Estrategias de Ciberdefensa para contrarrestar el uso malicioso de drones en el Ejército Nacional de Colombia.

Mayor (My) Julián Aldeisy Martinez Rueda

Artículo para optar al título profesional:

Magister en Ciberdefensa y Ciberseguridad

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	**:**	Julián Aldeisy Martinez Rueda
Identificación	**:**	1098605391
Programa académico	**:**	Maestría en Ciberseguridad y Ciberdefensa
Tutor metodológico	**:**	Jairo Andrés Becerra Ortiz
Tutor temático	**:**	Aldair José Bueno Atencio
Fecha de entrega	**:**	25-ago-2025
Extensión	**:**	8960

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.

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

Estrategias de Ciberdefensa para contrarrestar el uso malicioso de drones en el Ejército Nacional de Colombia.

Cyberdefense strategies to counter the malicious use of drones in the Colombian National Army.

Julián Aldeisy Martinez Rueda [1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: La proliferación de sistemas aéreos no tripulados (drones) y su adaptación para fines maliciosos constituye una amenaza asimétrica creciente para la seguridad nacional, desafiando las capacidades defensivas del Ejército Nacional de Colombia. Este artículo analiza las vulnerabilidades técnicas de los drones tipo multirrotor, con énfasis en sus sistemas de comunicación, navegación y firmware, y evalúa las herramientas de ciberseguridad actuales, incluyendo métodos de detección de spoofing y jamming. A través de una revisión sistemática de literatura especializada y del análisis de modelos internacionales, se propone un protocolo de ciberdefensa adaptado al contexto colombiano que incorpora elementos tecnológicos, jurídicos y éticos en el ámbito de la dimensión cognitiva del ciberespacio. Los hallazgos evidencian la necesidad de fortalecer la doctrina nacional en ciberseguridad mediante capacidades autónomas, interoperables y humanamente supervisadas.

Palabras clave: Ciberdefensa, UAV, Spoofing, Jamming, Ejército Nacional de Colombia, C-UAS, Guerra Asimétrica.

Abstract: The proliferation of unmanned aerial systems (drones) and their adaptation for malicious purposes pose an increasing asymmetric threat to national security, challenging the defensive capabilities of the Colombian National Army. This article analyzes the technical vulnerabilities of multirotor UAVs, focusing on their communication, navigation, and firmware systems, and evaluates current cybersecurity tools, including spoofing and jamming detection techniques. Through a systematic literature review and an analysis of international models, a cybersecurity protocol is proposed, tailored to the Colombian context, which integrates technological, legal, and ethical components within the cognitive dimension of cyberspace. The findings highlight the need to strengthen national cybersecurity doctrine through autonomous, interoperable capabilities that remain under meaningful human control.

[1] Mayor del Ejército Nacional de Colombia. Candidato a magíster en Ciberseguridad y Ciberdefensa, 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/0000-0003-2004-7466 - Contacto: julian.martinez@esdeg.edu.co.

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

Keywords: Cyberdefense, UAV, Spoofing, Jamming, Colombian National Army, C-UAS, Asymmetric Warfare

Introducción

La vertiginosa evolución y la creciente accesibilidad de los vehículos aéreos no tripulados (UAVs), comúnmente conocidos como drones, han transformado significativamente diversos sectores. Su versatilidad y capacidad para operar en entornos complejos los han convertido en herramientas indispensables. Sin embargo, esta misma versatilidad y relativa facilidad de adquisición han abierto una nueva y preocupante dimensión en el panorama de las amenazas a la seguridad. Los drones, particularmente los de tipo multirrotor, se han erigido como potenciales vectores para actividades maliciosas (Gupta et al., 2018; Motlagh et al., 2017). Esta emergente amenaza exige una comprensión profunda de las vulnerabilidades inherentes a estos sistemas y el desarrollo de estrategias de ciberdefensa robustas y efectivas.

La naturaleza inherentemente digital de los drones los convierte en objetivos atractivos para ataques cibernéticos. Su funcionamiento depende de intrincados sistemas de comunicación inalámbrica, de complejos sistemas de navegación basados en señales de satélite, y de software y firmware que orquestan sus funciones (Li et al., 2019). Cada uno de estos componentes representa un posible punto de entrada para actores malintencionados que buscan explotar debilidades para tomar el control del dron o interrumpir sus operaciones (Khan et al., 2020; Yan et al., 2019). Ante este escenario, la ciberdefensa contra drones maliciosos se ha convertido en un campo de investigación de vital importancia para garantizar la seguridad pública y proteger infraestructuras críticas.

El presente trabajo de investigación se inscribe en este contexto crítico y se articula en torno a tres objetivos específicos interrelacionados. En primer lugar, se busca identificar

las vulnerabilidades de ciberseguridad que afectan a los drones maliciosos tipo UAV multirrotores, analizando las debilidades presentes en sus sistemas de comunicación, navegación, software y firmware, así como en sus sensores y carga útil (Shafique et al., 2021; Kerns et al., 2014; Suryadi et al., 2020). Paralelamente, se explorarán las estrategias de ciberdefensa actualmente propuestas o implementadas a nivel internacional para mitigar estos riesgos (Islam et al., 2021).

En segundo lugar, la investigación se centrará en contrarrestar drones maliciosos a partir de la identificación de herramientas y protocolos de ciberseguridad específicamente diseñados para proteger el componente de GPS y navegación. Dado que la dependencia de las señales de navegación global por satélite (GNSS) representa una vulnerabilidad significativa, se explorarán técnicas de detección y mitigación de ataques como el GPS spoofing y el jamming (Takahashi et al., 2018; Psiaki & Humphreys, 2016). La identificación de protocolos y herramientas de ciberseguridad robustos en este ámbito resulta crucial para preservar la integridad de la navegación de los drones propios.

Finalmente, el tercer objetivo consiste en proponer un protocolo con una estrategia de ciberdefensa adaptada a las necesidades y el contexto del Ejército Nacional de Colombia, con base en las mejores prácticas internacionales identificadas en los objetivos anteriores (Magazzeni et al., 2022). Este protocolo buscará integrar medidas preventivas, mecanismos de detección temprana y estrategias de respuesta efectivas para contrarrestar el uso malicioso de drones en el ámbito de la seguridad nacional.

A través de la consecución de estos objetivos, esta investigación pretende contribuir al conocimiento y al desarrollo de capacidades en el campo de la ciberdefensa contra drones maliciosos, ofreciendo un análisis detallado de las vulnerabilidades existentes, las

estrategias de mitigación disponibles y una propuesta concreta para fortalecer la seguridad frente a esta creciente amenaza. La urgencia de abordar esta problemática radica en el potencial disruptivo y dañino que el uso malicioso de drones puede acarrear, haciendo imperativo el desarrollo de contramedidas efectivas.

Metodología

La presente investigación adopta una metodología de revisión sistemática de la literatura para abordar el objetivo de identificar las vulnerabilidades y estrategias de ciberdefensa frente a drones maliciosos tipo UAV multirrotores, así como para fundamentar el desarrollo de una propuesta de protocolo para el Ejército Nacional de Colombia. Una revisión sistemática se considera el método más apropiado para sintetizar el conocimiento existente sobre un tema específico, utilizando un proceso explícito y reproducible para identificar, seleccionar y evaluar críticamente la investigación relevante (Fink, 2019). Este enfoque permite obtener una visión integral y actualizada del estado del arte en la ciberdefensa contra drones, identificando tanto las áreas de consenso como las lagunas en la investigación.

La primera etapa de esta metodología consistió en la identificación de literatura relevante. Se llevó a cabo una búsqueda exhaustiva en diversas bases de datos académicas y repositorios digitales, incluyendo IEEE Xplore, ACM Digital Library, ScienceDirect, Scopus y Google Scholar. Se emplearon una combinación de palabras clave y operadores booleanos para asegurar la amplitud y precisión de la búsqueda. Los términos clave utilizados incluyeron: "ciberseguridad drones", "seguridad UAV", "amenazas drones", "vulnerabilidades drones", "ataques a drones", "ciberdefensa drones", "contramedidas

drones", "GPS spoofing drones", "GPS jamming drones", "seguridad comunicaciones UAV", "firmware seguridad drones", y "seguridad carga útil drones". Se consideraron artículos publicados en inglés y español, principalmente en el periodo comprendido entre 2014 y la actualidad, dada la relativa novedad y rápida evolución del campo.

