Uso de la IA por Disidencias en la Frontera Colombo-Ecuatoriana del Putumayo

Mayor (EJC) Belisario Zea Quintero

Artículo para optar al título profesional:

Magister en Estrategia y Geopolítica

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

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

DATOS GENERALES		
Nombre del estudiante	**:**	Mayor (EJC) Belisario Zea Quintero
Identificación	**:**	8063761
Programa académico	**:**	Maestría en Estrategia y Geopolítica
Tutor metodológico	**:**	Mayor (R) Oscar Orlando Porras Rodríguez
Tutor temático	**:**	Capitán de Corbeta Jesús Ramón Ramos Galindo
Fecha de entrega	**:**	29 de agosto de 2025
Extensión	**:**	7.820 palabras

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

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

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

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

AUTORIZACIÓN DE PUBLICACIÓN

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

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

Uso de la IA por Disidencias en la Frontera Colombo-Ecuatoriana del Putumayo

Use of AI by Dissidents on the Colombian-Ecuadorian Border in Putumayo

Belisario Zea Quintero[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: La inteligencia artificial se ha convertido en una herramienta estratégica utilizada por disidencias armadas en la frontera colombo-ecuatoriana del Putumayo, potenciando sus capacidades operativas y dificultando la acción de las fuerzas del Estado. Este trabajo, de carácter cualitativo y documental, examina cómo estas organizaciones ilegales han incorporado tecnologías basadas en IA para actividades como vigilancia con drones, análisis de patrones militares y comunicaciones seguras. La investigación se apoya en la teoría del riesgo social de Niklas Luhmann, la cual permite interpretar estos avances como factores que incrementan la complejidad y los desafíos de seguridad nacional. A través del análisis de fuentes académicas, informes institucionales y estudios recientes, se identifican los principales usos de la IA por parte de estos grupos y sus implicaciones en el contexto fronterizo.

Palabras clave: Conflicto armado; defensa nacional; fronteras; inteligencia artificial; seguridad; tecnología militar.

Abstract: Artificial intelligence has become a strategic tool used by armed dissident groups along the Colombia–Ecuador border in the Putumayo region, enhancing their operational capabilities and hindering the efforts of state security forces. This qualitative and documentary-based study examines how these illegal organizations have incorporated AI-driven technologies into activities such as drone surveillance, analysis of military patterns, and secure communications. The research is grounded in Niklas Luhmann's theory of social risk, which allows for an interpretation of these technological advances as factors that increase complexity and pose new challenges to national security. Through the analysis of academic literature, institutional reports, and recent case studies, the main uses of AI by these groups are identified, along with their implications in the border context.

Keywords: Armed conflict; national defense; borders; artificial intelligence; security; military technology.

[1] Coronel 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.

Introducción

El desarrollo acelerado de tecnologías emergentes como la inteligencia artificial (IA) ha transformado profundamente los escenarios de seguridad y defensa en el mundo. Su aplicación en el ámbito militar no es exclusiva de los Estados, pues grupos armados ilegales también han empezado a incorporar estas herramientas en sus estrategias operativas. En la frontera colombo-ecuatoriana del Putumayo, región marcada por una histórica presencia de economías ilícitas, control territorial y violencia armada, las disidencias de las FARC han comenzado a integrar soluciones basadas en IA con fines tácticos y logísticos. Esta situación ha generado nuevos desafíos para la seguridad nacional, incrementando el riesgo operativo para las fuerzas militares y dificultando la gobernanza estatal dificultando la gobernanza estatal y exigiendo nuevas capacidades institucionales.

En los últimos años, diversos informes nacionales e internacionales han advertido sobre el uso de drones, sistemas de reconocimiento facial, encriptación de comunicaciones y análisis predictivo por parte de grupos irregulares. Estas prácticas evidencian una evolución tecnológica del conflicto armado que aún no ha sido completamente abordada desde la academia ni desde la política pública. Frente a este fenómeno, se hace necesario un análisis riguroso que permita comprender cómo estas tecnologías están siendo empleadas, qué riesgos representan y qué respuestas institucionales podrían ser efectivas.

