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

Tecnologías Disruptivas y guerra especial

Mayor (EJC) Jairo Alejandro Higuita González

Capítulo de libro para optar al título profesional:

Magister en Seguridad y Defensa Nacionales

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

DATOS GENERALES		
Nombre del estudiante	**:**	Mayor (EJC) Jairo Alejandro Higuita Gonzalez
Identificación	**:**	9862810
Programa académico	**:**	Maestría en Seguridad y Defensa Nacionales
Tutor metodológico	**:**	SLP Omar Ferney Vanegas Rincón
Tutor temático	**:**	Dh Montero Alexander Luis
Fecha de entrega	**:**	
Extensión	**:**	

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

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

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

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

AUTORIZACIÓN DE PUBLICACIÓN

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

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

Tecnologías Disruptivas y guerra especial

Disruptive technologies and special warfare

Jairo Alejandro Higuita González [*]

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El objetivo de este capítulo es analizar el impacto de las tecnologías disruptivas en las Fuerzas Especiales (FF.EE.), examinando cómo estas innovaciones están transformando la guerra moderna y la operatividad militar, con especial atención al contexto colombiano. La metodología empleada es cualitativa, de tipo descriptivo-analítico, basada en revisión documental y análisis comparativo de doctrinas y experiencias operativas de la OTAN, Estados Unidos y Colombia. Se priorizaron fuentes publicadas entre 2010 y 2024, incluyendo estudios de caso como los conflictos en Nagorno-Karabaj y Ucrania, así como casos recientes en América Latina. Los resultados evidencian que tecnologías como la inteligencia artificial (IA), los vehículos aéreos no tripulados (UAV), la guerra cibernética y los sistemas autónomos potencian la flexibilidad, adaptabilidad y precisión de las FF.EE., pero también incrementan las capacidades de adversarios no estatales. En Colombia, aunque se han dado avances como la creación del Batallón de Aeronaves No Tripuladas (BANOT) y el fortalecimiento del Comando Conjunto de Ciberdefensa persisten brechas en infraestructura, capacitación y actualización doctrinal para la guerra multidominio. Se concluye que el futuro de las operaciones especiales dependerá de una integración efectiva y ética de estas tecnologías, asegurando control humano significativo y desarrollando capacidades propias. Esta adaptación permitirá mantener la ventaja estratégica en un entorno bélico cada vez más tecnológico, complejo y caracterizado por amenazas híbridas.

Palabras clave: Centro de gravedad, ejército, guerra, metodología, toma de decisiones.

Abstract: The objective of this chapter is to analyze the impact of disruptive technologies on Special Forces (FF.EE.), examining how these innovations are transforming modern warfare and military operations, with special attention to the Colombian context. The methodology used is qualitative, descriptive-analytical, based on documentary review and comparative analysis of doctrines and operational experiences of NATO, the United States, and Colombia. Sources published between 2010 and 2024 were prioritized, including case studies such as the conflicts in Nagorno-Karabakh and

[*] Mayor del Ejército Nacional de Colombia. Candidato a magíster en estrategia y geopolítica, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. https://orcid.org/0000-0003-2004-7466 - Contacto: landinezj@esdeg.edu.co.

Ukraine, as well as recent cases in Latin America. The results show that technologies such as artificial intelligence (AI), unmanned aerial vehicles (UAVs), cyber warfare, and autonomous systems enhance the flexibility, adaptability, and precision of the armed forces, but also increase the capabilities of non-state adversaries. In Colombia, although there have been advances such as the creation of the Unmanned Aircraft Battalion (BANOT) and the strengthening of the Joint Cyber Defense Command, gaps remain in infrastructure, training, and doctrinal updating for multidomain warfare. It is concluded that the future of special operations will depend on the effective and ethical integration of these technologies, ensuring meaningful human control and developing capabilities of their own. This adaptation will allow for maintaining strategic advantage in an increasingly technological and complex war environment characterized by hybrid threats.

Keywords: borders; geopolitics; Latin America; sociopolitical dynamics; State.

T1] Introducción

El impacto de las tecnologías disruptivas en la guerra especial ha sido evidente en los últimos años con la creciente implementación de UAV (Vehículo Aéreo No Tripulado) es, inteligencia artificial y ciberseguridad en operaciones militares de precisión. Un claro ejemplo de ello es el uso de UAV es en la eliminación de objetivos de alto valor por parte de Estados Unidos. En 2020, el ataque con UAV es MQ-9 Reaper que resultó en la muerte del general iraní Qasem Soleimani en Bagdad demostró la capacidad de estos sistemas para llevar a cabo operaciones quirúrgicas con mínima exposición de las tropas en el terreno. Esta tecnología, utilizada en conflictos como Afganistán, Siria y Yemen, ha redefinido la manera en que las Fuerzas Especiales pueden operar a distancia, minimizando riesgos y maximizando la efectividad táctica.

Igualmente, la inteligencia artificial de ahora en adelante (IA) ha tomado un papel significativo en la planificación y ejecución de operaciones especiales. En 2021, el Departamento de Defensa de Estados Unidos implementó el programa *Project Maven*, una iniciativa basada en IA que permite el análisis automatizado de imágenes captadas por UAV es para identificar amenazas en tiempo real. Igualmente, esta herramienta ha mejorado

significativamente la capacidad de las Fuerzas Especiales para procesar grandes volúmenes de información y reaccionar de manera inmediata ante posibles ataques. En el Reino Unido, el ejército ha desarrollado el sistema SAPIENT, que utiliza inteligencia artificial para gestionar la detección de amenazas en entornos urbanos complejos, facilitando la toma de decisiones en combate. Para ello, se planteó la siguiente pregunta de investigación: ¿**Cómo están transformando las tecnologías disruptivas los fundamentos estratégicos y doctrinales de la guerra especial en el siglo XXI, y qué desafíos plantea su integración en las Fuerzas Especiales colombianas?**

Al mismo tiempo, desde el campo de la ciberseguridad, las Fuerzas Especiales han enfrentado crecientes desafíos ante la sofisticación de los ciberataques. En 2022, el Comando Cibernético de Estados Unidos (*USCYBERCOM*) reveló que había llevado a cabo operaciones ofensivas para contrarrestar ataques cibernéticos rusos dirigidos a infraestructuras críticas en Ucrania(Warner, 2022). Este tipo de operaciones han resaltado la necesidad de integrar capacidades de ciberdefensa dentro de las estrategias militares tradicionales. En Colombia, la creciente amenaza de grupos criminales y cárteles ha llevado a la implementación de nuevas estrategias de ciberseguridad en las Fuerzas Militares, especialmente en la lucha contra la propaganda digital y el financiamiento ilícito de organizaciones terroristas mediante criptomonedas.

Por consiguiente, la Revolución en los Asuntos Militares (RMA) ha sido clave en la transformación de las doctrinas militares en torno a estas innovaciones tecnológicas. Durante la guerra en Nagorno-Karabaj en 2020, Azerbaiyán utilizó UAV es kamikaze *Bayraktar TB2* y *Harop* para neutralizar las defensas antiaéreas de Armenia, lo que marcó un punto de inflexión en la guerra moderna(Jordán, 2021). Este conflicto evidenció que las Fuerzas

Especiales y unidades convencionales deben integrar tecnología avanzada para mantener la superioridad operativa. En respuesta, países como Estados Unidos, China y Rusia han intensificado sus programas de desarrollo de armas autónomas y guerra electrónica.

En América Latina, el uso de UAV es por parte de organizaciones criminales ha representado un desafío creciente para las Fuerzas Especiales. En México, el Cartel Jalisco Nueva Generación (CJNG) ha empleado UAV es armados con explosivos improvisados para atacar fuerzas de seguridad desde 2021. En Colombia, el ELN y disidencias de las FARC han comenzado a utilizar UAV comerciales modificados para labores de vigilancia y ataques en zonas de conflicto. Estos acontecimientos han llevado al Ministerio de Defensa colombiano a fortalecer sus programas de vigilancia aérea y control del espacio electromagnético, adoptando estrategias similares a las utilizadas en conflictos de mayor escala.

Al tenor de lo anterior, las proyecciones futuras en torno a la guerra especial y las tecnologías disruptivas sugieren que el desarrollo de sistemas autónomos de combate, la computación cuántica y la integración de la inteligencia artificial en la toma de decisiones estratégicas seguirán marcando la evolución del campo de batalla. En 2023, el Pentágono anunció el desarrollo del *Replicator Initiative*, un programa destinado a la producción masiva de UAV autónomos capaces de operar en enjambres para enfrentar amenazas en conflictos asimétricos. Esta tecnología plantea interrogantes sobre el equilibrio entre el control humano y la autonomía de las máquinas en situaciones de combate.

En el caso de Colombia, la implementación de tecnologías disruptivas en las Fuerzas Especiales es un desafío clave para fortalecer la seguridad nacional. En 2024, el gobierno anunció un plan de modernización de las Fuerzas Armadas que incluye la adquisición de sistemas avanzados de vigilancia y reconocimiento ISR, así como el fortalecimiento del

Comando Conjunto de Ciberdefensa. La integración de inteligencia artificial en las operaciones de seguridad fronteriza también ha sido priorizada, con el objetivo de mejorar la detección y neutralización de amenazas transnacionales.

Finalmente, este capítulo se estructura en tres secciones principales. En primer lugar, se describen las capacidades y limitaciones operativas de las tecnologías disruptivas en el ámbito de las operaciones especiales, con especial énfasis en UAV -IA y ciberseguridad. En la segunda parte, se analiza el estado actual de estas tecnologías en el marco de la RMA y su impacto en las estrategias y tácticas de las Fuerzas Especiales a nivel global. Finalmente, en la tercera sección, se explora la proyección futura de las tecnologías disruptivas en la guerra especial, considerando su evolución tecnológica y el impacto que podrían tener en las operaciones de las Fuerzas Especiales colombianas.

Metodología

La presente investigación adopta un enfoque cualitativo, de tipo descriptivo-analítico, cuyo propósito es comprender la evolución de la guerra especial y el impacto de las tecnologías disruptivas en la seguridad y defensa nacional. Se emplea el análisis de contenido como técnica principal, complementado con un enfoque comparativo para identificar convergencias y divergencias entre doctrinas, casos y experiencias operativas relevantes.

El procedimiento metodológico se desarrollará en tres etapas. Primero, se realizará la recolección documental a partir de fuentes académicas, informes de organismos internacionales, literatura especializada en conflictos armados, ciberseguridad y doctrina militar. Se estima el análisis de entre 35 y 50 documentos, priorizando aquellos publicados

entre 2015 y 2024. Se aplicarán criterios de exclusión basados en la obsolescencia del contenido, ausencia de revisión por pares o falta de pertinencia temática.

Segundo, se aplicará una codificación temática, inicialmente con categorías emergentes, para luego construir ejes de análisis más robustos que permitan identificar patrones comunes sobre el uso de tecnologías disruptivas en Fuerzas Especiales. Estas categorías incluirán: impacto operativo, riesgos tecnológicos, nivel de adopción doctrinal, y desafíos éticos. La sistematización de la información se llevará a cabo mediante matrices de análisis cruzado entre casos internacionales y el contexto colombiano.

Tercero, se utilizará un enfoque comparativo para examinar la evolución de tácticas híbridas y el grado de integración tecnológica en contextos como EE. UU., OTAN, y Colombia, lo que permitirá establecer recomendaciones aplicables a la doctrina nacional.