La segunda etapa se centró en la selección de los estudios. Los resultados de la búsqueda inicial fueron filtrados en base a criterios de inclusión y exclusión predefinidos. Los criterios de inclusión consideraron artículos académicos que abordaran directamente las vulnerabilidades de ciberseguridad en drones UAV multirrotores o que propusieran o analizaran estrategias de ciberdefensa contra este tipo de amenazas. Se priorizaron artículos de investigación originales, revisiones sistemáticas y actas de conferencias de reconocido prestigio. Los criterios de exclusión incluyeron estudios que se centraran en aspectos no relacionados con la ciberseguridad (como la autonomía del vuelo o aplicaciones específicas no vinculadas a amenazas), artículos de divulgación no académica, y aquellos que no especificaran el tipo de dron analizado o que se centraran exclusivamente en drones de ala fija. Tras la aplicación de estos criterios, se seleccionaron los 30 artículos académicos que constituyen la base del análisis para el primer objetivo específico de esta investigación.

La tercera etapa implicó la extracción y síntesis de datos. Para cada uno de los 30 artículos seleccionados, se procedió a extraer información específica y relevante para los objetivos de la investigación. Esta información incluyó: autor(es), año de publicación, título del artículo, un resumen conciso del tema tratado, citas relevantes (directas o paráfrasis significativas), la editorial o publicación, y el enlace o DOI. Se diseñó una matriz de extracción de datos para asegurar la consistencia y sistematicidad en la recopilación de la información. Posteriormente, los datos extraídos fueron analizados mediante una síntesis

temática, buscando identificar patrones recurrentes en las vulnerabilidades reportadas y en las estrategias de ciberdefensa propuestas. Este proceso permitió agrupar las vulnerabilidades en categorías principales (comunicación, navegación, software/firmware, sensores/carga útil) y analizar las estrategias de ciberdefensa correspondientes.

Finalmente, la cuarta etapa consistió en la presentación de los resultados, integrando la información de los 30 artículos de manera lógica y coherente para dar respuesta al primer objetivo específico de la investigación. A lo largo de todo el proceso, se aplicaron rigurosamente las normas de la séptima edición de la American Psychological Association (APA) para la citación de fuentes y la elaboración de la lista de referencias, asegurando la integridad académica y la correcta atribución de las ideas y hallazgos de los autores consultados (American Psychological Association, 2020). La transparencia en el proceso de búsqueda, selección y análisis de la literatura busca garantizar la replicabilidad y la validez de los hallazgos de esta investigación.

Vulnerabilidades y Estrategias de Ciberdefensa en Drones Multirrotores: Un Análisis Técnico

El creciente despliegue de vehículos aéreos no tripulados (UAVs), o drones, en los ámbitos civil y militar, ha generado significativas preocupaciones en torno a su seguridad, especialmente ante la posibilidad de su utilización con fines maliciosos. Los drones multirrotores, caracterizados por su agilidad, capacidad de vuelo estacionario y relativa accesibilidad, representan una amenaza emergente que exige un análisis exhaustivo de sus debilidades inherentes y de las contramedidas cibernéticas necesarias para mitigar los riesgos asociados (Gupta et al., 2018). El presente desarrollo se centra en la identificación

precisa de las principales vulnerabilidades de ciberseguridad que afectan a los drones UAV multirrotores, así como en la evaluación de las estrategias de ciberdefensa propuestas o implementadas para su protección contra ataques cibernéticos. Este análisis se fundamenta en la revisión sistemática de 20 artículos académicos relevantes, con el objetivo de proporcionar una comprensión integral del estado actual de la ciberdefensa contra drones, destacando las vulnerabilidades más críticas que pueden ser explotadas para neutralizar drones enemigos en operaciones militares.

Vulnerabilidades en Drones Multirrotores

La intrincada arquitectura de los drones UAV multirrotores presenta diversos puntos de entrada para potenciales ataques cibernéticos, los cuales pueden clasificarse según los subsistemas del dron: comunicación, navegación, software/firmware, y sensores/carga útil.

Vulnerabilidades en la Comunicación

La operación de los drones depende críticamente de enlaces de comunicación inalámbricos para el control, la telemetría y la navegación. Estos enlaces, que a menudo utilizan protocolos como Wi-Fi, Bluetooth o protocolos propietarios, son susceptibles a la interceptación de datos sensibles (Khan et al., 2020), la interrupción de la señal mediante jamming (Motlagh et al., 2017), y la suplantación de identidad o spoofing para la inyección de comandos maliciosos (Yan et al., 2019). En este sentido, Shafique et al. (2021) señalan que "la ausencia de mecanismos de autenticación y cifrado robustos en los enlaces de comunicación hace que los drones sean objetivos vulnerables a la interceptación y manipulación, lo cual abre la posibilidad de interferir sus enlaces de control y neutralizarlos mediante técnicas de jamming o spoofing aplicadas por fuerzas propias." (p. 45). Esta vulnerabilidad se ve exacerbada por la frecuente utilización de protocolos de comunicación

diseñados para eficiencia y flexibilidad más que para seguridad robusta, y por la implementación a menudo laxa de medidas de seguridad incluso en protocolos que sí ofrecen capacidades de protección. La falta de una estandarización global en los protocolos de comunicación utilizados por diferentes fabricantes también complica la implementación de soluciones de seguridad universales y efectivas, generando un panorama fragmentado y, por ende, más vulnerable.

Esta carencia de autenticación y cifrado no solo expone a los drones a la interceptación, sino que abre la posibilidad de neutralizar enlaces de control mediante técnicas de interferencia dirigidas (jamming) o de suplantación (spoofing) aplicadas por fuerzas propias. En conflictos recientes y ejercicios C-UAS, la interrupción direccional del enlace de control ha demostrado ser efectiva para provocar pérdida de control o aterrizajes forzados en plataformas comerciales. Por tanto, el subsistema de comunicaciones constituye un objetivo operativo prioritario para acciones de neutralización tácticas." (Khan et al., 2020; Motlagh et al., 2017).

Vulnerabilidades en el Sistema de Navegación

Los sistemas de navegación global por satélite (GNSS), como el GPS, son fundamentales para la navegación autónoma de los drones; sin embargo, esta dependencia introduce riesgos significativos. El GPS spoofing, que implica la transmisión de señales falsas para desviar el dron (Takahashi et al., 2018), y el GPS jamming, que bloquea o degrada las señales de GPS (Psiaki & Humphreys, 2016), son amenazas relevantes. La relativa facilidad con la que se pueden adquirir o construir dispositivos capaces de realizar estos ataques aumenta considerablemente el nivel de riesgo. Kerns et al. (2014) indican que "los ataques al sistema de navegación representan una seria amenaza, ya que comprometen

directamente la capacidad del dron para llevar a cabo su misión de manera segura y precisa, y al mismo tiempo constituyen un punto de entrada viable para inducir fallas de navegación y desviar drones enemigos hacia zonas seguras" (p. 58). Además de los ataques directos a la señal de GPS, las vulnerabilidades en la propia implementación del receptor GPS en el dron pueden ser explotadas. Fallos en el procesamiento de las señales o en la lógica de navegación pueden permitir a un atacante manipular la posición reportada por el dron sin necesidad de un sofisticado ataque de spoofing, abriendo una vía de ataque más sutil y potencialmente más difícil de detectar.

Dado que la navegación GNSS es a la vez crítica y frágil, los ataques de spoofing/jamming no solo degradan la misión, sino que se emplean operacionalmente para inducir desvíos, pérdida de orientación o aterrizajes controlados. Estudios de campo y casos documentados muestran que el GPS es el subsistema más explotado para la neutralización de drones comerciales, por lo que constituye un punto clave para contramedidas activas y para diseñar acciones de interdicción en zonas de riesgo. (Kerns et al., 2014)

Vulnerabilidades en Software y Firmware

El software y el firmware que controlan las funciones del dron son también puntos críticos de vulnerabilidad. Fallos en el código, como desbordamientos de búfer o inyecciones de código (Li et al., 2019 pueden ser explotados para obtener control no autorizado del dispositivo, lo que en el caso de drones adversarios permitiría intervenir su firmware, interrumpir misiones hostiles o incluso tomar control parcial de la plataforma. La complejidad creciente del software embebido en los drones modernos, que incluye sistemas operativos en tiempo real, algoritmos de control de vuelo, procesamiento de datos de sensores y lógica de comunicación, incrementa la superficie de ataque y la probabilidad de

que existan vulnerabilidades sin descubrir. Suryadi et al. (2020) enfatizan que "la integridad del firmware es crítica para la seguridad del dron, ya que cualquier modificación no autorizada puede tener consecuencias devastadoras" (p. 112). La falta de actualizaciones de seguridad oportunas por parte de los fabricantes, ya sea por la naturaleza de ciclo de vida corto de algunos drones o por la falta de un mecanismo de actualización robusto y fácil de usar, agrava significativamente el riesgo de explotación de estas vulnerabilidades, dejando a los sistemas expuestos a amenazas conocidas durante períodos prolongados.