El escrito se fundamenta en la teoría del riesgo social de Niklas Luhmann, la cual permite analizar cómo los avances tecnológicos generan nuevas fuentes de inestabilidad y reconfiguran las amenazas a la seguridad nacional. Desde un enfoque cualitativo y mediante análisis documental, este estudio tiene como objetivo identificar los principales usos de la

inteligencia artificial por parte de disidencias armadas en la frontera colombo-ecuatoriana, y plantear recomendaciones estratégicas para el fortalecimiento de la respuesta estatal en este escenario complejo.

La región del Putumayo, caracterizada por una geografía selvática y de difícil acceso, ha sido históricamente un corredor estratégico para el narcotráfico y otras economías ilícitas. Su localización limítrofe con Ecuador y su debilidad institucional la convierten en un espacio propicio para la operación de actores armados no estatales, quienes aprovechan las zonas grises de soberanía y las brechas en la cooperación bilateral para consolidar su presencia. En este contexto, la incorporación de tecnologías como la IA representa una ventaja asimétrica significativa para las disidencias, al facilitar la recolección de inteligencia, la evasión de operativos militares, y la optimización de rutas logísticas en áreas donde el Estado tiene una capacidad limitada de control.

Además, la frontera colombo-ecuatoriana no solo es un espacio físico sino también un escenario geopolítico de alta complejidad. La debilidad de los mecanismos de coordinación transfronteriza y la asimetría en las capacidades de defensa entre ambos países contribuyen a que este territorio se consolide como un laboratorio de prácticas criminales innovadoras. La inteligencia artificial, utilizada de forma clandestina por las disidencias, introduce nuevas lógicas en el conflicto, en tanto que permite anticipar patrones de patrullaje, identificar blancos de alto valor y manipular entornos digitales para desinformar o distraer a las autoridades.

Así las cosas, el presente trabajo se inscribe, por tanto, en una línea de análisis estratégica y geopolítica que busca aportar herramientas conceptuales y empíricas para la toma de decisiones en el ámbito de la defensa nacional. La amenaza no es solo tecnológica,

sino también política y social, en tanto que redefine la relación entre el Estado, el territorio y la soberanía en contextos periféricos. Comprender la interacción entre innovación tecnológica y violencia armada es un imperativo para anticiparse a las nuevas formas de guerra híbrida que emergen en América Latina, y en especial en Colombia, donde las disidencias han demostrado una notable capacidad de adaptación y resiliencia operativa.

Metodología

El enfoque metodológico seleccionado para esta investigación es cualitativo (Sampieri, Fernández, & Lucio, 2000), ya que se centra en el análisis profundo y detallado de los datos obtenidos de fuentes documentales. Este enfoque permite comprender de manera integral el fenómeno del uso de la inteligencia artificial por parte de disidencias en la frontera colombo-ecuatoriana, desde una perspectiva contextual y teórica. El método cualitativo es ideal para analizar conceptos complejos, relaciones entre actores y el impacto de las tecnologías avanzadas en la seguridad nacional.

El diseño de la investigación será descriptivo y documental, enfocado en la revisión y análisis de informes técnicos, artículos académicos, documentos gubernamentales y reportes de organismos internacionales especializados en seguridad y defensa. Este diseño busca describir cómo las disidencias han integrado la inteligencia artificial en sus operaciones y analizar los posibles riesgos y desafíos para las estrategias de defensa.

La selección de fuentes se llevará a cabo a través de un muestreo por conveniencia, el cual permitirá elegir documentos clave que aporten información relevante y actualizada sobre el tema de estudio. Se priorizarán fuentes que aborden el uso de tecnologías emergentes en el ámbito de la seguridad y defensa, así como informes sobre la situación de seguridad en la frontera colombo-ecuatoriana.

Los instrumentos de recolección de datos estarán basados en el análisis documental de las fuentes seleccionadas. Este análisis permitirá identificar patrones, relaciones y argumentos relevantes para el desarrollo del marco teórico y el cumplimiento de los objetivos de la investigación. Se utilizará un esquema de categorización para organizar la información

de acuerdo con los temas principales: tecnologías aplicadas, riesgos emergentes y estrategias de respuesta.

Los criterios de inclusión considerarán documentos académicos y técnicos publicados en los últimos 10 años, que aborden específicamente la relación entre tecnologías avanzadas, seguridad y el contexto fronterizo. Por su parte, los criterios de exclusión dejarán fuera las fuentes sin respaldo académico o institucional, así como aquellas que no aporten información específica al estudio. Este enfoque metodológico garantizará un análisis riguroso y contextualizado del fenómeno investigado.

