en la Fuerza Aeroespacial Colombiana (FAC) frente al uso creciente de drones por actores no estatales. Esta situación compromete la seguridad de instalaciones estratégicas, evidencia vacíos tecnológicos y limita la capacidad de anticipación. Desde la doctrina nacional (Ley 1621 de 2013) y el enfoque formativo de EIAEC, existen lineamientos sobre inteligencia y defensa, pero no una doctrina específica sobre contramedidas tecnológicas frente a amenazas híbridas aéreas. En este marco, la pregunta de investigación que guía este artículo es:

¿Qué estrategias ha implementado la FAC para adaptar las operaciones de contrainteligencia frente al empleo de drones con nuevas tecnologías en el área circunvecina de las Unidades Militares Aéreas?

Para responderla, se formuló el siguiente objetivo general:

Analizar las estrategias de adaptación de las operaciones de contrainteligencia de la FAC frente al uso de drones en las áreas circunvecinas de las UMAS.

Y los objetivos específicos: 1. Identificar las adaptaciones realizadas en las operaciones de contrainteligencia de la FAC ante el empleo de drones. 2. Describir las estrategias actuales implementadas por la FAC para contrarrestar amenazas con drones en las UMAS. 3. Proponer estrategias para fortalecer las capacidades de contrainteligencia de la FAC frente al uso de drones.

Desde la academia, estudiar esta problemática permite aportar soluciones teóricas y prácticas para modernizar la defensa nacional. Desde lo institucional, la FAC requiere con urgencia incorporar tecnologías disruptivas, fortalecer la interoperabilidad interagencial y cerrar las brechas operativas en el ciclo de inteligencia. Atender esta necesidad permitirá proteger de manera efectiva las instalaciones críticas, anticipar amenazas híbridas y optimizar los recursos estratégicos. A largo plazo, este estudio busca contribuir a la formulación de una doctrina sólida en contramedidas aéreas y mejorar la capacidad de respuesta de la FAC frente a los retos tecnológicos emergentes (Rodríguez, 2015).

Los hallazgos evidencian que la respuesta actual de la Fuerza Aeroespacial Colombiana ante el uso de drones por actores no estatales presenta limitaciones significativas, caracterizándose por medidas mayoritariamente reactivas, fragmentadas y sin un marco doctrinal unificado. Esta situación se refleja en la ausencia de un manual específico de contramedidas electrónicas, la carencia de sistemas C-UAS instalados en las UMAS y la dependencia de recursos de vigilancia convencionales, lo que reduce la capacidad de anticipación frente a incursiones tecnológicas (Corredor, 2024).

Metodología

Este estudio se enmarcó en un enfoque metodológico cualitativo, siguiendo los lineamientos propuestos por Sampieri et al. (2000), lo cual permitió comprender en profundidad fenómenos operativos y sociales complejos, como las amenazas híbridas emergentes enfrentadas por la Fuerza Aeroespacial Colombiana. Este enfoque fue pertinente para analizar las estrategias de contrainteligencia aplicadas en contextos reales, especialmente aquellas relacionadas con el uso de drones por parte de actores no estatales y su impacto sobre la seguridad operativa de las Unidades Militares Aéreas (UMAS).

La recolección de datos se llevó a cabo mediante una revisión documental exhaustiva. Se analizaron informes de gestión, manuales operacionales, planes estratégicos, documentos doctrinales y publicaciones académicas, tanto nacionales como internacionales, con énfasis en fuentes oficiales del Ministerio de Defensa, de la FAC, y estudios especializados sobre inteligencia y amenazas híbridas. Asimismo, se incorporaron casos documentados sobre el uso de drones hostiles y la respuesta institucional ante estos hechos (Villamizar & Pedraza, 2023).

El análisis de la información se realizó mediante análisis de contenido, lo que permitió identificar patrones y categorías emergentes dentro del ciclo de inteligencia: recolección, procesamiento, análisis y difusión. Se prestó especial atención a los vacíos existentes en la implementación de contramedidas electrónicas dentro de dicho ciclo, aspecto que limita la capacidad de anticipación y respuesta operativa. Finalmente, se efectuó un análisis comparativo con Fuerzas Aéreas de otros países, como Israel y España, que han avanzado en la integración de tecnologías defensivas frente a este tipo de amenazas.

Adaptaciones realizadas en las operaciones de contrainteligencia de la FAC ante el empleo de drones.

El uso de sistemas aéreos remotamente tripulados, comúnmente conocidos como drones, se ha consolidado como una de las principales amenazas tecnológicas emergentes para las fuerzas militares en el siglo XXI. En Colombia, actores no estatales han empleado estas plataformas para espionaje, contrabando, vigilancia ilegal e incluso interferencia electrónica, desafiando los modelos tradicionales de defensa y vigilancia aérea (Pulido, 2017).

Desde la perspectiva doctrinal, esta investigación se enmarca en los postulados de la Teoría de la Seguridad Nacional (Wolfers, 1952) y la Teoría de la Guerra Asimétrica (Mack, 1975), las cuales explican cómo las amenazas no convencionales como los drones requieren respuestas flexibles, adaptativas y tecnológicamente innovadoras. En línea con estas teorías, la Fuerza Aeroespacial Colombiana (FAC) ha debido ajustar progresivamente sus operaciones de contrainteligencia, especialmente en zonas críticas como el entorno circunvecino de las Unidades Militares Aéreas (UMAS).

Este capítulo aborda el primer objetivo específico del estudio: identificar las adaptaciones realizadas en las operaciones de contrainteligencia de la FAC frente al uso de drones. Para ello, se analizan las cuatro fases del ciclo de inteligencia recolección, procesamiento, análisis y difusión en función de su adecuación ante amenazas híbridas.

Es importante señalar que, a diferencia de otras doctrinas como la estadounidense o la OTAN, la doctrina de la FAC no se adscribe formalmente a un modelo ARP (Apreciación, Resolución, Planificación), aunque sí incorpora elementos similares bajo la doctrina nacional definida en el marco de la Ley 1621 de 2013 y la Escuela de Inteligencia Aérea, Espacial y

Ciberespacial (EIAEC) creada en 1998, ha sido clave en el desarrollo doctrinal propio y en la especialización del personal FAC en inteligencia operativa y estratégica frente a nuevas amenazas tecnológicas (Contreras, 2010).

A partir de una revisión documental, doctrinal y técnica, se identificaron múltiples acciones de ajuste. Por ejemplo, el uso de sensores FLIR en plataformas aéreas, la incorporación de patrullajes técnicos en zonas vulnerables, y el entrenamiento básico de personal en reconocimiento visual y auditivo de drones. No obstante, también se evidencian vacíos importantes, como la ausencia de sistemas automatizados de detección a baja altitud y la no implementación de doctrinas específicas para contramedidas electrónicas.