Desde el punto de vista ético, aunque se trata de una investigación documental, se garantiza la debida citación de todas las fuentes utilizadas, respetando los derechos de autor y evitando cualquier uso indebido de información confidencial o sensible. Se sigue lo planteado por Monje (2011), quien resalta que en investigaciones cualitativas la transparencia metodológica y el rigor en el tratamiento de fuentes es esencial para la validez del análisis. También se integrarán otros referentes metodológicos para respaldar la consistencia del diseño investigativo.

Prisma Metodología

Para la elaboración del presente capítulo se desarrolló un riguroso proceso de revisión documental, fundamentado en una adaptación cualitativa del enfoque PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses). El objetivo fue identificar, seleccionar y analizar literatura académica y técnica relevante sobre tecnologías disruptivas

aplicadas a la guerra especial, con énfasis en casos internacionales y en el contexto de las Fuerzas Especiales colombianas.

En total, se ubicaron 28 referencias especializadas que abarcan un amplio espectro temático, desde doctrinas militares, inteligencia artificial y sistemas no tripulados, hasta ciberseguridad, interoperabilidad y operaciones multidominio. Estas fuentes se localizaron mediante búsquedas dirigidas en bases de datos como Google Scholar, Scopus, IEEE Xplore, Springer, Revue Défense Nationale, AI and Society, así como en repositorios institucionales de organismos como el Centro de Análisis de Políticas Europeas (CEPA), el Ministerio de Defensa de España, la Escuela Superior de Guerra de Colombia, y diversas universidades, incluyendo Los Andes y San Pablo-CEU.

El proceso de selección se basó en criterios de inclusión claramente definidos: (i) pertinencia temática con el objeto de estudio (guerra especial y tecnologías emergentes), (ii) actualidad del contenido (se priorizaron textos entre 2010 y 2024), (iii) calidad académica o técnica (publicaciones revisadas por pares, documentos oficiales o estudios institucionales), y (iv) aplicabilidad al contexto operativo colombiano o comparado. Se excluyeron registros duplicados, documentos obsoletos o aquellos centrados exclusivamente en aplicaciones civiles sin correlato militar.

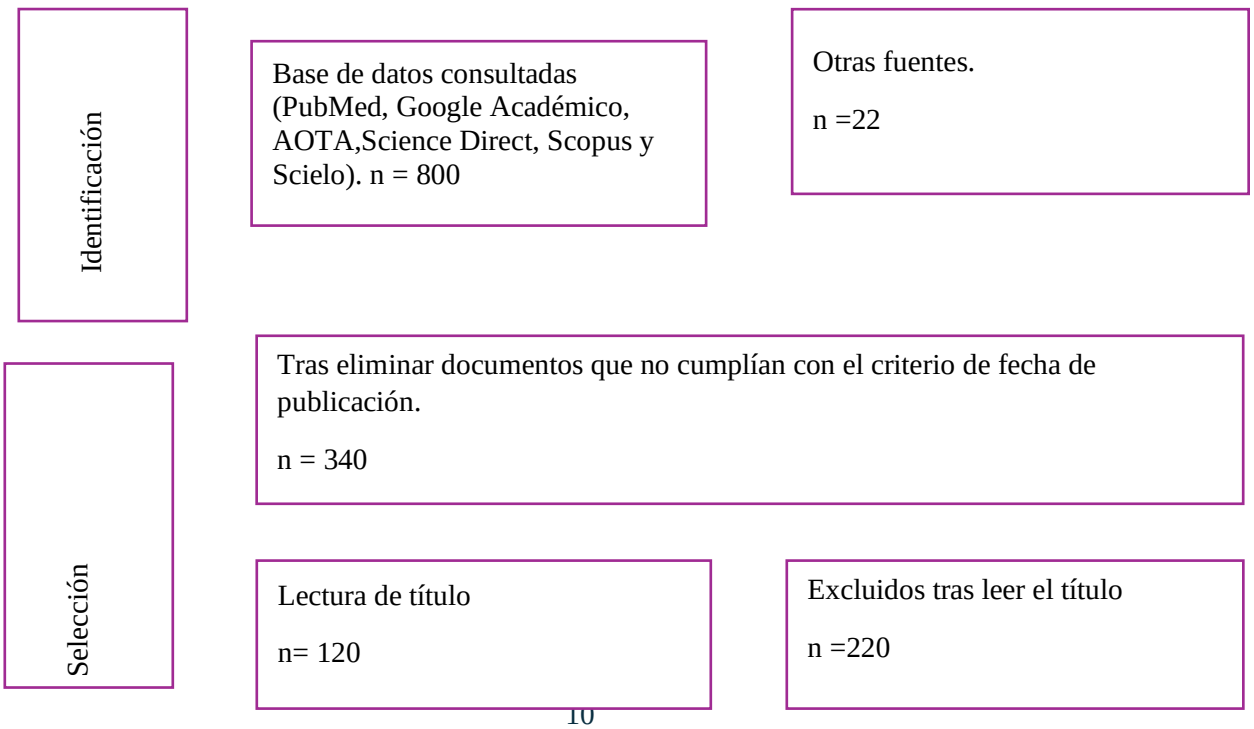
La revisión final incluyó fuentes de diversas naturalezas: artículos científicos como los de Adamski (2020), Panigrahi & Tripathy (2021), y Ghioni et al. (2024); informes institucionales como los del Centro Conjunto de Desarrollo de Conceptos (2020) y CEPA (2022); textos doctrinales como el manual del Ejército Nacional de Colombia (2007); estudios de caso como los de Jordán (2021) y Palacios (2024); y literatura académica aplicada como la de Serna, Montero y González (2024). Se dio especial atención a los documentos

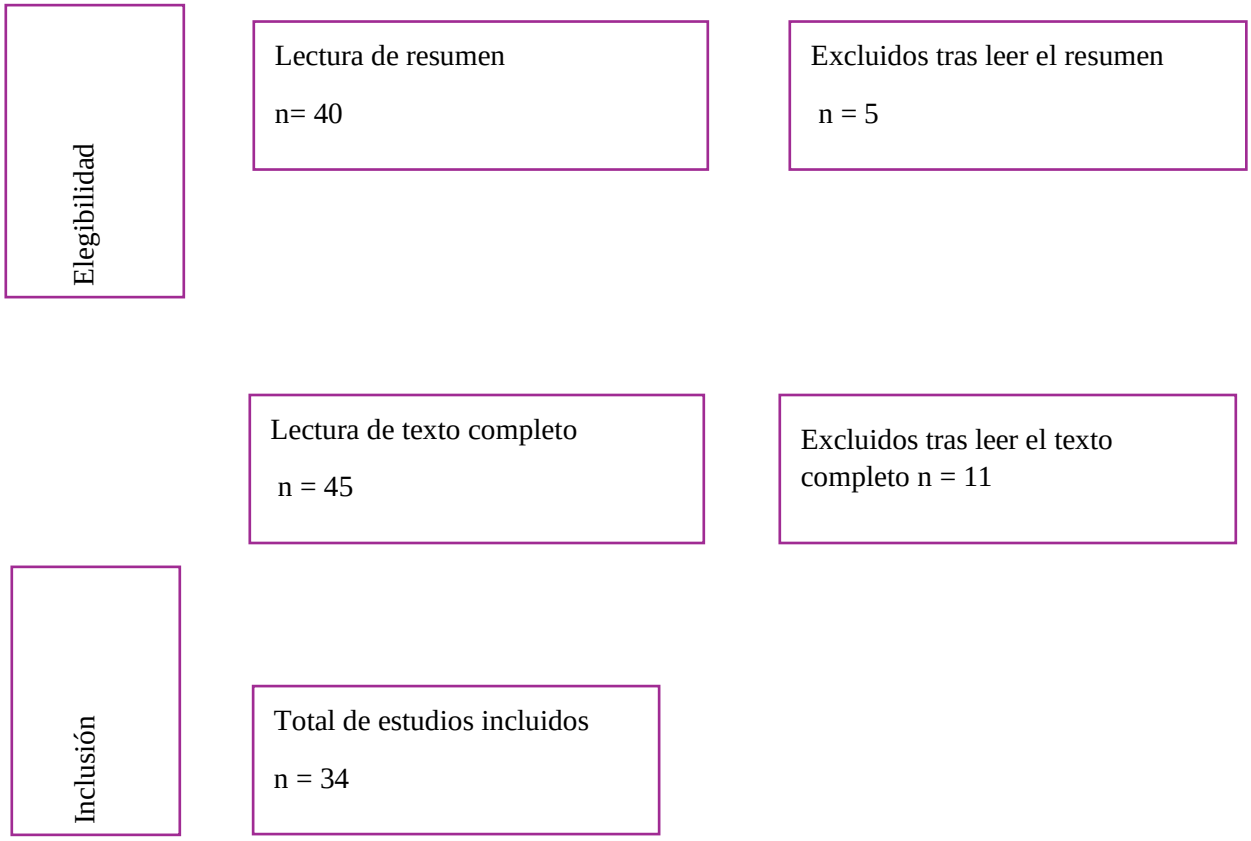
que permitieran entender la evolución doctrinal de las Fuerzas Especiales, la incorporación de capacidades tecnológicas avanzadas y los desafíos ético-operativos asociados.

Este corpus bibliográfico fue analizado mediante codificación temática emergente, que permitió identificar patrones, categorías analíticas y vacíos críticos en la implementación de tecnologías disruptivas en contextos de guerra especial. Asimismo, se utilizó un enfoque comparativo, contrastando doctrinas OTAN, estadounidenses y colombianas, y se incorporó el enfoque de estudios de caso para ilustrar el impacto real de estas tecnologías en conflictos recientes como el de Nagorno-Karabaj (2020) o la guerra en Ucrania (desde 2022).

En síntesis, el uso estratégico de 28 referencias seleccionadas no solo aporta robustez teórica al capítulo, sino que garantiza una base empírica sólida para el análisis crítico, asegurando la pertinencia y profundidad del estudio frente a los retos actuales y futuros que enfrentan las Fuerzas Especiales en escenarios multidominio y de guerra híbrida.

Figura 1. *Diagrama de flujo PRISMA*





Fuente: Elaboración propia

La guerra especial se encuentra en un punto de inflexión estratégico, marcado por la incorporación de tecnologías disruptivas que están redefiniendo los paradigmas de combate, inteligencia y decisión táctica. Dentro de este espectro, los sistemas no tripulados, la inteligencia artificial (IA), la robótica autónoma, el big data y la computación cuántica son los principales vectores de transformación del entorno operacional.

En los próximos diez años, se prevé que las operaciones de guerra especial estarán profundamente mediadas por sistemas autónomos capaces de ejecutar misiones críticas con mínima intervención humana. Estos sistemas abarcarán desde Unmanned Aerial Vehicles

(UAV) de reconocimiento con algoritmos de detección predictiva hasta plataformas robóticas terrestres con funciones ofensivas controladas por IA táctica. La integración de estos sistemas será facilitada por redes de comunicación de alta velocidad, 5G e incluso 6G, permitiendo una sincronización multi-dominio entre fuerzas especiales, unidades convencionales y medios cibernéticos.

El uso de sensores biométricos y nanotecnología en el equipamiento individual permitirá que los comandos de operaciones especiales monitoricen su salud, nivel de fatiga y señales ambientales en tiempo real, optimizando su desempeño en entornos hostiles. Asimismo, el combate cognitivo, entendido como el intento por alterar la percepción del adversario mediante técnicas informáticas avanzadas, se convertirá en un recurso clave, donde la guerra informacional, la manipulación de redes sociales y la generación de narrativas falsas adquirirán un nuevo nivel de sofisticación (Rid, 2020).