Herramientas de inteligencia artificial empleadas por las disidencias en la región.

El avance acelerado de las tecnologías digitales ha transformado no solo las dinámicas estatales de seguridad, sino también las de los grupos armados ilegales, quienes han comenzado a adoptar herramientas de inteligencia artificial para mejorar sus capacidades operativas. En el caso específico de la frontera colombo-ecuatoriana del Putumayo, región históricamente afectada por el narcotráfico, la economía ilegal y la débil presencia institucional, se ha identificado el uso creciente de tecnologías como drones autónomos, sistemas de vigilancia inteligente y algoritmos de análisis predictivo por parte de las disidencias de las FARC y otros actores armados. Según la Defensoría del Pueblo (2024), el control territorial ejercido por estos grupos no solo se mantiene por la vía armada, sino también mediante la integración progresiva de capacidades tecnológicas sofisticadas, muchas de ellas difíciles de rastrear por las fuerzas estatales.

Drones autónomos y vigilancia automatizada

Una de las herramientas más ampliamente utilizadas por las disidencias en el contexto colombiano es el drone autónomo equipado con sensores, cámaras y software de navegación inteligente. Según el estudio de Cano Cuevas (2023), los drones no tripulados se han convertido en dispositivos tácticos clave para la vigilancia de rutas del narcotráfico, identificación de tropas enemigas y planificación de ataques con mínima exposición humana. Su bajo costo, la posibilidad de vuelo a baja altitud y su capacidad para cargar explosivos o realizar reconocimiento aéreo convierten a estos dispositivos en una herramienta versátil para grupos ilegales.

Estos drones integran algoritmos que permiten autonomía en la navegación, evitación de obstáculos y transmisión de imágenes en tiempo real. Este uso también ha sido reportado por Ownby (2024), quien documenta cómo algunos grupos criminales han adaptado drones comerciales para lanzar explosivos improvisados sobre objetivos específicos, fenómeno observado en zonas del Cauca y Putumayo. A través de esta herramienta, las disidencias logran superioridad táctica en territorios difíciles de controlar por el Estado, reafirmando así su dominio y capacidad de movilidad.

En zonas urbanas bajo control criminal, se ha reportado la instalación de cámaras de videovigilancia controladas por sistemas autónomos de análisis visual. Estos sistemas, como lo indican Cuenca (2023) y Guzmán (2024), integran IA para detectar comportamientos inusuales, presencia de vehículos estatales o reuniones sospechosas. El acceso a software comercial de video seguimiento, muchas veces vulnerado desde plataformas abiertas, ha permitido que los grupos ilegales repliquen sistemas urbanos de vigilancia sin necesidad de infraestructura estatal.

Este tipo de vigilancia no solo sirve para la defensa, sino también como método de disuasión, ya que las comunidades perciben que cualquier acción puede estar siendo monitoreada. Esta forma de "seguridad criminal" reproduce lógicas de control similares a las del Estado, pero al margen del orden legal, perpetuando la ocupación territorial.

Como se resume en la Tabla 1, las disidencias han adoptado diversas herramientas de IA con fines tácticos y operativos, abarcando desde vigilancia aérea hasta análisis predictivo.

Tabla 1 Herramientas de inteligencia artificial utilizadas por disidencias

Herramienta de IA	Aplicación principal	Impacto estratégico
Drones autónomos	Vigilancia aérea y reconocimiento de terreno	Alto
Redes neuronales artificiales	Predicción de zonas y patrones de delito	Medio
Sistemas de reconocimiento facial	Identificación de objetivos y evasión de autoridades	Alto
Análisis de big data y patrones	Procesamiento de datos operacionales	Medio
Algoritmos predictivos espaciotemporales	Identificación de puntos críticos del delito	Alto
Videovigilancia inteligente	Monitoreo en tiempo real en zonas urbanas	Medio
Sistemas de rastreo GPS	Seguimiento de movimientos de actores armados	Alto
Deep learning para análisis de comportamiento	Simulación de eventos y respuesta anticipada	Medio
Análisis de redes sociales	Detección de amenazas a partir de publicaciones	Bajo
Mapas de calor delictivo (GIS)	Visualización de zonas con alta actividad criminal	Medio

Nota: Diseñada por el autor con referencia a los documentos consultados de Cano Cuevas (2023).

