Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), Noviembre-Diciembre 2025,
Volumen 9, Número 6.

https://doi.org/10.37811/cl_rcm.v9i6

IMPACTO DEL CONFLICTO RUSIA-UCRANIA EN LA DOCTRINA DE ARTILLERÍA ECUATORIANA: LECCIONES EN GUERRA DE DRONES

IMPACT OF THE RUSSIA-UKRAINE CONFLICT ON ECUADORIAN ARTILLERY DOCTRINE: LESSONS FROM DRONE WARFARE

Brian Rafael Torres Tarabata
Ejército Ecuatoriano

Karen Johanna Procel Hidalgo
Investigador independiente, Ecuador

Lorena Marley Hidalgo Carrillo
Escuela de Educación General Básica Dr. Leónidas García Ortiz, Ecuador,

DOI: https://doi.org/10.37811/cl_rcm.v9i6.21946

Impacto del Conflicto Rusia-Ucrania en la Doctrina de Artillería Ecuatoriana: Lecciones en Guerra de Drones

Brian Rafael Torres Tarabata[1]
brtorrest21@gmail.com
https://orcid.org/0009-0009-0246-5622
Ejército Ecuatoriano

Karen Johanna Procel Hidalgo
kprocel8@gmail.com
https://orcid.org/0000-0001-8568-7566
Investigador independiente
Ecuador

Lorena Marley Hidalgo Carrillo
marley.hidalgo@docentes.educacion.edu.ec
https://orcid.org/0009-0009-2255-098X
Escuela de Educación General Básica
Dr. Leónidas García Ortiz
Ecuador

RESUMEN

El Impacto que desencadeno el conflicto Rusia-Ucrania, transformo por completo la perspectiva sobre la doctrina de artillería ecuatoriana, mostrándose susceptible ante tecnologías asimétricas. El problema radica en que nuestro país no se encuentra ajeno a esta realidad por lo cual busca determinar las adaptaciones doctrinales necesarias para enfrentar de manera efectiva la amenaza de drones mediante las lecciones aprendidas del conflicto Rusia-Ucrania. La metodología fue cualitativa, documental, con un enfoque interpretativo, basado en el análisis de literatura científica, noticias de alto impacto y demás documentos publicados entre el año 2021 y 2025. En conclusión, los drones han revolucionado la guerra moderna, actualmente se desempeñan batallas multidimensionales por lo cual el ejército ecuatoriano debe potenciar sus capacidades técnicas y de defensa, transformándose hacia la innovación tecnológica y soberanía digital.

Palabras clave: conflicto rusia-ucrania, guerra de drones, artillería antiaérea, doctrina militar, ciberdefensa

[1] Autor principal.
Correspondencia: brtorrest21@gmail.com

Impact of the Russia-Ukraine Conflict on Ecuadorian Artillery Doctrine: Lessons from Drone Warfare

ABSTRACT

The impact triggered by the Russia-Ukraine conflict completely transformed the perspective of Ecuadorian artillery doctrine, revealing its vulnerability to asymmetric technologies. The problem lies in the fact that Ecuador is not exempt from this reality; therefore, the study seeks to determine the doctrinal adaptations necessary to effectively confront the drone threat through the lessons learned from the Russia-Ukraine conflict. The methodology was qualitative and documentary, with an interpretative approach based on the analysis of scientific literature, high-impact news, and other documents published between 2021 and 2025. In conclusion, drones have revolutionized modern warfare, and battles are now fought in multidimensional environments. Consequently, the Ecuadorian Army must strengthen its technical and defensive capabilities, transforming itself toward technological innovation and digital sovereignty.

***Keywords*:** russia-ukraine conflict, drone warfare, anti-aircraft artillery, military doctrine, cyber defense

Artículo recibido 10 diciembre 2025
Aceptado para publicación: 10 enero 2026

INTRODUCCIÓN

El conflicto armado entre Rusia y Ucrania se viene dando desde 2022 lo cual ha transformado por completo la perspectiva sobre la artillería moderna. Aquello que antes se percibía como un sistema robusto y seguro, ahora se muestra susceptible ante tecnologías asimétricas, sobre todo los drones de reconocimiento y ofensiva, estos pequeños dispositivos que parecían inofensivos pasatiempos de consumo, ahora logran desmantelar equipos de artillería con una máxima exactitud. De acuerdo con Center for Strategic and International Studies (Slusher, 2025), las bajas de artillería en esta guerra se atribuyen precisamente a drones comerciales adaptados.

En el caso de Ecuador, este país no se encuentra ajeno a la realidad, ya que grupos irregulares se apoyan de tecnologías accesibles como drones baratos, cámaras térmicas o sistemas improvisados de observación para vigilar posiciones o realizar ataques con una precisión que antes solo se veía por parte de Fuerzas Armadas.

La investigación propone analizar el aporte en la actualización y modernización de la doctrina de artillería antiaérea del Ejército Nacional Ecuatoriano tras el conflicto Rusia-Ucrania, en especial sobre lecciones en guerra de drones. Analiza cómo los progresos pueden servir a la defensa aérea y artillera.

El presente trabajo tiene el objetivo determinar las adaptaciones doctrinales necesarias para enfrentar de manera efectiva la amenaza drones mediante el uso de las lecciones aprendidas del conflicto en Europa del Este.

Entonces, aborda las preguntas: ¿cuáles son las principales lecciones sobre el uso y contramedidas de drones que la guerra rusa-ucraniana puede enseñarnos? ¿Qué importancia tienen estas modificaciones en la seguridad y operación del Ejército Nacional en el presente y el futuro?

Este estudio tiene un carácter investigativo con naturaleza cualitativa, de tipo documental y enfoque interpretativo que se sustenta en fuentes confiables y actuales como: publicaciones especializadas, análisis de expertos en estrategia militar y reportes oficiales de defensa. La importancia de esta nace de una necesidad, permitir que el Ejército Nacional Ecuatoriano mantenga una doctrina viva, actualizada y realmente efectiva frente a las nuevas formas de amenaza que imponen los avances tecnológicos.

Hoy en día, la defensa de la soberanía no solo depende del coraje y la disciplina de los soldados, sino de su adaptación a un entorno donde la tecnología modifica constantemente las reglas del juego.