El desarrollo de estas tecnologías no solo transformará la capacidad letal de las Fuerzas Especiales, sino también su doctrina operativa, ya que exigirá mayor integración con el ciberespacio, mayor adaptabilidad a entornos tecnológicos fluidos y una formación integral en ciencia de datos, ciberseguridad y ética de combate digital (Singer & Brooking, 2018).

Tendencias tecnológicas y su evolución en conflictos futuros

Las guerras del futuro estarán mediadas por plataformas automatizadas, decisiones algorítmicas y superioridad informacional. Un análisis prospectivo evidencia que las principales tendencias tecnológicas girarán en torno a cinco ejes: (1) la autonomía táctica, (2) la conectividad multisensorial, (3) la integración hombre-máquina, (4) el cibercontrol del

espacio electromagnético y (5) la convergencia entre inteligencia artificial y capacidades cinéticas.

Primero, los UAV y UAS están evolucionando de plataformas remotamente controladas a sistemas autónomos con capacidad de aprendizaje y adaptación en tiempo real. Un ejemplo paradigmático es el reciente anuncio del gobierno alemán sobre el suministro a Ucrania de 4.000 drones con IA autónoma, desarrollados por la empresa Helsing, que pueden ejecutar misiones sin necesidad de intervención humana directa (Werkhäuser, 2024). Este tipo de desarrollos marca el inicio de una era donde los enjambres de drones, dotados de capacidades de autoorganización, podrán ejecutar misiones complejas en zonas de combate urbano o selvas densas, como las que enfrenta Colombia.

Segundo, la evolución de los conflictos híbridos ha demostrado la necesidad de control del espectro electromagnético. Las operaciones en el ciberespacio y las capacidades de guerra electrónica se integrarán plenamente en las campañas de guerra especial, permitiendo neutralizar comunicaciones, sistemas GPS y sensores enemigos. Esta tendencia es especialmente relevante frente a amenazas asimétricas como las que enfrenta Colombia, donde grupos armados ilegales han comenzado a emplear drones comerciales modificados para tareas de vigilancia y ataque.

Tercero, la interfaz cerebro-máquina (BCI, por sus siglas en inglés) es una tendencia emergente que promete aumentar exponencialmente las capacidades de los operadores especiales, al facilitar una interacción directa con sistemas autónomos, reduciendo el tiempo de respuesta y mejorando la precisión de las acciones (Gibson, 2021). Si bien su aplicación militar aún está en etapa experimental, su adopción futura es altamente probable.

Estas tendencias proyectan un escenario de conflictos más tecnológicos, con ciclos operacionales más cortos, mayor precisión letal y desafíos éticos sin precedentes.

Adaptación de las Fuerzas Especiales Colombianas a la nueva realidad tecnológica

El contexto colombiano, caracterizado por amenazas híbridas, actores armados organizados y entornos geográficos adversos, demanda una transformación urgente en las Fuerzas Especiales del país. En este sentido, el Ejército Nacional ha iniciado avances importantes, como la creación del primer Batallón de Aeronaves No Tripuladas (BANOT), orientado a la gestión, mantenimiento, operación y neutralización de drones, en respuesta a los ataques perpetrados por grupos armados con UAVs modificados

Se realizó una búsqueda exhaustiva en seis bases de datos especializadas PubMed, Google Académico, AOTA, Science Direct, Scopus y Scielo que arrojó un total inicial de 800 registros. Posteriormente, se aplicó un primer filtro basado en el criterio de fecha de publicación, lo que redujo el corpus a 340 documentos. Tras una primera revisión por título, se excluyeron 220 registros por no estar alineados con los objetivos del estudio, dejando 120 documentos para una evaluación más detallada. De estos, se leyeron 40 resúmenes, y 5 fueron descartados por falta de relevancia metodológica o temática. Finalmente, se procedió a la lectura completa de 35 textos, de los cuales 28 estudios cumplieron con todos los criterios de inclusión y fueron seleccionados para el análisis cualitativo final. Este proceso garantizó la pertinencia, actualidad y solidez académica de las fuentes incluidas.

Capacidades y limitaciones de las tecnologías disruptivas en la guerra especial

La evolución de las tecnologías militares ha redefinido la manera en que se planean y ejecutan las operaciones especiales, particularmente con la incorporación de UAV de combate. Estas aeronaves no tripuladas han transformado el campo de batalla al proporcionar capacidades avanzadas de inteligencia, vigilancia y reconocimiento (ISR), así como la capacidad de llevar a cabo ataques de precisión sin exponer a las tropas al peligro directo. En este análisis, se explorará el impacto de los UAV de combate en las operaciones especiales a través del estudio del caso de su implementación en el conflicto de Nagorno-Karabaj (2020), donde Azerbaiyán empleó de manera innovadora UAV Bayraktar TB2 y Harop para obtener una ventaja decisiva sobre las fuerzas armenias(Marín, 2021).

Sin embargo, el uso intensivo de UAV y sistemas autónomos no está exento de limitaciones críticas. Uno de los riesgos más debatidos es la vulnerabilidad electrónica, ya que estos sistemas pueden ser interferidos, hackeados o bloqueados mediante guerra electrónica enemiga. Además, la creciente dependencia tecnológica puede comprometer la autonomía operativa de fuerzas militares que no desarrollan capacidades propias. En términos éticos, el uso de fuerza letal autónoma plantea dilemas jurídicos y morales sobre la atribución de responsabilidad, el principio de distinción y la proporcionalidad en el uso de la fuerza (Foggo et al., 2022).

Desde la perspectiva colombiana, aunque las Fuerzas Especiales han comenzado a incorporar tecnologías como el RQ-11 Raven (Saumeth, 2024), aún existen brechas significativas en infraestructura, formación y actualización doctrinal. La doctrina nacional,

por ejemplo, no contempla de manera específica la guerra multidominio ni el uso extensivo de sistemas autónomos, lo que puede limitar la capacidad de respuesta frente a amenazas híbridas. Incorporar las lecciones del caso de Nagorno-Karabaj al contexto colombiano exige avanzar hacia una modernización integral de capacidades ISR, protección contra guerra electrónica y entrenamiento técnico-operacional.

Figura 2. *Conflicto Nagorno-Karabaj*

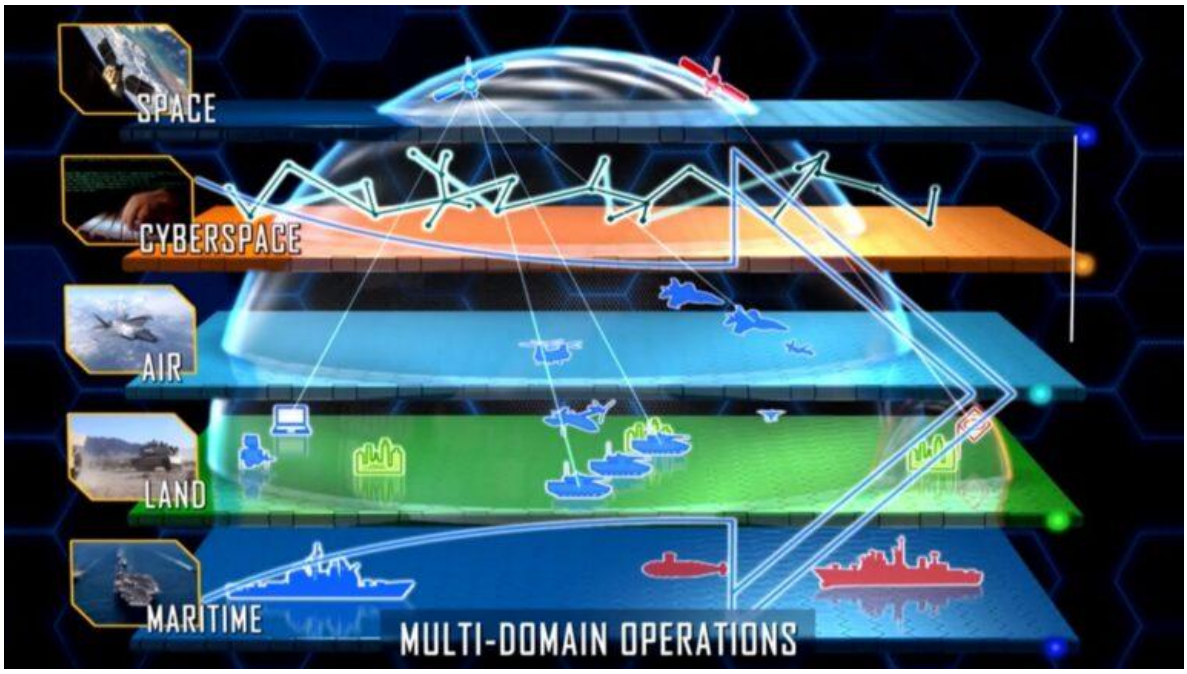
Nota: Fuente (Palacios, 2024)

Los UAV han demostrado una capacidad sin precedentes para realizar ataques de precisión minimizando los daños colaterales. En el conflicto de Nagorno-Karabaj, Azerbaiyán utilizó Bayraktar TB2 de fabricación turca y Harop de origen israelí para neutralizar sistemas antiaéreos, blindados y posiciones fortificadas armenias con gran efectividad. Estos dispositivos permiten identificar y atacar objetivos específicos sin exponer

a los soldados en el campo de batalla, reduciendo así las bajas propias y maximizando la eficiencia táctica(Palacios, 2024).

El uso masivo de UAV ha otorgado a fuerzas con menor poder militar convencional una ventaja estratégica en conflictos asimétricos. En el caso de Nagorno-Karabaj, Azerbaiyán no contaba con superioridad aérea mediante aviones tripulados, pero compensó esta limitación con el despliegue de UAV los cuales no solo realizaron ataques precisos, sino que también neutralizaron las defensas aéreas armenias, permitiendo un avance terrestre más seguro. Esta estrategia demostró cómo las tecnologías disruptivas pueden alterar el equilibrio del poder en el campo de batalla sin la necesidad de una aviación convencional dominante.

Figura 3. *Operaciones Multidominio*



Nota. Fuente: (Takabatake, 2024)

La imagen figura una representación visual del concepto de Operaciones Multidominio (Multi-Domain Operations, MDO), una estrategia militar contemporánea que reconoce la necesidad de operar y coordinar acciones simultáneamente en diversos dominios para alcanzar la superioridad estratégica frente a adversarios cada vez más integrados tecnológicamente. Esta aproximación busca trascender las barreras tradicionales de la guerra convencional (marítima, terrestre y aérea), integrando también los dominios emergentes de ciberespacio y espacio ultraterrestre, lo que evidencia la evolución de la guerra hacia escenarios interconectados, complejos y dinámicos(Hordiichuk et al., 2023).

En la figura, se representan cinco dominios clave: marítimo, terrestre, aéreo, ciberespacio y espacio. En la parte inferior se observa el dominio marítimo (color azul), donde interactúan buques de guerra y submarinos. Inmediatamente encima se encuentra el dominio terrestre (verde), donde unidades blindadas, fuerzas terrestres y sistemas informáticos desarrollan operaciones apoyadas por redes de comando y control. En el dominio aéreo (celeste), se evidencian aeronaves tripuladas y no tripuladas como UAV, realizando patrullajes y proporcionando inteligencia en tiempo real(Takabatake, 2024).