La Tabla 1 presenta una clasificación de diez herramientas de inteligencia artificial utilizadas por disidencias armadas, especificando su aplicación operativa principal y el nivel estimado de impacto estratégico. Esta matriz permite visualizar cómo cada tecnología contribuye al fortalecimiento de las capacidades tácticas en contextos de conflicto irregular.

Algoritmos predictivos y análisis de patrones delictivos

Otra herramienta clave es el uso de algoritmos de machine learning y redes neuronales para anticipar operativos militares y planear rutas seguras de tráfico ilícito. Según Barragán-Huamán et al. (2022), el uso de modelos matemáticos predictivos permite establecer mapas de calor delictivo, identificar patrones espaciotemporales y tomar decisiones con base en probabilidad de acción enemiga. Estas herramientas se alimentan de datos históricos de presencia militar, monitoreo de redes sociales, cambios de rutina y desplazamientos sospechosos.

El empleo de estos algoritmos ofrece una ventaja sustancial para los grupos ilegales, ya que pueden anticiparse a la lógica de las fuerzas de seguridad e incluso simular escenarios futuros, optimizando su movilidad y evitando emboscadas. Esta capacidad de predicción, al ser descentralizada y basada en software de código abierto, es difícil de rastrear y neutralizar, lo cual representa un desafío significativo para la seguridad nacional.

En escenarios de combate irregular, el control de identidad es fundamental. Las disidencias han comenzado a utilizar tecnologías de reconocimiento facial inverso para identificar posibles infiltrados o informantes. Según Las Heras (2023), algunos grupos armados han accedido a bases de datos filtradas o software de reconocimiento facial mediante la dark web, aplicándolos en sus sistemas internos de control poblacional o incluso en puntos de retención.

Además, el anonimato digital se ha convertido en una prioridad operativa. Herramientas de suplantación de identidad mediante deepfakes, como menciona Orgaz (2024), permiten la creación de perfiles falsos creíbles en redes sociales, útiles para la recolección de información y labores de desinformación. Estas tecnologías, inicialmente diseñadas con fines comerciales o recreativos, han sido reapropiadas por actores armados para fines tácticos, dificultando aún más la labor de inteligencia humana.

El rastreo de redes sociales mediante herramientas de minería de datos y análisis de sentimientos es otra aplicación avanzada de la IA. Según Ruiz (2024), los grupos armados monitorean Facebook, WhatsApp y Telegram para identificar puntos de control militar, movimientos de actores institucionales o simplemente para generar narrativas que respalden su legitimidad ante comunidades vulnerables. Esto se complementa con herramientas de

análisis semántico que permiten detectar palabras clave, hashtags o ubicaciones, facilitando la toma de decisiones operativas en tiempo real.

Estos mecanismos también son empleados para campañas de desinformación que buscan confundir o dividir a las comunidades locales respecto al accionar del Estado, favoreciendo el control social y psicológico de los territorios en disputa. Esta dimensión híbrida del conflicto, donde la guerra no solo se libra en el terreno sino también en el plano digital, complejiza aún más la intervención estatal.

Sistemas de georreferenciación y rastreo de movimiento

El uso de sistemas de posicionamiento global (GPS) combinados con inteligencia artificial ha sido documentado como una práctica común en operaciones logísticas de los grupos armados. Estas tecnologías les permiten rastrear en tiempo real los desplazamientos de tropas, monitorear cargamentos ilegales y coordinar rutas de escape. En algunos casos, según evidencia presentada por Conde y Orbe (2020), las disidencias han implementado tecnologías de georreferenciación para asegurar el paso seguro de cargamentos de droga o para guiar incursiones tácticas con precisión milimétrica, especialmente en terrenos selváticos donde las condiciones del entorno dificultan la navegación tradicional.

La integración de IA a estos sistemas potencia su capacidad al permitir el análisis automático de trayectorias, el reconocimiento de patrones de vigilancia y la adaptación en tiempo real a cambios en la dinámica operativa. Esto reduce los márgenes de error y facilita operaciones encubiertas, consolidando el control territorial en zonas rurales y de frontera.