En síntesis, la adaptación doctrinal y operativa de la FAC ante el fenómeno de los drones ha sido progresiva, pero todavía limitada. Aunque se ha fortalecido la vigilancia, la respuesta sigue siendo reactiva. Se requiere, por tanto, el diseño e implementación de una doctrina específica de defensa activa contra drones, que incorpore capacidades tecnológicas avanzadas y una articulación interinstitucional eficiente.

Contexto doctrinal y operacional de la contrainteligencia en la FAC

La contrainteligencia en Colombia ha estado históricamente orientada a neutralizar las amenazas internas dirigidas contra la seguridad institucional del Estado. En el caso de la Fuerza Aeroespacial Colombiana, esta función ha estado regulada por el marco de la Ley 1621 de 2013, que establece los principios y competencias de la inteligencia y contrainteligencia para garantizar la defensa de la soberanía, la integridad territorial y el orden constitucional. En este marco, la FAC ha definido estructuras específicas para la producción de inteligencia, incluyendo unidades encargadas de proteger el secreto operativo, prevenir la filtración de información y detectar amenazas de espionaje o sabotaje.

Asimismo, existen documentos estratégicos como el Plan Estratégico Institucional 2030 (FAC, 2025) y los lineamientos de EAIEC (2025) han enfatizado la necesidad de actualizar las prácticas de contrainteligencia con enfoque prospectivo y adaptativo (Corredor, 2024) La incorporación de tecnologías disruptivas, como sistemas de vigilancia automatizados, radares de baja altitud y software de procesamiento de datos en tiempo real, hace parte del proceso de modernización iniciado desde finales de la década de 2010.

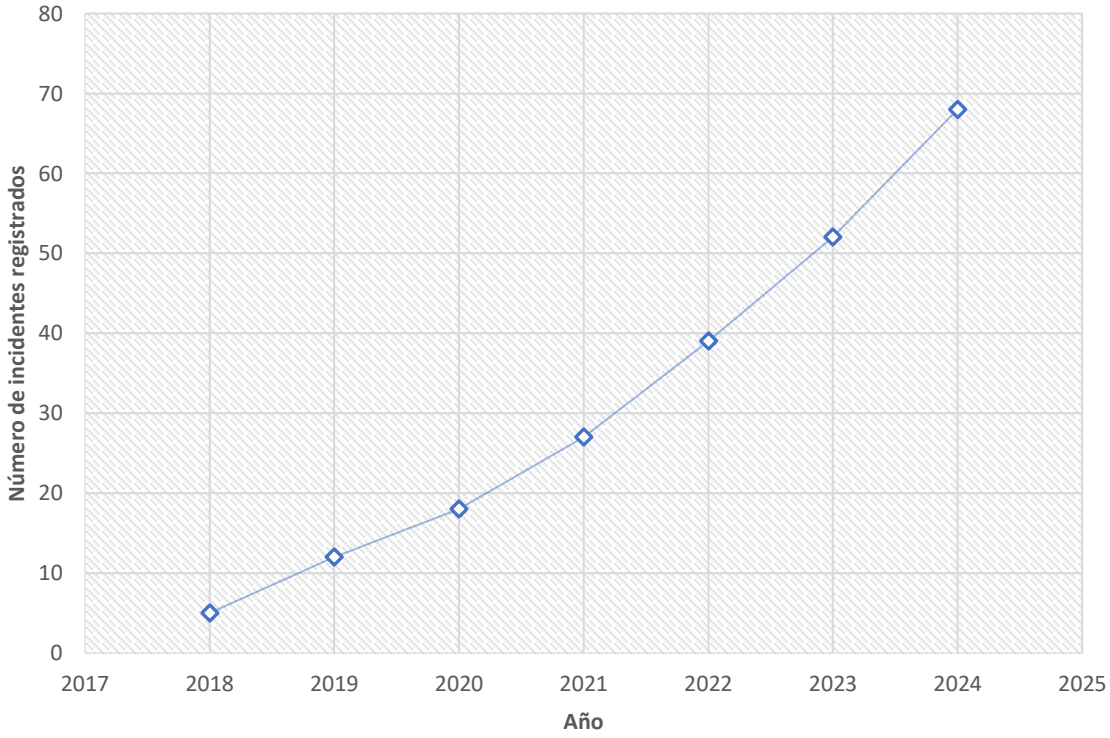
En cuanto al ámbito operacional, la FAC ha centrado su contrainteligencia en la protección del entorno inmediato de las bases aéreas, instalaciones de radar, plataformas de control aéreo y unidades de mantenimiento logístico. Sin embargo, el uso de drones por parte de actores externos plantea nuevas complejidades, ya que permite la intrusión aérea sin contacto físico y con bajo perfil de detección. Ante esto, el reto institucional ha sido no solo doctrinal, sino también técnico y operativo: pasar de una visión reactiva a una preventiva, sustentada en el fortalecimiento del ciclo de inteligencia y en el desarrollo de capacidades específicas frente a esta amenaza.

En los últimos años, el uso de drones por parte de actores no estatales en Colombia ha dejado de ser una posibilidad hipotética para convertirse en una amenaza real y creciente dentro del espectro de riesgos híbridos (Carrasquilla, 2021). Estas aeronaves, de fácil adquisición y manipulación, han sido empleadas para misiones de reconocimiento, seguimiento a instalaciones militares e incluso actividades de interferencia sobre sistemas de comunicación. La progresiva sofisticación de estos dispositivos y su bajo costo operativo han facilitado su expansión en contextos urbanos y rurales (Carbajal, 2024). A continuación, se presenta una gráfica que muestra la evolución del número de incidentes registrados en Colombia entre 2018 y 2024, lo cual evidencia el crecimiento sostenido de esta amenaza y

su impacto en la planificación de las operaciones de contrainteligencia de la Fuerza Aeroespacial Colombiana.

Figura 1

Evolución de incidentes con drones por actores no estatales



Fuente: Los datos presentados en esta figura son de carácter ilustrativo y han sido construidos con base en una revisión cualitativa de fuentes especializadas sobre seguridad y defensa en Colombia. La tendencia al alza refleja una proyección fundamentada en estudios recientes que documentan el incremento en el uso de drones por actores no estatales con fines ilícitos. Fuentes consultadas incluyen: Corredor (2024), Elguera (2024), Carrasquilla (2021) y documentación institucional de la FAC.

