EL PODER AÉREO EN UN ESCENARIO VOLÁTIL Y TECNOLÓGICAMENTE AVANZADO: HACIA UN NUEVO ENFOQUE

AIR POWER IN A VOLATILE AND TECHNOLOGICALLY ADVANCED ESCENARIO: TOWARDS A NEW APPROACH

Eduardo Cárdenas Tovar [1]

Resumen

El artículo analiza la transformación del poder aéreo en un entorno internacional marcado por amenazas tecnológicas avanzadas y la proliferación de sistemas no tripulados. La superioridad aérea, antes considerada un dominio asegurado, se ha vuelto efímera y altamente disputada debido a la aparición de tecnologías como misiles hipersónicos, armas de energía dirigida, enjambres de drones y la integración de la inteligencia artificial en los sistemas de combate. Estas innovaciones han reducido los tiempos de reacción y aumentado la letalidad y precisión de los ataques, obligando a las fuerzas aéreas a repensar sus doctrinas y estrategias.

La guerra electrónica y la cibernética han adquirido un rol central, permitiendo degradar la capacidad de mando, control y vigilancia del adversario, y potenciando las estrategias de anti-acceso y negación de área. El artículo destaca la necesidad de adoptar modelos operativos distribuidos y multidominio, integrando capacidades espaciales, cibernéticas y electromagnéticas para generar ventajas tácticas y estratégicas.

En el ámbito de la seguridad interna, el poder aéreo se presenta como una herramienta clave para enfrentar el crimen organizado, gracias a su capacidad de vigilancia, inteligencia y ataque selectivo mediante drones. Se enfatiza la importancia de desarrollar doctrinas específicas, fortalecer la interoperabilidad entre fuerzas armadas y policiales, y adaptar la legislación nacional para regular el uso de nuevas tecnologías en operaciones de seguridad.

Finalmente, el artículo concluye que la superioridad aérea del futuro dependerá menos de la potencia de fuego y más de la capacidad para controlar el espectro electromagnético, integrar inteligencia artificial y operar en entornos altamente digitalizados. La adaptación doctrinal, tecnológica y cultural será esencial para mantener la relevancia y eficacia del poder aéreo ante las amenazas emergentes.

Palabras clave: Poder aéreo, guerra electrónica, seguridad interna.

Abstract

The article analyzes the transformation of air power in an international environment marked by advanced technological threats and the proliferation of unmanned systems. Air superiority, once considered an assured domain, has become fleeting and highly contested due to the emergence of technologies such as hypersonic missiles, directed energy weapons, drone swarms, and the integration of artificial intelligence into combat systems. These innovations have reduced reaction times and increased the lethality and precision of attacks, forcing air forces to rethink their doctrines and strategies.

Electronic and cyber warfare have acquired a central role, enabled the degradation of the adversary's command, control, and surveillance capabilities, and enhancing anti-access and area denial strategies. The article highlights the need to adopt distributed and multi-domain operational models, integrating space, cyber, and electromagnetic capabilities to generate tactical and strategic advantages.

In the field of internal security, air power is presented as a key tool to confront organized crime, thanks to its surveillance, intelligence, and selective attack capabilities through drones. The importance of developing specific doctrines, strengthening interoperability between armed forces and police, and adapting national legislation to regulate the use of new technologies in security operations is emphasized.

Finally, the article concludes that future air superiority will depend less on firepower and more on the ability to control the electromagnetic spectrum, integrate artificial intelligence, and operate in highly digitalized environments. Doctrinal, technological, and cultural adaptation will be essential to maintain the relevance and effectiveness of air power in the face of emerging threats.

Keywords: Air power, electronic warfare, internal security

1 El Brigadier General SP Eduardo Cárdenas Tovar es investigador del Centro de Estudios Estratégicos de la ESPE, especialista en estrategia aeroespacial, fue director de la Academia de Guerra Aérea, comandante del Ala de Combate No 23 y del Ala de Combate No 21 Taura. Máster en Estudios Estratégicos por el Air War College

Introducción

En un escenario global cada vez más volátil y tecnológicamente avanzado, la superioridad aérea ya no puede entenderse como un dominio asegurado, sino como un espacio altamente disputado, efímero y dinámico. Los adversarios contemporáneos están equipándose con tecnologías de detección de largo alcance, fuegos de precisión multidominio y capacidades avanzadas de ataque electrónico, todas ellas en constante evolución y cada vez más disponibles. Este arsenal emergente les permite detectar amenazas en profundidad y ejecutar ataques a gran distancia con una eficacia sin precedentes.

La aceleración de la automatización en los procesos militares ha transformado radicalmente la cadena de destrucción, reduciendo los tiempos necesarios para detectar, seguir, apuntar y neutralizar objetivos. Esta evolución permite aplicar efectos de combate con rapidez quirúrgica y eleva la precisión y letalidad de los sistemas de armas. Paralelamente, la proliferación de sistemas no tripulados ha abierto la puerta a nuevas formas de proyectar poder en entornos hostiles, facilitando la ejecución de misiones de alto riesgo sin comprometer vidas humanas, y aumentando significativamente la capacidad de saturar el campo de batalla.

Este panorama se complejiza aún más con la incorporación de tecnologías disruptivas como los misiles hipersónicos, las armas de energía dirigida y los enjambres de sistemas autónomos. Estas innovaciones amplían las zonas de empleo de armas y reducen drásticamente los tiempos de respuesta para interceptar o neutralizar amenazas. Como resultado, el entorno operativo del futuro se caracterizará por una densidad sin precedentes de amenazas sofisticadas, persistentes y de múltiples dominios, lo cual representa un desafío crítico tanto para la supervivencia como para la eficacia operativa de las fuerzas aéreas.