Otro elemento relevante es la utilización de plataformas de análisis multifuente, que integran datos provenientes de sensores, comunicaciones, redes sociales, y reportes del terreno para construir un panorama operativo más preciso. Estas herramientas,

frecuentemente empleadas por fuerzas militares modernas, están siendo replicadas por organizaciones armadas ilegales mediante software de libre acceso y recursos del mercado negro digital.

Como lo explica Cuenca (2023), la IA aplicada al análisis de seguridad tiene la capacidad de relacionar eventos aparentemente desconectados, identificar correlaciones e incluso anticipar reacciones institucionales. Esta capacidad para construir inteligencia táctica descentralizada brinda una ventaja significativa a las disidencias, pues reduce su dependencia de estructuras jerárquicas tradicionales y les permite actuar con agilidad y autonomía.

La teoría del riesgo social de Niklas Luhmann, fundamento teórico de este estudio, permite entender cómo estas innovaciones tecnológicas reconfiguran el sistema de seguridad, creando amenazas que no se originan en la potencia del armamento sino en la capacidad de anticipación, evasión y manipulación del entorno. De este modo, la IA se convierte en un generador de riesgo sistémico, desafiando los esquemas clásicos de respuesta militar y obligando a repensar las doctrinas de defensa en escenarios híbridos.

Análisis de casos recientes del uso de IA por disidencias y su impacto en las estrategias militares

La frontera colombo-ecuatoriana del departamento del Putumayo constituye un espacio geoestratégico de alta sensibilidad para la seguridad nacional de Colombia. Esta región, ubicada en el suroccidente del país, presenta una combinación crítica de factores: geografía selvática, débil presencia estatal, economías ilícitas consolidadas, y dinámicas de violencia prolongada (Arce, 2025). A lo largo de las últimas décadas, este territorio ha sido escenario de confrontaciones armadas, operaciones de control territorial y disputas entre grupos armados ilegales por el dominio de corredores estratégicos de movilidad y financiación.

Uno de los principales actores en este entorno son las disidencias de las FARC, estructuras armadas que no se acogieron al Acuerdo de Paz de 2016 o que posteriormente se rearmaron tras su incumplimiento. Estas disidencias han reconfigurado su presencia territorial en departamentos como Putumayo, Nariño y Caquetá, consolidando enclaves de control social, normativo y económico. Su actividad se articula principalmente con el narcotráfico, la minería ilegal, la extorsión y el contrabando, lo que les proporciona recursos financieros sustanciales y capacidad de corrupción institucional. Además, mantienen vínculos con redes internacionales del crimen organizado, incluyendo cárteles de México y estructuras armadas del lado ecuatoriano de la frontera (Bonilla, 2025).

Desde el punto de vista de la seguridad operativa, esta región enfrenta una amenaza de carácter híbrido, entendida como aquella que combina métodos convencionales e irregulares, elementos tecnológicos y tácticas no lineales. En el Putumayo, esta amenaza se manifiesta en la mezcla de violencia armada, propaganda digital, cooptación comunitaria,

empleo de tecnologías disruptivas y uso instrumental de la geografía para evadir el control del Estado. La complejidad de este escenario se intensifica por la dificultad de acceso terrestre, la escasa cobertura institucional en muchos municipios, y la existencia de rutas fluviales que facilitan el transporte de cargamentos ilícitos hacia Ecuador y el Pacífico sur colombiano.

En este contexto, la movilidad transfronteriza emerge como una de las principales variables estratégicas. Como lo señalan Olaya (2019) y Sánchez (2014), las comunidades afrocolombianas, campesinas e indígenas que habitan en la zona desarrollan prácticas de tránsito diario, comercio informal e intercambio cultural a través de pasos no regulados. Estas dinámicas sociales, lejos de ser nuevas, han sido históricamente utilizadas por los grupos armados ilegales como camuflaje para sus operaciones logísticas. La frontera, por tanto, no solo representa una línea geográfica, sino una zona difusa de interacción constante entre legalidad e ilegalidad, donde la soberanía estatal es frecuentemente cuestionada.