La explotación del software y firmware en drones adversarios permite ataques de mayor persistencia —por ejemplo, reprogramación parcial, implantación de payloads lógicos o interrupción de funciones críticas— que en escenarios tácticos traducen en la neutralización sostenida de la plataforma. Operativamente, el compromiso del firmware ha sido identificado como vector para tomar control o inutilizar dispositivos en entornos hostiles, por lo que la identificación de firmas y la auditoría forense del firmware son medidas útiles tanto para defensa propia como para diseñar contramedidas ofensivas dirigidas. (Suryadi et al., 2020).

Vulnerabilidades en Sensores y Carga Útil

Los sensores (cámaras, infrarrojos, etc.) y la carga útil de los drones también pueden ser atacados. La manipulación de los datos de los sensores puede inducir errores en el control del dron, afectando su estabilidad o la información que proporciona al operador; en el caso de drones enemigos, estas debilidades pueden inducirse deliberadamente para degradar sus capacidades de vigilancia o anular la efectividad de la carga útil. (Floreano & Wood, 2015). Un ataque a la carga útil podría comprometer su funcionalidad específica, ya sea la transmisión de información, la realización de mediciones o incluso la manipulación

de objetos. Gunduz y Ozdemir (2020) afirman que "la protección de los datos de los sensores y la integridad de la carga útil es esencial para garantizar la fiabilidad y seguridad de las operaciones con drones" (p. 78). La ausencia de mecanismos de cifrado y autenticación en los datos transmitidos desde los sensores y hacia la carga útil facilita su manipulación por parte de atacantes que hayan logrado acceder al sistema del dron o interceptar sus comunicaciones, comprometiendo la integridad de la información recopilada y la operatividad de la misión.

La manipulación deliberada de sensores o la degradación de la carga útil en drones enemigos puede **anular su capacidad de reconocimiento o de entrega**, reduciendo su valor operacional sin recurrir a destrucción cinética. Técnicas de interferencia de imagen o falsificación de telemetría, junto con detección multisensorial, permiten contrarrestar la función de inteligencia de plataformas adversarias con menor riesgo colateral. (Floreano & Wood, 2015).

Vulnerabilidades técnicas explotables en el uso malicioso de drones

El aprovechamiento operativo de los drones con fines maliciosos depende, en gran medida, de un conjunto de vulnerabilidades técnicas que permiten comprometer su comportamiento, control o funcionalidad. Estas debilidades, si bien han sido abordadas en secciones anteriores desde un enfoque técnico, merecen una exposición específica como puntos de entrada comunes para actores hostiles.

Una de las más críticas es la dependencia del GPS, que convierte a los UAV en blancos accesibles para ataques de jamming (interferencia) y spoofing (suplantación de señal). Estas técnicas permiten desde desorientar un dron hasta desviarlo hacia zonas no

autorizadas o hacerlo aterrizar de manera controlada por el atacante (Psiaki & Humphreys, 2016; Takahashi et al., 2018). Por tanto, el GPS se configura como el subsistema más explotado internacionalmente para contrarrestar drones maliciosos en conflictos reales

La interferencia por radiofrecuencia (RF) representa otra vía de ataque frecuente. El canal de control entre el dron y su estación base puede ser interrumpido, saturado o interceptado, especialmente si emplea protocolos sin cifrado o autenticación robusta (Motlagh et al., 2017). En ese contexto, la pérdida de señal o la toma de control a distancia pueden ejecutarse sin necesidad de vulnerar físicamente el sistema.

Asimismo, muchos drones comerciales utilizan protocolos estándar como Wi-Fi o Bluetooth, los cuales, al carecer de medidas avanzadas de seguridad, son vulnerables a ataques de autenticación, inyección de comandos o suplantación del operador. Tal como señala Shafique et al. (2021), un atacante puede introducir paquetes maliciosos o suplantar la identidad de la estación de control para dirigir el dron con fines hostiles.

Finalmente, las vulnerabilidades del software y firmware constituyen un vector de ataque sofisticado, pero altamente efectivo. La explotación de errores en el código, el acceso a versiones sin parches de seguridad o la modificación del firmware pueden otorgar al atacante un control persistente del UAV. En escenarios militares, esto puede traducirse en la alteración de misiones, captura de imágenes sensibles, o incluso el uso del dron como vehículo para cargas explosivas.

En conjunto, estas vulnerabilidades no solo exponen fallas técnicas, sino que explican cómo los drones pueden convertirse en herramientas eficaces dentro de esquemas de guerra asimétrica, reconocimiento encubierto o sabotaje táctico. Abordarlas requiere no

solo protección de hardware y software, sino una comprensión doctrinal del dron como un vector de amenaza cibernética.

En síntesis, desde una perspectiva operacional los subsistemas con mayor potencial de explotación para neutralizar drones enemigos son, en orden de relevancia práctica: 1) GNSS (navegación), 2) enlaces RF (comunicaciones), y 3) software/firmware. Esta priorización guía la selección de contramedidas y la propuesta de un modelo de defensa escalonada, tal como se desarrolla en las siguientes secciones.

Análisis de Estrategias de Ciberdefensa

Para contrarrestar estas vulnerabilidades, se han propuesto e implementado diversas estrategias de ciberdefensa.

Técnicas de Autenticación y Cifrado para Comunicaciones Seguras

Una de las piedras angulares en la defensa de los drones reside en asegurar sus enlaces de comunicación. La implementación de mecanismos de autenticación robustos, capaces de verificar fehacientemente la identidad tanto del operador como del dron, se erige como una primera línea de defensa contra la suplantación. Paralelamente, el empleo de protocolos de cifrado de alta seguridad, como el ampliamente reconocido Estándar de Cifrado Avanzado (AES), se torna esencial para garantizar la confidencialidad e integridad de los datos que fluyen entre el operador y el vehículo aéreo no tripulado (Dorri et al., 2017). Al respecto, Islam et al. (2021) enfatizan que "la adopción de protocolos de comunicación seguros y la implementación de una gestión de claves robusta son esenciales para proteger los enlaces de control y datos de los drones" (p. 92). Más allá del cifrado estándar, la investigación también se centra en técnicas de comunicación más resilientes a la interferencia, como el espectro ensanchado por salto de frecuencia (FHSS), que dificulta

el jamming al variar constantemente las frecuencias de transmisión (Lin et al., 2019). La implementación de estas técnicas, sin embargo, debe considerar el impacto en el rendimiento y la latencia de la comunicación, especialmente en aplicaciones en tiempo real.

Métodos para la Detección y Prevención de Ataques a la Navegación

La vulnerabilidad de los sistemas de navegación, especialmente el GPS, exige el desarrollo e implementación de métodos efectivos de detección y prevención de ataques. En el ámbito de la detección de spoofing, se están perfeccionando técnicas que analizan las señales de GPS en busca de anomalías sutiles, como inconsistencias en la potencia, la fase o el tiempo de llegada de las señales (Scott et al., 2015). Complementariamente, la integración de sistemas de navegación inercial (INS) en los drones proporciona una fuente de navegación redundante que permite identificar discrepancias significativas con las lecturas del GPS, alertando sobre un posible ataque (Gao et al., 2019). Magazzeni et al. (2022) concluyen que "la combinación de múltiples fuentes de navegación y la implementación de algoritmos de detección de anomalías son estrategias clave para mitigar los riesgos asociados al GPS spoofing y jamming" (p. 135). A futuro, la exploración de técnicas de cifrado de las propias señales de GPS y el desarrollo de sistemas de navegación alternativos que no dependan de la infraestructura GNSS podrían ofrecer soluciones aún más robustas, aunque su implementación a gran escala presenta desafíos técnicos y de infraestructura considerables.