En este contexto, el concepto tradicional de proyección de poder aéreo está siendo puesto en entredicho. Las rutas de acceso para lograr o mantener el control del espacio aéreo estarán cada vez más limitadas, y la libertad de maniobra, profundamente condicionada por la presencia constante de sensores y sistemas de armas adversarios. Sin un cambio de enfoque estratégico, las fuerzas aéreas podrían encontrarse en una era de “pos proyección de poder”, donde su capacidad para operar con libertad y eficacia quede gravemente comprometida.

Para revertir esta tendencia, resulta urgente repensar el concepto de poder de combate aéreo. Enfrentar los desafíos emergentes en materia de superioridad aérea requerirá abandonar enfoques convencionales centrados exclusivamente en efectos cinéticos —como el modelo de “bombas sobre el objetivo”— para adoptar estrategias multidominio que integren capacidades cinéticas y no cinéticas en un entorno operacional convergente. El dominio del entorno electromagnético será cada vez más decisivo, al igual que la integración entre guerra electrónica y guerra cibernética, todo ello potenciado por tecnologías de automatización e inteligencia artificial que permitan decisiones más rápidas, mejor informadas y anticipadas a los movimientos del adversario.

Este replanteamiento del poder aéreo implica, además, una reconfiguración operativa basada en modelos distribuidos. La capacidad de generar misiones desde múltiples ubicaciones con baja huella logística, combinada con una postura de combate desde la distancia, puede ofrecer ventajas significativas en términos de agilidad, resiliencia y supervivencia. Aprovechar vectores de acceso temporales mediante maniobras rápidas será clave para mantener la iniciativa y operar desde posiciones ventajosas.

Sin embargo, esta transformación estratégica no está exenta de consecuencias. A medida que las fuerzas aéreas redirigen sus capacidades hacia una lógica más flexible y distribuida, se abren nuevas fronteras en la competencia internacional, cuyos impactos podrían ser más amplios y profundos de lo que actualmente anticipan los tomadores de decisiones en el ámbito del poder aéreo. La capacidad para adaptarse a estos desafíos será, en última instancia, la diferencia entre la irrelevancia y la ventaja estratégica.

El panorama de amenazas

El entorno operativo contemporáneo está experimentando una transformación sin precedentes debido al auge de sistemas no tripulados, tecnologías emergentes y la creciente integración entre dominios, junto con las municiones merodeadoras y drones tácticos de bajo costo, están redefiniendo la forma en que se proyecta el poder de combate. Esta evolución permite a los actores estatales y no estatales emplear una gama cada vez más amplia de plataformas —tanto de ataque directo como de apoyo remoto— que combinan flexibilidad operativa con bajos costos logísticos. La proliferación de estas tecnologías ha generado un efecto disruptivo sobre las tradicionales cadenas de destrucción, facilitando formas más ágiles y despersonalizadas de ejecutar operaciones ofensivas y defensivas.

En los últimos años, los sistemas no tripulados han permitido una reducción significativa del contacto físico entre fuerzas opuestas, ampliando los márgenes de acción estratégica en escenarios altamente disputados. Con cientos de modelos en despliegue o fase de desarrollo —cada uno con características únicas en términos de velocidad, alcance operativo y firmas de radar—, estas plataformas han mejorado la capacidad de adaptación de las fuerzas armadas a múltiples escenarios y misiones. La capacidad de cargar municiones diversas o sensores especializados permite a estos sistemas operar desde una gama más amplia de ubicaciones, incluso desde zonas cercanas al objetivo, y hacerlo en grandes volúmenes que desafían las capacidades de defensa tradicionales. (Fig.1).

Figura 1
Sistemas no tripulados

Fuente: Cazas no tripulados YFQ-42A (abajo) y YFQ-44A. General Atomics Aeronautical Systems, Inc. y Anduril Industries. Tomado de: (Gordon, 2025)

El avance acelerado de la inteligencia artificial (IA) ha sido un catalizador para esta transformación. La IA no solo mejora la autonomía y la eficiencia de estos sistemas, sino que también impulsa el desarrollo de conceptos como las aeronaves de combate colaborativas, que permitirán crear fuerzas mixtas más resilientes, capaces de absorber pérdidas sin comprometer el cumplimiento de la misión. Al reducir los costos de entrada para la proyección de poder aéreo, se espera que la escala, variedad y letalidad de las amenazas no tripuladas continúe expandiéndose, incluyendo operaciones en enjambres autónomos coordinados que desborden las defensas convencionales.

Los enjambres autónomos representan una revolución táctica, habilitando nuevas capacidades en misiones de supresión y destrucción de defensas aéreas enemigas, así como en ataques de precisión profunda contra blancos estratégicos (Chamola, 2021). A ello se suman desarrollos tecnológicos disruptivos como los misiles balísticos lanzados desde el aire (ALBMs) por sus siglas en inglés, los vehículos planeadores hipersónicos (HGVs) y las armas de energía dirigida (DEWs), cada uno de los cuales plantean retos estratégicos y operativos de gran envergadura. Los HGVs, por ejemplo, fusionan la maniobrabilidad de un misil de crucero con velocidades superiores a las de un misil balístico tradicional, comprimiendo los tiempos de reacción ante ataques desde horas a apenas unos minutos. Su tamaño reducido y trayectoria rasante los hace particularmente difíciles de detectar para los radares terrestres, incluso aquellos integrados con sensores espaciales avanzados (Khan, 2024).

Frente a estas amenazas, los sistemas actuales de alerta temprana y defensa antimisil en capas muestran limitaciones significativas. Tanto los misiles balísticos lanzados desde el

aire, como los vehículos de planeo hipersónico pueden neutralizar, en cuestión de minutos, instalaciones críticas como bases aéreas, centros de mando o pistas estratégicas, erosionando la capacidad operativa de una fuerza antes de que pueda responder. Las Armas de Energía Dirigida, por su parte, ofrecen la posibilidad de atacar con precisión a velocidad lumínica, redefiniendo los principios de letalidad, inmediatez y persistencia en el combate aéreo.