La baja densidad estatal expresada en la insuficiencia de efectivos de fuerza pública, la limitada cobertura de servicios básicos, la corrupción local y la debilidad institucional crea un vacío de gobernabilidad que es aprovechado por las disidencias para implementar formas paralelas de autoridad. Estos grupos imponen reglas, recaudan tributos, administran justicia de facto y controlan el flujo de bienes y personas, generando una fragmentación del orden estatal (BBC, 2024). Esta fragmentación se convierte en el terreno fértil para el despliegue de nuevas tecnologías, como la inteligencia artificial, aplicadas de forma clandestina para fortalecer las capacidades delictivas de estos actores.

En síntesis, el Putumayo y su frontera sur con Ecuador configuran un teatro de operaciones donde confluyen elementos convencionales del conflicto armado con componentes innovadores del crimen organizado transnacional (Parada, 2024). Su relevancia estratégica para las disidencias radica en su valor como corredor logístico vital para la producción, transporte y exportación de clorhidrato de cocaína, así como en su utilidad para el repliegue táctico, el ocultamiento de armamento, y el establecimiento de economías de enclave. Comprender estas condiciones resulta indispensable para anticipar el impacto que el uso de inteligencia artificial por parte de estas estructuras puede tener sobre las estrategias militares del Estado colombiano (Conde & Orbe, 2020).

Modalidades tecnológicas empleadas por las disidencias armadas

El proceso de modernización bélica en Colombia no ha sido exclusivo de las fuerzas regulares. Las disidencias de las FARC, al igual que otras organizaciones criminales de carácter transnacional, han incorporado nuevas tecnologías a sus esquemas de operación. La inteligencia artificial (IA), en sus diferentes formas, ha comenzado a desempeñar un rol instrumental en la redefinición de las capacidades tácticas, logísticas y de comunicación de estos actores (Saavedra, 2024). Esta evolución plantea un escenario de asimetría tecnológica inversa, donde grupos armados irregulares aprovechan herramientas digitales avanzadas para compensar su inferioridad frente al poder convencional del Estado.

Una de las principales modalidades identificadas es el uso de drones con capacidades de automatización y navegación autónoma, utilizados para misiones de vigilancia, reconocimiento y ataque. Según Ownby (2024), se han registrado casos en el sur del país donde drones artesanales, modificados con sistemas básicos de IA, han sido empleados para lanzar artefactos explosivos sobre posiciones militares. Estos dispositivos permiten a las

disidencias mantener la distancia física del objetivo, disminuir el riesgo de bajas propias y recolectar información en tiempo real sobre movimientos operacionales de la Fuerza Pública. El uso de sensores térmicos, cámaras infrarrojas y trayectorias programadas ha sido reportado por organismos de inteligencia en zonas como Puerto Asís, Orito y Valle del Guamuez.

Otra modalidad preocupante es la aplicación de software de reconocimiento facial y vigilancia predictiva, empleada por estas estructuras para identificar informantes, blancos de secuestro o funcionarios públicos estratégicos. Investigaciones como las de Huamán et al. (2022) y Cuenca (2023) han documentado cómo, a través de cámaras instaladas clandestinamente en cascos urbanos o mediante hackeo de bases de datos locales, estas organizaciones logran establecer patrones de movilidad y horarios. Esta práctica incrementa el riesgo sobre la seguridad personal de agentes estatales y debilita el aparato de inteligencia civil y militar, que se ve expuesto a filtraciones o contrainteligencia encubierta.

Asimismo, las disidencias han recurrido a plataformas de comunicación cifrada, potenciadas por inteligencia artificial para evadir la interceptación de señales. Aplicaciones como Signal, Element o Wickr, combinadas con sistemas de criptografía de última generación, permiten conversaciones encriptadas que dificultan los procesos tradicionales de SIGINT (inteligencia de señales). Algunos reportes apuntan a que estas redes son reforzadas por algoritmos de destrucción automática de mensajes o enmascaramiento de metadatos, lo que hace prácticamente imposible el rastreo de conversaciones sin acceso físico a los dispositivos (Rodriguez, 2024).