Este trabajo busca contribuir al desarrollo de capacidades que permitan responder de manera inteligente, rápida y precisa a los desafíos que plantea la guerra moderna.

Entre los conceptos clave que sustentan esta investigación se encuentran la doctrina militar, la artillería, la guerra de drones, la defensa aérea y la evolución tecnológica en los conflictos armados. Todos ellos forman parte de una misma realidad: la transformación constante del campo de batalla y la obligación de estar siempre un paso adelante.

METODOLOGÍA

Este artículo forma parte de una investigación de carácter cualitativo, tipo documental y con un enfoque interpretativo. La elección metodológica surge de la necesidad de analizar a fondo fenómenos complejos, como es el impacto del conflicto Rusia-Ucrania en la doctrina de artillería ecuatoriana y el papel de los drones, que no pueden entenderse del todo a través de números o estadísticas. En el campo militar, y especialmente en el de la artillería, hay dinámicas que solo se comprenden cuando uno las examina con contexto, mirada crítica y la experiencia que da haber estado en terreno.

Los datos se obtuvieron mediante una revisión sistemática de literatura académica basada en Artículos de Revistas Científicas (12), Militares o de Seguridad (6), Capítulos en Colecciones o Libros Especializados (6), Trabajos Académicos (6), Reportes, Noticias y Publicaciones en Línea (6). Se priorizó en literatura comprendida entre 2021 y 2025 para ofrecer una visión general oportuna de los avances tecnológicos y militares actuales.

El análisis de datos se realizó mediante un análisis de contenido temático, con el objetivo de identificar tendencias, categorías recurrentes y tensiones conceptuales en la literatura. Estas unidades de análisis se organizaron en torno a tres áreas principales: (1) Lecciones extraídas del conflicto Rusia-Ucrania; (2) Relevancia para el Ejército Ecuatoriano; y (3) Proyección hacia escenarios futuros. Este marco permitió la triangulación de teorías y observaciones, fortaleciendo así la interpretación de los resultados y las hipótesis. Todo ello tiene como objetivo demostrar la exactitud de la metodología y sobre todo brindar conocimientos útiles a quienes servimos en las fuerzas armadas y comprender que cada lección en esta profesión puede ser útil en combate.

RESULTADOS Y DISCUSIÓN

Lecciones Extraídas Del Conflicto Rusia-Ucrania

Lección: La Asimetría Económica Define la Superioridad en el Campo de Batalla

La guerra de drones demostró que la superioridad tecnológica en la fase terminal del ataque ya no depende del costo de la plataforma, sino de la capacidad de infligir daño crítico a activos de alto valor con medios desechables (Kubatz, 2025). El conflicto ruso-ucraniano evidencia que la utilización masiva de RPAS (Remotely Piloted Aircraft Systems) ha provocado un salto operacional exponencial (Fayal & Rodrigues, 2025)(Carrión, 2024). La gran revolución ha sido el empleo de drones pequeños, incluyendo los drones FPV (First Person View) para misiones de ataque, reconocimiento y corrección de fuego de artillería (Romero & Lapeña, 2025). Esta es la clave de la economía de enjambre (Swarming):

Coste Optimizado vs. Daño Estratégico: Un BM-21, un sistema de cohetes múltiple, ahora es vulnerable a drones de $1,000 equipados con cámaras económicas (Chaari, 2025). Se ha demostrado que la mayor de las oportunidades para modernizar un activo militar es incorporar un sistema anti drones, ante la vulnerabilidad de los carros de combate que no poseen un sistema contra estos y que han sido destruidos fácilmente (López, 2022).

Disponibilidad y Proliferación: El empleo de drones FPV en el frente se ha generalizado. Las unidades ucranianas utilizan drones de combate propios y drones más pequeños, producidos localmente. Por ejemplo, el dron “Wild Hornet FPV, the Punisher”, de fabricación local en Ucrania, tiene un costo que oscila entre $450 y $550 dólares estadounidenses (Romero & Lapeña, 2025). Además, sus componentes están fácilmente disponibles en el mercado y no requieren permiso para obtenerlos y usarlos (Chaari, 2025).

La guerra de Ucrania demuestra que no se trata de tener el tanque más grande o el avión más caro. Es como si una hormiga, armada con una aguja, pudiera destruir un elefante. Cuando un dron que cuesta menos que un smartphone de gama alta puede inmovilizar un blindado de millones de dólares, la lógica del poder militar cambia por completo. El enemigo más astuto ya no es el que tiene más dinero, sino el que sabe fabricar miles de "aguijones" a bajo costo para agobiar y desangrar al gigante.

Lección: Adaptación puede ser más rápida que el refinamiento técnico.

El conflicto más reciente ha revelado una verdad que ningún estratega responsable puede ignorar: en los escenarios bélicos contemporáneos, la permanencia y el dominio no dependen del poderío material, sino de la capacidad para asimilar las circunstancias con inmediatez y responder con precisión ante lo inesperado. La superioridad técnica, por sí sola, carece de valor cuando el adversario demuestra una comprensión más ágil del entorno operativo y una voluntad firme para transformar sus medios conforme evoluciona la amenaza. El valor real de una fuerza moderna se mide en su habilidad para absorber conocimiento en plena contienda, reinterpretar sus tácticas y reorganizar sus recursos antes de que el enemigo logre anticipar el siguiente movimiento. En tales condiciones, la plataforma inicial se convierte en un punto de partida transitorio, pues lo que determina la victoria es la velocidad con que se incorporan innovaciones, se perfeccionan procedimientos y se neutralizan las maniobras adversarias. Solo quienes comprenden esta dinámica son capaces de sostener la iniciativa y preservar la eficacia de sus armas en medio del caos cambiante del combate.

El escenario ruso-ucraniano es un claro ejemplo de ello. Es lo que muchos analistas han denominado una guerra de umbral (threshold warfare), una etapa de transición en la que las tecnologías avanzadas evolucionan a un ritmo vertiginoso (Gómez et al., 2025)(Muñoz Pairet, 2025).