La figura No. 1 muestra un incremento sostenido en el número de incidentes relacionados con el uso de drones por parte de actores no estatales. Desde 2018, cuando se registraban apenas cinco casos documentados, se ha evidenciado una escalada significativa hasta alcanzar 68 eventos en 2024. Este comportamiento responde al bajo costo de adquisición de estos sistemas, su fácil adaptación a condiciones tácticas y su creciente disponibilidad en mercados informales. La tendencia obliga a las instituciones de defensa,

especialmente a la FAC, a revisar y ajustar sus protocolos de vigilancia y reacción inmediata frente a estas amenazas.

Adaptaciones operativas de la FAC frente al uso de drones

La FAC, como parte esencial del sistema de defensa nacional, ha enfrentado la necesidad de adaptar sus operaciones de contrainteligencia ante la creciente amenaza representada por los drones. Si bien esta adaptación ha sido progresiva y aún presenta vacíos importantes, pueden identificarse acciones concretas en los ámbitos doctrinal, técnico y operacional.

Como primera medida, desde el plano doctrinal, la FAC ha incorporado el fenómeno de las amenazas híbridas en sus procesos de planeamiento estratégico y capacitación institucional. La Escuela de Inteligencia Aérea, Espacial y Ciberespacial (EIAEC) ha fortalecido sus programas académicos con módulos relacionados con inteligencia aérea aplicada a tecnologías emergentes, incluyendo el uso hostil de sistemas no tripulados (Contreras, 2010). Estos esfuerzos buscan preparar al personal para escenarios de recolección de información no tradicional, lo cual es fundamental frente a drones utilizados con fines de vigilancia clandestina.

De otro modo, en el plano técnico, se ha avanzado en la adquisición de equipos con capacidad de vigilancia electrónica y detección de movimientos a baja altitud. La FAC ha incorporado sistemas FLIR (*Forward Looking Infrared*) en plataformas como el AC-47T "Fantasma" y el helicóptero Arpía IV, lo que ha permitido fortalecer la cobertura en zonas críticas del territorio nacional (Carrasquilla, 2021). No obstante, estos sistemas están orientados principalmente a operaciones ofensivas y no incluyen, hasta el momento, dispositivos de interferencia específicos contra drones, como inhibidores de frecuencia o bloqueadores de señal GPS.

Operacionalmente, la FAC ha integrado el uso de sistemas de vigilancia aérea en entornos rurales y urbanos, con especial atención en las áreas de alta vulnerabilidad, como las circunvecinas a las UMAS. Según el Informe de Gestión de la FAC (2021), se ha fortalecido el monitoreo mediante patrullajes aéreos regulares y sobrevuelos de reconocimiento en zonas donde se han reportado incursiones no autorizadas de drones (Carbajal, 2024). Asimismo, se ha promovido la cooperación interinstitucional con otras fuerzas y agencias de inteligencia para compartir información técnica sobre dispositivos detectados, rutas sospechosas y patrones de vuelo anómalos.

Una de las principales adaptaciones ha sido la inclusión de observadores técnicos entrenados en la identificación visual y auditiva de drones durante misiones de patrullaje. Esta práctica, aunque elemental, ha sido útil para establecer patrones de aparición de estos dispositivos, especialmente en horas nocturnas o en condiciones meteorológicas adversas. Sin embargo, la ausencia de herramientas automatizadas de detección, como radares específicos para bajas altitudes o sistemas electroópticos multiespectrales, limita seriamente la capacidad de respuesta.

Así las cosas, si bien la FAC ha realizado avances en términos de vigilancia, capacitación y cooperación institucional, sus operaciones de contrainteligencia aún carecen de una arquitectura tecnológica robusta para enfrentar eficazmente la amenaza que representan los drones. Las adaptaciones realizadas han respondido a un enfoque reactivo más que preventivo, y no se ha incorporado aún una doctrina específica de contramedidas electrónicas o físicas que permitan neutralizar esta amenaza antes de que comprometa la seguridad de sus instalaciones.

Para comprender con mayor claridad los avances y limitaciones de la Fuerza Aeroespacial Colombiana frente al uso de drones por parte de actores no estatales, resulta pertinente examinar el estado actual del ciclo de inteligencia en sus cuatro fases fundamentales: recolección, procesamiento, análisis y difusión. La siguiente tabla presenta un resumen comparativo entre las capacidades institucionales disponibles y las limitaciones que persisten específicamente frente a este tipo de amenaza tecnológica.

Tabla 1

Comparación del ciclo de inteligencia FAC frente a amenazas con drones

Fase del ciclo de inteligencia	Capacidades actuales de la FAC	Limitaciones frente a drones
Recolección	Uso de plataformas aéreas con sensores (FLIR, cámaras HD), observadores entrenados en campo	Ausencia de radares específicos de baja altitud y sistemas de detección automatizados
Procesamiento	Procesamiento manual y digital de imágenes y señales mediante softwares institucionales	Falta de integración con inteligencia artificial para clasificación de amenazas en tiempo real
Análisis	Análisis doctrinal con base en patrones de vuelo y registros de incursiones, uso de informes compartidos	Escasa capacidad predictiva ante nuevos tipos de drones o rutas no convencionales
Difusión	Difusión interna en canales militares, coordinación limitada con otras fuerzas y ausencia de alertas preventivas automatizadas	Difusión reactiva y poco oportuna, sin protocolos activos de respuesta inmediata ni alertas comunitarias

Fuente: Elaboración propia con base en doctrina institucional de la FAC, el Informe de Gestión FAC (2021), Carbajal (2024) y literatura especializada sobre drones y amenazas híbridas en seguridad nacional de Aya (2021).

Discusión y hallazgos

El análisis desarrollado en este capítulo permite identificar que la Fuerza Aeroespacial Colombiana ha iniciado un proceso de adaptación institucional ante el uso de drones por actores no estatales, especialmente en zonas de influencia directa como las áreas circunvecinas a las UMAS. Estas adaptaciones han estado centradas, en su mayoría, en el fortalecimiento del monitoreo aéreo, la capacitación básica del personal y la incorporación de sensores ópticos en plataformas de vigilancia táctica. Sin embargo, al examinar el ciclo de inteligencia en sus fases de recolección, procesamiento, análisis y difusión, se evidencian vacíos significativos en cuanto a la integración de tecnologías específicas para enfrentar esta amenaza híbrida.