Más arriba, el ciberespacio (naranja) aparece como un entorno de flujo de datos e interferencias electrónicas, donde se llevan a cabo operaciones de guerra informática, defensa de redes, inteligencia de señales y manipulación de sistemas enemigos. Finalmente, en la parte superior, se destaca el dominio espacial (azul oscuro), donde satélites y sensores orbitales cumplen un papel crítico en la navegación, la vigilancia global y la coordinación interdominios, siendo a la vez vulnerables a interferencias o ataques cinéticos o electrónicos(Manolache, 2023).

La interconexión entre estos niveles se muestra mediante líneas y vectores que indican la interacción constante y fluida entre plataformas, sensores y unidades operativas en distintos entornos. Esto pone de manifiesto cómo las capacidades de vigilancia, ataque y defensa ya no se ejecutan de manera aislada, sino en una red de interdependencia táctica y estratégica. Esta concepción moderna del combate busca anticiparse y responder a amenazas simultáneas en múltiples dominios, promoviendo una superioridad decisiva a través de la integración tecnológica, la información en tiempo real y el mando unificado.

Los UAV en Operaciones Especiales

En las operaciones especiales, los UAV han revolucionado tanto la obtención de inteligencia como la ejecución precisa de acciones tácticas en ambientes hostiles. Estos sistemas, conocidos como Sistemas de Vehículos No Tripulados (UVS), ofrecen capacidades únicas que reducen el riesgo para las tropas y aumentan la eficiencia operativa. Un ejemplo paradigmático es el uso del PD-100 Black Hornet Nano, un micro UAV de solo 18 gramos desarrollado por la empresa noruega *Prox Dynamics* y utilizado desde 2012 por las Fuerzas Especiales del Reino Unido (SAS) y Noruega(Freire & García, 2024). Este nano UAV permite a los operadores en terreno urbano obtener reconocimiento en tiempo real sin delatar su presencia, gracias a su bajo nivel de ruido y tamaño casi indetectable. Según *Janes Defence Weekly* (2016), el Black Hornet ha sido vital para misiones de localización de insurgentes en Afganistán y Siria(Panigrahi & Tripathy, 2021).

Al mismo tiempo, otro caso relevante en operaciones de gran escala es el empleo del MQ-9 Reaper, fabricado por *General Atomics*, y desplegado por la Fuerza Aérea de los

Estados Unidos (USAF) y otras fuerzas aliadas desde 2007(Adamski, 2020). Este UAV de combate es capaz de realizar patrullajes de más de 27 horas continuas, portar hasta 1.5 toneladas de armamento (incluidos misiles AGM-114 Hellfire y bombas guiadas GBU-12 Paveway II) y ejecutar misiones de inteligencia, vigilancia, adquisición de objetivos y reconocimiento (ISTAR). En 2020, durante una operación en Bagdad, un MQ-9 fue responsable del ataque que dio muerte al general iraní Qasem Soleimani, lo que evidenció su precisión letal y su papel estratégico en operaciones de decapitación militar(Roberts & Capezzuto, 1999).

Figura 4. *UAV (Unmanned Aerial Vehicle) RQ-11 Raven*

Nota. Fuente: (Saumeth, 2024)

En Colombia, las Fuerzas Especiales del Ejército Nacional han adoptado el sistema RQ-11 Raven, un UAV portátil diseñado por *AeroVironment*, que pesa menos de 2 kg y se lanza a mano. Según el Ministerio de Defensa, este sistema ha sido clave desde mediados de la década de 2010 para operaciones contra el narcotráfico y grupos armados ilegales en zonas rurales del Cauca, Putumayo y Nariño, al permitir vigilancia en tiempo real sin arriesgar a las tropas de reconocimiento(Saumeth, 2024).

En el ámbito naval, sobresale el sistema Camcopter S-100 de la empresa austriaca *Schiebel*, un UAV tipo helicóptero desplegado por la marina alemana (Deutsche Marine) y otros países de la OTAN desde 2010. Puede operar desde corbetas y buques de patrulla en misiones de vigilancia marítima, detección de amenazas asimétricas y control de tráfico marítimo. El S-100 ha sido probado en operaciones de la misión EUNAVFOR Med, para detectar embarcaciones ilegales en el Mediterráneo. Su capacidad de despegue y aterrizaje vertical le permite operar desde espacios reducidos sin necesidad de una pista(De Biasio et al., 2010).

Figura 5. *UAV Terrestres*

Nota. Fuente: (Gallois, 2018)

En terrenos hostiles y minados, UAV terrestres como el TALON o el MAARS, (Ver figura 3)desarrollados por *QinetiQ North America*, han transformado las operaciones de desminado y neutralización de artefactos explosivos improvisados (AEI). Utilizados

ampliamente por el U.S. Army, estos robots pueden equiparse con sensores, cámaras térmicas e incluso armamento ligero, operando en Afganistán e Irak desde mediados de los años 2000. Un informe del *Pentágono de 2013* reconocía que estos UAV (Unmanned Aerial Vehicle)es habían salvado "cientos de vidas" en entornos de guerra urbana.

Incluso en escenarios submarinos, la guerra especial se ha beneficiado del uso de UVS. El REMUS 600, un vehículo submarino autónomo desarrollado por *Hydroid (Kongsberg Maritime)*, ha sido empleado por la US Navy SEALs para misiones de reconocimiento costero y detección de minas submarinas. Su uso fue documentado en la Operación Tormenta del Golfo (2014), cuando escaneó las aguas del Golfo Pérsico para asegurar rutas de ingreso de fuerzas aliadas(Tawil Kuri, 2009).

Estas aplicaciones evidencian cómo los UAV han redefinido el concepto de visión táctica, permitiendo a las fuerzas especiales operar con mayor autonomía, precisión y sigilo. La tendencia global apunta a su integración en doctrinas regulares de combate, y a una creciente hibridación entre sistemas autónomos y tripulados, marcando el camino hacia una guerra más tecnológica, eficiente y menos dependiente de la exposición humana directa. La pregunta ya no es si los UAV deben emplearse en operaciones especiales, sino cómo optimizar su uso dentro de un entorno doctrinal, ético y legal.

Inteligencia Artificial y Toma de Decisiones en el Campo de Batalla

En el marco de las operaciones de Fuerzas Especiales (FF.EE.), la inteligencia artificial (IA) representa una capacidad transformadora que impacta transversalmente el ciclo de inteligencia, la planeación operativa y la ejecución táctica. De acuerdo con el MCE 3-18,

las FF.EE. requieren operar en entornos inciertos, complejos y en permanente cambio (MCE 3-18, p. 1-4). En ese contexto, la IA facilita la integración de múltiples fuentes de información (HUMINT, SIGINT, GEOINT) y permite generar patrones predictivos que mejoran la toma de decisiones en tiempo real.

Herramientas como los algoritmos de aprendizaje automático ya son empleados para anticipar movimientos de fuerzas enemigas, priorizar blancos y optimizar rutas de infiltración en zonas negadas. Ejemplos como el *Project Maven* del Departamento de Defensa de EE. UU. ilustran cómo la IA puede automatizar el análisis de grandes volúmenes de video captado por UAV, liberando recursos humanos para tareas críticas. La IA también potencia la guerra cognitiva, al permitir campañas de desinformación basadas en análisis de comportamiento social y modelos de lenguaje generativo.

Para las FF.EE. colombianas, el desafío es doble: integrar progresivamente estas tecnologías sin comprometer la ética operativa, y desarrollar capacidades propias que no dependan completamente de actores externos, especialmente cuando se trata de misiones de inteligencia estratégica o de defensa de la soberanía en zonas grises.

.

Ciberseguridad y Guerra Electrónica: Protección de Infraestructura Crítica

El MCE 3-18 establece que las Fuerzas Especiales deben estar preparadas para operar en todos los dominios del conflicto, incluido el ciberespacio (MCE 3-18, p. 4-7). En este entorno, las amenazas se manifiestan en forma de ataques a redes militares, sabotaje a infraestructuras críticas y guerra de la información, donde la narrativa y el control de datos son tan relevantes como la potencia de fuego.

Las operaciones especiales ya incorporan capacidades de ciberinteligencia (cyber ISR), guerra electrónica ofensiva y defensa activa de sistemas. Un ejemplo relevante es la integración entre comandos de ciberoperaciones y unidades de operaciones psicológicas (PSYOPS), que permite desarticular estructuras enemigas mediante la difusión selectiva de información y la manipulación del entorno cognitivo de líderes adversarios.

En el contexto colombiano, la interrelación entre ciberseguridad y operaciones especiales es clave para enfrentar amenazas híbridas como el crimen organizado transnacional y la desinformación empleada por actores armados ilegales. Esto exige una arquitectura cibernética robusta, interoperable y adaptada a los entornos operativos multisectoriales.

Estado actual de las tecnologías disruptivas en la Revolución en los Asuntos Militares (RMA)

La Revolución en los Asuntos Militares (RMA) ha alcanzado un punto de madurez en el que las tecnologías disruptivas no solo complementan el poder militar tradicional, sino que lo transforman estructuralmente. Hoy en día, las Fuerzas Especiales deben operar en un entorno marcado por la hibridación de amenazas y la convergencia de dominios físicos, digitales y cognitivos. La doctrina MCE 3-18 destaca que estas unidades deben actuar con autonomía, adaptabilidad y precisión quirúrgica en contextos volátiles, ambiguos y saturados de información. En este escenario, tecnologías como la inteligencia artificial (IA), los sistemas autónomos, y las capacidades cibernéticas ya no son futuras promesas, sino realidades operativas que redefinen la guerra contemporánea.

La inteligencia artificial se posiciona como el núcleo de esta transformación. En las Fuerzas Especiales, su implementación mejora la fusión de inteligencia (HUMINT, SIGINT, GEOINT), facilita la toma de decisiones en tiempo real y reduce la carga cognitiva de los operadores en misiones críticas. Proyectos como *Maven* del Departamento de Defensa de EE. UU. demuestran que algoritmos de aprendizaje automático pueden identificar objetivos a partir de imágenes de UAV con mayor precisión que los analistas humanos. En Colombia, aunque estas capacidades están en etapa inicial, el desafío es incorporar IA sin perder el control ético ni la soberanía sobre los datos estratégicos, especialmente en escenarios como la selva, la frontera y el ciberespacio.

En paralelo, la ciberseguridad y la guerra informacional han tomado protagonismo como dimensiones operativas. El MCE 3-18 reconoce que las FF.EE. deben ser capaces de actuar en el ciberespacio, no solo como defensores de infraestructuras, sino como actores ofensivos capaces de desarticular redes de mando enemigas, manipular entornos cognitivos y garantizar la supremacía narrativa. Esto implica dominar herramientas de ciberinteligencia, operaciones psicológicas digitales y guerra electrónica ofensiva. En Colombia, estas capacidades son especialmente relevantes frente a organizaciones armadas ilegales que usan redes sociales, servicios encriptados y narrativas polarizantes como armas de combate no convencional.

El estado actual de la RMA también refleja una transición organizacional: de doctrinas estáticas a estructuras flexibles, descentralizadas y basadas en el pensamiento crítico. Las tecnologías disruptivas requieren operadores que no solo ejecuten órdenes, sino que lideren en entornos sin contacto directo con el escalón superior. Esta transformación doctrinal implica entrenamiento en autonomía, agilidad adaptativa y dominio multidominio.