Carrera de innovación y emulación: Lo que se observa en este conflicto es una auténtica carrera de innovación-emulación, casi inmediata, entre las fuerzas enfrentadas (Gómez et al., 2025) . Cada avance de un bando es imitado o contrarrestado por el otro en cuestión de días, a veces de horas. Este ritmo tan acelerado exige una capacidad de adaptación que, sinceramente, no es común en los procesos tradicionales de desarrollo del poder militar. Los ciclos de planeamiento del Ejército suelen ser más pausados, estructurados, pensados a largo plazo. Pero la guerra actual no espera. Aquí, la lentitud se paga caro.

Evolución rápida de tácticas: El uso de drones es quizás el ejemplo más contundente. En apenas dos años, la guerra ha visto pasar cuatro generaciones distintas de tácticas y tecnologías (Fayal & Rodrigues, 2025). Este ritmo de cambio es impresionante. Y no solo eso: el Ejército ucraniano ha dado un paso audaz al crear una rama independiente dedicada exclusivamente a operaciones con drones (Amran, 2024).

Esa decisión muestra algo más profundo: una mentalidad institucional que entiende que la tecnología no es un complemento, sino el eje mismo de la estrategia contemporánea.

Ataques estratégicos profundos: La agilidad también se ha reflejado en la forma de planificar y ejecutar operaciones de gran impacto. Un ejemplo claro es la llamada Operación Telaraña, llevada a cabo en junio de 2025. En cuestión de horas, drones lanzados desde camiones destruyeron alrededor del 30% de la aviación estratégica rusa (Pizarro, 2025). Este tipo de ataque, dirigido a la retaguardia enemiga, no solo desorganiza la logística, sino que también cambia las reglas del juego: lograr superioridad de fuego y maniobra a partir de la sorpresa tecnológica (Goncharova & Zadorozhny, 2025; Márquez et al., 2024).

Para el artillero el peso decisivo no se mide exclusivamente en toneladas de acero ni en el alcance nominal del cañón sino en la capacidad colectiva para desensamblar un dispositivo enemigo, comprender su lógica operativa y devolver esa comprensión convertida en táctica propia antes de que el adversario complete la misma operación; en escenarios de este tipo la inventiva técnica y la prontitud para ejecutar variantes experimentales resultan factores de vida o muerte, obligaciones ineludibles que condicionan la disposición de hombres y equipos y que exigen una mentalidad orientada al ensayo constante, la réplica inmediata y la protección de la iniciativa.

Lección: La ciber resiliencia y la dualidad de las contramedidas

El conflicto actual ha dejado una enseñanza contundente: la defensa aérea ya no puede separarse de la guerra electrónica ni de la ciberdefensa. Hoy, el cielo y el ciberespacio están tan entrelazados que cualquier ventaja en uno repercute de inmediato en el otro. Y es que la dinámica del enfrentamiento ha derivado en una escalada constante entre jamming y anti-jamming, entre interferir y resistir la interferencia.

El caso ruso-ucraniano es, sin duda, un ejemplo paradigmático de esta nueva realidad. Se ha visto un uso masivo y variado de drones, junto con el despliegue acelerado de capacidades de guerra electrónica (EW) que se reinventan día a día (Gómez et al., 2025). Además, la capa cibernética ya no es un soporte técnico: se ha convertido en parte integral de la maniobra táctica. En este contexto, la resiliencia de las redes se ha transformado en un auténtico factor de combate (Kubatz, 2025).

Lucha guerra electrónica constante: Rusia ha empleado la guerra electrónica con una intensidad impresionante, llegando a inutilizar hasta la mitad de las aeronaves ucranianas en algunas zonas del frente. Ante esto, Kiev se ha visto forzada a responder con enjambres de drones FPV, una táctica que combina volumen, saturación y autonomía (Gómez et al., 2025)(Patiño Villa & Almario García, 2025). Y la verdad es que ambos bandos han comprendido algo esencial: el dominio cibernético también es un espacio de decisión. No solo se combate con misiles o drones, sino con datos, con algoritmos, con información que fluye a la velocidad de la luz.

Innovación en contra-contramedidas: En este tipo de guerra, cada avance tecnológico genera de inmediato una respuesta. La efectividad de un dron, por ejemplo, ya no depende solo de su alcance o carga útil, sino de su capacidad para resistir o evadir las contramedidas enemigas. Ucrania ha desarrollado tácticas ingeniosas para contrarrestar los sistemas rusos de EW (Gómez et al., 2025).

Un ejemplo revelador es el nuevo método para derrotar los drones FPV rusos controlados por fibra óptica, un tipo de conexión inmune a las interferencias tradicionales (Chaari, 2025). Además, la inteligencia artificial ha empezado a jugar un papel decisivo: desde el desarrollo de software de guía terminal para drones FPV, hasta sistemas avanzados de fusión de datos que permiten una mejor coordinación en tiempo real (Gómez et al., 2025; Romero & Lapeña, 2025).

Urgencia de las capacidades C-UAS: El conflicto también ha puesto en evidencia las limitaciones de las contramedidas actuales para destruir o neutralizar drones (Chaari, 2025). En este nuevo escenario, la ciberdefensa se ha vuelto un pilar esencial: sin ella, ni la artillería antiaérea ni los misiles pueden garantizar la seguridad operativa de los sistemas no tripulados. Y es que los drones, con toda su eficacia, son vulnerables a los hackeos y manipulaciones (Balladares et al., 2024)

El campo de batalla moderno ya no es solo terreno y fuego: es también un duelo invisible de señales. El enemigo lanza interferencias digitales para cegar tus drones, y tú respondes con un sistema conectado por fibra óptica, imposible de jampear. En el escenario contemporáneo el enfrentamiento se libra en un plano invisible donde el hacker y el defensor sostienen una contienda permanente por el dominio de la información y la integridad de los sistemas, una pugna silenciosa que no deja rastros de humo ni estruendo metálico pero que define el rumbo de las operaciones con una precisión implacable.

Quien logra conservar intacta su red de comunicaciones no solo preserva una ventaja técnica, sino que asegura el control del espacio operativo, el flujo de órdenes y la coherencia de toda maniobra. En este contexto la ciberseguridad ha adquirido el mismo peso que la artillería y la logística, pues sin ella el poder de fuego se dispersa y pierde dirección, mientras que su solidez convierte cada disparo, cada movimiento y cada señal en una acción viva y coordinada que sostiene la estructura de la guerra moderna.