Simultáneamente, la guerra electrónica ha evolucionado radicalmente. Ya no es simplemente un recurso defensivo, sino un componente esencial de la guerra centrada en redes. Su fusión creciente con la guerra cibernética permite alterar la calidad de la información y manipular el entorno electromagnético para degradar el mando y control, las comunicaciones, la vigilancia y la adquisición de objetivos enemigos. Al introducir interferencias en los sistemas de localización, redes de sensores, control de fuego y centros de mando, la guerra electrónica puede obstaculizar o neutralizar por completo la efectividad de los sistemas de armas adversarios (Álvarez, 2025).

En este sentido, la guerra electrónica potencia las estrategias de Anti-Acceso y Negación de Área (A2/AD), dificultando o directamente impidiendo la libertad de acción del oponente en el espacio aéreo. La tendencia hacia sistemas de guerra electrónica más móviles, automatizados y con mayor alcance refuerza su papel protagónico en los conflictos de alta intensidad, donde el control de los flujos de datos e información será tan —o más— determinante que la potencia de fuego convencional (Castellanos, 2022).

Todo esto configura un espectro de amenazas aéreas y misilísticas altamente complejo. Desde misiles tácticos heredados de la Guerra Fría hasta fuegos de precisión de largo alcance, sistemas no tripulados, municiones merodeadoras y defensas aéreas multicapas dotadas de misiles tierra-aire y capacidades de guerra electrónica avanzadas, el campo de batalla moderno es un entorno de letalidad elevada y decisiones aceleradas. No obstante, lo que verdaderamente transforma la guerra no son los sistemas individuales, sino su sincronización e integración: la capacidad de operar simultáneamente con armas de diferentes generaciones, niveles tecnológicos y dominios operativos.

El acceso creciente al espacio y el uso de sensores persistentes reforzarán aún más esta integración, permitiendo fuegos interdominio con alcances extendidos y una precisión inédita. Conforme las cadenas de destrucción integren mayores niveles de automatización, el ritmo operativo aumentará exponencialmente. La inteligencia artificial permitirá a los adversarios procesar y explotar grandes volúmenes de datos de múltiples fuentes en tiempo real, optimizando sus ciclos operativos. Esta capacidad mejorará la protección de fuerzas propias, reducirá los tiempos de respuesta y facilitará decisiones más dinámicas para acortar la cadena de destrucción enemiga y ampliar las ventanas de oportunidad en el campo de batalla.

Hacia una nueva doctrina de superioridad aérea

Ante la proliferación de sensores de alta precisión y sistemas de fuego de largo alcance con velocidades hipersónicas, los enfoques tradicionales sobre la superioridad aérea han dejado de ser suficientes. La superioridad aérea —entendida como “el grado de control del espacio aéreo que impide al adversario interferir eficazmente con medios aéreos o misilísticos en un área de operaciones”— ya no puede asumirse como un estado continuo o garantizado (Rojo, 2025). En cambio, debe concebirse como una serie de ventanas de dominio temporales y localizadas, que requieren ser ganadas y explotadas con agilidad y precisión.

La obtención de la superioridad aérea sigue siendo un factor decisivo para permitir la libertad de maniobra de las fuerzas conjuntas. Ya sea mediante defensa aérea activa para evitar ataques enemigos, o acciones ofensivas para desarticular sus capacidades, el control del espacio aéreo permite ejecutar operaciones terrestres, navales y aéreas con menores riesgos y mayor efectividad. No obstante, los métodos convencionales centrados en “bombas sobre el blanco” o campañas prolongadas de desgaste aéreo se vuelven insostenibles frente a un entorno caracterizado por amenazas persistentes, automatizadas y multidominio.

Nuevas lógicas de acceso y dominio

Frente a un entorno operacional altamente disputado, las fuerzas aéreas deben generar vectores de acceso temporales, que les permitan operar de forma segura y eficaz dentro o cerca de zonas de negación aérea adversarias. Para ello, es fundamental superar la fragmentación de capacidades y avanzar hacia modelos de operaciones multidominio, integrando medios espaciales, cibernéticos y del entorno electromagnético.

Frente a un entorno operacional altamente disputado —caracterizado por la presencia intensiva de sensores, sistemas de armas antiaéreas de largo alcance y capacidades de guerra electrónica por parte de actores adversarios— las fuerzas aéreas enfrentan crecientes restricciones para acceder, maniobrar y operar de forma sostenida dentro de zonas consideradas de negación aérea (Anti-Access/Area Denial, A2/AD). En este contexto, resulta indispensable que las fuerzas aéreas desarrollen vectores de acceso temporales, es decir, ventanas tácticas y estratégicas que habiliten su proyección dentro o en las cercanías de estas zonas hostiles, de forma segura, efectiva y con un grado aceptable de riesgo.

La creación de estos vectores no puede depender únicamente de plataformas tradicionales o de la superioridad tecnológica aislada. Por el contrario, requiere una superación deliberada de la fragmentación de capacidades, es decir, del uso descoordinado de recursos y medios disponibles en dominios distintos. La realidad actual del campo de batalla impone la necesidad de un enfoque operativo multidominio, en el cual las capacidades del espacio (por ejemplo, satélites para inteligencia, vigilancia y comunicaciones), del ciberespacio (para operaciones ofensivas y defensivas que afecten los sistemas enemigos), y del entorno electromagnético (como la guerra electrónica para suprimir o engañar sensores y comunicaciones adversarias) trabajen en conjunto con las plataformas aéreas tripuladas y no tripuladas.