Las FF.EE. colombianas enfrentan el reto de incorporar estas dinámicas a su doctrina operativa, asegurando interoperabilidad, respuesta en tiempo real y despliegue efectivo tanto en operaciones urbanas como en jungla, montaña y litoral.

Desarrollo de la RMA en el contexto de la guerra moderna

La Revolución en los Asuntos Militares (RMA) se refiere a un proceso transformador profundo en la forma de concebir y conducir la guerra, donde los avances tecnológicos, doctrinales y organizacionales convergen para modificar radicalmente las capacidades operativas de las fuerzas armadas. Este concepto tomó fuerza en la década de 1990, cuando el Departamento de Defensa de los Estados Unidos, tras observar el desempeño de sus tropas en la Guerra del Golfo (1991), reconoció el potencial disruptivo de tecnologías como el GPS, los misiles guiados de precisión y los sistemas de comando y control digitalizados(Rodríguez, 1992). El dominio abrumador mostrado por la coalición liderada por EE. UU. frente a las fuerzas iraquíes demostró que la superioridad tecnológica podía traducirse en efectos militares decisivos con un número reducido de bajas y una ejecución operativa de alto impacto.

William H. McRaven, en su obra *Spec Ops: Case Studies in Special Operations Warfare* (1995), plantea que el éxito de las operaciones especiales se fundamenta en seis principios universales: simplicidad, seguridad, repetición, sorpresa, velocidad y propósito. Estos principios se articulan para permitir que fuerzas reducidas logren objetivos estratégicos de alto impacto mediante acciones precisas y de corto plazo. La simplicidad se refiere a la claridad en la planificación y ejecución; la seguridad, a la protección de la información y la integridad de la misión; la repetición, al entrenamiento constante para perfeccionar

procedimientos; la sorpresa, a la capacidad de actuar en momentos y lugares inesperados; la velocidad, a la rápida ejecución antes de que el adversario pueda reaccionar; y el propósito, a la orientación hacia un objetivo decisivo. En el contexto contemporáneo, las tecnologías disruptivas como la inteligencia artificial (IA), los vehículos aéreos no tripulados (UAV) y la guerra cibernética amplifican la aplicación de estos principios, permitiendo mayor precisión, rapidez y flexibilidad en entornos de alta complejidad. Sin embargo, su uso también introduce nuevos desafíos de seguridad y control, especialmente cuando la autonomía tecnológica puede reducir la supervisión humana directa.

Uno de los hitos clave de esta primera ola de RMA fue la operación "Tormenta del Desierto" (enero-febrero de 1991), donde más de 2.000 bombas guiadas por láser y satélite fueron utilizadas para destruir infraestructuras estratégicas iraquíes con una precisión sin precedentes. Esta campaña aérea evidenció el paso de una guerra de desgaste a una guerra basada en información, sensores y precisión quirúrgica. La coordinación entre satélites, aviones de vigilancia AWACS y unidades terrestres permitió una sincronización operativa sin comparación con conflictos anteriores. Este evento marcó el inicio de una doctrina basada en el concepto de *Dominio de Espectro Completo*, en la que la superioridad informacional es tan crucial como la potencia de fuego.

Posteriormente, la RMA evolucionó hacia una segunda fase más compleja tras los atentados del 11 de septiembre de 2001. La "Guerra contra el Terrorismo" transformó la naturaleza del combate, pasando del enfrentamiento entre ejércitos regulares al conflicto contra actores no estatales, móviles y descentralizados. En Afganistán (2001) e Irak (2003), las fuerzas estadounidenses y aliadas incorporaron tecnologías como los UAV armados MQ-1 Predator y los sistemas de vigilancia persistente. Por ejemplo, en 2002, un UAV Predator

lanzó por primera vez un misil Hellfire sobre un objetivo terrorista en Yemen, estableciendo el precedente del uso letal de sistemas no tripulados en conflictos asimétricos. Esta nueva etapa de la RMA ya no se centró exclusivamente en tecnología de punta, sino en la integración entre inteligencia, precisión táctica y operaciones especiales.

En la actualidad, la RMA se encuentra en una tercera fase marcada por la convergencia digital. Tecnologías disruptivas como la inteligencia artificial, la computación cuántica, los enjambres de UAV, la robótica autónoma y la guerra cibernética están redefiniendo los límites del campo de batalla. Un ejemplo contemporáneo es la guerra en Ucrania (desde 2022), donde se ha evidenciado un uso intensivo de UAV civiles adaptados al combate, inteligencia geoespacial en tiempo real y guerra electrónica para neutralizar comunicaciones enemigas(Vera et al., 2023). Rusia y Ucrania han convertido el ciberespacio en un frente activo, con ataques a infraestructuras energéticas, campañas de desinformación y sabotajes digitales. Estos elementos muestran que la guerra moderna ya no se define por el tamaño de las tropas, sino por la capacidad de recolectar, procesar y actuar con base en datos en tiempo real(Morales, 2021).

Además, países como China y Estados Unidos están inmersos en una carrera por la supremacía tecnológica militar. China, por ejemplo, ha incorporado inteligencia artificial a sus sistemas de mando y ha probado prototipos de enjambres de UAV controlados por algoritmos en sus ejercicios militares. EE. UU., por su parte, ha lanzado iniciativas como JADC2 (Joint All-Domain Command and Control) para integrar fuerzas terrestres, aéreas, navales, espaciales y cibernéticas en una sola red interoperable de combate. Esta lógica representa el núcleo de la actual RMA: lograr una ventaja decisiva mediante la fusión de

dominios, la rapidez en la toma de decisiones y la capacidad adaptativa frente a amenazas híbridas y no lineales(Centro Conjunto de Desarrollo de Conceptos, 2020).

Integración de Tecnologías Disruptivas en las Fuerzas Especiales

La integración de tecnologías emergentes y disruptivas (EDT) en las Fuerzas Especiales constituye un paso estratégico imprescindible para garantizar la superioridad operativa de los Estados occidentales frente a adversarios cada vez más tecnológicamente equiparados. En el contexto actual, dominado por la competencia estratégica entre potencias, la OTAN y la Unión Europea enfrentan el reto de no quedarse rezagadas frente a los avances de Rusia y China en áreas como inteligencia artificial, sistemas no tripulados, guerra electrónica e hipersónica. Estas tecnologías han dejado de ser meramente experimentales y ya están redefiniendo las lógicas del conflicto moderno, donde la velocidad, la autonomía, la precisión y la resiliencia digital se convierten en factores diferenciales. Las Fuerzas Especiales, tradicionalmente diseñadas para operar en escenarios de alta complejidad y discreción, deben adoptar estas capacidades disruptivas para mantener su capacidad de infiltración, reconocimiento, sabotaje, contrainsurgencia y operaciones de precisión en entornos multidominio(Foggo et al., 2022).

El estudio liderado por el CEPA resalta que, si bien las potencias occidentales han generado estrategias para integrar estas tecnologías (como DIANA en la OTAN o HEDI en la UE), aún subsisten importantes brechas en interoperabilidad, inversión, gobernanza y velocidad de adopción. Las Fuerzas Especiales requieren tecnologías que permitan actuar de manera autónoma en el terreno, utilizando inteligencia artificial para análisis en tiempo real, UAV de vigilancia y ataque que puedan operar en ambientes hostiles, redes de

comunicaciones cifradas basadas en computación cuántica, y capacidades de guerra cognitiva y cibernética para desorganizar al enemigo sin disparar un solo proyectil. Además, las plataformas espaciales y satelitales, esenciales para la navegación y el posicionamiento, están siendo amenazadas por las capacidades ASAT (antisatélite) de Rusia y China, lo cual exige que las Fuerzas Especiales desarrollen redundancias tecnológicas y sistemas alternativos para operar en contextos de "apagón espacial"(Saunders & Lutes, 2007).

A través de una estrategia transatlántica común, se busca fortalecer la cooperación en I+D, acelerar la experimentación de prototipos y fomentar la conexión entre militares, académicos, startups y sectores industriales. En el caso de las Fuerzas Especiales, esto implica entrenamientos conjuntos, ejercicios de simulación con tecnologías emergentes, e incorporación de personal técnico especializado en robótica, bioingeniería y sistemas autónomos. La interoperabilidad, como uno de los pilares estratégicos, es clave para asegurar que unidades multinacionales operen con estándares comunes, especialmente en operaciones conjuntas en escenarios como el Báltico, el Ártico o el Indo-Pacífico. Igualmente, la estandarización permitirá una respuesta más rápida ante amenazas híbridas, que combinan ataques cibernéticos, sabotaje de infraestructuras críticas y manipulación de la opinión pública a través de desinformación digital.

Asimismo, la integración de tecnologías disruptivas exige replantear el marco ético de las Fuerzas Especiales, que deben operar bajo principios democráticos incluso cuando utilizan sistemas de inteligencia artificial autónomos(Narváez, 2024). La gobernanza de estas tecnologías y el control sobre su uso deben ser garantizados para evitar abusos, escaladas accidentales o deshumanización del combate. En este sentido, los estándares éticos deben

estar presentes desde la fase de desarrollo tecnológico hasta la planificación de misiones.(Serna et al., 2024)

Influencia de las Nuevas Tecnologías en las Tácticas de Guerra Especial

La influencia de las nuevas tecnologías en las tácticas de guerra especial ha reconfigurado sustancialmente las doctrinas militares contemporáneas, dando paso a un entorno operacional dominado por la información, la conectividad y la rapidez en la toma de decisiones. Tal como expone H. A. Hernández Fernández en su análisis sobre la Revolución en los Asuntos Militares (RAM), la evolución tecnológica no solo ha transformado el arte de la guerra, sino que ha dotado a las fuerzas especiales de nuevas capacidades para actuar en escenarios cada vez más complejos, híbridos y asimétricos.

En primer lugar, la tecnología ha modificado la forma de planear y ejecutar operaciones especiales, incorporando herramientas como la inteligencia artificial, los sistemas no tripulados, la guerra electrónica y las redes de comunicaciones encriptadas. Estos avances permiten a las unidades de operaciones especiales operar con mayor sigilo, letalidad y precisión quirúrgica. La posibilidad de geolocalizar objetivos en tiempo real, extraer datos de inteligencia de fuentes abiertas y coordinar ataques desde plataformas remotas ha hecho que las operaciones especiales se conviertan en elementos decisivos en conflictos de baja y media intensidad.

Asimismo, el uso de tecnologías disruptivas ha permitido redefinir el concepto de "teatro de operaciones". La guerra especial ya no se limita al combate físico en tierra, mar o aire, sino que se extiende al dominio cibernético y espacial. Las unidades especiales, apoyadas por capacidades de ciberinteligencia y ciberdefensa, pueden desarticular infraestructuras críticas del enemigo sin necesidad de una intervención convencional. Esto es

particularmente relevante en conflictos donde los actores estatales enfrentan amenazas difusas, como redes terroristas o grupos paramilitares transnacionales.

Esta transformación tecnológica se refleja directamente en las misiones doctrinales definidas por el Ejército Nacional de Colombia en el manual EJC 3-223 M. Las operaciones de acción directa, por ejemplo, se ven potenciadas por el uso de UAV armados, sensores remotos y comunicaciones satelitales, permitiendo golpear objetivos de alto valor con un margen de error mínimo (Ejército Nacional de Colombia., 2007). Las misiones de reconocimiento especial se benefician de sistemas de vigilancia persistente, inteligencia geoespacial y análisis de big data, proporcionando a los comandantes una conciencia situacional táctica más precisa y en tiempo real. Por su parte, la guerra no convencional se transforma mediante la capacidad de generar desinformación estratégica, interrumpir redes logísticas enemigas mediante ataques cibernéticos y movilizar poblaciones a través del control del entorno informativo.