Lección: deshumanización y el impacto ético del ataque remoto: el uso extendido de drones armados ha transformado la naturaleza misma del combate al distanciar al ejecutor del objetivo y relegar el riesgo a la dimensión de los algoritmos, una realidad que erosiona la noción tradicional del enfrentamiento cara a cara y convierte la decisión de abrir fuego en un acto casi administrativo. Esa separación física, aunque preserva vidas propias, introduce dilemas éticos de enorme complejidad porque diluye la percepción del enemigo como ser humano y reduce el conflicto a datos en una pantalla.

El uso de drones en operaciones militares ha traído ventajas operativas innegables, pero también ha abierto un debate urgente sobre sus implicaciones legales, éticas y humanitarias (E. García, 2016). No por nada, algunos autores han descrito esta forma de combate como "una guerra de videojuego con víctimas reales" (Calvo, 2014).

Despersonalización y distancia: El dron representa, quizá la culminación de la guerra a distancia. En él, la víctima y el agresor nunca se ven. La interacción humana desaparece, y con ella se diluye el peso moral de la acción. Esta despersonalización no es un detalle técnico: es un cambio profundo en la forma en que entendemos la responsabilidad en la guerra. El operador, al no enfrentar directamente las consecuencias físicas de su decisión, puede verse arrastrado a un tipo de desconexión moral que preocupa tanto como el daño que inflige. Y es que cuando la muerte se ejecuta con un clic, el umbral entre decisión y destrucción se vuelve peligrosamente delgado.

Impacto psicológico en los operadores: Paradójicamente, esa misma distancia que pretende proteger al soldado también lo hiere de otro modo. Muchos operadores de drones, pese a no estar en el campo de batalla, sufren estrés postraumático, ansiedad o culpa al ver en sus pantallas las consecuencias de sus decisiones. Es una guerra silenciosa, interior.

No hay explosiones alrededor ni balas cruzando el aire, pero la mente del operador carga con el peso invisible de haber quitado vidas sin moverse de una base. Es un recordatorio brutal de que la distancia física no siempre protege la conciencia.

Controversias éticas: La verdad es que el uso de drones ha generado controversias que aún no encontramos cómo resolver del todo. Su operación requiere menos entrenamiento que el de un piloto tradicional, y sus ataques pueden ejecutarse con escasa supervisión legal o ética. (J. García, 2024) Más grave aún: la posibilidad de delegar decisiones letales a algoritmos o sistemas autónomos amenaza con borrar la última barrera humana entre la vida y la muerte (Loaiza, 2025). Este desafío toca los cimientos del derecho internacional humanitario, que fue concebido en un mundo donde las decisiones las tomaban personas, no máquinas.

Los drones fueron concebidos para transformar el acto de matar en una operación aparentemente limpia, ejecutada con precisión quirúrgica y sin el contacto directo que durante siglos definió la esencia del combate, pues el operador observa al objetivo con la nitidez de una lente digital y la frialdad de un observador distante, como si el enfrentamiento transcurriera dentro de un entorno simulado. Sin embargo, esa claridad visual oculta una distorsión más profunda, ya que la distancia física diluye la carga emocional y desdibuja la frontera entre la acción real y la percepción de un juego controlado, lo que convierte la guerra en un ejercicio menos terrible en apariencia, aunque deja en el ejecutor una marca invisible, una herida que no se muestra en el cuerpo, pero permanece en la memoria cada vez que una vida desaparece en la superficie luminosa de una pantalla.

La enseñanza ética se impone con una sencillez que contrasta con su hondura moral, porque la reducción del riesgo no elimina la responsabilidad ni la culpa que acompañan al acto de combatir, del mismo modo que la distancia tecnológica no puede anular la dimensión humana del conflicto. Aunque los drones representen una herramienta de eficacia táctica innegable, la guerra continúa siendo una decisión tomada por hombres y mujeres que deben responder por las consecuencias de sus órdenes, razón por la cual ninguna máquina debe sustituir la conciencia que orienta el juicio moral del combatiente, principio que, según Loaiza (2025), constituye la última defensa frente a la deshumanización del campo de batalla.

Relevancia Para El Ejército Ecuatoriano

Requisito operacional: protección 360º y capacidad anti enjambre. La guerra moderna no da segundas oportunidades. Los drones ya no atacan solos; atacan como bandadas coordinadas, rápidas y letales, saturando las defensas y buscando el punto ciego del enemigo. En este nuevo escenario, la defensa antiaérea debe ver y responder en todas direcciones, de forma automática, casi instintiva, como si el vehículo tuviera un sistema nervioso propio.

Los sistemas AAA tradicionales fueron diseñados para enfrentar amenazas únicas y visibles. Hoy en día, el reto es diferente: neutralizar múltiples objetivos simultáneamente, desde diferentes ángulos y altitudes (López, 2022). Por lo tanto, se vislumbra un nuevo requisito operativo: los sistemas anti drones deben garantizar una protección integral de 360 grados, permitiendo una respuesta y acción inmediatas ante ataques de saturación.

Además, estos sistemas deben operar de forma automática y segura, sin dejar a la tripulación en una posición vulnerable. Ya no es aceptable que un soldado utilice un vehículo para lanzar un interceptor o un cañón antiaéreo; hacerlo significaría entregar su vida a un enemigo digital. En cuanto al diseño, la lógica actual se centra en plataformas ligeras, modulares y asequibles, capaces de integrarse en diferentes tipos de vehículos sin comprometer su movilidad ni sus costes operativos (López, 2022).

La lección de Ucrania es clara: si lanzas diez drones baratos a un tanque y la defensa puede derribar ocho, los dos restantes son suficientes para destruirlos. En una guerra donde cada dron cuesta cientos de dólares y cada vehículo millones, la asimetría es brutal. Por eso, el Ejército Ecuatoriano necesita un sistema multitarea, inteligente y completamente automatizado, que pueda detectar, decidir y responder sin demora. Modernizar no es una opción; es una cuestión de supervivencia institucional. Porque en la próxima guerra, quien no vea primero, no disparará nunca.