Uno de los hallazgos más relevantes es la ausencia de contramedidas tecnológicas activas, como inhibidores de frecuencia, sistemas de neutralización electrónica o plataformas autónomas de detección temprana. Estas falencias responden tanto a limitaciones doctrinales como presupuestales, así como a la falta de una política institucional clara sobre la amenaza que representan los drones. Aunque existen esfuerzos interinstitucionales para compartir información e identificar patrones de comportamiento de estas aeronaves, la respuesta continúa siendo reactiva, con baja capacidad de anticipación. La evidencia revisada también muestra que otras fuerzas aéreas, como las de Israel o España, han integrado contramedidas como parte de su doctrina estándar de defensa en instalaciones militares, lo cual debe ser una referencia obligada para la FAC.

Estrategias actuales implementadas por la FAC para contrarrestar amenazas con drones en las UMAS

El incremento de amenazas híbridas en Colombia, particularmente el empleo de drones por actores no estatales en las zonas circunvecinas a las Unidades Militares Aéreas (UMAS), ha exigido una respuesta inmediata por parte de la Fuerza Aeroespacial Colombiana (FAC). Este capítulo tiene como propósito describir las estrategias actuales implementadas por la FAC para contrarrestar este tipo de incursiones, analizando tanto las acciones doctrinales y operativas como las capacidades tecnológicas puestas en marcha. La revisión se sustentará en documentos oficiales, manuales institucionales y literatura académica, incorporando además una mirada comparativa frente a experiencias internacionales relevantes, como las de Israel y España. Este análisis permitirá evidenciar fortalezas, vacíos y áreas de mejora dentro del ciclo de inteligencia y las operaciones de contrainteligencia desarrolladas por la FAC.

Doctrina y planificación estratégica en la respuesta a amenazas híbridas

La respuesta de la Fuerza Aeroespacial Colombiana (FAC) frente a las amenazas híbridas, en particular el uso de drones por actores no estatales se ha fundamentado en el marco doctrinal establecido por el Estado colombiano y en la planificación estratégica institucional. La Ley 1621 de 2013, que regula las actividades de inteligencia y contrainteligencia, constituye el pilar normativo que orienta las acciones de la FAC en materia de protección de infraestructuras críticas como las Unidades Militares Aéreas (UMAS). Adicionalmente, la Escuela de Inteligencia Aérea, Espacial y Ciberespacial y el Plan Estratégico Institucional

2030 han definido líneas de acción prioritarias en materia de vigilancia, control y respuesta frente a amenazas tecnológicas emergentes (Ministerio de Defensa Nacional, 2024).

Desde el plano doctrinal, la FAC ha fortalecido la formación especializada de su personal mediante la EIAEC, creada en 1998. Esta institución ha desarrollado programas académicos orientados a la inteligencia aérea, espacial y ciberespacial, incluyendo módulos específicos sobre amenazas asimétricas y el uso hostil de sistemas no tripulados (Contreras, 2010). Esta preparación doctrinal busca garantizar que las operaciones de contrainteligencia estén alineadas con los nuevos desafíos estratégicos.

La planificación estratégica de la FAC también se ha visto influenciada por conceptos como la superioridad aérea y el control del espacio aéreo, fundamentales para garantizar la libertad de operación y la protección de activos militares (Amaya, 2018). Estos enfoques doctrinales son compatibles con los postulados de la Teoría de la Seguridad Nacional (Wolfers, 1952) y la Teoría de la Guerra Asimétrica (Mack, 1975), que destacan la necesidad de adaptar las capacidades defensivas frente a actores que utilizan tácticas no convencionales.

A nivel operacional, la doctrina de respuesta frente a drones aún presenta vacíos importantes, ya que la FAC no cuenta con una directriz específica de contramedidas electrónicas para este tipo de amenaza. Sin embargo, se han iniciado procesos de actualización doctrinal, integrando el fenómeno de las amenazas híbridas dentro de los manuales de inteligencia operativa, en línea con recomendaciones del Congreso de Inteligencia Estratégica (ESICI, 2021) y experiencias regionales (Buelvas, Cabrera, & Vera, 2023). Cabe resaltar que la doctrina FAC ha comenzado a incorporar buenas prácticas internacionales. Casos como el de Israel y España, donde se han implementado sistemas de

defensa activa contra drones, han sido analizados por la FAC como referentes para futuras actualizaciones doctrinales y operativas (Gil, 2019).

Capacidades técnicas y operativas implementadas por la FAC

Frente al incremento del uso de drones como herramientas de amenaza híbrida, la Fuerza Aeroespacial Colombiana (FAC) ha implementado diversas estrategias operativas y técnicas orientadas a fortalecer la protección de las Unidades Militares Aéreas (UMAS). Estas medidas buscan optimizar la vigilancia, detección y respuesta ante incursiones aéreas no autorizadas.

En el ámbito tecnológico, la FAC ha potenciado el uso de plataformas aéreas dotadas de sensores avanzados como el sistema FLIR (*Forward Looking Infrared*), cámaras de alta definición y radares de vigilancia táctica (Hernández, 2019). Estos equipos han sido instalados en aeronaves como el AC-47T "Fantasma" y el helicóptero Arpía IV, lo que ha permitido mejorar la cobertura de áreas vulnerables. Además, la FAC ha fortalecido sus capacidades de vigilancia mediante el desarrollo de patrullajes aéreos regulares y sobrevuelos de reconocimiento en zonas con mayor índice de incidentes reportados (Carbajal, 2024).

Desde el plano humano, la institución ha capacitado a observadores técnicos en la identificación visual y auditiva de drones, especialmente en condiciones adversas y horarios nocturnos (ESICI, 2021). Estos observadores cumplen un rol clave dentro de las misiones de patrullaje y monitoreo de perímetro en las UMAS, actuando como la primera línea de alerta frente a posibles amenazas.

En cuanto a la coordinación interinstitucional, la FAC ha promovido el intercambio de información operativa con el Ejército Nacional, la Policía Nacional y agencias de inteligencia. Esta articulación busca establecer patrones de comportamiento de los drones

detectados y fortalecer los protocolos de respuesta conjunta, en línea con las recomendaciones del Ministerio de Defensa Nacional (2024) y las prácticas sugeridas por Buelvas et al. (2023). Pero, aun así, persisten limitaciones significativas.

La FAC aún carece de sistemas específicos de contramedidas electrónicas para la neutralización activa de drones, tales como inhibidores de frecuencia, bloqueadores de señal GPS o sistemas de detección automática a baja altitud (Corredor, 2024). Esta carencia tecnológica sitúa a la institución en una posición reactiva, donde las acciones de respuesta dependen, en gran medida, de la capacidad de vigilancia humana y de los medios de detección convencionales.