Estrategias para el Fortalecimiento del Software y Firmware

Garantizar la integridad y seguridad del software y firmware que gobiernan el funcionamiento de los drones es una tarea crítica. Esto se aborda mediante la adopción de prácticas de desarrollo seguro, que incorporan consideraciones de seguridad desde las

etapas iniciales del ciclo de vida del software. La realización de pruebas de penetración exhaustivas permite identificar y corregir vulnerabilidades antes de que puedan ser explotadas. Asimismo, la implementación diligente de actualizaciones de seguridad periódicas es fundamental para abordar las nuevas amenazas y las vulnerabilidades descubiertas (Roman et al., 2018). El uso de mecanismos de arranque seguro (secure boot) y la verificación de la integridad del firmware al inicio del sistema previenen la ejecución de código no autorizado (Potkonjak et al., 2016). Zhang et al. (2023) enfatizan que "la implementación de un ciclo de vida de desarrollo seguro y la aplicación de mecanismos de protección en tiempo de ejecución son cruciales para garantizar la integridad y la seguridad del software y firmware de los drones" (p. 201). Adicionalmente, la segmentación del software en módulos con privilegios mínimos limita el impacto potencial de una vulnerabilidad explotada en un componente específico, conteniendo así la propagación de un ataque.

Soluciones para la Protección de Sensores y Carga Útil

La protección de los sensores y la carga útil de los drones requiere la implementación de mecanismos de autenticación que aseguren la integridad de los datos recopilados y el empleo de técnicas de cifrado para garantizar su confidencialidad durante la transmisión y el almacenamiento (Yazdani & Kazemi, 2020). Alrajeh et al. (2019) señalan que "la autenticación de los datos de los sensores y el cifrado de la información sensible son medidas esenciales para proteger la integridad y confidencialidad de los datos recopilados por los drones" (p. 67). En el caso de cargas útiles especializadas o sensibles, se deben implementar controles de acceso estrictos y mecanismos de protección contra la manipulación física o lógica no autorizada. La investigación también se centra en el

desarrollo de técnicas de detección de anomalías en los datos de los sensores, con el objetivo de identificar posibles manipulaciones o inyecciones de datos maliciosos que podrían comprometer la toma de decisiones basada en la información del dron. La implementación de estas medidas debe equilibrarse con los requisitos de procesamiento en tiempo real y el ancho de banda disponible, especialmente en aplicaciones con limitaciones de recursos.

Herramientas y protocolos de ciberseguridad para contrarrestar drones maliciosos: protección de sistemas de navegación frente a ataques de spoofing y jamming

El uso creciente de vehículos aéreos no tripulados (UAV) en operaciones militares ha transformado el escenario táctico contemporáneo, al tiempo que ha generado vulnerabilidades operacionales nuevas. Una de las más críticas es su dependencia estructural de tecnologías de navegación satelital como el GPS o el sistema global de navegación por satélite (GNSS), lo que los expone a técnicas de interferencia como el *spoofing* y el *jamming*. estas amenazas no solo afectan la capacidad de navegación de UAV propios, sino que constituyen **puntos de entrada tácticos para contrarrestar drones enemigos**, al permitir redirigirlos, capturarlos o inutilizarlos con consecuencias decisivas en contextos operacionales. Como advierten Omolara, Alawida y Abiodun (2023), "la dependencia estructural de los UAV en tecnologías de navegación por satélite ha abierto un frente crítico en términos de seguridad operativa" (p. 2).

En el caso del *spoofing*, el ataque consiste en transmitir señales falsas de GPS que el receptor del UAV interpreta como auténticas, generando así una desviación deliberada de

su trayectoria. Wei et al. (2022) señalan que "las señales falsificadas pueden alterar significativamente la trayectoria del UAV sin activar alertas inmediatas, ya que el sistema interpreta los datos como legítimos" (p. 3). Esta técnica es especialmente peligrosa en drones civiles modificados o comerciales sin capacidades de verificación cruzada, ya que el engaño puede mantenerse sin ser detectado, permitiendo al atacante tomar el control o inducir fallos de navegación. En operaciones militares, esta vulnerabilidad se explota deliberadamente para inducir aterrizajes controlados o desvíos de drones hostiles hacia áreas seguras, reduciendo el riesgo para tropas e instalaciones

En contraste, el *jamming* se basa en saturar las frecuencias por las cuales se transmiten las señales GNSS, impidiendo su recepción. Esto resulta en una pérdida completa o intermitente del posicionamiento satelital, lo que puede provocar comportamientos erráticos o la activación de protocolos de emergencia que, en zonas montañosas o de combate, podrían resultar en accidentes o pérdida de activos en escenarios prácticos, el jamming direccional ha sido utilizado como medida de neutralización rápida contra drones comerciales modificados, al interrumpir su enlace GNSS y forzarlos a aterrizar o perder control. Khan, Jhanjhi, Brohi y Nayyar (2020) afirman que "la naturaleza pasiva de los receptores GPS los convierte en blancos vulnerables ante transmisiones activas dirigidas a interrumpir su sincronización satelital" (p. 117).

Para mitigar estos riesgos, la literatura propone un conjunto de herramientas centradas en la detección, la respuesta automatizada y la resiliencia estructural de los sistemas de navegación. Una de las estrategias más destacadas en los últimos años es la aplicación de algoritmos de detección basados en aprendizaje automático. Wei, Wang y Sun (2022) desarrollaron el sistema PerDet, que utiliza los sensores internos del dron —

como acelerómetros, magnetómetros y barómetros— para identificar patrones de vuelo normales y detectar desviaciones sutiles asociadas a ataques. Esta metodología presenta una ventaja notable en términos de flexibilidad, ya que puede adaptarse a múltiples plataformas UAV sin requerir hardware adicional.

Ahora bien, su aplicación práctica en el Ejército Nacional de Colombia exige considerar diversos factores. En primer lugar, el entrenamiento requerido para interpretar y mantener sistemas con algoritmos de inteligencia artificial no es menor, y debe incorporarse dentro de los programas de formación avanzada. En segundo lugar, la variabilidad climática y topográfica del país (selva densa, montañas abruptas, zonas urbanas con interferencias múltiples) puede afectar la precisión de los sensores, reduciendo su fiabilidad. No obstante, en operaciones planificadas con UAV propios, estas técnicas podrían ser una primera capa defensiva ante posibles interferencias.

Otra herramienta emergente es el sistema ConstDet, también propuesto por Wei et al. (2022), basado en la detección semántica de anomalías. Este enfoque compara los comandos de navegación que el UAV debería seguir con las posiciones que realmente reporta el GPS. Las inconsistencias sistemáticas se interpretan como evidencia de un ataque de spoofing. Su ventaja radica en que no requiere múltiples sensores, lo cual podría ser útil para plataformas más ligeras o entornos hostiles. Sin embargo, su efectividad disminuye si los comandos de navegación también han sido comprometidos o si el entorno presenta condiciones ambiguas de señal, como puede suceder en zonas montañosas del Cauca o el Catatumbo.

En paralelo, los métodos tradicionales de análisis de señales mantienen su vigencia. El monitoreo de la frecuencia Doppler y de la relación portadora-ruido (C/N_0) permite

identificar variaciones anómalas en la propagación de la señal que podrían delatar un ataque. Wei, Sun, Li y Ma (2024) destacan que "las características estadísticas de la señal pueden revelar patrones que no corresponden a las condiciones normales de propagación satelital" (p. 7). Estas técnicas, si bien robustas, requieren cierto nivel de infraestructura técnica y procesamiento que limita su despliegue en misiones móviles o improvisadas, donde la velocidad de respuesta es crítica.

Además de los sistemas de detección, una de las líneas más sólidas en materia de resiliencia ante ataques de spoofing y jamming es la implementación de **sistemas de navegación inercial (INS)**. Estos operan de forma autónoma mediante sensores internos —como giróscopos y acelerómetros— que permiten calcular desplazamientos relativos sin depender de señales externas. Al combinar datos del INS con lecturas de GPS, se logra una verificación cruzada que permite identificar discrepancias abruptas causadas por interferencias. Wei, Sun, Li y Ma (2024) subrayan que "la fusión de datos entre el GPS y el INS puede no solo reducir la dependencia del satélite, sino también servir como mecanismo de validación cruzada" (p. 6).

En el contexto colombiano, el uso de INS cobra especial relevancia para UAV propios operando en zonas con cobertura satelital irregular, como áreas selváticas del Guaviare o cañones montañosos del Tolima. Sin embargo, su efectividad frente a drones enemigos depende de que estos sistemas estén presentes en las plataformas hostiles, lo cual no es común en drones comerciales modificados —frecuentemente usados por grupos armados no estatales— pero sí posible en drones militares avanzados. Por tanto, el INS es útil como protección en sistemas propios, pero limitado como estrategia de neutralización externa.