Igualmente, las operaciones de asistencia militar extranjera encuentran en la tecnología una herramienta clave para entrenar, asesorar y equipar a fuerzas aliadas, utilizando simuladores de combate, plataformas virtuales de instrucción y evaluaciones remotas de desempeño(Gómez, 2021). Estas capacidades permiten extender el alcance geopolítico de las Fuerzas Especiales colombianas, alineándolas con estándares internacionales y fortaleciendo su rol como actor estratégico regional.

Por otro lado, la integración tecnológica en las tácticas de guerra especial exige un cambio doctrinal y organizativo. La interoperabilidad entre ramas militares, el uso compartido de datos entre agencias y la adaptabilidad a los entornos digitales se vuelven fundamentales (Gonzalez, 2011). En este sentido, la tecnología no solo provee nuevas

herramientas, sino que impone una transformación cultural dentro de las Fuerzas Militares. La formación de operadores especiales ahora requiere competencias en tecnologías de la información, inteligencia artificial, sistemas de mando y control, y análisis de datos.

Ahora bien, la revolución tecnológica también presenta riesgos, como el dilema de seguridad y la posibilidad de que actores no estatales accedan a tecnología avanzada, las tácticas de guerra especial deben entonces contemplar la ciberseguridad como parte integral de sus operaciones. La vulnerabilidad a ataques cibernéticos, la guerra informacional y el espionaje digital son amenazas reales que pueden comprometer misiones altamente sensibles. La respuesta a estas amenazas exige estrategias multidimensionales donde la tecnología sea un medio, pero no un fin en sí misma.

Proyección futura de las tecnologías disruptivas en la guerra especial

La era actual se caracteriza por una digitalización acelerada de todos los aspectos del conflicto. Los expertos afirman que vivimos en el marco de las guerras de quinta generación", marcadas por la transición de la analogización a la digitalización de la sociedad(Maldonado, 2024). En este entorno, la información se ha convertido en el recurso estratégico clave: "Vivimos un mundo […] inmensamente rico en datos, donde incluso un gesto o un número son considerados datos gestionados por sistemas computacionales. En efecto, el libro *Tecnologías disruptivas, logística, seguridad y defensa nacional* destaca que actualmente hay «un muy evidente avance en el conocimiento» y que "jamás había habido tanta gente con maestrías y doctorados. Vivimos, literalmente, una edad de luz en ciencia y tecnología.

De la misma manera, estos avances auguran un futuro en el que las capacidades de las Fuerzas Especiales se potenciarán dramáticamente mediante tecnología disruptiva. En las próximas décadas es previsible la adopción de sistemas autónomos y semiautónomos basados en inteligencia artificial para tareas de reconocimiento, vigilancia y ataque. Por ejemplo, se están desarrollando drones de combate que, una vez programados, vuelan de forma independiente y atacan sin necesidad de un piloto a distancia(Werkhäuser, 2024). Además, las armas de energía dirigida (láseres o microondas) y la robótica desplegada en entornos hostiles permitirán una mayor precisión y letalidad. Paralelamente, el ciberespacio se consolida como un teatro de guerra: los futuros escenarios exigirán que las unidades de guerra especial actúen también en el quinto dominio (cibernético), donde una mentalidad estilo "hacker" resulta imprescindible.

Asimismo, las tecnologías emergentes modificarán la naturaleza de la información en el campo de batalla. Las técnicas de inteligencia artificial (IA) y big data preparan "los escenarios para una nueva era de guerra política, económica y de alto impacto(Bernal & Salgado, 2024). A corto plazo será aún más difícil discernir lo real de lo falso (por ejemplo, audio y video manipulados por IA), lo que dificultará la identificación de información confiable. Redes de datos persistentes, sensores conectados y comunicación global permitirán operaciones encubiertas y ataques remotos con una latencia casi nula. En suma, la revolución tecnológica promete transformar las operaciones de Fuerzas Especiales, ampliando su alcance y velocidad de reacción en entornos cada vez más complejos.

Tendencias tecnológicas y su evolución en conflictos futuros

Los conflictos del futuro estarán cada vez más marcados por una combinación de elementos tecnológicos avanzados. Drones y vehículos no tripulados juegan ya un rol protagonista en teatros como el de Ucrania: ambos bandos emplean diarios drones de bajo costo para ataque y reconocimiento(Werkhäuser, 2024). En este sentido, se observa una tendencia global hacia el empleo de armas autónomas o semiautónomas: por ejemplo, Alemania está suministrando a Ucrania 4.000 drones de ataque controlados por IA que pueden penetrar 30–40 km en retaguardia enemiga y eludir las defensas electrónicas del enemigo. Los analistas prevén que en el futuro próximo este tipo de sistemas que combinan IA y capacidades autónomas– serán comunes en Fuerzas Militares de todo el mundo.

David Kilcullen, reconocido estratega australiano, desarrolla en obras como *The Accidental Guerrilla* (2009) y *Out of the Mountains* (2013) una teoría de la guerra irregular basada en la adaptación de las fuerzas armadas a entornos híbridos, donde actores estatales y no estatales se mezclan en un espacio de conflicto difuso(Evans, 2012). Kilcullen identifica que las operaciones exitosas en este tipo de escenarios requieren no solo capacidades cinéticas, sino también control informacional, adaptación cultural y presencia sostenida en el terreno. La guerra irregular se caracteriza por su asimetría: el adversario evita enfrentamientos directos y emplea tácticas como insurgencia, terrorismo, guerra urbana y ciberataques. Las Fuerzas Especiales, por su flexibilidad y alcance estratégico, son las más adecuadas para operar en este tipo de conflictos. En la actualidad, tecnologías disruptivas como sensores remotos, algoritmos de análisis predictivo y herramientas de guerra electrónica potencian la capacidad de las FF.EE(Rosen, 2010). para actuar con ventaja en este entorno. No obstante, Kilcullen advierte que la dependencia excesiva de tecnología

puede generar vulnerabilidades, especialmente si el adversario desarrolla contramedidas o aprovecha las mismas herramientas.

Otra tendencia clave es la guerra cibernética e informacional. El libro *Comandos: Retos de las Fuerzas Especiales* destaca que las tecnologías digitales han ampliado "la importancia de la dimensión informacional" del conflicto, generando nuevas herramientas para manipular opiniones y desinformar(Bernal & Salgado, 2024). El análisis prospectivo de Polyakova & Boyer señala que los avances en IA, aprendizaje automático y big data han preparado el terreno para "una nueva era de guerra política" donde los actores maliciosos utilizarán estos medios para atacar a la sociedad de forma más eficaz. En la práctica, esto se traduce en el uso de campañas masivas de desinformación, propaganda automatizada y ataques a infraestructura crítica (energía, comunicaciones, finanzas) mediante software malicioso. De hecho, ya se advierte que será cada vez más difícil distinguir entre información auténtica y deepfakes, lo cual pone en jaque la credibilidad en medios y redes sociales.

La tercera tendencia son los sistemas de guerra electrónicos y de contrainteligencia. Las conflagraciones actuales muestran un uso intensivo de interferencia electrónica, satélites de comunicaciones por ejemplo en Starlink en Ucrania y radares avanzados para vigilancia y defensa aérea. Se espera que aumente la inversión en sistemas antidrón y jammers de comunicación, así como en contramedidas cibernéticas para proteger los sistemas críticos de mando y control. De hecho, la competencia global por el dominio tecnológico (EE. UU., China, Rusia, entre otros) está creando una carrera por el "próximo salto" en guerra política y electrónica, lo cual intensifica la militarización de estas tecnologías.

Martin van Creveld, en *The Transformation of War* (1991), expone que el conflicto armado ha transitado desde formas convencionales, dominadas por ejércitos estatales, hacia

guerras no lineales en las que intervienen múltiples actores y dominios. La noción de "guerra no trinitaria" que plantea Van Creveld rompe con el paradigma clausewitziano, al reconocer que el Estado ya no es el único actor legítimo de la violencia organizada. El autor identifica que la proliferación de actores irregulares, la urbanización del combate, la expansión del ciberespacio y la globalización han erosionado las fronteras entre lo civil y lo militar. En este marco, las operaciones especiales adquieren un papel protagónico, ya que combinan la capacidad de actuar en dominios físicos tierra, mar y aire con operaciones en ciberespacio e información(Van Creveld, 2002). La transformación tecnológica, según Van Creveld, exige doctrinas más flexibles, redes de mando descentralizadas y una integración plena de inteligencia en tiempo real.

Finalmente, la innovación en guerra militar también incluye áreas como la nanotecnología o la biotecnología aplicadas al campo de batalla. Aunque menos visible en el corto plazo, se anticipa que los avances en sensores biológicos o en ciberseguridad a nivel molecular podrían influir en la preparación de tropas especiales, por ejemplo, mediante implantes que mejoren la resistencia o interfaces cerebro–máquina para una mejor coordinación táctil. En conjunto, las tendencias actuales indican que los conflictos futuros serán multidimensionales, integrando simultáneamente el espacio terrestre, aéreo, marítimo, cibernético e incluso cognitivo. Las Fuerzas Especiales tendrán que operar en un escenario donde estos dominios converjan tecnológicamente.

Adaptación de las Fuerzas Especiales Colombianas a la nueva realidad tecnológica

Frente a este panorama tecnológico global, las Fuerzas Especiales de Colombia han iniciado un proceso de adaptación para integrar nuevos sistemas en sus operaciones. En el ámbito

ciberespacial, estudios recientes destacan la necesidad de fortalecer las capacidades de respuesta ante amenazas digitales. Según Realpe y Cano, el Ejército colombiano enfrenta riesgos crecientes por "amenazas cibernéticas impuestas por las tecnologías disruptivas" que comprometen la seguridad nacional(R. J. N. Rodríguez & Garzón, 2024). Para contrarrestarlos, proponen una estrategia de ciberdefensa militar que analiza prospectivamente tecnologías emergentes (con la herramienta Ventana AREM) y promueve la inmersión tecnológica en las unidades. Es decir, se busca que los comandos de guerra especial desarrollen habilidades propias de ciberoperadores –con los equipamientos adecuados para participar activamente en las operaciones digitales defensivas y ofensivas.

En el nivel organizativo, el marco constitucional y doctrinal colombiano apunta en la misma dirección. La Política de Ciberseguridad de las Fuerzas Militares insiste en fortalecer continuamente sus capacidades digitales y cooperar con aliados (como la OTAN) para proteger la infraestructura crítica del país(Peña, 2023). En este sentido, Colombia ha fortalecido su vinculación con organismos internacionales: desde 2017 es socio global de la OTAN y participa en ejercicios y estandarización tecnológica. A principios de 2025 el Ejército inició una hoja de ruta con la Alianza Atlántica para aplicar estándares operacionales a unidades clave, extendiendo esta política al manejo de vehículos aéreos no tripulados (VANT).