Adicionalmente, informes recientes señalan que los procedimientos actuales de la FAC en materia de drones no están estandarizados doctrinalmente, lo que genera diferencias operativas entre las diversas unidades desplegadas en el territorio nacional (Carrasquilla, 2021). Esta falta de homogeneidad limita la efectividad de las estrategias implementadas y evidencia la necesidad de consolidar una doctrina específica para la defensa anti drones.

En ese orden, el proceso de modernización tecnológica avanza de forma gradual, incluyendo la evaluación de sistemas extranjeros de defensa activa contra drones, con miras a futuras adquisiciones e integración de capacidades (Ministerio de Defensa Nacional, 2024).

Análisis comparativo: experiencias internacionales y aplicabilidad en Colombia

La creciente amenaza que representan los drones para la seguridad de las instalaciones militares ha llevado a diversas fuerzas aéreas del mundo a implementar estrategias avanzadas de detección, neutralización y respuesta. En este contexto, resulta pertinente analizar las experiencias de países como Israel y España, cuya gestión frente a amenazas híbridas ofrece lecciones aplicables a la realidad colombiana.

En el caso de Israel, la doctrina de defensa aérea se ha caracterizado por la adopción de un enfoque preventivo y tecnológicamente avanzado. Según Bajo (2019) y Aya (2021), las Fuerzas de Defensa de Israel (FDI) han integrado sistemas C-UAS (*Counter Unmanned Aircraft Systems*) que incluyen radares de baja altitud, inhibidores de señal GPS y tecnologías de interferencia electrónica. Estos dispositivos permiten la detección temprana y la neutralización automática de drones hostiles antes de que comprometan la seguridad de las bases militares.

España, por su parte, ha desarrollado un marco normativo y operativo orientado a la protección de infraestructuras críticas frente a amenazas con drones. Según Gil (2019), el Ministerio de Defensa español ha implementado procedimientos estándar de detección y neutralización de drones, integrando vigilancia electrónica, sensores multiespectrales y sistemas de bloqueo de comunicaciones. Además, se han fortalecido los protocolos de coordinación interinstitucional, involucrando a fuerzas armadas, cuerpos de seguridad y agencias de inteligencia.

Comparando estas experiencias con la situación actual de la FAC, se evidencian diferencias significativas en términos de capacidades tecnológicas y doctrinales. Mientras Israel y España han logrado consolidar doctrinas específicas para el combate contra drones, la FAC aún carece de un documento doctrinal exclusivo para este tipo de amenazas. Asimismo, las limitaciones en la adquisición de tecnología de contramedidas electrónicas colocan a Colombia en una posición de desventaja operativa (Sánchez & Rodríguez, 2006).

Sin embargo, algunos aspectos de estas experiencias internacionales son replicables. La FAC podría avanzar en la implementación de sistemas de detección automatizada, el fortalecimiento de la interoperabilidad con otras fuerzas y la actualización de sus manuales

de operación incorporando procedimientos específicos de defensa anti drones. En este sentido, el fortalecimiento de la formación técnica del personal, como lo han hecho las fuerzas israelíes y españolas, resulta una prioridad inmediata para garantizar la protección efectiva de las UMAS frente a amenazas aéreas no tripuladas. La revisión de estos casos de estudio resalta la necesidad de una transformación doctrinal y tecnológica en la FAC, orientada hacia un modelo de defensa activa y proactiva frente a las amenazas híbridas actuales (Suarez, 2023).

A partir del análisis doctrinal, técnico y operativo realizado, resulta oportuno sintetizar los principales hallazgos mediante una comparación estructurada entre las estrategias actuales de la FAC y las mejores prácticas internacionales en defensa anti drones. Esta comparación permitirá visualizar de manera integral las capacidades existentes, las limitaciones identificadas y las oportunidades de mejora que tiene la Fuerza Aeroespacial Colombiana frente a las amenazas híbridas generadas por el uso de drones en las áreas circunvecinas a las UMAS (Taborda & Palacio, 2020). La siguiente tabla presenta un análisis de contenido profundo, que integra criterios doctrinales, tecnológicos, de formación, interoperabilidad e inteligencia, con el fin de ofrecer un panorama claro y fundamentado que sirva como insumo para el diseño de futuras estrategias de adaptación (Villamizar & Pedraza, 2023).

Tabla 2 Análisis de las estrategias actuales de la FAC frente a amenazas con drones: comparación con experiencias internacionales

Dimensión de análisis	Situación actual en la FAC	Limitaciones identificadas	Buenas prácticas internacionales (Israel y España)	Implicaciones para la FAC
Doctrina y normatividad	Basada en la Ley 1621 de 2013 y en lineamientos generales del Sistema Nacional de Inteligencia (EIAEC). Ausencia de un manual específico para contramedidas frente a drones.	Falta de doctrina específica en defensa anti drones. No existen protocolos estandarizados para UMAS.	Israel ha desarrollado doctrinas específicas para amenazas aéreas no tripuladas (Bajo, 2019). España cuenta con procedimientos normativos de respuesta rápida (Gil, 2019).	Es urgente que la FAC elabore un manual doctrinal exclusivo para defensa anti drones, ajustado al contexto nacional.
Capacidades tecnológicas	Uso de sensores FLIR, cámaras HD y plataformas de patrullaje aéreo (Hernández, 2019).	No existen sistemas automatizados de detección a baja altitud ni inhibidores de frecuencia o bloqueadores GPS (Corredor, 2024).	Israel dispone de sistemas C-UAS integrados; España ha implementado sistemas de inhibición y detección electrónica.	La FAC debe priorizar la adquisición de tecnología C-UAS de última generación, adecuada a la topografía y amenaza local.
Formación y capacitación	La formación está centrada en inteligencia aérea tradicional y observación visual (Contreras, 2010; FAC, 2021).	Limitada especialización en técnicas de detección electrónica y en neutralización de drones.	Israel ha establecido centros de entrenamiento específicos para contramedidas electrónicas; España incluye simulación de amenazas híbridas en su formación militar (Aya, 2021).	La FAC debe crear módulos de entrenamiento en guerra electrónica y defensa anti drones dentro de su Escuela de Inteligencia Aérea.
Interoperabilidad interinstitucional	Existen acuerdos básicos de intercambio de información con Ejército y Policía (FAC, 2021; Ministerio de Defensa Nacional, 2024).	Limitada articulación táctica. Falta de protocolos de respuesta conjunta y de mecanismos de alerta temprana.	España ha implementado centros de comando conjunto (C2) para amenazas híbridas. Israel tiene canales permanentes de coordinación entre inteligencia militar y civil.	Se requiere fortalecer la interoperabilidad mediante la creación de un Centro de Fusión de Inteligencia Anti drones que involucre a todas las fuerzas armadas y agencias de seguridad.
Inteligencia y análisis de amenazas	La FAC realiza análisis post-incidente y monitoreo reactivo basado en reportes de campo (Villamizar & Pedraza, 2023).	Ausencia de capacidades predictivas y de análisis en tiempo real. No se usa inteligencia artificial para el procesamiento de patrones de vuelo.	Israel emplea análisis de *big data* e inteligencia artificial para anticipar incursiones. España usa sistemas automatizados de reconocimiento de patrones de amenaza (Osorio, 2023; Pulido, 2017).	La FAC debería integrar herramientas de análisis predictivo y procesamiento de datos en tiempo real para fortalecer la fase de análisis del ciclo de inteligencia.