Relevancia para la Seguridad Nacional: Integración Tecnológica en Contextos Internos: La necesidad de sistemas AAA especializados va más allá de la defensa externa, ya que son esenciales para las Fuerzas Armadas ecuatorianas en la lucha contra el narcotráfico y las amenazas internas, especialmente en zonas como Manabí. La integración de vehículos aéreos no tripulados (UAV) es un factor clave para mejorar las capacidades operativas de las Fuerzas Armadas del Ecuador.

Los UAV son una tecnología existente para la vigilancia y el reconocimiento (Jara, 2025; Villarreal, 2021)Haga clic o pulse aquí para escribir texto.

Economía y Eficacia: La plataforma UAV es un elemento que contribuye a un sistema de capacidades superior y, por sí sola, no constituye una capacidad completa. Su utilidad se evalúa por su asequibilidad, pues ofrece la probabilidad de lograr los objetivos establecidos a un costo menor que otras alternativas (Jara, 2025).

Necesidad de Integración: La utilidad militar del sistema se logra solo si se desarrolla la doctrina para el empleo de los medios y se establece una estructura organizacional adecuada para la operación de estas aeronaves (Jara, 2025).

Cuando el Ejército patrulla Manabí o las fronteras, no solo está buscando ejércitos tradicionales, sino rutas de contrabando y movimientos de bandas criminales. El dron se convierte en el "ojo" más económico y eficaz para esta tarea. Si se usa un dron de Categoría II (Táctico) para inteligencia, vigilancia y reconocimiento) en lugar de un helicóptero tripulado, el Ejército ahorra dinero y mantiene la vigilancia por más tiempo.

La Especialización en Ciberdefensa y la Adaptación Doctrinal: El sistema AAA especializado en la era post-Ucrania requiere una integración indisoluble con la ciberseguridad, ya que la amenaza aérea es, en esencia, una amenaza digital que requiere nuevas doctrinas y prioridades de capacitación (Loaiza, 2025).

La instrucción militar basada únicamente en los métodos convencionales ha quedado rebasada ante la naturaleza cambiante de las amenazas modernas, pues los escenarios actuales exigen una preparación que trascienda el dominio de las armas y abrace con igual rigor el conocimiento tecnológico y la defensa digital, tal como advierte Kubatz (2025), quien señala que los conflictos contemporáneos ya no se definen por la cantidad de proyectiles disparados sino por la capacidad para proteger la información y anticipar ataques invisibles. La formación tradicional, centrada en la maniobra física y la potencia de fuego, resulta insuficiente cuando el enemigo puede vulnerar la estructura operativa a través de una simple intrusión en los sistemas de comunicación, lo que transforma cada red en un frente de combate.

Vulnerabilidad Digital: Los drones militares son vulnerables a los intentos de hackeo y manipulación (Balladares, 2024; Loaiza Ledesma, 2025). Por lo tanto, el sistema AAA especializado debe ser capaz

de operar contra amenazas físicas y digitales mediante tecnologías de interferencia (Jamming), GPS spoofing y hackeo Wi-Fi (Romero & Lapeña, 2025).

Necesidad de Adaptación: La adaptación de esta nueva capacidad no requiere necesariamente cambios en la doctrina formal sino modificaciones en las tácticas, técnicas y procedimientos (TTPs). Esta transformación debe ser continua para garantizar que los equipos estén a la par con los de otros países y para que el personal cuente con el adiestramiento y capacitación necesarios (Cabezas & Utreras, 2019).

Prioridad Nacional: La investigación, desarrollo tecnológico, innovación y producción, constituyen ámbitos fundamentales para el sector Defensa del país, pues permiten reducir la brecha tecnológica y disminuir la dependencia exógena, garantizando la superioridad tecnológica necesaria para defender la soberanía (Mosquera et al., 2022).

El sistema antiaéreo moderno es un instrumento que va más allá del proyectil y la trayectoria conocida, pues además de disparar municiones físicas es capaz de emitir pulsos electromagnéticos destinados a confundir, cegar o inmovilizar plataformas no tripuladas; esa capacidad convierte la instalación en una estación de guerra electrónica donde la señal resulta tan decisiva como la explosión y donde la caja de herramientas del operador incluye ahora protocolos de red, análisis de espectro y algoritmos de bloqueo, de modo que el cañón tradicional comparte espacio operativo con consolas y terminales que exigen conocimientos técnicos precisos y actualización constante.

Proyección Hacia Escenarios Futuros

Escenario de Proyección 1: Consolidación de la Capacidad de Vigilancia y Reconocimiento (ISR): Desde la experiencia acumulada en labores de investigación y en operaciones de artillería, la proyección más previsible —y a la vez más práctica— es la consolidación de la capacidad de Vigilancia, Inteligencia y Reconocimiento (ISR) del Ejército Ecuatoriano, apoyada en UAVs de bajo coste operativo. La verdad es que, bien aprovechados, estos sistemas cambian las reglas del juego: ofrecen permanencia, alcance y una relación costo-beneficio que antes era impensable (Cruz, 2024; Torres González et al., 2025).

La tecnología de integración de vehículos aéreos no tripulados UAVs, como la desarrollada en el proyecto DOCR del Ministerio de Defensa Nacional, tiende a convertirse en un pilar operativo para las

Fuerzas Armadas. La proyección implica el empleo sostenido de plataformas de Categoría I y II (tácticas y pequeñas) en áreas sensibles —por ejemplo, Manabí— donde conviven problemas complejos: narcotráfico, minería ilegal y delincuencia en el litoral y en vías fluviales (Jara, 2025). Estos sistemas, dotados de sensores electroópticos avanzados y transmisión en tiempo real, integran información que antes tardaba horas o días en consolidarse. Y eso, créase o no, marca la diferencia entre reaccionar tarde o neutralizar a tiempo.

Imaginemos la siguiente escena: patrullas que deben cubrir selva, costa y ríos sin descanso. Antes, esa tarea implicaba helicópteros o aeronaves tripuladas —costosas, exigentes en logística y riesgosas para la tripulación—. En el futuro cercano, el dron es el "ojo" que no se cansa: vigila por horas, detecta movimientos sospechosos, retransmite evidencia en vivo y permite al comandante tomar decisiones informadas sin arriesgar vidas. Es una jugada eficiente y económica: menos gasto, más información y una capacidad de respuesta que antes simplemente no era asequible.