Un aspecto crucial de la adaptación ha sido responder a amenazas tecnológicas específicas en el conflicto colombiano. Desde 2023, las disidencias de las antiguas FARC y otros grupos armados comenzaron a usar drones comerciales modificados para lanzar explosivos contra puestos militares y civiles. El tema se agudizó en 2024 en zonas como el

Cauca y Norte de Santander, con al menos 19 ataques registrados(El País, 2024). Como respuesta, el Comando de las Fuerzas Militares aceleró la adquisición de sistemas antidrón y jammers de señal Además, el Ejército anunció la creación del Batallón de Aeronaves No Tripuladas (BANOT), una unidad táctica especializada exclusivamente en operar drones y neutralizar amenazas aéreas. Este batallón, equiparable en despliegue a un batallón de Fuerzas Especiales, desarrollará doctrina propia para el uso ofensivo y defensivo de VANT en escenarios de guerra irregular.

La modernización no se limita a los sistemas, sino que incluye entrenamiento y doctrina. El Ejército colombiano ya emplea drones comerciales de fabricantes como DJI (equipados con visión nocturna o cámaras térmicas) en misiones de inteligencia y reconocimiento. Con el BANOT se busca consolidar y estandarizar estas capacidades. De hecho, se planea aplicar en el 2025–2026 estándares de interoperabilidad de la OTAN a las fuerzas de drones, aprovechando la experiencia ganada en ejercicios conjuntos(Cepeda, 2025). Como resultado, las Fuerzas Especiales colombianas están desarrollando un modelo operativo cada vez más integrado con tecnología emergente, lo que las posiciona como referente regional en esta materia.

En suma, la adaptación de las Fuerzas Especiales Colombianas se basa en una estrategia de transformación digital y doctrinal. Esto implica fortalecer el elemento humano (capacitación en ciberdefensa, análisis de inteligencia digital) y proveerles equipos avanzados (UAVs, sistemas de vigilancia electrónica, ciber-herramientas) para mantener la iniciativa ante cualquier amenaza. De cara al futuro, se prevé un Ejército nacional más moderno, interoperable y preparado tecnológicamente, capaz de operar con eficacia en un

entorno de conflicto cada vez más caracterizado por la convergencia de dominios tradicionales y digitales.

Consideraciones éticas y estratégicas en la implementación de tecnología militar

La incorporación de tecnologías avanzadas en la guerra plantea complejos dilemas éticos y estratégicos. En primer lugar, el uso de armas autónomas choca con principios morales básicos. Como señala un artículo de Silicon, "la inclusión de sistemas de IA en el campo de batalla conlleva la deshumanización intrínseca a la delegación de procesos letales sobre entes no humanos, capaces de matar personas sin control humano significativo. Incluso se afirma que la idea de robots asesinos no es ciencia ficción: Naciones Unidas debate desde hace años sobre los sistemas letales autónomos (LAWS), capaces de seleccionar y atacar objetivos sin supervisión humana(Aravena, 2024). Esto violaría normas fundamentales del Derecho Internacional Humanitario (Convenios de Ginebra), diseñado para proteger a la población civil. En palabras de Joaquín Rodríguez Álvarez (UAB), la IA "conduce al quebrantamiento de las normas que regulan la guerra" porque los sistemas inteligentes son altamente débiles en los análisis contextuales en tiempo real que estas normas requieren.

Otro problema es la responsabilidad legal y moral. La opacidad de los algoritmos militares genera la pregunta: si un sistema IA provoca víctimas civiles, ¿quién responde? Los especialistas subrayan que "el límite ético infranqueable es que nunca esa responsabilidad debe estar fuera de un ser humano (Pugliese & Griffini, 2021). En la guerra tradicional, quien aprieta el gatillo asume esa responsabilidad; en la guerra digital el "gatillo" puede estar en el

software, pero siempre debe haber una persona supervisando cuándo disparar o no. Sin embargo, la realidad tiende a difuminar esa responsabilidad. Además, los algoritmos pueden contener **sesgos** de entrenamiento que identifiquen erróneamente objetivos, debilitando el juicio humano en el proceso.

Adicionalmente, la autonomía tecnológica aumenta los riesgos de pérdida de control y vulnerabilidad ante ataques externos. Por ejemplo, los sistemas IA más avanzados funcionan a velocidades o profundidades inalcanzables para las comunicaciones actuales, lo que eleva la posibilidad de desconexión o interferencia. También se destaca la posibilidad de que un adversario cibernético comprometa sistemas autónomos y los utilice contra sus propios creadores. De manera colateral, el uso de IA en inteligencia y vigilancia implica una doble tensión: por un lado, facilita la defensa anticipativa contra amenazas, pero por otro puede generar vigilancia masiva que vulnere la privacidad de civiles tanto en paz como en conflicto.

Frente a estos retos, las recomendaciones estratégicas coinciden en mantener siempre un control humano significativo en los sistemas armados y en desarrollar marcos regulatorios actualizados. Expertos sugieren incorporar en la Convención de Ginebra principios específicos sobre IA militar y acordar de manera multilateral estándares éticos (supervisión humana, transparencia en el desarrollo de software, prohibición de ciertos usos. Sin embargo, la realidad geopolítica complica esta tarea: organizaciones internacionales como Campaign to Stop Killer Robots han propuesto prohibiciones totales, pero potencias como EE. UU. y Rusia rechazan restricciones que limiten su arsenal tecnológico. En la actualidad no existe un tratado vinculante sobre IA militar: iniciativas como la Declaración de La Haya de 2023 o la Política de la Casa Blanca sobre responsabilidad en IA carecen de compromisos

concretos. Todo ello indica que la carrera tecnológica militar avanza más rápido que cualquier acuerdo ético o legal, por lo que la vigilancia civil y el debate institucional deben intensificarse para evitar consecuencias incontrolables.

La convergencia de los postulados de McRaven, Kilcullen y Van Creveld proporciona una base teórica sólida para comprender el papel de las Fuerzas Especiales en el siglo XXI. Los principios operativos de McRaven se ven potenciados por las capacidades que ofrecen las tecnologías disruptivas, mientras que la visión de Kilcullen sobre la guerra irregular subraya la necesidad de adaptarse a adversarios ágiles y tecnologizados. Por su parte, el enfoque de Van Creveld anticipa un escenario multidominio donde la supremacía ya no se logra únicamente por medios convencionales, sino mediante la integración sinérgica de capacidades tecnológicas, cognitivas y doctrinales. En el contexto colombiano, esta articulación teórica permite analizar cómo la incorporación de UAV, IA, ciberoperaciones y sistemas autónomos no solo amplía el alcance táctico de las Fuerzas Especiales, sino que redefine su doctrina para enfrentar amenazas híbridas, urbanas y transnacionales en un entorno globalizado(Lillbacka, 2014).

Conclusiones

La guerra especial se encuentra en un punto de inflexión estratégico, marcado por la incorporación de tecnologías disruptivas que están redefiniendo los paradigmas de combate, inteligencia y decisión táctica. Dentro de este espectro, los sistemas no tripulados, la inteligencia artificial (IA), la robótica autónoma, el big data y la computación cuántica son los principales vectores de transformación del entorno operacional. En los próximos diez

años, se prevé que las operaciones de guerra especial estarán profundamente mediadas por sistemas autónomos capaces de ejecutar misiones críticas con mínima intervención humana. Estos sistemas abarcarán desde *Unmanned Aerial Vehicles* (UAV) de reconocimiento con algoritmos de detección predictiva hasta plataformas robóticas terrestres con funciones ofensivas controladas por IA táctica. La integración de estos sistemas será facilitada por redes de comunicación de alta velocidad, 5G e incluso 6G, permitiendo una sincronización multi-dominio entre fuerzas especiales, unidades convencionales y medios cibernéticos.

El uso de sensores biométricos y nanotecnología en el equipamiento individual permitirá que los comandos de operaciones especiales monitoricen su salud, nivel de fatiga y señales ambientales en tiempo real, optimizando su desempeño en entornos hostiles. Asimismo, el combate cognitivo, entendido como el intento por alterar la percepción del adversario mediante técnicas informáticas avanzadas, se convertirá en un recurso clave, donde la guerra informacional, la manipulación de redes sociales y la generación de narrativas falsas adquirirán un nuevo nivel de sofisticación.El desarrollo de estas tecnologías no solo transformará la capacidad letal de las Fuerzas Especiales, sino también su doctrina operativa, ya que exigirá mayor integración con el ciberespacio, mayor adaptabilidad a entornos tecnológicos fluidos y una formación integral en ciencia de datos, ciberseguridad y ética de combate digital.

Las guerras del futuro estarán mediadas por plataformas automatizadas, decisiones algorítmicas y superioridad informacional. Un análisis prospectivo evidencia que las principales tendencias tecnológicas girarán en torno a cinco ejes: (1) la autonomía táctica, (2) la conectividad multisensorial, (3) la integración hombre-máquina, (4) el cibercontrol del

espacio electromagnético y (5) la convergencia entre inteligencia artificial y capacidades cinéticas.

Primero, los UAV y UAS están evolucionando de plataformas remotamente controladas a sistemas autónomos con capacidad de aprendizaje y adaptación en tiempo real. Un ejemplo paradigmático es el reciente anuncio del gobierno alemán sobre el suministro a Ucrania de 4.000 drones con IA autónoma, desarrollados por la empresa Helsing, que pueden ejecutar misiones sin necesidad de intervención humana directa (Werkhäuser, 2024). Este tipo de desarrollos marca el inicio de una era donde los enjambres de drones, dotados de capacidades de autoorganización, podrán ejecutar misiones complejas en zonas de combate urbano o selvas densas, como las que enfrenta Colombia.

Segundo, la evolución de los conflictos híbridos ha demostrado la necesidad de control del espectro electromagnético. Las operaciones en el ciberespacio y las capacidades de guerra electrónica se integrarán plenamente en las campañas de guerra especial, permitiendo neutralizar comunicaciones, sistemas GPS y sensores enemigos. Esta tendencia es especialmente relevante frente a amenazas asimétricas como las que enfrenta Colombia, donde grupos armados ilegales han comenzado a emplear drones comerciales modificados para tareas de vigilancia y ataque.

Tercero, la interfaz cerebro-máquina (BCI, por sus siglas en inglés) es una tendencia emergente que promete aumentar exponencialmente las capacidades de los operadores especiales, al facilitar una interacción directa con sistemas autónomos, reduciendo el tiempo de respuesta y mejorando la precisión de las acciones (Gibson, 2021). Si bien su aplicación militar aún está en etapa experimental, su adopción futura es altamente probable. Estas

tendencias proyectan un escenario de conflictos más tecnológicos, con ciclos operacionales más cortos, mayor precisión letal y desafíos éticos sin precedentes.

El contexto colombiano, caracterizado por amenazas híbridas, actores armados organizados y entornos geográficos adversos, demanda una transformación urgente en las Fuerzas Especiales del país. En este sentido, el Ejército Nacional ha iniciado avances importantes, como la creación del primer Batallón de Aeronaves No Tripuladas (BANOT), orientado a la gestión, mantenimiento, operación y neutralización de drones, en respuesta a los ataques perpetrados por grupos armados con UAVs modificados

En conclusión, el escenario futuro de la guerra especial estará dominado por la interacción de tecnología de punta con la doctrina militar. Las tecnologías disruptivas drones autónomos, inteligencia artificial, cibervigilancia, robótica avanzada, entre otros. prometen aumentar la capacidad operativa de las unidades de fuerzas especiales, amplificando su alcance, precisión y adaptabilidad. No obstante, ese mismo avance impone una doble exigencia: por un lado, es urgente que las Fuerzas Especiales colombianas continúen incorporando innovación (como lo demuestra la creación del BANOT y la adopción de sistemas cibernéticos) para no perder ventaja operativa; por otro, deben hacerlo dentro de un marco ético y estratégico que preserve el control humano y minimice riesgos colaterales.