Fuente: Elaboración propia con base en Contreras (2010), FAC (2021), Corredor (2024), Gil (2019), Aya (2021), Ministerio de Defensa Nacional (2024), entre otros.

La presentación de esta tabla resulta oportuna y necesaria dentro del estudio de caso que aborda el presente artículo, ya que permite consolidar, de manera clara y comparativa, los principales aspectos que determinan la capacidad de la FAC para enfrentar amenazas híbridas como el uso de drones por actores no estatales. Además, facilita la identificación de las brechas tecnológicas, doctrinales y operativas que aún persisten, sirviendo como una herramienta de diagnóstico estratégico (Giraldo, 2023).

Este análisis comparativo no solo contextualiza las acciones actuales de la FAC, sino que también proporciona una base sólida para el desarrollo del siguiente capítulo, en el cual se formularán propuestas concretas orientadas a fortalecer las capacidades de contrainteligencia en las UMAS, alineadas con estándares internacionales y con la realidad operacional del país.

Estrategias prospectivas para fortalecer la contrainteligencia aérea frente a las diferentes amenazas hibridas

En el contexto actual de las amenazas híbridas, el uso de drones por parte de actores no estatales se ha consolidado como un recurso táctico que combina capacidades tecnológicas con métodos asimétricos para vulnerar la seguridad nacional. Si bien la neutralización física de estas aeronaves corresponde a las unidades de seguridad y defensa de bases, la contrainteligencia desempeña un papel fundamental en el ciclo previo a la acción: identificar, obtener, procesar y difundir información que permita anticipar y desarticular la amenaza antes de que se materialice (FAC, 2024).

Este enfoque implica que la Contrainteligencia Aérea concentre sus esfuerzos en la recolección de información de diversas fuentes, el análisis de patrones de empleo de drones y la integración de datos con otros organismos para generar alertas tempranas y recomendaciones operativas. De esta manera, la contrainteligencia no solo apoya las operaciones defensivas, sino que contribuye a una estrategia integral de protección de las Unidades Militares Aéreas (UMAS) frente a un adversario que evoluciona constantemente y emplea tácticas propias de la guerra híbrida.

Recolección y análisis de información sobre amenazas híbridas con drones

La primera línea de acción de la contrainteligencia frente a amenazas híbridas como el uso de drones por actores no estatales es la recolección sistemática de información que permita caracterizar el riesgo y anticipar posibles ataques. En este proceso, la recolección no se limita a la observación directa, sino que involucra una amplia gama de fuentes y técnicas, combinando inteligencia humana (HUMINT), inteligencia de señales (SIGINT), inteligencia

de fuentes abiertas (OSINT) y medios técnicos especializados para identificar patrones de empleo de estos sistemas aéreos no tripulados (Arquilla & Ronfeldt, 2001).

La HUMINT permite a la Fuerza Aeroespacial Colombiana acceder a información obtenida de contactos en el terreno, comunidades y fuentes infiltradas, quienes pueden aportar datos sobre la adquisición, modificación o uso de drones en áreas cercanas a las Unidades Militares Aéreas. Por su parte, la SIGINT ofrece capacidades para interceptar comunicaciones y señales electromagnéticas asociadas al control y navegación de estos dispositivos, mientras que la OSINT aprovecha la información disponible en redes sociales, foros y mercados en línea donde los grupos irregulares intercambian conocimiento técnico o comercializan componentes (LISA Institute, 2024).

Una vez recopilada, la información debe ser sometida a un proceso de análisis integral, orientado a transformar datos fragmentados en inteligencia procesable. Este análisis implica identificar tendencias geográficas, horarios recurrentes de incursiones, tipos de drones empleados, capacidades de carga y posibles rutas de aproximación. La integración de estas variables permite elaborar perfiles de amenaza y mapas de riesgo que sirven como insumo para operaciones preventivas.

La contrainteligencia, además, debe garantizar que la información relevante sea difundida de manera oportuna a las unidades responsables de la defensa física y al alto mando, asegurando que las medidas tácticas respondan a datos verificados y actualizados. En este sentido, la generación de alertas tempranas, basadas en evidencia y en el cruce de datos interinstitucionales, constituye un elemento crítico para la neutralización de la amenaza.

Procesamiento y difusión de inteligencia para neutralizar la amenaza

El valor de la información recolectada por la contrainteligencia de la Fuerza Aeroespacial Colombiana frente a amenazas híbridas con drones radica en su capacidad para ser transformada en inteligencia procesable, oportuna y útil para la toma de decisiones operativas y estratégicas. El procesamiento de la información implica clasificar, verificar y correlacionar los datos obtenidos de diversas fuentes, con el fin de identificar patrones confiables que permitan anticipar las acciones del adversario (Dekens, 2025).

Este proceso se apoya en herramientas de análisis de datos, software de correlación y técnicas de fusión de inteligencia, que permiten integrar insumos de naturaleza diversa como registros visuales, intercepciones de comunicaciones, reportes de patrullaje y observaciones de campo en un marco analítico coherente. De esta forma, es posible establecer vínculos entre incidentes aparentemente aislados y construir una narrativa de amenaza que oriente la respuesta institucional (Fajardo, 2018).

La difusión de la inteligencia es igualmente crítica. Una vez procesada, la información debe transmitirse a las unidades responsables de la defensa física de las Unidades Militares Aéreas, así como a los mandos operacionales y estratégicos, de forma que puedan planificar acciones preventivas o reactivas. Este flujo debe realizarse bajo criterios de oportunidad, pertinencia y seguridad, evitando filtraciones que puedan comprometer las operaciones.

La contrainteligencia, además, tiene la responsabilidad de producir alertas tempranas, basadas en indicadores confiables, que permitan activar protocolos de protección antes de que el adversario ejecute su acción. Estas alertas, cuando se difunden de manera coordinada

con otras agencias del Estado, aumentan la capacidad de respuesta conjunta y mejoran la efectividad de las medidas defensivas.