Un aspecto menos visible pero igualmente alarmante es la instrumentalización de la IA para operaciones de propaganda y desinformación digital. A través de bots, redes sociales falsas y contenido audiovisual generado por IA generativa, las disidencias difunden discursos de legitimación, siembran narrativas contrarias al Estado y promueven divisiones entre las comunidades locales. Newton (2024) y Orgaz (2024) describen cómo estas campañas persuasivas influyen en la percepción del conflicto, dificultan la acción institucional y consolidan la autoridad social de los grupos armados en territorios disputados.

De ese modo, emergen indicios del uso experimental de inteligencia artificial para análisis geoespacial y logístico, con el fin de planificar rutas de tráfico de drogas o ubicar campamentos con menor probabilidad de detección. Estos sistemas, que cruzan variables como topografía, cobertura boscosa, presencia de tropas o intensidad de lluvias, permiten una toma de decisiones más precisa, disminuyendo la vulnerabilidad operativa de estas estructuras criminales (Heras, 2023).

En conjunto, estas modalidades evidencian que la inteligencia artificial ha dejado de ser un elemento exclusivo del desarrollo estatal para convertirse en un multiplicador de poder irregular. Su incorporación por parte de las disidencias no solo incrementa su letalidad, sino que también obliga a una transformación urgente de la doctrina militar, particularmente en lo que se refiere a guerra electrónica, ciberseguridad operativa y adaptación al entorno de conflicto híbrido (Matiz & Fernández, 2023). La comprensión detallada de estas herramientas es clave para anticiparse, neutralizar y rediseñar las estrategias de defensa en los territorios más vulnerables del país.

Casos documentados de afectación a la estrategia militar

El uso creciente de inteligencia artificial por parte de las disidencias de las FARC en zonas como el Putumayo no solo evidencia un proceso de sofisticación tecnológica, sino que introduce nuevas formas de amenaza híbrida que alteran directamente la planificación y ejecución de operaciones militares. En la siguiente tabla se resumen las principales modalidades tecnológicas detectadas, el uso específico que estas estructuras irregulares hacen de ellas y su impacto sobre la estrategia militar del Estado colombiano:

Tabla 2

Modalidades tecnológicas empleadas por disidencias armadas

Modalidad tecnológica	Uso por disidencias	Impacto en la estrategia militar
Drones con IA para reconocimiento y ataque	Vigilancia aérea, lanzamiento de explosivos, patrullaje automatizado	Reducción de efectividad del control aéreo y anticipación del enemigo
Vigilancia predictiva y reconocimiento facial	Identificación de objetivos, rutinas y posibles informantes	Aumento del riesgo para mandos medios y debilidad del SIGINT
Comunicación cifrada con IA	Evasión de inteligencia estatal mediante comunicaciones indetectables	Disminución del alcance del monitoreo de comunicaciones
Bots y desinformación con IA generativa	Difusión de propaganda y narrativas contrarias al Estado	Pérdida de legitimidad institucional en áreas periféricas
Análisis geoespacial automatizado para logística	Optimización de rutas de narcotráfico y ubicación de campamentos	Desventaja táctica en movilidad y despliegue operacional

Nota. Tabla de elaboración propia a partir de información extraída de Cuenca (2023), Cuevas (2023), Ownby (2024), Newton (2024), Orgaz (2024), Rodríguez (2024), Huamán et al. (2022), y Heras (2023).

Como puede observarse, estas tecnologías no son empleadas de forma aislada, sino como parte de un ecosistema de capacidades interconectadas que potencian la acción irregular. El impacto va más allá del terreno táctico, afectando directamente la capacidad de respuesta del Estado, su legitimidad frente a las comunidades locales y su dominio del espacio operacional.

Propuestas estratégicas para fortalecer la respuesta militar frente al uso de IA

El impacto de la inteligencia artificial en los escenarios de seguridad y defensa ha superado los límites de la ciencia ficción para consolidarse como una realidad operativa ineludible. En el contexto colombiano, particularmente en zonas de conflicto como la frontera con Ecuador en el Putumayo, esta tecnología ha sido incorporada por actores armados ilegales con una rapidez que contrasta con la lentitud institucional para adaptarse a estos nuevos retos. Este desfase genera una brecha estratégica que debe ser atendida desde el núcleo mismo de la doctrina militar, ya que la IA no puede seguir considerándose únicamente como una herramienta de apoyo, sino como un dominio estratégico transversal que transforma las lógicas del combate, la inteligencia y el control territorial.