Los casos recientes en Colombia y en el mundo muestran que la respuesta rápida y coordinada (asociación con aliados, capacitación continua, actualización doctrinal) es esencial para enfrentar amenazas emergentes. En definitiva, la eficacia futura de las operaciones especiales dependerá de un balance dinámico: integrar creativamente la innovación tecnológica disruptiva mientras se refuerzan los mecanismos de ética, transparencia y responsabilidad que eviten que los sistemas armados escapen al control

humano. Solo así las Fuerzas Especiales podrán mantener su ventaja estratégica en un entorno de conflicto cada vez más complejo y tecnificado.

Referencias

Adamski, M. (2020). Effectiveness analysis of UCAV used in modern military conflicts. *Aviation*, *24*(2). https://doi.org/10.3846/aviation.2020.12144

Aravena, F. M. A. (2024). Dilemas derivados del uso de sistemas autónomos de armas letales en el derecho internacional humanitario. *Justicia*, *29*(45). https://doi.org/10.17081/just.29.45.7143

Bernal, V. O. M., & Salgado, L. I. U. (2024). Operaciones de Fuerzas Especiales frente a sistemas de amenazas basados en guerra política y guerra de información. In *Comandos. Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 115–139). Escuela Superior de Guerra. https://doi.org/10.25062/9786287602809.05

Centro Conjunto de Desarrollo de Conceptos. (2020). *Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R)*. https://publicaciones.defensa.gob.es/media/downloadable/files/links/u/s/usos_militares_inteligencia_artificial.pdf

Cepeda, B. (2025). *El Ejército de Colombia avanza en diseño y creación de su primer Batallón de Aeronaves No Tripuladas para la lucha contra drones. Zona Militar.* https://www.zona-militar.com/2025/07/09/el-ejercito-de-colombia-avanza-en-diseno-y-creacion-de-su-primer-batallon-de-aeronaves-no-tripuladas-para-la-lucha-contra-drones/

De Biasio, M., Arnold, T., Leitner, R., McGunnigle, G., & Meester, R. (2010). UAV-based environmental monitoring using multi-spectral imaging. *Airborne Intelligence, Surveillance, Reconnaissance (ISR) Systems and Applications VII*, *7668*. https://doi.org/10.1117/12.864470

Ejército Nacional de Colombia. (2007). Resolución núm. XXXX de 2007: Por la cual se aprueba el "Manual de Misiones de Fuerzas Especiales". . *Comando Del Ejército Nacional.*

El País. (2024). Drones que lanzan bombas: la nueva etapa del conflicto colombiano. *El País*. https://elpais.com/america-colombia/2024-06-19/drones-que-lanzan-bombas-la-nueva-etapa-del-conflicto-colombiano.html

Evans, M. (2012). The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One. *Small Wars & Insurgencies*, *23*(1). https://doi.org/10.1080/09592318.2012.632871

Foggo, J., Merwe, J., & Luzum, N. (2022). Elevando nuestra ventaja: Un camino hacia la integración de tecnologías emergentes y disruptivas. . *Centro de Análisis de Políticas Europeas (CEPA).* . https://cepa.org/comprehensive-reports/elevating-our-edge-a-path-to-integrating-emerging-and-disruptive-technologies/

Freire, T., & García, M. (2024). Optimización de cobertura con UAVs para situaciones de emergencia . *Trabajo de Grado, Universidad*. https://repositorio.uniandes.edu.co/entities/publication/0109aa6b-df30-4aa1-a9c0-661a6b6b64b6

Gallois, F. (2018). Drone de neutralisation chirurgicale à réponse graduée. *Revue Défense Nationale*, *N° Hors-série*(HS1). https://doi.org/10.3917/rdna.hs04.0083

Gómez, E. H. (2021). Capacidades de las Fuerzas Militares de Colombia en escenarios de asistencia humanitaria y respuesta a desastres. *Estudios En Seguridad y Defensa*, *16*(32), 319–342. https://doi.org/10.25062/1900-8325.317

Gonzalez, L. M. (2011). La interoperabilidad en las operaciones conjuntas y combinadas de defensa aeroespacial. *Escuela Superior de Guerra Conjunta*.

Hordiichuk, V., Andriianova, N., & Peredrii, O. (2023). The joint all-domain command and control system as the basis of the multi-domain operations of concept for the defence of Ukraine. In *Theoretical And Applied Aspects Of The Russian-Ukrainian War: Hybrid Aggression And National Resilience*.

Jordán, J. (2021). Innovación y revolución en los asuntos militares: una perspectiva no convencional. *Seguridad, Ciencia & Defensa*, *2*(2). https://doi.org/10.59794/rscd.2016.v2i2.pp127-140

Lillbacka, R. (2014). Special Operations Principles and Finnish Long Range Patrols during WWII. *Journal of Military Studies*, *5*(2). https://doi.org/10.1515/jms-2016-0191

Maldonado, C. E. (2024). Ciencias de punta y tecnologías disruptivas en el ciberespacio y su impacto para la ciberdefensa de Colombia. In *Tecnologías disruptivas, logística, seguridad y defensa en el ciberespacio* (pp. 111–142). Escuela Superior de Guerra. https://doi.org/10.25062/9786287602700.04

Manolache, I. C. (2023). The Role of Multi-Domain Operations in Modern Warfare. *Land Forces Academy Review*, *28*(3). https://doi.org/10.2478/raft-2023-0020

Marín, D. J. A. (2021). Guerra de drones en el Cáucaso Sur: lecciones aprendidas de Nagorno Karabaj. *Bie3: Boletín IEEE, 21*.

Morales, C. L. (2021). Uso de tecnologías disruptivas con BIM (Building Information Modelling). *Revista Tecnología En Marcha*. https://doi.org/10.18845/tm.v34i7.6017

Narváez, A. H. A. (2024). Las Fuerzas Especiales del Ejército Nacional de Colombia y su aporte a la Seguridad y Defensa Nacional. *Revista Estado, Paz y Sistema Internacional*, *3*(5), 27–43. https://doi.org/10.25062/2981-3034.4858

Palacios, C. (2024). La II Guerra del Nagorno Karabaj (2020): Breve análisis de las consecuencias geopolíticas y militares del empleo del arma dron. . *Universidad San Pablo-CEU.* https://d1wqtxts1xzle7.cloudfront.net/113630405/Rodrigo_Palacios_Trabajo_GyP-libre.pdf?1713795407=&response-content-disposition=inline%3B+filename%3DLa_II_Guerra_del_Nagorno_Karabaj_breve_a.pdf&Exp

ires=1738136834&Signature=A5NTTSHNm1EzQ8ZvQTYN3NQacajQBZ0YfMyyVmR~wGLbzvlmUKgEasSMhvZGoDGHgFGC8NEIW64WrfIDRDDBn3mUVssbarJY-7rHdBpwnSvlvpuH6mwMEVtdwzaPPHNnWU6hhNV1~lwoD2Ykkrnmg95kIyW2bo95TkVYkGY7hxW9hpMLXdz6gsiZvAtEamUgPib9JjP~sJVkRgyyVALFWMsPZL5NfI~5vXZBZklMfb09EDixfHDOA~MZ3s0l6ygt5f51-18zI0jvNHtK9jkuksDHkK2zixuX3REZz~DJ6kLmbTeHObt1Y6IEPYEt01p0j~Xx3HwM6aI-sXPkWhbtTg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Panigrahi, N., & Tripathy, S. (2021). Design Criteria of a UAV for ISTAR and Remote Sensing Applications. *Journal of the Indian Society of Remote Sensing*, *49*(3). https://doi.org/10.1007/s12524-020-01249-7

Peña, suarez, J. stiven. (2023). Ciberseguridad, un desafío para las Fuerzas Militares colombianas en la era digital. *Perspectivas En Inteligencia*, *15*(24), 333–359. https://doi.org/10.47961/2145194X.628

Pugliese, P., & Griffini, B. (2021). Implicaciones del uso de los Sistemas de Armas Autónomas Letales (Laws) en los conflictos armados modernos. *Perspectivas Revista de Ciencias Sociales*, *11*, 383–404. https://doi.org/10.35305/prcs.vi11.456

Roberts, D., & Capezzuto, R. (1999). AGM-114 hellfire missile system and FLIR/LASER test and integration on the H-60 aircraft. *IEEE Aerospace Applications Conference Proceedings*, *3*. https://doi.org/10.1109/aero.1999.789765

Rodríguez, F. P. (1992). La Guerra del Golfo Pérsico: 1990-1991. Las nuevas formas de hacer la guerra. La utilización de la prensa como estrategia de enseñanza por descubrimiento. *Campo Abierto*, *9*.

Rodríguez, & Garzón, G. O. A. (2024). Amenazas cibernéticas contemporáneas: retos y desafíos para las operaciones especiales en Colombia. In *Comandos. Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 93–113). Escuela Superior de Guerra. https://doi.org/10.25062/9786287602809.04

Rosen, S. D. (2010). A Review of: "David Kilcullen. The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One ." . *Terrorism and Political Violence*, *22*(3). https://doi.org/10.1080/09546553.2010.485114

Saumeth. (2024). *Colombia recibe 25 drones tácticos donados por Estados Unidos. Infodefensa.* https://www.infodefensa.com/texto-diario/mostrar/4688962/016-colombia-colombia-recibe-25-drones-tacticos-donados-estados-unidos#:~:text=potencialmente%20riesgosos

Saunders, P. C., & Lutes, C. D. (2007). China's ASAT: Test Motivations and Implications. *National Defense University Press - Joint Force Quarterly*, *1*(46).

Serna, J., Montero, M. L. A., & González, M. A. (2024). Fuerzas Especiales en la guerra contemporánea. In *Comandos. Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 13–31). Escuela Superior de Guerra. https://doi.org/10.25062/9786287602809.01

Takabatake, F. (2024). NATO's Approach to Multi-Domain Operations: From the Perspective of the Economics of Alliances. *Defence and Peace Economics*, *35*(3). https://doi.org/10.1080/10242694.2023.2235502

Tawil Kuri, M. (2009). Diálogos de política exterior. El eje tripartita sirio-saudita-egipcio y la política de poder de Siria 1991-2007. *Estudios de Asia y África*. https://doi.org/10.24201/eaa.v44i2.1957

Van Creveld, M. (2002). The transformation of war revisited. *International Journal of Phytoremediation*, *13*(2). https://doi.org/10.1080/09592310208559177

Vera, P. D., Prieto, A. P., & Garzón, D. (2023). Los cambios tecnológicos y su impacto en las estrategias de seguridad y defensa. In *Transición del orden mundial: Impactos en las estrategias de seguridad y defensa en Colombia y la región*. https://doi.org/10.25062/9786287602489.06

Warner, M. (2022). US Cyber Command's First Decade. In *The United States' Defend Forward Cyber Strategy*. https://doi.org/10.1093/oso/9780197601792.003.0004

Werkhäuser, N. (2024). *Alemania entregará a Ucrania 4.000 drones controlados con IA. Deutsche Welle.* . https://www.dw.com/es/alemania-entregar%C3%A1-a-ucrania-4000-drones-controlados-con-ia/a-70825862#:~:text=Es%20el%20software%20lo%20que,de%20un%20piloto%20a%20distancia