Para enfrentar el jamming específicamente, se han desarrollado **técnicas de espectro ensanchado**, que dispersan la señal legítima en múltiples frecuencias, haciendo más difícil su interferencia. Métodos como el *Frequency Hopping Spread Spectrum* (FHSS) o el *Direct Sequence Spread Spectrum* (DSSS) permiten que el canal de navegación o control varíe de manera dinámica, dificultando el seguimiento por parte de atacantes. Además, algunos sistemas incorporan **algoritmos de cancelación de interferencias**, que filtran señales no deseadas del entorno para preservar la integridad operativa del enlace. Omolara et al. (2023) destacan que "el uso de técnicas como la modulación adaptativa y el cambio dinámico de frecuencias puede reducir significativamente la vulnerabilidad de los enlaces de comunicación" (p. 8).

En términos operativos, estas estrategias presentan retos importantes. La implementación de FHSS requiere que tanto el UAV como la estación base compartan protocolos y frecuencias compatibles, lo cual limita su utilidad para interceptar drones enemigos. En zonas urbanas o con alta densidad de señales —como Bogotá o Medellín—, los saltos de frecuencia pueden interferir con otros dispositivos, generando riesgos colaterales. Además, los sistemas de espectro ensanchado son poco efectivos frente a interferencias de banda ancha, por lo que su utilidad depende del tipo de amenaza y del entorno, no obstante, comprender estas técnicas también es vital para el Ejército, pues permite **diseñar interferencias selectivas que anulen drones enemigos que carezcan de protocolos avanzados de espectro ensanchado**

Otra alternativa en desarrollo es el uso de **sistemas de navegación alternativos basados en visión artificial, LIDAR o mapas internos**. Estas tecnologías permiten que el UAV oriente su desplazamiento mediante la interpretación del entorno físico, sin necesidad

de GPS. En contextos de guerra electrónica o zonas de exclusión satelital, representan una opción viable para mantener el control autónomo del dron. Khan et al. (2020) afirman que "la navegación basada en visión, combinada con inteligencia artificial, representa una vía prometedora para operar UAVs en escenarios de guerra electrónica" (p. 120).

Sin embargo, estas soluciones requieren condiciones específicas: buena visibilidad, entornos estructurados y gran capacidad de procesamiento. En regiones rurales colombianas con vegetación densa, niebla frecuente o cambios abruptos de terreno, la eficacia de la navegación visual se ve limitada. A ello se suma el elevado costo de los sensores LIDAR y las exigencias de calibración, que los hacen poco accesibles para unidades operativas móviles o con recursos limitados. En UAV adversarios de alta gama, esta capacidad de navegación por visión constituye un desafío adicional, que obliga a considerar contramedidas cinéticas o multisensoriales más allá de la simple interferencia de señales.

La **seguridad de los enlaces de comunicación** entre el dron y su estación de control es otra dimensión clave. Protocolos con cifrado avanzado y autenticación mutua pueden prevenir ataques de secuestro de señal o manipulación remota. Khan, Jhanjhi, Brohi y Almazroi (2022) proponen un esquema que "incorpora cifrado, autenticación y mecanismos de integridad para garantizar una comunicación segura y confiable entre el UAV y la estación de control" (p. 3). Esta estrategia no solo protege la navegación, sino que impide el acceso no autorizado a telemetría y comandos.

No obstante, en zonas de difícil cobertura, el cifrado de datos puede generar latencia o pérdida de paquetes si no se acompaña de infraestructura adecuada. Además, en drones comerciales intervenidos, el uso de protocolos propietarios o no actualizados puede hacer

que incluso el mejor sistema de defensa de enlace sea inútil. En consecuencia, el Ejército Nacional debe priorizar plataformas propias con estándares interoperables y realizar auditorías técnicas frecuentes sobre sus UAV adquiridos.

La **Zero Trust Architecture (ZTA)** representa una visión más holística de la ciberdefensa, al eliminar la suposición de confianza entre componentes del sistema. Bajo este enfoque, cada solicitud de acceso, transmisión o comando debe ser verificada, segmentada y auditada. Haque et al. (2024) explican que "la ZTA aplicada a UAVs permite una autenticación continua y segmentación del acceso, reduciendo el riesgo de control malicioso aun cuando un nodo ha sido comprometido" (p. 2). Combinada con inteligencia artificial explicable (XAI), esta arquitectura permite detectar decisiones anómalas y trazar su origen, facilitando la respuesta temprana.

Desde la perspectiva del Ejército Nacional, este modelo podría incorporarse en UAV de vigilancia o combate de alta prioridad. Sin embargo, requiere una arquitectura digital madura, políticas de acceso bien definidas y personal capacitado en seguridad lógica. En zonas donde la conectividad es limitada y las decisiones deben tomarse en segundos, una verificación continua puede ralentizar la operación si no se implementa con criterio estratégico. Por tanto, la ZTA es ideal como capa de protección en sistemas centrales, pero debe ajustarse para no obstaculizar misiones tácticas en terreno.

En el ámbito estrictamente militar, las condiciones de uso de UAV del Ejército Nacional de Colombia presentan particularidades que obligan a adaptar las soluciones tecnológicas a contextos geográficos y operacionales altamente diversos. A diferencia de los ejércitos que operan en teatros de guerra convencionales con alta infraestructura digital, las operaciones militares colombianas suelen desarrollarse en entornos hostiles

caracterizados por selva espesa, climas impredecibles, terrenos montañosos y limitaciones logísticas.

Esto significa que muchas de las herramientas descritas, aunque prometedoras en términos teóricos, enfrentan restricciones reales al momento de su despliegue. Por ejemplo, sistemas de detección basados en IA como PerDet o ConstDet requieren no solo algoritmos entrenados, sino también procesamiento continuo, estabilidad eléctrica y condiciones controladas de vuelo, lo que los hace más útiles para UAV propios en vigilancia planificada que para contrarrestar amenazas dinámicas en terreno.

Asimismo, debe considerarse el tipo de dron que representa la amenaza. Los drones **comerciales modificados (DIY)**, usualmente empleados por grupos armados ilegales, presentan vulnerabilidades técnicas significativas: carecen de cifrado, utilizan protocolos abiertos y dependen casi exclusivamente de GPS sin redundancia. En estos casos, estrategias como el spoofing inverso, el secuestro de señal, el jamming controlado o incluso la detección acústica pueden resultar efectivas, siempre que se implementen con precisión y sin comprometer sistemas amigos.

En contraste, los **drones militares avanzados**, dotados de sistemas redundantes, navegación por visión, comunicaciones cifradas y contramedidas electrónicas, requieren enfoques más sofisticados que incluyan guerra electrónica ofensiva, bloqueadores direccionales de alta precisión y análisis multisensorial. En este sentido, la literatura técnica coincide en que "la efectividad de cualquier estrategia de defensa depende no solo de la tecnología empleada, sino del nivel de sofisticación del atacante y del entorno operacional" (Tlili et al., 2024, p. 6).

De ahí que la recomendación estratégica para el Ejército Nacional de Colombia sea adoptar un enfoque **escalonado y selectivo**. Para zonas rurales con amenazas de bajo perfil, bastan soluciones ligeras, portables y de bajo costo, como el jamming direccional, el análisis Doppler o la detección por RF. Para entornos urbanos sensibles o misiones críticas, deben emplearse plataformas más complejas que integren navegación inercial, ZTA, cifrado multinivel y monitoreo continuo por IA.

Por último, la incorporación efectiva de estas herramientas exige **capacitación técnica continua**, protocolos doctrinales claros, interoperabilidad entre fuerzas y un marco normativo actualizado. Solo así será posible traducir las capacidades tecnológicas en ventajas tácticas reales, minimizando riesgos colaterales y fortaleciendo la resiliencia institucional frente a amenazas híbridas.

Tabla 1. Experiencias internacionales en el uso de técnicas C-UAS contra drones maliciosos.

Caso / País	Técnica utilizada	Subsistema explotado	Efectividad observada	Limitación principal	Fuente / ejemplo
Ucrania (2022–2024)	Spoofing y jamming de GNSS	Navegación satelital (GPS)	Alta contra drones comerciales y enjambres pequeños; permitió desviarlos o inutilizarlos	Limitado frente a drones militares con redundancia	Informes OSINT y análisis de campo
Israel (operaciones defensivas)	Multisensorialidad + jamming + interceptores	RF, radar, óptico	Eficaz en entornos urbanos; reducción de falsos positivos	Costos altos e interoperabilidad C2	Programas C-UAS y reportes industriales
EE. UU. (teatros de operación)	Guerra electrónica, microondas y láseres	Comunicaciones, carga útil	Efectivos contra plataformas avanzadas en escenarios autorizados	Riesgo de daño colateral y restricciones normativas	Documentos militares y adquisiciones

Caso / País	Técnica utilizada	Subsistema explotado	Efectividad observada	Limitación principal	Fuente / ejemplo
Yemen / Libia (grupos insurgentes)	Jamming improvisado y captura de control	GNSS y enlaces de mando	Muy eficaces contra drones DIY comerciales	Limitados frente a drones con redundancia o cifrado	Reportes de conflictos y análisis periodístico

Fuente: Elaboración propia

En síntesis, el análisis de estas herramientas demuestra que las vulnerabilidades más explotadas para neutralizar drones enemigos se concentran en la navegación GNSS y los enlaces RF. Estas lecciones, sumadas a la revisión de experiencias internacionales, constituyen la base sobre la cual se diseña el protocolo de defensa escalonada que se presenta en el siguiente objetivo.