La adquisición de drones no garantiza capacidades operativas, pues la eficacia real se manifiesta cuando existe doctrina clara, personal instruido y una estructura capaz de interpretar y explotar los flujos de información que los UAV suministran, consideración respaldada por Jara (2025) y por Linares (2021) quienes subrayan la necesidad de integrar los nuevos medios en un entramado disciplinario que transforme datos en decisiones tácticas y en ventaja estratégica.

Escenario de Proyección 2: Amenaza Híbrida y Guerra de Drones del Crimen Organizado: El escenario más perturbador se manifiesta cuando el monopolio aéreo del Estado se diluye frente al empleo masivo y coordinado de drones por parte de los grupos criminales transnacionales, situación en la que la amenaza deja de ser una abstracción estratégica para convertirse en una condición operativa inmediata, asimétrica y de alto riesgo, dado que estas plataformas permiten proyectar violencia desde el anonimato y con costos logísticos reducidos.

En Ecuador se detectan indicios de esta transformación del espacio aéreo y en la práctica los drones han fortalecido las capacidades operativas del crimen organizado en varias regiones, hallazgo documentado por Cevallos (2025) y por informes de InSight Crime (2025), mientras que episodios como el intento de ataque a la cárcel La Roca en Guayaquil ejemplifican cómo actores no estatales experimentan y

emplean estas tecnologías en operaciones reales, prueba palpable de que la superioridad aérea estatal puede quedar cuestionada si no se reaccionan las doctrinas y las capacidades defensivas.

Desde la mirada técnica y táctica la lógica de la amenaza resulta simple y despiadada, un dron puede destruir o penetrar objetivos a una fracción del costo que implica un blindado o una infraestructura fortificada, circunstancia que impone la obligación de repensar defensas, disposiciones y manuales con celeridad; la asimetría económica y operativa obliga a concebir un "escudo digital" capaz de neutralizar enjambres y derribar múltiples plataformas económicas simultáneamente, sin ese paraguas protector las piezas más sensibles del aparato militar y logístico permanecerán expuestas a ataques de baja complejidad técnica pero alto impacto, conclusión en consonancia con las advertencias de López (2022).

La proyección estratégica exige imaginar una contienda a baja altitud donde quien se retrase pierde el control territorial y donde la sofisticación tradicional resulta prescindible ante la capacidad de saturación y coordinación; por esta razón la respuesta debe articular dos ejes complementarios y simultáneos, por un lado fortalecer ISR y defensas anti-UAV a escala táctica dotando a unidades de sensores, sistemas de identificación y contramedidas electrónicas rígidas y flexibles, por otro fomentar capacidades de inteligencia, marcos legales y mecanismos de cooperación interinstitucional que permitan anticipar, desmantelar y neutralizar las cadenas logísticas que sostienen el accionar criminal, estrategia integral que busca restituir la ventaja estatal y preservar la seguridad del territorio.

En síntesis, el futuro cercano puede consolidar una vigilancia persistente y asequible que mejore la seguridad interna, Pero también puede abrir la puerta a una guerra híbrida donde actores no estatales usen enjambres para neutralizar la capacidad estatal.

Escenario de Proyección 3: Imperativo de la Soberanía Tecnológica y Ciberdefensa: La proyección del uso de drones no será efectiva si el Ejército Ecuatoriano no prioriza la infraestructura tecnológica local, la ciberseguridad y la generación de doctrina especializada. La verdad es que ya no basta con adquirir equipos modernos: hoy, la soberanía militar depende tanto de la tecnología como del conocimiento para operarla y protegerla.

La transformación debe entenderse como un ciclo ininterrumpido de adaptación donde la incorporación de medios novedosos no concluye con la entrega del equipo sino que exige actualización doctrinal,

adiestramiento constante y capacidad logística para sostener cambios operativos (Covarrubias, 2022) y que obligan a concebir la modernización como tarea permanente; la adopción de drones y de inteligencia artificial ofrece ventajas operativas de gran alcance, sin embargo también abre vectores de riesgo real que incluyen ciberataques dirigidos, manipulación de sistemas autónomos y potencial pérdida de control sobre plataformas desplegadas en teatros complejos, amenazas que requieren una respuesta técnica y ética alineada con los imperativos del servicio.

La planificación estratégica debe integrar tres dimensiones no negociables que guíen cualquier compra o programa de implementación, la primera es la efectividad operacional que determina la capacidad de la tecnología para cumplir misiones concretas bajo condiciones reales, la segunda es la idoneidad doctrinal que evalúa si el medio se ajusta a las tácticas, al adiestramiento y a la cultura de la unidad y la tercera es la asequibilidad sostenida que contempla no solo el costo inicial sino el ciclo de vida, el mantenimiento y la formación especializada, (Loaiza, 2025)presenta como columna vertebral para evitar inversiones tecnológicas que no se traduzcan en ventaja estratégica duradera.

Doctrina y entrenamiento (Idoneidad): Un dron no sustituye a una doctrina operativa específica para su empleo, pues las reglas que rigen las aeronaves no tripuladas difieren en técnica y en propósito de las aplicables a plataformas tripuladas, y por ello las Fuerzas Armadas deben orientar la investigación, el desarrollo y la innovación hacia sistemas aeronáuticos que respondan a necesidades urgentes y estratégicas del país tal como plantea (Jara, 2025) lo que exige un proceso formativo integral.

Ciberresiliencia (Efectividad): La guerra de drones es, ante todo, una guerra digital. Los UAVs son vulnerables a hackeos y manipulación, y cualquier fallo en la ciberdefensa puede neutralizar toda la inversión (Balladares et al., 2024). El Ejército debe fortalecer el Comando de Ciberdefensa e invertir en tecnologías anti-drones avanzadas, asegurando que las infraestructuras críticas estén protegidas y que las operaciones puedan mantenerse incluso ante ataques cibernéticos (Espinoza. Christian et al., 2025).