La integración de estos medios heterogéneos no solo permite penetrar zonas A2/AD, sino que también amplía el abanico de opciones tácticas disponibles, permitiendo a los comandantes crear confusión, sobrecargar la toma de decisiones del enemigo, desorganizar sus sistemas defensivos y explotar sus vulnerabilidades. Además, estos vectores de acceso pueden tener una duración limitada, por lo que la agilidad, la sincronización y la capacidad de acción rápida se vuelven fundamentales para aprovecharlos plenamente antes de que el entorno vuelva a volverse hostil o cerrado. Solo mediante la articulación efectiva entre tecnologías, dominios operativos y una doctrina que priorice la adaptabilidad, será posible superar las limitaciones impuestas por los entornos negados y proyectar poder aéreo con eficacia en los conflictos del futuro.

La incorporación de capacidades espaciales —especialmente en detección, rastreo de misiles, comunicaciones y control de fuego— será crucial para anticipar amenazas y coordinar respuestas en tiempo real. Asimismo, el dominio del entorno electromagnético a través de operaciones de guerra electrónica permitirá degradar las capacidades sensoriales y de mando del adversario, facilitando condiciones más favorables para obtener superioridad aérea (Alvarez, 2025).

Comando, control y decisión acelerada

Para capitalizar las oportunidades que ofrecen estas capacidades combinadas, se requiere un Sistema de Comando y Control (C2) ágil, que integre sensores, plataformas y sistemas de armas en una sola arquitectura operacional. Esta arquitectura debe estar apoyada por procesos automatizados y asistidos por inteligencia artificial (IA) que acorten los ciclos de decisión —el clásico ciclo OODA (observar, orientar, decidir y actuar)— por debajo del tiempo de respuesta del adversario (Prats, 2001).

La IA no solo permitirá procesar grandes volúmenes de datos en tiempo real, sino también anticipar patrones de comportamiento enemigo, calcular riesgos de misión y sugerir cursos de acción, liberando al mando humano para tareas estratégicas más complejas. Un ejemplo del rol de la IA en el mando y control multidominio, liderado por la Fuerza Aérea, se encuentra en la figura 2.

Figura 2
Fundamentos de El Mando y Control Conjunto en Todos los Dominios

Fuente 1 (Deptula, 2024) A New Battle Command Architecture for Air Force-Led All Domain Operations

Nuevos Enfoques de Planificación Operacional

A nivel táctico, es imprescindible que las fuerzas aéreas transformen radicalmente su actitud operacional para adaptarse a las nuevas exigencias del entorno bélico contemporáneo. Tradicionalmente, las operaciones aéreas se han estructurado en torno a grandes bases fijas, altamente equipadas y con una logística robusta. Sin embargo, esta configuración ha demostrado ser cada vez más vulnerable ante sistemas de ataque de precisión a larga distancia, como misiles balísticos, de crucero y drones kamikaze, que pueden neutralizar capacidades críticas con poco aviso y gran efectividad.

Frente a esta amenaza creciente, las fuerzas aéreas deben migrar hacia un modelo de operaciones distribuidas, caracterizado por el despliegue ágil y flexible de plataformas tripuladas y no tripuladas desde una red de nodos dispersos, móviles y de bajo perfil. Estos nodos pueden ser pistas improvisadas, carreteras adaptadas, bases avanzadas temporales o incluso plataformas navales o terrestres en movimiento. Lo esencial es que cada uno de ellos funcione como un punto autónomo de generación de misiones, logística básica y capacidad de recuperación, sin depender completamente de la infraestructura centralizada.

Este enfoque distribuido ofrece tres ventajas importantes:

- Mayor supervivencia: al reducir la concentración de activos en puntos predecibles, se complica enormemente la cadena de destrucción del adversario. Dispersar aeronaves, drones, sistemas de soporte y personal entre múltiples ubicaciones, significa que un solo ataque no puede neutralizar una parte significativa del poder aéreo disponible.

- Mayor flexibilidad táctica: operar desde nodos múltiples permite a los comandantes responder rápidamente a cambios en el entorno operacional, reposicionar medios de forma dinámica, explotar ventanas de oportunidad (por ejemplo, brechas en las defensas enemigas), y adaptarse a nuevas

prioridades estratégicas sin necesidad de una reconfiguración logística extensa.

- Presencia persistente en zonas de interés: al tener medios distribuidos y listos para operar desde distintas ubicaciones, se facilita una presencia continua y sostenida en áreas críticas. Esto puede implicar vigilancia ininterrumpida, disuasión activa o capacidad de respuesta inmediata ante eventos en desarrollo, incluso dentro de entornos hostiles o de acceso restringido.

Implementar este modelo requiere más que infraestructura física; exige una doctrina operacional renovada, entrenamiento orientado a la movilidad y la descentralización, y tecnologías que respalden la autonomía operativa, como sistemas de mantenimiento automatizados, comunicaciones satelitales resilientes y logística ligera de reabastecimiento. También implica cambiar la cultura organizacional, de una mentalidad dependiente de bases y cadenas de mando centralizadas a una de misión comando, donde las unidades puedan operar de manera más autónoma dentro de un marco estratégico claro.

Aquí entra en juego la noción de "kill web", una red descentralizada de sensores, nodos de mando y plataformas de ataque que reemplaza al modelo lineal tradicional. En este nuevo esquema, la capacidad de generación de misiones se distribuye, se hace más autónoma, y se adapta rápidamente a los cambios del entorno (Alderman, 2020).

La guerra electrónica y guerra cibernética como núcleo del combate

Un aspecto clave en la evolución del poder aéreo contemporáneo es el rol central y cada vez más protagónico de la guerra electrónica, la cual ha dejado de ser vista como un simple complemento defensivo para consolidarse como un pilar estratégico dentro de la guerra en red. Esta transformación responde a la creciente importancia del dominio electromagnético como un espacio de combate por derecho propio, donde se disputan ventajas críticas de información, control y sincronización operativa.