Protocolo de Ciberdefensa en Capas para el Ejército Nacional de Colombia

El protocolo propuesto en este objetivo surge como resultado directo de las vulnerabilidades y técnicas de neutralización identificadas en los objetivos anteriores. En el Objetivo 1 se evidenció que los sistemas de navegación GNSS y los enlaces de comunicación por radiofrecuencia constituyen los puntos más críticos y explotables de los drones multirrotor, mientras que en el Objetivo 2 se revisaron herramientas de detección y mitigación que han probado eficacia en diferentes conflictos. Estos hallazgos permiten concluir que cualquier estrategia de defensa contra drones maliciosos debe comenzar por una detección temprana y confiable, ya que sin este primer eslabón resulta imposible activar las fases posteriores de clasificación y neutralización. A partir de esa premisa, la primera capa del protocolo se orienta a consolidar la **detección e identificación** como capacidad institucional prioritaria.

Capa 1: Detección e Identificación

La amenaza que representan los UAV no autorizados se expresa en distintos niveles: desde drones comerciales modificados por actores ilegales, hasta plataformas más sofisticadas con sistemas de navegación redundantes. En todos los casos, el Ejército Nacional necesita identificar la intrusión con la mayor antelación posible, reduciendo falsos positivos y garantizando que la información llegue a tiempo a los centros de mando. El análisis de vulnerabilidades realizado en los objetivos anteriores mostró que los drones dependen de emisiones RF para mantener el enlace de control y de GNSS para orientarse; estos vectores, por tanto, constituyen señales de oportunidad para detección y alerta temprana.

En entornos estáticos, como bases militares, aeródromos o infraestructuras críticas, la literatura internacional recomienda el uso de radares especializados en UAS, diseñados para detectar objetos pequeños y lentos en rangos de hasta dos kilómetros. Su ventaja frente a radares convencionales es que permiten distinguir multirrotores de aves u otros objetos, reduciendo falsos positivos. En el contexto colombiano, la instalación de estos radares en anillos concéntricos alrededor de instalaciones estratégicas ofrecería una cobertura robusta y continua, priorizando zonas de frontera y bases de aviación donde la amenaza es más latente.

Sin embargo, en operaciones móviles o en zonas rurales con acceso limitado, los radares no siempre son viables. En esos escenarios cobran relevancia los analizadores portátiles de espectro de radiofrecuencia, capaces de escanear en tiempo real las bandas más utilizadas por drones comerciales (2.4 y 5.8 GHz). Estos equipos permiten detectar la

emisión de señales de control y, en modelos más avanzados, triangular la ubicación del operador. Para patrullajes en regiones como el Catatumbo, Arauca o el sur del Meta, donde grupos armados emplean UAV improvisados para reconocimiento o transporte de cargas, esta capacidad portátil representa una ventaja táctica inmediata.

A la par de la detección electromagnética, resulta útil incorporar sensores ópticos y acústicos. Las cámaras térmicas y de alta resolución permiten confirmar visualmente la presencia del dron y seguir su trayectoria, mientras que los micrófonos direccionales capturan el perfil sonoro característico de los multirrotores. Aunque estas tecnologías pueden verse afectadas por el clima o el ruido ambiental, su combinación con radares y RF genera redundancia y disminuye la tasa de error. Este enfoque multisensorial, respaldado por software de fusión de datos, es la práctica más recomendada a nivel internacional, pues transforma datos dispersos en una única imagen operacional que alimenta directamente los centros de mando y control.

En el caso colombiano, la aplicación de esta primera capa exige diferenciar por entorno. En selvas densas y cañones montañosos, donde las señales GNSS suelen ser irregulares y la visibilidad es limitada, los sensores acústicos y los detectores RF portátiles resultan más eficaces que los radares. En cambio, en entornos urbanos con alta densidad de interferencias, la fusión de radar, óptico y RF se vuelve imprescindible para discriminar amenazas de actividades civiles inofensivas. De este modo, la detección temprana no se plantea como una capacidad única, sino como un sistema modular adaptado a la diversidad geográfica y operacional del país.

En suma, la primera capa del protocolo responde directamente a los hallazgos técnicos de los objetivos previos: explota la dependencia de los drones respecto de sus emisiones RF y de las señales GNSS, y las convierte en vectores de detección y alerta. Para el Ejército Nacional, esta capa constituye la base sobre la cual se construye todo el esquema de defensa, al fortalecer la vigilancia temprana en bases fijas, patrullajes móviles y operaciones en frontera, reduciendo así el riesgo de sorpresa táctica y facilitando decisiones oportunas en escenarios reales.

Tabla 2. Capacidades de detección recomendadas por entorno en Colombia

Entorno operacional	Tecnologías más viables	Justificación principal
Bases militares / instalaciones críticas	Radares UAS de corto alcance + fusión multisensorial	Cobertura continua y reducción de falsos positivos
Operaciones móviles rurales	Detectores RF portátiles + sensores acústicos	Portabilidad y eficacia frente a drones comerciales modificados
Zonas urbanas densas	Radar + óptico/térmico + RF con fusión de datos	Discriminación precisa en ambientes con interferencias
Selvas y montañas	RF portátil + acústico	Viabilidad en entornos con baja visibilidad y cobertura GNSS limitada

Fuente: Elaboración propia

Capa 2: Clasificación y Alerta

Una vez que se ha logrado la detección temprana de un dron potencialmente hostil, el siguiente paso en el modelo de defensa en capas es su clasificación precisa y la emisión de alertas operativas oportunas. Este segundo nivel resulta crítico porque, sin un proceso de clasificación robusto, existe el riesgo de confundir aves, aeronaves civiles o drones propios con plataformas adversarias, lo que podría generar falsas alarmas, decisiones erradas y, en el peor de los casos, daños colaterales. Por tanto, la clasificación no es únicamente un

ejercicio técnico, sino también un requisito doctrinal para asegurar que las respuestas sean proporcionales y acordes con el marco del Derecho Internacional Humanitario (DIH).

Los hallazgos de los objetivos anteriores sustentan esta capa. En el Objetivo 1 se identificó que los subsistemas de comunicación RF y navegación GNSS son vulnerables a interferencias y manipulación; en el Objetivo 2 se revisaron algoritmos y herramientas de detección basados en inteligencia artificial y análisis estadístico de señales. Estos mismos mecanismos pueden ser aprovechados no solo para descubrir la presencia de un dron, sino para inferir su tipo, nivel de amenaza y origen. De esta manera, la clasificación se convierte en el puente entre la simple detección de un objeto en el aire y la decisión informada de neutralizarlo o descartarlo como inofensivo.

En la práctica, la clasificación se fundamenta en la fusión de datos multisensoriales. Los radares especializados aportan información sobre velocidad, altitud y trayectoria; los detectores RF identifican patrones de enlace y frecuencias de operación; los sensores ópticos y térmicos permiten validar visualmente características físicas como número de rotores, tamaño y firma térmica; mientras que los sensores acústicos ayudan a distinguir el sonido característico de multirrotores frente a otros objetos voladores. La combinación de estas fuentes, procesada en tiempo real mediante software de fusión de datos, reduce significativamente la probabilidad de error.

A nivel internacional, el uso de algoritmos de aprendizaje automático ha demostrado ser un complemento esencial para este proceso. Al entrenar modelos con bases de datos de firmas electromagnéticas, perfiles de vuelo y patrones acústicos de drones conocidos, es posible que el sistema identifique con rapidez si un objeto corresponde a un

UAV comercial modificado, a un dron avanzado con redundancias o a un simple falso positivo. Este enfoque, señalado en el Objetivo 2 con los sistemas PerDet y ConstDet, tiene la ventaja de acortar los tiempos de clasificación y reducir la dependencia del juicio humano en situaciones de alta presión. Sin embargo, no sustituye la supervisión humana, que sigue siendo indispensable para garantizar la proporcionalidad en la respuesta.