Asequibilidad y continuidad: La incorporación de vehículos aéreos no tripulados exige una planificación de largo aliento que contemple no solo la compra inicial sino el ciclo de vida completo, mantenimiento programado, actualizaciones tecnológicas periódicas y la expansión gradual de la flota conforme se validen doctrinas de empleo y capacidades logísticas, por cuanto la inteligencia artificial

incorpora una frontera de optimización capaz de racionalizar recursos, automatizar labores repetitivas y mejorar la planificación de misiones con menor carga humana, factores que (Loaiza, 2025) identifica como elementos que reducen costos operativos y elevan la eficiencia del despliegue.

Carece de sentido disponer de plataformas avanzadas si el adversario posee la capacidad de vulnerarlas o si la institución no cuenta con personal formado para emplearlas de manera coherente, por ello el porvenir de la defensa ecuatoriana exige la formación de lo que se podría denominar "cerebros tecnológicos", profesionales que combinen pericia en sistemas, análisis de datos y disciplina operativa, de igual modo resulta imprescindible la actualización de manuales militares para incorporar procedimientos específicos de guerra con drones y la conformación de equipos de ciberdefensa.

La gran lección es clara: De nada sirve tener los drones más avanzados si el enemigo puede hackearlos o si el Ejército no sabe cómo emplearlos correctamente. El futuro de la defensa ecuatoriana requiere "cerebros tecnológicos" tanto como hardware. Esto significa actualizar manuales militares para incluir la guerra de drones y formar equipos de ciber defensores capaces de proteger comunicaciones, sensores y sistemas críticos.

CONCLUSIONES

Los drones han revolucionado la guerra moderna, son necesarios para el reconocimiento, la vigilancia, el ataque y la defensa. Su uso creciente demuestra que las capacidades de combate ya no dependen de la mano de obra, sino de tecnologías, información y adaptabilidad táctica. Los sistemas ofensivos deben evolucionar continuamente integrando operaciones electrónicas, cibernéticas y de tráfico, entre otros.

Las lecciones aprendidas sugieren que el control del campo electromagnético y la eficiencia tecnológica son factores críticos para la supervivencia militar en el campo de batalla moderno. Esto representa un cambio en la educación hacia una guerra multidimensional, donde la información y la comunicación se vuelven tan importantes como la mano de obra, o incluso más importantes.

Finalmente, se concluyó que el Ejército Ecuatoriano debe potenciar su adiestramiento, tanto en capacidades técnicas de vigilancia aérea remota y defensa, como en ciberseguridad y seguridad electrónica de la estructura que garanticen la operación continua de sistemas de comando y control. A la vez se puede formar trabajadores con diferentes atributos: aquellos que operan y dan mantenimiento a sistemas complejos en entorno exigente.

Las consecuencias de este estudio se ubican a nivel estratégico, donde contaríamos con la opción de desarrollar las capacidades nacionales de acumulación tecnológica y adaptación ante amenazas emergentes, de tal manera que se reduzca la dependencia externa y se fortaleza el grado de autonomía militar.

La proyección a futuro indica que los conflictos de este tipo serán determinados por los sistemas autónomos automatizados e interconectados en los distintos dominios de la guerra, entre la inteligencia artificial. Así, el Ejército Nacional Ecuatoriano debe orientar su transformación hacia la innovación tecnológica y soberanía digital como pilares de su defensa.

En este contexto, la institución debe avanzar estratégicamente en tres líneas de acción:

Fortalecer las capacidades inmediatas, mediante la adquisición y adaptación de sistemas de defensa anti-dron modulares.

Consolidar una doctrina especializada de guerra electrónica y ciberdefensa, incorporando a su uso la integración de vehículos aéreos no tripulados (UAV) e inteligencia artificial en la planificación táctica.

Fomentar la investigación, el desarrollo y la cooperación interinstitucional con universidades y centros tecnológicos para generar producción nacional de sistemas ISR y contramedidas.

REFERENCIAS BIBLIOGRAFICAS

Amran, R. (2024). *Zelensky: el ejército ucraniano creará una división separada dedicada a los drones*. https://kyivindependent.com/zelensky-to-create-separate-division-of-military-focused-on-drones/

Balladares, P., Bustos-Estrella, A., Albuja, G., & Alarcón, M. (2024). Advances in military drone technologies. *Athenea Engineering sciences journal*, *5*(18), 7-18. https://doi.org/10.47460/ATHENEA.V5I18.81

Cabezas, M., & Utreras, B. (2019). *Propuesta de adquisición de una capacidad mecanizada para operaciones de reconocimiento y seguridad para la Fuerza Terrestre* [Universidad de las Fuerzas Armadas ESPE].]. https://redi.cedia.edu.ec/explore/documents?p=1&f=area_investigator_str:%22Militar%22&f=letter:P*

Calvo, J. (2014). *Informe 23: Drones militares. La guerra de videojuego con víctimas reales - Delas*. https://centredelas.org/publicacions/informe-23-drones-militares-la-guerra-de-videojuego-con-victimas-reales/?lang=es

Carrión, P. (2024). La logística en el campo de batalla: influencia de los drones en el conflicto Rusia-Ucrania. *Revista Ensayos Militares*, *10*(1), 66-81. https://revistaensayosmilitares.cl/index.php/acague/article/view/434

Chaari, M. Z. (2025). Analysis of the power of drones and limitations of the anti-drone solutions on the Russian-Ukrainian battlefield. *Security and Defence Quarterly*, *51*(3), 38-73. https://doi.org/10.35467/SDQ/208347

Covarrubias, J. G. G. (2022). Reflexión Sobre el Futuro de la Transformación Militar. *Revista Seguridad y Poder Terrestre*, *1*(2), 199-216. https://doi.org/10.56221/SPT.V1I2.18

Cruz, W. (2024). *Empleo de Drones en el Sistema de Inteligencia, Vigilancia y Reconocimiento Para las Acciones Militares en el Ce Vraem, 2021* [Escuela Superior de Guerra del Ejército. Escuela de Postgrado]. https://hdl.handle.net/20.500.14141/330