La guerra electrónica, cuando se integra con la guerra cibernética, permite crear efectos disruptivos de gran alcance sobre las capacidades del adversario. Estas incluyen la distorsión del flujo de información, el bloqueo o interferencia de sensores y radares, la interrupción de enlaces de comunicación y sistemas de mando y control (C2), así como la desorientación de unidades enemigas mediante falsos objetivos o alteraciones de navegación. En paralelo, también contribuye a la protección activa de los propios activos, al interferir con los sistemas de adquisición de blancos y seguimiento de amenazas, y al aumentar la resiliencia frente a ataques electrónicos y cibernéticos externos.

Este entrelazamiento entre guerra electrónica y ciberdefensa crea un espacio estratégico donde la superioridad ya no se basa solo en tener más plataformas o mayor capacidad de fuego, sino en poseer superioridad informacional: la capacidad de ver primero, decidir más rápido y actuar con mayor precisión. En entornos altamente automatizados y multidominio, donde los tiempos de reacción se reducen a segundos y las decisiones críticas dependen de sensores y algoritmos, controlar el espectro electromagnético equivale a controlar el ritmo del combate. Las fuerzas aéreas que logren reinventarse en esta dirección serán las que conserven su relevancia estratégica en el escenario de conflictos del siglo XXI (Bolaños Ramírez, 2022).

Dominando el entorno electromagnético del conflicto

Durante décadas, los fuegos de largo alcance han constituido la principal herramienta para degradar las defensas aéreas del enemigo. Mediante ataques precisos contra radares, baterías de misiles tierra-aire, nodos de comando y control (C2) y sistemas de guerra electrónica, se ha buscado erosionar la capacidad del adversario para sostener operaciones aéreas y proteger su espacio aéreo. Sin embargo, esta lógica centrada en la superioridad cinética está siendo desafiada por un entorno operativo en el que la maniobra profunda se vuelve cada vez más difícil y costosa. En los escenarios futuros, marcados por zonas altamente disputadas y por amenazas persistentes, las misiones ofensivas requerirán una nueva arquitectura táctica. Las fuerzas aéreas deberán moverse y maniobrar con rapidez, explotando momentos y posiciones de ventaja táctica para ejecutar sus misiones sin exponerse a la detección y al fuego letal del enemigo.

Una arquitectura completa de guerra electrónica

En este nuevo paradigma, la guerra electrónica ya no puede concebirse como un complemento pasivo o una herramienta de protección limitada. Debe asumirse como un

medio activo de maniobra electromagnética, capaz de modelar el entorno operativo, degradar la conciencia situacional del adversario y ampliar las posibilidades tácticas de las fuerzas amigas.

Las capacidades de interferencia electrónica a distancia (stand-off jamming) y en el interior de zonas enemigas (stand-in jamming) se volverán fundamentales. Su valor no solo radica en proteger plataformas propias, sino en garantizar la supervivencia de activos que operan cerca de las amenazas, al permitir la supresión puntual de defensas enemigas y la generación de nuevos vectores de acceso para otras aeronaves o sistemas de armas (Annulli, 2021).

La guerra electrónica moderna exige una arquitectura integral y distribuida que abarque todas sus dimensiones:

- Apoyo a la guerra electrónica (ES): incluye la recolección de inteligencia electrónica (ELINT), esencial para mapear y entender el comportamiento de los sistemas enemigos, sus frecuencias, patrones y niveles de emisión. Esta información es crítica para diseñar misiones exitosas.

- Contramedidas electrónicas (ECM): técnicas activas de perturbación que alteran o anulan el funcionamiento de sensores, radares o sistemas de guía del adversario.

- Ataque electrónico (EA): acciones ofensivas diseñadas para inutilizar, engañar o destruir directamente sistemas electromagnéticos del enemigo.

- Protección electrónica (EP): incorpora capacidades de contra-contramedidas electrónicas (ECCM), que aseguran que los propios sistemas funcionen de manera fiable incluso en entornos electromagnéticos contaminados.

En los conflictos de alta intensidad, dominar el espectro electromagnético se convertirá en un factor de éxito igual o incluso superior al control físico del espacio aéreo. Quien controle el flujo de información, degrade las comunicaciones del enemigo y preserve las propias, poseerá una ventaja estratégica y táctica decisiva.

Redefiniendo la estrategia de ataque en profundidad

La creciente integración de sensores persistentes con sistemas de ataque de largo alcance y alta precisión, está transformando radicalmente el entorno operativo. Los adversarios cuentan ahora con la capacidad de identificar y atacar objetivos estratégicos con escaso o nulo preaviso, incluyendo bases aéreas, pistas de aterrizaje, aviones en tierra y centros logísticos. En este contexto, mantener una postura de ataque a distancia ya no es solo una ventaja táctica, sino una necesidad estratégica para asegurar la continuidad operativa y la supervivencia de las fuerzas aéreas.

Para enfrentar esta amenaza, la protección contra la detección y la selección de blancos por parte del adversario debe evolucionar más allá de la protección electrónica (EP). Es imprescindible adoptar una doctrina más amplia de camuflaje, ocultamiento y engaño, capaz de alargar las cadenas de destrucción del enemigo, reducir su precisión y ganar tiempo crítico para maniobrar.

El camuflaje moderno ya no es un simple complemento visual, es una herramienta operativa clave. Pinturas adaptativas, insignias de baja visibilidad, uso dinámico de hangares y estacionamiento aleatorio son elementos que dificultan la identificación satelital y el análisis automatizado de inteligencia. Del mismo modo, el despliegue de señuelos térmicos y electromagnéticos puede saturar o confundir los sensores enemigos, desviando fuego de los activos reales y reduciendo la efectividad de los ataques (Pikner, 2021).