En el contexto colombiano, la implementación de esta capa enfrenta retos importantes. En zonas urbanas, la densidad de señales RF y la cercanía de aeropuertos civiles exigen una clasificación muy precisa para no afectar operaciones legítimas. En selvas y montañas, en cambio, la visibilidad limitada y la propagación irregular de las señales dificultan la confirmación visual, lo que hace aún más valiosa la fusión de múltiples fuentes. Por ello, la doctrina C-UAS para Colombia debería establecer protocolos diferenciados: uno para entornos urbanos con fuerte énfasis en discriminación entre amenazas y aeronaves civiles, y otro para áreas rurales y de frontera donde el riesgo de falsos positivos es menor, pero la cobertura tecnológica es más limitada.

La emisión de alertas constituye el último componente de esta capa. Una vez clasificado un dron como potencialmente hostil, el sistema debe generar una señal inmediata al centro de mando y control (C2), acompañada de información relevante: ubicación, tipo estimado de dron, trayectoria prevista y nivel de riesgo. Esta información permite a los operadores decidir si activar o no la capa de neutralización. En escenarios de patrullajes móviles, las alertas podrían transmitirse a dispositivos portátiles de los comandantes de unidad; en instalaciones estratégicas, deberían integrarse directamente a los sistemas de vigilancia perimetral y a los centros de operaciones conjuntas.

La clasificación y alerta temprana fortalecen la capacidad del Ejército Nacional para gestionar recursos de manera eficiente. Al reducir falsas alarmas y priorizar amenazas reales, se evita el desgaste operativo y se protege la legitimidad institucional frente a la ciudadanía. Además, esta capa convierte el cúmulo de datos técnicos obtenidos en la primera fase en información útil para la toma de decisiones tácticas y estratégicas, respondiendo así a la necesidad de transformar hallazgos técnicos en ventajas operacionales.

Tabla 3. Funciones principales de la clasificación y alerta en el modelo C-UAS

Fuente de información	**Aporte a la clasificación**	**Limitaciones principales**
Radar especializado	Velocidad, altura, trayectoria	Puede confundir aves con drones pequeños
RF (comando y control)	Identificación de frecuencias y patrones de enlace	Saturación de espectro en zonas urbanas
Óptico / Térmico	Validación visual y firma térmica	Dependencia de condiciones de luz/clima
Acústico	Perfil sonoro distintivo	Menor eficacia en ambientes ruidosos
IA / fusión de datos	Síntesis y discriminación rápida	Requiere entrenamiento y supervisión humana

Fuente: elaboración propia

Capa 3: Neutralización

La tercera capa del protocolo se orienta a la neutralización de la amenaza una vez que ha sido detectada y clasificada como hostil. Esta etapa cierra el ciclo operativo del modelo y traduce la información técnica obtenida en acciones concretas de defensa. Los hallazgos de los objetivos anteriores demostraron que los sistemas GNSS y los enlaces RF

son los subsistemas más vulnerables, y que técnicas como el *jamming* y el *spoofing* inverso se han mostrado eficaces en escenarios reales contra drones comerciales modificados. Con base en ello, la neutralización en el contexto colombiano debe seguir un enfoque escalonado, que privilegie las contramedidas no cinéticas antes de recurrir al uso de fuerza destructiva.

En el nivel inicial se encuentran las técnicas denominadas *soft-kill*. El *jamming* direccional, al interferir las señales de navegación o de control, puede provocar la pérdida de enlace y forzar al dron a aterrizar o desviarse hacia un área segura. El *spoofing* activo, por su parte, introduce señales falsas que inducen al UAV a cambiar de trayectoria, lo que permite reconducirlo lejos de instalaciones críticas. Estas medidas son de bajo costo, portátiles y adecuadas para enfrentar drones improvisados o comerciales empleados por grupos armados ilegales, que suelen carecer de redundancia técnica. En áreas rurales o de frontera, su implementación puede marcar la diferencia entre una amenaza controlada y un ataque exitoso.

Cuando las técnicas no destructivas no resultan suficientes —por ejemplo, frente a plataformas militares avanzadas dotadas de comunicaciones cifradas o navegación inercial—, se requiere un segundo nivel de respuesta. En este se incluyen métodos de interdicción no destructiva, como el uso de redes lanzadas desde drones aliados o sistemas de interferencia electromagnética localizada, que buscan inmovilizar al dron sin destruirlo. Estas opciones, aunque más complejas, permiten recuperar el UAV enemigo para análisis forense, aportando inteligencia valiosa sobre sus configuraciones técnicas y tácticas.

Finalmente, en situaciones de alta peligrosidad, se activa el nivel *hard-kill*, que contempla la destrucción física del dron. Sistemas de energía dirigida como microondas de alta potencia o láseres, interceptores cinéticos y munición antiaérea guiada forman parte de este arsenal. Su empleo debe estar regulado bajo criterios estrictos de proporcionalidad y distinción, dado el riesgo de daño colateral. En el contexto colombiano, el despliegue de capacidades *hard-kill* tendría sentido principalmente en instalaciones estratégicas como bases aéreas, complejos energéticos o eventos de alta seguridad, mientras que en operaciones móviles podría resultar contraproducente por su complejidad logística.

Consideraciones estratégicas y cierre

La neutralización escalonada asegura que la respuesta del Ejército Nacional no sea uniforme, sino adaptable al nivel de amenaza, al entorno geográfico y al tipo de dron enfrentado. Esta estructura protege la legitimidad institucional al mostrar un uso responsable y proporcional de la fuerza, en coherencia con el Derecho Internacional Humanitario. Además, permite integrar progresivamente nuevas tecnologías sin alterar la lógica general del modelo, garantizando flexibilidad frente a un panorama de amenazas en constante evolución.

En conclusión, la defensa en capas propuesta no surge como un listado de herramientas desconectadas, sino como la síntesis de los hallazgos técnicos y operativos obtenidos en los objetivos anteriores. Al integrar detección temprana, clasificación precisa y neutralización escalonada, este protocolo fortalece las capacidades del Ejército Nacional de Colombia para **contrarrestar drones enemigos en escenarios rurales, urbanos y**

fronterizos, respondiendo de manera explícita a la pregunta de investigación que orienta este trabajo.

Conclusiones

El análisis desarrollado en este artículo permitió examinar con rigor los desafíos que plantea el uso malicioso de drones multirrotor en el contexto colombiano y, a la vez, proponer lineamientos concretos para fortalecer la capacidad del Ejército Nacional en materia de ciberdefensa. Los hallazgos obtenidos en cada objetivo específico aportan una visión integral que combina diagnóstico técnico, revisión internacional y una propuesta doctrinal aplicable al escenario nacional.

En relación con el **Objetivo 1**, se concluye que las amenazas más relevantes para Colombia provienen de drones comerciales modificados por actores no estatales, antes que de plataformas militares sofisticadas. Estos dispositivos, de bajo costo y fácil acceso, aprovechan vulnerabilidades en los sistemas de navegación GNSS, en los enlaces de comunicación RF y en el firmware, lo que los convierte en herramientas de guerra asimétrica empleadas para reconocimiento, transporte de cargas ilícitas y ataques puntuales. La identificación de estos subsistemas vulnerables constituye la primera evidencia de que la neutralización efectiva de drones enemigos debe centrarse en debilidades técnicas comunes y accesibles.

Respecto al **Objetivo 2**, el análisis crítico de herramientas y protocolos de ciberseguridad permitió priorizar aquellas con mayor viabilidad técnica y operativa para el Ejército Nacional. Estrategias como el *jamming* direccional de señales GNSS y de enlace de control, el *spoofing* activo como mecanismo de desviación de trayectorias, la detección

multisensorial reforzada con inteligencia artificial y la validación mediante sistemas inerciales destacan como opciones eficaces, portátiles y ajustadas a entornos complejos como la selva, la montaña o los centros urbanos. En contraste, soluciones que dependen de infraestructura costosa o de condiciones ambientales muy controladas —como LIDAR, navegación basada en visión o armas láser de alta potencia— presentan baja viabilidad en el corto plazo, aunque se reconocen como líneas de desarrollo futuro.