Por último, la etapa de difusión no debe limitarse al ámbito militar. En situaciones donde la amenaza pueda impactar a la población civil o a infraestructura estratégica de carácter dual, la FAC debe coordinar con autoridades locales y organismos civiles para garantizar que la respuesta sea integral. Así, el procesamiento y la difusión de inteligencia se convierten en un multiplicador de fuerza que incrementa la capacidad de neutralizar amenazas híbridas antes de que se materialicen.

Coordinación interinstitucional e interoperabilidad en el marco de amenazas híbridas

La naturaleza interdisciplinaria de las amenazas híbridas con drones exige que la contrainteligencia de la Fuerza Aeroespacial Colombiana actúe dentro de un esquema de cooperación interinstitucional e interoperabilidad operativa (CACOM2, 2023). Ninguna entidad, por sí sola, posee todas las capacidades necesarias para identificar, monitorear y neutralizar estas amenazas; por ello, la articulación entre fuerzas militares, organismos de inteligencia, autoridades civiles y agencias especializadas resulta esencial.

En este marco, la contrainteligencia desempeña el rol de nodo central de información, encargada de recibir, analizar y compartir datos con el Ejército Nacional, la Armada de Colombia, la Policía Nacional, la Dirección Nacional de Inteligencia y otras instituciones que participan en la defensa y seguridad (CEDOE, 2017). Este intercambio de información, cuando se realiza de manera sistemática y bajo protocolos de seguridad bien definidos, fortalece la capacidad de detección temprana y la planeación de operaciones preventivas.

La interoperabilidad no se limita al ámbito técnico, como el uso de plataformas compartidas de análisis y comunicación segura, sino que también implica la armonización de doctrinas, procedimientos y estándares. Esto asegura que, ante una amenaza detectada, las distintas entidades involucradas actúen con rapidez, coherencia y coordinación, evitando duplicidad de esfuerzos y lagunas de responsabilidad (Rueda, 2021).

Asimismo, la contrainteligencia debe fomentar la cooperación internacional en este campo, aprovechando las experiencias de países que han desarrollado doctrinas y tecnologías avanzadas contra drones empleados en conflictos híbridos. La participación en ejercicios combinados, seminarios especializados y redes de intercambio de inteligencia fortalece la preparación de la FAC para enfrentar escenarios cada vez más complejos (Arias, 2020).

En definitiva, la coordinación interinstitucional y la interoperabilidad son multiplicadores estratégicos de la capacidad de respuesta nacional frente a amenazas híbridas con drones. En la medida en que la contrainteligencia logre integrar eficazmente la información y los recursos de todos los actores relevantes, se incrementará la probabilidad de neutralizar las amenazas antes de que comprometan la seguridad de las Unidades Militares Aéreas y de la infraestructura crítica del país.

El análisis desarrollado a lo largo de esta sección demuestra que la respuesta eficaz de la contrainteligencia de la Fuerza Aeroespacial Colombiana frente a amenazas híbridas con drones depende de un ciclo integral compuesto por recolección precisa de información, procesamiento y difusión oportuna de inteligencia, y una coordinación interinstitucional robusta. La recolección y análisis permiten detectar patrones de uso, identificar actores y anticipar posibles escenarios de riesgo. El procesamiento y difusión aseguran que la información se convierta en inteligencia útil para la toma de decisiones y que llegue, de

manera segura y a tiempo, a quienes deben ejecutar las acciones preventivas o de neutralización. Finalmente, la coordinación e interoperabilidad potencian la capacidad de respuesta al integrar recursos, capacidades y conocimientos de múltiples actores nacionales e internacionales.

Este modelo de actuación posiciona a la contrainteligencia no como un elemento periférico, sino como el eje articulador de la defensa estratégica frente a drones en el contexto de amenazas híbridas. Su valor radica en anticiparse a la acción del adversario mediante información verificada y análisis riguroso, generando alertas tempranas y líneas de acción que permiten reducir la ventana de vulnerabilidad. Así, la SINA fortalece la capacidad de la FAC para proteger las Unidades Militares Aéreas y la infraestructura crítica del país, contribuyendo de forma decisiva a la seguridad y estabilidad nacional.

Conclusiones

El presente estudio ha evidenciado que el uso de drones por parte de actores no estatales constituye una amenaza híbrida de alta complejidad para la seguridad nacional y, en particular, para la protección de las Unidades Militares Aéreas (UMAS) de la Fuerza Aeroespacial Colombiana (FAC). Este fenómeno, caracterizado por su adaptabilidad tecnológica y capacidad de operar de forma asimétrica, exige respuestas integrales que trasciendan la neutralización física de los artefactos para centrarse en la anticipación, el análisis y la desarticulación temprana de la amenaza.

La investigación ha demostrado que el verdadero potencial de la contrainteligencia radica en su capacidad de detectar patrones de amenaza, procesar información de manera rigurosa y coordinar acciones interinstitucionales, generando inteligencia procesable que

alimente las decisiones estratégicas y tácticas. En este sentido, la recolección sistemática de información a través de HUMINT, SIGINT, OSINT y medios técnicos, el análisis de datos orientado a la generación de perfiles de riesgo y la difusión oportuna de alertas tempranas son elementos esenciales para incrementar la capacidad de anticipación operativa de la FAC.

Asimismo, el fortalecimiento de la coordinación e interoperabilidad con otras Fuerzas, agencias de inteligencia y organismos internacionales se presenta como un multiplicador estratégico indispensable. Esta articulación no solo optimiza recursos y capacidades, sino que también permite integrar experiencias y doctrinas que han demostrado eficacia en otros escenarios de confrontación tecnológica.

Acorde a lo anterior, el estudio subraya que la eficacia de cualquier estrategia frente a drones en el marco de amenazas híbridas depende de la consolidación de un ciclo de contrainteligencia robusto, ágil y tecnológicamente respaldado, capaz de adaptarse a la rápida evolución del adversario. La FAC, al situar a la contrainteligencia como pilar de su respuesta, no solo mejora su capacidad de protección de las UMAS, sino que refuerza su contribución a la defensa del espacio aéreo nacional y a la preservación de la soberanía.