Esta nueva realidad operativa obliga a repensar por completo el diseño y uso de las bases aéreas. Las grandes instalaciones fijas, altamente visibles y con infraestructura pesada, se han convertido en blancos obvios y vulnerables. Frente a esto, las fuerzas aéreas deben migrar hacia un modelo distribuido, austero y ágil.

Este modelo implica la dispersión geográfica de la generación de misiones en una red de nodos pequeños y versátiles — bases que puedan operar con distintos tipos de plataformas y realizar ciclos completos de misión, no solo despegar o aterrizar aeronaves específicas. Esta red distribuida, o “kill web”, no solo complica la planificación enemiga, sino que también permite movilidad constante, con activos rotando entre ubicaciones varias veces por semana, dificultando la determinación de objetivos y forzando al adversario a reaccionar ante una huella operacional menos predecible.

Además, la postura de ataque a distancia no implica únicamente alejarse del frente, sino operar desde posiciones de ventaja, utilizando

velocidad, sorpresa y maniobra inteligente para explotar ventanas de acceso temporales dentro de las zonas de empleo de armas enemigas. Esta flexibilidad estructural será clave para asegurar la superioridad aérea en un entorno donde la inmovilidad equivale a vulnerabilidad.

El necesario empleo del poder aéreo frente a las amenazas del crimen organizado

Varios países atraviesan una crisis sin precedentes en materia de seguridad. La presencia creciente de grupos criminales y organizaciones narcotraficantes ha desafiado la capacidad de los Estados para garantizar el orden interno. Sin embargo, el uso tradicional de las fuerzas militares ha demostrado limitaciones frente a enemigos que actúan de forma descentralizada, violenta y con alto grado de movilidad. En este contexto, se vuelve urgente repensar el uso del poder aéreo como una herramienta clave para fortalecer las capacidades estatales de inteligencia, detección, seguimiento y ataque contra el crimen organizado.

Los grupos delictivos están lejos de ser estructuras improvisadas. Se trata de redes criminales transnacionales que combinan el narcotráfico con actividades como el contrabando de armas, la extorsión, el secuestro y el lavado de activos. Utilizan tecnologías avanzadas, rutas complejas y estrategias asimétricas para evadir la acción estatal. Muchos cuentan incluso con armamento de uso militar y acceso a plataformas de comunicación cifrada.

En este escenario, las Fuerzas Armadas y la Policía enfrentan no solo una amenaza delictiva, sino una amenaza de carácter estratégico que compromete la estabilidad interna y el control soberano del territorio. Esta situación exige un enfoque interagencial y multidominio donde el componente aéreo se convierta en pilar fundamental para restaurar la superioridad del Estado.

Repensar el uso del poder aéreo en seguridad interna

Históricamente, el poder aéreo ha sido concebido para escenarios de defensa externa. Sin embargo, su versatilidad permite adaptarlo a operaciones de seguridad interna, especialmente frente a amenazas difusas como el crimen organizado. El poder aéreo no se limita a la capacidad de ataque: abarca también inteligencia, vigilancia, detección temprana, disuasión y apoyo logístico.

Los siguientes factores deben ser considerados al momento de integrar el poder aéreo de forma eficiente en la lucha contra el crimen organizado:

- **Dominio de la información**. La inteligencia aérea permite detectar patrones de movilidad, identificar rutas de tráfico, ubicar campamentos o centros logísticos del narcotráfico y obtener evidencia para investigaciones judiciales. El uso sistemático de plataformas ISR (Inteligencia, Vigilancia y Reconocimiento), como drones de mediana y larga autonomía, es esencial.

- **Capacidad de seguimiento y monitoreo continuo**. El uso de drones permite realizar operaciones de observación 24/7 en zonas sensibles. Además, su carácter no tripulado reduce los riesgos para el personal y su discreción es clave para evitar alertar a los grupos criminales.

- **Ataques quirúrgicos**. La posibilidad de equipar drones con cargas letales permite realizar operaciones de neutralización selectiva, minimizando daños colaterales y respondiendo de forma rápida a amenazas inmediatas. Para ello, se requiere una cadena de mando eficiente, protocolos de uso de la fuerza claros y un marco legal que respalde estas acciones.

- **Soporte a operaciones terrestres**. La vigilancia aérea puede coordinarse con operativos de interdicción en tierra, anticipando emboscadas, monitoreando avances y facilitando extracciones rápidas en zonas hostiles.

- **Apropiación tecnológica nacional**. Es crucial desarrollar capacidades propias de diseño, mantenimiento y operación de sistemas no tripulados. Esto reduce la dependencia externa, fortalece la industria nacional y permite adaptar la tecnología a las realidades del entorno ecuatoriano.

Hacia una nueva doctrina de empleo del poder aéreo en seguridad interna

El nuevo escenario de seguridad demanda una doctrina operacional específica que oriente el empleo del poder aéreo contra amenazas criminales. Esta doctrina debe considerar:

- Un enfoque inter-agencial, donde la Fuerza Aérea trabaje en coordinación con Policía, Fiscalía y otras instituciones. Esto requiere sistemas de interoperabilidad, protocolos de comunicación segura y mandos conjuntos.

- Segmentación del espacio aéreo para identificar zonas de interés prioritario (zonas fronterizas, centros logísticos del narcotráfico, rutas de tráfico) que permita un patrullaje aéreo intensivo y coordinado.

- Desarrollo de doctrina en entorno urbano y rural, el crimen organizado actúa tanto en grandes ciudades como en zonas rurales remotas. La doctrina debe contemplar operaciones adaptadas a cada escenario, considerando el uso de micro drones, sensores, herramientas de reconocimiento facial, detección térmica, etc.

- Doctrina de empleo de fuego letal desde el aire, esto incluye definir protocolos de empleo de drones armados, uso proporcional de la fuerza, reglas de enfrentamiento y autorización legal. El componente aéreo no debe sustituir la investigación ni la judicialización, pero puede ser clave en neutralizaciones urgentes.