Espinoza. Christian, Sotomayor, D., Viera, M., & Cano, V. (2025). Seguridad militar inteligente: integración de tecnologías emergentes y gobernanza contractual en la protección de infraestructuras estratégicas del Ejército Ecuatoriano. *Pacha. Revista de Estudios Contemporáneos del Sur Global*, *6*(19), e250466-e250466. https://doi.org/10.46652/PACHA.V6I19.466

Fayal, R., & Rodrigues, R. (2025). Drones, inteligência artificial, cibersegurança e seus impactos sobre a preparação militar: uma visão da Escola Superior de Guerra do Brasil. En Asociación de Colegios de Defensa Iberoamericanos (Ed.), Preparación militar y ciberseguridad en la era de los drones y la IA. En *Preparación militar y ciberseguridad en la era de los drones y la IA (oportunidad o amenaza): la visión de los Colegios de Defensa Iberoamericanos* (p. 48). Instituto de Altos Estudios Estratégicos (IAEE). https://repositorio.esg.br/handle/123456789/2117

García, E. (2016). Altas tecnologías, conflictos armados y seguridad humana. *Araucaria*, *18*(36), 265-293. https://doi.org/10.12795/araucaria.2016.i36.12

García, J. (2024). *Tendencias y perspectivas futuras de la IA en el ámbito militar.* [Escuela Superior de Guerra "General Rafael Reyes Prieto"]. https://www.esdegrepositorio.edu.co//handle/20.500.14205/11258

Gómez, G. A., Triana. Ervin, & Espinosa, L. (2025). Guerra de umbral: Entre la automatización y la hiperguerra plena. En Preparación militar y ciberseguridad en la era de los drones y la IA. En *Preparación militar y ciberseguridad en la era de los drones y la IA (oportunidad o amenaza): la visión de los Colegios de Defensa Iberoamericanos*. Instituto de Altos Estudios Estratégicos (IAEE). https://repositorio.esg.br/handle/123456789/2117

Goncharova, O., & Zadorozhny, T. (2025). *Ukrainian drone strike on Russian airfield hits bomb depot, aircraft*. https://kyivindependent.com/ukraine-strikes-deep-into-russia-with-drones-after-record-kyiv-barrage-06-2025/

Jara, L. (2025). Aeronaves no tripuladas como nueva tecnología para mejorar las capacidades de las fuerzas armadas. *Revista de la Academia del Guerra del Ejército Ecuatoriano*, *18*(01), 16-16. https://doi.org/10.24133/AGE.VOL18.N01.2025.10

Kubatz, P. C. (2025). Preparación militar y ciberseguridad en la era de los drones y la IA: ¿Oportunidad o amenaza? En Preparación militar y ciberseguridad en la era de los drones y la IA (oportunidad o amenaza). En *Preparación militar y ciberseguridad en la era de los drones y la IA (oportunidad o amenaza): la visión de los Colegios de Defensa Iberoamericanos* (pp. 02-26). Instituto de Altos Estudios Estratégicos (IAEE). https://repositorio.esg.br/handle/123456789/2117

Loaiza, J. (2025). Ciberdefensa militar ante drones e inteligencia artificial. En Preparación militar y ciberseguridad en la era de los drones y la IA. En *Preparación militar y ciberseguridad en la era de los drones y la IA (oportunidad o amenaza): la visión de los Colegios de Defensa Iberoamericanos* (pp. 132-147). Instituto de Altos Estudios Estratégicos (IAEE). https://repositorio.esg.br/handle/123456789/2117

López, A. (2022). *Estudio comparativo de sistemas anti-drones para dotar al Leopardo 2E Comparative study of anti-drone systems for equipping the Leopard 2E Trabajo Fin de Grado*. http://zaguan.unizar.es

Márquez, Á., Martínez De Baños, A., & López, L. (2024). *NECESIDADES DERIVADAS DEL EMPLEO DEL CAS DEL COMBATE ASIMÉTRICO AL COMBATE SIMÉTRICO Nombre y apellidos del autor Trabajo Fin De Grado GRADOGRAGrado*. Universidad de Zaragoza. http://zaguan.unizar.es

Mosquera, O. M. G., Hernández, W. G. L., Sáenz, F. J. A., & Ger, G. A. P. (2022). Hacia las nuevas tendencias tecnológicas de defensa en Fuerzas Armadas del Ecuador: DOI: http://dx.doi.org.10.18847/1.16.8. *Revista de Estudios en Seguridad Internacional*, *8*(2), 125-148. https://doi.org/10.18847/1.16.8

Muñoz Pairet, Pau. (2025). Las grandes potencias en la guerra de la información. *Torrosa, Online Digital Booksotre*, 1-530.

Patiño Villa, C. A., & Almario García, Ó. (2025). Internacionalización y entramado global de la guerra en Ucrania. *Análisis Político*, *38*(110), 26-54. https://doi.org/10.15446/ANPOL.V38N110.122247

Pizarro. (2025). *"OPERACIÓN TELARAÑA" - Centro de Estudios de la Academia de Guerra*. https://www.ceeag.cl/operacion-telarana/

Romero, M., & Lapeña, R. (2025). ¿Qué podemos esperar del empleo de losdrones y cuál será su impacto en la seguridad de la región? En *Preparación militar y ciberseguridad en la era de los drones y la IA (oportunidad o amenaza): la visión de los Colegios de Defensa Iberoamericanos* (pp. 408-435). Instituto de Altos Estudios Estratégicos (IAEE). https://repositorio.esg.br/handle/123456789/2117

Slusher, M. (2025). *Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience*.

Torres González, M. D. J., Zapata Cortes, J. A., Aguirre Restrepo, Y., Jiménez Navia, B., Paipa Sanabria, E. G., Torres González, M. D. J., Zapata Cortes, J. A., Aguirre Restrepo, Y., Jiménez Navia, B., & Paipa Sanabria, E. G. (2025). Tecnologías en el sector defensa: una revisión internacional. *Revista Logos Ciencia & Tecnología*, *17*(2), 142-165. https://doi.org/10.22335/RLCT.V17I2.2007

Villarreal, R. (2021). Doctrina de seguridad nacional en Ecuador: influencia y relaciones estado ↔ Fuerzas Armadas. *Revista de Ciencias de Seguridad y Defensa*, *6*(1), 18-18. https://doi.org/10.24133/RCSD.VOL06.N01.2021.02