Referencias

Amaya, M. F. (2018). *La superioridad aérea y su relación con las operaciones conjuntas* . Obtenido de https://bit.ly/4hDeYap

Arias, J. C. (2020). *Consideraciones de contrainteligencia en la formulación de estrategias de seguridad: utopía o evolución pragmática*. Obtenido de https://revistas.flacsoandes.edu.ec/urvio/article/view/4226/3258

Arquilla, J., & Ronfeldt, D. (2001). *Networks and Netwars. The Future of Terror, Crime, and Militancy.* Obtenido de https://www.rand.org/pubs/monograph_reports/MR1382.html

Aya, L. A. (2021). *Las amenazas híbridas, un nuevo escenario para el Ejército Nacional*. Obtenido de https://revistascedoc.com/index.php/bep/article/view/529

Bajo, M. G. (2019). *Reflexiones sobre la guerra asimétrica a través de la historia*. Obtenido de https://revistas.flacsoandes.edu.ec/urvio/article/download/3522/2644

Buelvas, E. P., Cabrera, F., & Vera, D. (2023). *Transición del orden mundial: impactos en las estrategias de seguridad y defensa en Colombia y la región*. Obtenido de https://esdeglibros.edu.co/index.php/editorial/catalog/view/257/214/3276

CACOM2. (2023). *Capacidad anti drones es implementada en el Comando Aéreo de Combate No.2*. Obtenido de https://www.fac.mil.co/es/noticias/capacidad-anti-drones-es-implementada-en-el-comando-aereo-de-combate-no2

Carbajal, F. E. (2024). *Uso de drones en las operaciones policiales para mejorar el patrullaje integrado y combatir la inseguridad ciudadana*. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=9728151

Carrasquilla, P. A. (2021). *Capacidades distintivas de la FAC como elementos de disuasión en el marco de cooperación con la OTAN*. Obtenido de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1909-30632021000100049

CEDOE. (2017). *MFRE 2-0*. Obtenido de https://www.cedoe.mil.co/enio/recurso_user/doc_contenido_pagina_web/800130633_4/458748/mfre_2_0_inteligencia.pdf

Contreras, T. E. (2010). *Escuela de Inteligencia Aérea*. Obtenido de https://bit.ly/4jGEAFo

Corredor, H. C. (2024). *El uso de drones en seguridad y como amenaza: Análisis y medidas defensivas en Colombia* . Obtenido de https://colpap.org/2024/10/27/el-uso-de-drones-en-seguridad-y-como-amenaza-analisis-y-medidas-defensivas-en-colombia/?utm_source=chatgpt.com

Dekens, N. (2025). *Open Source Intelligence (OSINT): What It Is, How It Works, and Why It Matters (+ Tools, Techniques & Use Cases)*. Obtenido de https://shadowdragon.io/blog/what-is-osint/

EIAEC. (2025). *Escuela de Inteligencia Aérea Espacial y Ciberespacial.* Obtenido de https://www.fac.mil.co/es/esina

ESICI. (2021). *Congreso de Inteligencia Estratégica*. Obtenido de https://esici.edu.co/index.php/ii-congreso-internacional-de-inteligencia-estrategica/

FAC. (2021). *Informe de Gestión Fuerza Aérea Colombiana 2021* . Obtenido de https://bit.ly/42U5pzZ

FAC. (2024). *Ciudadanos, recuerden que el uso de los drones está prohibido cerca de las Unidades Militares.* Obtenido de https://www.fac.mil.co/es/noticias/ciudadanos-recuerden-que-el-uso-de-los-drones-esta-prohibido-cerca-de-las-unidades

FAC. (2025). *Estrategia para el Desarrollo Aéreo y Espacial de la Fuerza Aérea Colombiana 2042.* Obtenido de https://www.fac.mil.co/planeacion/planes-estrategicos-sector-defensa-y-fuerza-aerea-colombiana

Fajardo, J. A. (2018). *Analytics, Big Data y BI - Transformar datos en conocimiento*. Obtenido de https://repository.umng.edu.co/items/585bfbe0-ac25-476a-8879-9dea74002936

Gil, J. M. (2019). *El tratamiento informativo de la guerra híbrida de Rusia*. Obtenido de https://www.redalyc.org/journal/5526/552661588007/html/

Giraldo, E. J. (2023). *Drones: la tecnología avanza pero, ¿y la regulación?* -. Obtenido de https://lexir.co/2023/03/20/drones-la-tecnologia-avanza-pero-y-la-regulacion/

Hernández, D. (2019). *Armas aire-superficie en la Fuerza Aérea Colombiana*. Obtenido de https://bit.ly/4hhkQ9F

LISA Institute. (2024). *HUMINT: Ejemplos, tipos y motivaciones de las Fuentes Humanas*. Obtenido de https://www.lisainstitute.com/blogs/blog/humint-ejemplos-tipos-fuentes-humanas

Mack, A. (1975). *Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict*. Obtenido de https://www.jstor.org/stable/2009880

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*. Obtenido de https://www.mindefensa.gov.co/prensa/noticia-visualizacion/noticias-prensa-colombia-refuerza-su-seguridad

Pulido, J. (2017). *La amenaza de la insurgencia criminal en ColombiaEl concepto de Inteligencia híbrida como nueva forma de adaptación de las estrategias tradicionales contrainsurgentes* . Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=6289770

Rodríguez, A. G. (2015). *La importancia del poder aéreo integral en la defensa, seguridad y progreso del Estado Nación*. Obtenido de https://bit.ly/3EeaCIy

Rueda, G. R. (2021). *Interoperabilidad, una capacidad de la Fuerza con valor exponencial*. Obtenido de https://www.fac.mil.co/es/editorial-comandante-fac/interoperabilidad-una-capacidad-de-la-fuerza-con-valor-exponencial

Sampieri, M. e., Fernández, D., & Lucio, D. (2000). *Metodología de la Investigación*. Obtenido de https://www.uv.mx/personal/cbustamante/files/2011/06/Metodologia-de-la-Investigaci%C3%83%C2%B3n_Sampieri.pdf

Sánchez, R., & Rodríguez, F. (2006). *Seguridad nacional: el realismo y sus contradictores* . Obtenido de https://revistas.urosario.edu.co/index.php/desafios/article/view/758

Suarez, J. S. (2023). *Ciberseguridad, un desafío para las Fuerzas Militares colombianas en la era digital*. Obtenido de https://revistascedoc.com/index.php/pei/article/view/628

Taborda, A. E., & Palacio, L. (2020). *La inteligencia militar como actor fundamental en el afianzamiento de los escenarios de paz*. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=7647693

Villamizar, A. O., & Pedraza, L. (2023). *Características metodológicas del análisis de información en la inteligencia policial de Colombia*. Obtenido de https://www.redalyc.org/journal/5177/517775572006/html/

Wolfers, A. (1952). *National Security" as an Ambiguous Symbol*. Obtenido de https://www.jstor.org/stable/2145138