- Uso de la información como poder, el dominio informativo es clave. Las imágenes y datos recopilados desde el aire deben ser integrados a bases de datos, sistemas de análisis y plataformas compartidas para alimentar el ciclo de inteligencia estratégica.

Implicaciones para la planificación de la fuerza del futuro

El escenario operativo del siglo XXI está marcado por una complejidad sin precedentes: amenazas densas, tecnologías disruptivas, dominios entrelazados y tiempos de decisión comprimidos. En este contexto, la capacidad de las fuerzas aéreas para adaptarse determinará su relevancia futura. La reconfiguración del poder de combate aéreo —basada en el uso estratégico de sistemas no tripulados, la integración efectiva de capacidades no cinéticas, y la inteligencia artificial como motor operativo— representa no solo una evolución tecnológica, sino una transformación doctrinal profunda.

Planificar la fuerza del futuro no es una tarea técnica: es un imperativo estratégico. Implica romper con inercias organizacionales, repensar el valor de cada plataforma y cada persona en el ecosistema de combate, y tener el coraje institucional de anticiparse a una guerra que aún no ha empezado. Transformar el poder aéreo para que sea más ágil, descentralizado y asistido por inteligencia artificial no solo mejora la capacidad de respuesta: redefine qué significa tener superioridad en un mundo donde los dominios ya no están separados.

Reestructuración de la fuerza y desarrollo de multiplicidad de habilidades

La automatización creciente y el auge de sistemas autónomos hacen ineludible una redistribución funcional. Las misiones más riesgosas o repetitivas deben migrar hacia plataformas no tripuladas, permitiendo que los activos tripulados se reserven para decisiones críticas o entornos impredecibles. Esta transición también requiere una fuerza laboral con múltiples habilidades, capaz de operar, mantener y redirigir operaciones desde variadas ubicaciones.

- Integrar sistemas no tripulados resistentes a entornos electromagnéticos hostiles, complementados por equipos humano-máquina en esquemas colaborativos de combate.

- Entrenar al personal para cumplir múltiples funciones operativas, especialmente en contextos dispersos o de despliegue ágil.

- Fortalecer alianzas internacionales para desarrollar redes multinacionales de generación de misiones, ampliando el teatro de operaciones más allá de las fronteras nacionales.

Expansión de capacidades espaciales y cibernéticas

La superioridad aérea no se gana solo en el cielo, hoy se decide en órbitas, cables de datos y entornos digitales invisibles. Las capacidades espaciales y cibernéticas son pilares indispensables para anticipar amenazas, coordinar respuestas y desorganizar al adversario desde antes del primer disparo. Para lograr este objetivo se debe:

- Desarrollar sensores espaciales avanzados y capacidades de guerra electrónica orbital que amplíen la cadena de alerta y respuesta.

- Invertir en redes de comunicación seguras, descentralizadas y resistentes a interferencias, fundamentales para operaciones distribuidas.

- Combinar ciber y guerra electrónica para generar efectos convergentes que desactiven las capacidades enemigas y generen ventaja informacional.

Explotación del Big Data y la Inteligencia Artificial

La velocidad y precisión en la toma de decisiones serán el factor más determinante del éxito operacional. La integración de inteligencia artificial y aprendizaje automático no sustituirá el juicio humano, pero sí lo potenciará al acelerar el ciclo de toma de decisiones y permitir respuestas calibradas en tiempo real. Algunas de las acciones a tomarse en cuenta son:

- Construir una infraestructura de datos segura, confiable y compartida, que permita alimentar algoritmos en tiempo real con insumos operativos.

- Promover la innovación mediante entornos simulados, ejercicios tipo "juegos de guerra" y asociaciones activas con centros académicos y tecnológicos.

- Aplicar sistemas de soporte a decisiones con IA que ayuden a identificar amenazas emergentes, calcular riesgos operativos y sugerir cursos de acción antes de que el adversario actúe.

Optimización de las capacidades del poder aéreo en la seguridad interna del Estado

La crisis de seguridad que viven varios países exige respuestas audaces, creativas y sostenidas. El poder aéreo, adecuadamente re conceptualizado, puede jugar un rol central en la restauración de la seguridad interna. No se trata de militarizar la respuesta, sino de dotar al Estado de herramientas inteligentes, eficaces y precisas para enfrentar una amenaza que ha evolucionado en escala, letalidad y sofisticación. La adopción de una nueva doctrina de empleo del poder aéreo, basada en inteligencia, tecnología y coordinación interinstitucional, les permitirá recuperar el control del territorio y restablecer el imperio de la ley.

Una inversión sostenida en tecnología aérea no tripulada es prioritaria para dotar a la Fuerza Aérea de una flota diversificada de drones (corto, mediano y largo alcance) para vigilancia, seguimiento y ataque selectivo. Del mismo modo, se deben establecer laboratorios de innovación y centros de formación especializada en sistemas de Inteligencia, Vigilancia y Reconocimiento (ISR).

Es mandatorio actualizar la legislación nacional para realizar una reforma legal y normativa que regule el empleo del poder aéreo en funciones de seguridad interna, incluyendo el uso de drones armados, protección de datos, privacidad, cadena de custodia de evidencia y control judicial.

Se debe fortalecer al capital humano, capacitando a pilotos, técnicos, analistas e inteligencia en el uso de herramientas modernas de vigilancia aérea, guerra no convencional, vigilancia remota e inteligencia artificial aplicada a seguridad. Del mismo modo la Fuerza Aérea debe participar en la elaboración de una doctrina conjunta con la Policía, para definir límites, responsabilidades, interoperabilidad y coordinación de misiones.