El **Objetivo 3** dio lugar a la propuesta de un protocolo en defensa escalonada frente a drones maliciosos. Este modelo articula tres capas interdependientes: detección e identificación (radar, RF, óptico y acústico); clasificación y alerta (fusión de datos, algoritmos de IA y supervisión humana); y neutralización progresiva, priorizando contramedidas *soft-kill* frente a amenazas de bajo riesgo y reservando opciones *hard-kill* para escenarios críticos. La coherencia de este esquema reside en que cada capa se deriva directamente de las vulnerabilidades y técnicas revisadas en los objetivos anteriores, lo que asegura un marco doctrinal sólido y adaptable al teatro operacional colombiano. Asimismo, el protocolo incorpora el principio de proporcionalidad del Derecho Internacional Humanitario, garantizando eficacia operativa sin comprometer legitimidad institucional.

De manera transversal, se recomienda avanzar en la construcción de una doctrina C-UAS propia, que defina reglas de enfrentamiento, protocolos diferenciados por tipo de amenaza y ejercicios de validación en campo. Paralelamente, deben promoverse líneas de investigación sobre enjambres autónomos, inteligencia artificial explicable y experiencias de interoperabilidad regional, a fin de anticipar tendencias emergentes y fortalecer alianzas estratégicas.

En síntesis, este trabajo demuestra que fortalecer las capacidades de ciberdefensa del Ejército Nacional para contrarrestar drones enemigos requiere priorizar la explotación de vulnerabilidades en GNSS y RF, adoptar un modelo de defensa escalonada en tres capas y consolidar una doctrina nacional C-UAS que integre tecnología, entrenamiento y marco normativo. Con ello, el Ejército se posiciona para responder de manera efectiva, proporcional y legítima a un desafío híbrido que ya es una realidad en el escenario de seguridad contemporáneo.

Referencias

Alrajeh, N. A., Khan, M. A., & Masood, S. (2019). Security challenges in unmanned aerial vehicles (UAVs): A survey. *International Journal of Advanced Computer Science and Applications, 10*(1), 62–71.

American Psychological Association. (2020). *Publication manual of the American Psychological Association* (7th ed.).

Cortellese, N. (2022). Algorithmic warfare and human rights: Charting the course of an arms race. *International Review of Law, Computers & Technology*.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* (pp. 618–623). IEEE.

Fink, A. (2019). *Conducting research literature reviews: From the internet to paper* (5th ed.). Sage Publications.

Floreano, D., & Wood, R. J. (2015). Science, technology and the future of small flying robots. *Nature, 521*(7553), 460–466.

Gao, G., Grove, T., Lo, S., & Lachapelle, G. (2019). Anti-jamming and anti-spoofing techniques for GNSS: Recent advances. *Sensors, 19*(19), 4315.

Gunduz, M. Z., & Ozdemir, M. A. (2020). Internet of drones (IoD) security issues and challenges. In *Cyber Security and Privacy: Second International Conference, ICSP 2020* (pp. 71–85). Springer.

Gupta, R., Tanwar, S., Tyagi, S., & Kumar, N. (2018). Security and privacy challenges in unmanned aerial vehicles. *IEEE Internet of Things Journal, 5*(5), 4295–4304.

Haque, S., Azad, M. A., Rahman, M. S., & Hasan, M. K. (2024). Zero trust architecture and deep learning: Enhancing cyber defense of UAV networks. *Computers & Security, 134*, 103175.

Hasan, M., Azad, M. A., & Rahman, M. S. (2022). Predictive cyber defense frameworks in autonomous aerial vehicles. *IEEE Transactions on Aerospace and Electronic Systems, 58*(6), 5012–5024.

Horowitz, M. C., Allen, G., Bekoff, A., & Scharre, P. (2018). Artificial intelligence and international security. *Belfer Center for Science and International Affairs, Harvard Kennedy School*. https://www.belfercenter.org/publication/artificial-intelligence-and-international-security

Islam, S. H., Islam, M. M., Sarker, I. H., & Hossain, M. A. (2021). A systematic literature review on security and privacy issues in unmanned aerial vehicles. *Journal of Network and Computer Applications, 184*, 103075.

Kerns, A. J., Shepard, D. P., Bhatti, J. A., & Humphreys, T. E. (2014). Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics, 31*(4), 617–636.

Khan, S., Jhanjhi, N. Z., Brohi, S. N., & Nayyar, A. (2020). UAVs cyber security and threats analysis. *Computer Standards & Interfaces, 69*, 103408.

Khan, S., Jhanjhi, N. Z., Brohi, S. N., & Almazroi, A. A. (2022). Secure UAV communication protocol using blockchain and lightweight cryptography. *Journal of Network and Computer Applications, 198*, 103279.

Li, B., Zhang, Y., & Chen, J. (2019). Security vulnerabilities and countermeasures in drone systems: A survey. *Journal of Computer and System Sciences, 105*, 1–16.

Lin, C. H., Chen, Y. P., & Chen, K. T. (2019). Anti-jamming communication techniques for unmanned aerial vehicles: A survey. *IEEE Access, 7*, 178656–178673.

Magazzeni, D., McInnes, L., & Teso, S. (2022). Secure satellite navigation: Cryptographic approaches in Galileo and beyond. *Journal of Navigation, 75*(1), 137–154.

Motlagh, N. H., Taleb, T., & Zeadally, S. (2017). Internet of drones: Challenges, opportunities, and open issues. *IEEE Internet of Things Journal, 3*(6), 879–902.

Moyes, L. (2021). Autonomous weapons systems: What does 'meaningful human control' really mean in practice? *Journal of Conflict & Security Law, 26*(2), 205–231. https://doi.org/10.1093/jcsl/krz041

Omolara, A. E., Alawida, M., & Abiodun, O. I. (2023). Cyber-physical security threats in unmanned aerial vehicles: Spoofing, jamming and countermeasures. *Future Generation Computer Systems, 145*, 1–15.

Potkonjak, M., & Rabaey, J. M. (2016). Secure embedded systems: Design challenges. *Proceedings of the IEEE, 104*(6), 1200–1219.

Psiaki, M. L., & Humphreys, T. E. (2016). GNSS spoofing and detection. *Proceedings of the IEEE, 104*(6), 1258–1270.

Roff, H. M. (2016). Meaningful human control in weapon systems: A primer. *The RUSI Journal, 161*(1), 14–21. https://doi.org/10.1080/03071847.2016.1149360

Santoro, C. (2019). The ethics of neurotechnology in warfare: Emerging issues. In J. Forge (Ed.), *Emerging military technologies: Ethical and legal perspectives* (pp. 105–121). Springer.

Shafique, K., Khawaja, B. A., Sabir, F., Qayyum, A., & Mustaqim, M. (2021). Internet of drones for smart cities: Recent advancements and challenges. *IEEE Access, 9*, 44583–44600.

Sharkey, N. (2015). Saying 'No!' to lethal autonomous robots. *AI & Society, 30*(2), 177–183. https://doi.org/10.1007/s00146-014-0541-7

Suryadi, K., Putra, D. A., & Setiawan, R. (2020). Firmware security analysis of unmanned aerial vehicle. In *2020 6th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)* (pp. 109–114). IEEE.

Takahashi, T., Kubo, N., & Arai, T. (2018). A study on GPS spoofing attack against unmanned aerial vehicle. In *2018 International Conference on Unmanned Aircraft Systems (ICUAS)* (pp. 1247–1253). IEEE.

Tlili, M., Ayed, H. B., & Fourati, L. C. (2024). Legal implications of predictive analytics in UAV-based military operations. *Journal of Military Ethics, 23*(1), 55–73.

UNIDIR. (2017). *The weaponization of increasingly autonomous technologies: Considering ethics and international law*. United Nations Institute for Disarmament Research. https://unidir.org/publication/weaponization-increasingly-autonomous-technologies-considering-ethics-and-international-law

Wei, Z., Sun, J., Li, K., & Ma, H. (2024). Lightweight GPS spoofing detection techniques in low-cost UAVs. *IEEE Transactions on Aerospace and Electronic Systems, 60*(2), 1334–1346.

Wei, Z., Wang, J., & Sun, J. (2022). PerDet: A perception-based framework for detecting GPS spoofing and jamming in UAVs. *Ad Hoc Networks, 130*, 102781.

Wei, Z., Zhang, Y., & Ma, H. (2022). ConstDet: Semantic control anomaly detection under spoofing attacks in UAV navigation. *Sensors, 22*(9), 3251.

Yazdani, M., & Kazemi, A. (2020). The internet of drones: Architecture, applications, and challenges. *Journal of Industrial Information Integration, 20*, 100172.

Zhang, Y., Chen, J., & Li, B. (2023). A survey on security in unmanned aerial vehicle networks. *IEEE Access, 11*, 195–210.