Conclusiones

El entorno operativo del futuro no premiará únicamente la potencia de fuego, sino la capacidad para controlar el espectro electromagnético, distorsionar la percepción del adversario y proteger la toma de decisiones propias. En este contexto, la guerra electrónica y otras capacidades no cinéticas ya no son complementos: son pilares estratégicos de la nueva arquitectura del poder aéreo.

Al combinar la guerra electrónica con inteligencia artificial, ciber-operaciones y capacidades espaciales, las fuerzas aéreas podrán multiplicar su agilidad estratégica y reducir su vulnerabilidad ante amenazas dinámicas, saturadas y automatizadas. Esta fusión permitirá pasar de la simple reacción al control activo del campo de batalla electromagnético, otorgando ventaja no por la fuerza bruta, sino por la capacidad de desorganizar, confundir y desactivar al enemigo.

Las fuerzas que inviertan hoy en una red resiliente, inteligente y flexible de capacidades no cinéticas, estarán mejor posicionadas no solo para proteger sus activos más valiosos, sino para liderar la evolución doctrinaria del poder aéreo en los próximos conflictos. La superioridad aérea del mañana no será el resultado exclusivo del dominio del cielo, sino del dominio invisible, silencioso y decisivo del espectro.

Las crisis de seguridad que viven varios países exigen respuestas audaces, creativas y sostenidas. Un poder aéreo, adecuadamente re conceptualizado, puede jugar un rol central en la restauración de la seguridad interna. No se trata de militarizar la respuesta, sino de dotar a los Estados de herramientas inteligentes, eficaces y precisas para enfrentar una amenaza que ha evolucionado en escala, letalidad y sofisticación.

El replanteamiento operativo exige no solo cambios tecnológicos, sino también un cambio cultural dentro de las fuerzas aéreas. Requiere abandonar la dependencia de modelos logísticos centralizados, apostar por una mentalidad de adaptabilidad constante y formar una nueva generación de líderes y operadores entrenados para actuar en escenarios dispersos, impredecibles y altamente digitalizados. Apostar por la movilidad, el engaño y la modularidad no es una concesión frente a amenazas emergentes: es una evolución estratégica necesaria para preservar la relevancia y eficacia del poder aéreo en las próximas décadas.

Referencias Bibliográficas

Altschul, C. (2016). Gestionar cambios complejos: Cuentas y cuentos del liderazgo transformacional. EDICON. Alderman, R. (2020). Orígenes de la Kill Web. Military Embedded Systems.

Alvarez, S. (2025). Guerra Electrónica: El Campo de Batalla Silencioso del Futuro. OESIA. Obtenido de Guerra electrónica: el campo de batalla silencioso del futuro: https://grupooesia.com/insight/guerra-electronica-el-campo-de-batalla-silencioso-del-futuro/

Álvarez, S. (2025). Nube de combate o nube táctica, el futuro de la defensa ya está aquí. OESIA Grupo.

Annulli, M. (2021). Tarea de Interferencia de Separación. Emsopedia.

Bolaños Ramírez, I. ,. (2022). Fuerza Aérea Ecuatoriana: En camino al multidominio. Un análisis transdiciplinario. Ciencia y Poder Aéreo, 52-64.

Castellanos, J. J. (2022). Global Strategy. Obtenido de https://global-strategy.org/un-sistema-antiacceso-denegacion-de-area-a2-ad-espanol-en-el-siglo-xvi/

Chamola, V. (2021). A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques. ELSEVIER.

Day, R. A. (2005). Cómo escribir y publicar trabajos científicos (Vol. Publicación Científica y Técnica No. 598). Washington DC, USA: Panamerican Health Organization.

Defensa, M. d. (2019). Plan Nacional de Seguridad Integral 2019-2030. Quito: Instituto Geográfico Militar (IGM). Recuperado el 13 de Abril de 2021, de https://www.defensa.gob.ec/wp-content/uploads/downloads/2019/07/plan-matriz-web.pdf

Deptula, D. A. (2024). A New Battle Command Architecture for Air Force-Led All Domain Operations. Obtenido de The Air Power Journal: https://theairpowerjournal.com/battle-command-architecture-all-domain-operations/

Gómez, M. (2006). Introducción a la metodología de la investigación científica. (U. N. Plata, Ed.) La Plata, Argentina: Editorial Brujas.

Gordon, C. (4 de April de 2025). Allvin Makes the Case for More Airpower. Obtenido de Air & Space Forces Magazine: https://www.airandspaceforces.com/article/world-airpower-2/

Khan, S. (2024). Rethinking Combat Power: Air Superiority in the Age of Pervasive Threats. Air Power Journal.

Kreuter, J. (2021). The Tools for Empirical Analysis—The Method of Qualitative Content Analysis. (C. E. Politicization, Ed.) Switzerland: Springer, Cham, .

Manterola Carlos, P. V. (febrero de 2007). ¿Cómo presentar los resultados de una investigación científica? II. El manuscrito y el proceso de publicación. Revista de Cirujía Española, 81 N°2, 70-77. doi:DOI: 10.1016/S0009-739X(07)71266-6

Pikner, T. c. (2021). El engaño militar multidominio para exponer al enemigo en 2035. Military Review.

Prats, J. M. (2001). La Guerra de Mando Y Control y la Teoría del OODA Loop. CESEDEN, 31-40.

Rojo, A. (2025). La superioridad aérea en la era de los drones y misiles: ¿una idea obsoleta? Zona Militar.

Sampieri, R. H. (2014). Metodología de la Investigación (ISBN: 978-1-4562-2396-0 ed., Vol. 6ta. Edición). México: McGraw-Hill Education,.

Suárez-Montes, N. D.-G.-V. (12 de 2016). Elementos esenciales del diseño de la investigación. Sus características. Dominio de las Ciencias, 2, 72-85. Obtenido de https://www.dominiodelasciencias.com/ojs/index.php/es/article/viewFile/294/349