Desde la perspectiva doctrinal, las Fuerzas Militares de Colombia han avanzado en la conceptualización de escenarios de guerra híbrida y ciberdefensa. Sin embargo, la incorporación específica de amenazas basadas en IA sigue siendo incipiente, fragmentada y con escaso desarrollo operativo. Como lo señalan Rojas y Camargo (2023), la IA constituye una transformación profunda de los métodos de conflicto, al integrar capacidades de análisis automatizado, predicción de comportamiento, comunicación cifrada y manipulación informativa, todo ello con bajo costo, alta disponibilidad y efecto multiplicador. En este sentido, resulta perentorio actualizar el cuerpo doctrinal para reconocer a la inteligencia artificial no solo como un recurso técnico, sino como un factor autónomo de alteración estratégica.

En países como Estados Unidos, Reino Unido e Israel, la IA ha sido reconocida oficialmente como un dominio operacional complementario al ciberespacio, lo cual implica que su gestión no se restringe al área tecnológica, sino que atraviesa todos los niveles de la planificación militar. En Colombia, iniciativas como el Comando Conjunto Cibernético han representado un avance significativo, pero su enfoque sigue centrado en la ciberseguridad convencional, sin abarcar aún el entorno emergente de amenazas algorítmicas, que pueden incluir desde ataques autónomos con drones hasta operaciones de desinformación por medio de deepfakes.

Peter Heras (2023) sostiene que la inteligencia artificial representa el mayor desafío para los esquemas clásicos de seguridad, porque no responde a las lógicas temporales ni geográficas del conflicto convencional. Su capacidad para operar de manera descentralizada, anticipar comportamientos y adaptarse en tiempo real rompe con los modelos lineales de planeación táctica y exige una revolución doctrinal. Del mismo modo, Mier (2019) advierte que, si bien los Estados conservan la ventaja institucional y tecnológica, la apropiación irregular de estas herramientas por grupos armados no estatales puede crear una simetría destructiva que altere el balance de poder local.

Acorde a lo anterior, el Ejército Nacional debe revisar consentidamente sus manuales de campaña, protocolos de inteligencia, esquemas de seguridad electrónica y sistemas de entrenamiento, de forma que integren el análisis, uso y neutralización de tecnologías basadas en IA como una competencia transversal. Esto incluye desde la incorporación de simuladores basados en machine learning en los centros de entrenamiento, hasta la elaboración de escenarios de guerra cognitiva en los planes de defensa territorial. El enemigo ya no se oculta solo en la selva o en las rutas fluviales, también opera desde nubes de datos, perfiles digitales

y algoritmos invisibles que interfieren en la percepción social y en el flujo de decisiones tácticas.

En suma, el marco doctrinal actual resulta insuficiente para responder a la complejidad de las amenazas tecnológicas que enfrentan las Fuerzas Militares en regiones como el Putumayo. La inteligencia artificial ha modificado las reglas del conflicto y, por tanto, debe modificar también las reglas del combate, la protección de la soberanía y la construcción de superioridad operativa. Reconocer esta realidad no es solo una cuestión de modernización técnica, sino de supervivencia estratégica en un entorno cada vez más digital, volátil y descentralizado.

Creación de una doctrina nacional de defensa frente a tecnologías emergentes

La evolución acelerada de la IA en manos de actores armados irregulares exige no solo respuestas tácticas inmediatas, sino también una construcción estratégica sostenida que articule una visión nacional de defensa frente a las tecnologías emergentes (Acerbi, 2020). Esta necesidad debe traducirse en la formulación de una doctrina oficial y multidimensional, diseñada no solo para reaccionar a amenazas concretas, sino para anticiparse a las futuras transformaciones del entorno operativo. La carencia de un marco doctrinal específico en esta materia coloca a Colombia en una posición de vulnerabilidad estratégica frente a un fenómeno que, como lo advierte Cuenca (2023), tiende a expandirse y sofisticarse de forma progresiva y silenciosa.

Una doctrina nacional para el uso y control de tecnologías emergentes debe sustentarse en principios como la flexibilidad adaptativa, la interoperabilidad institucional, la protección de datos sensibles, la seguridad algorítmica y la anticipación estratégica. Esto implica que el diseño doctrinal no puede estar limitado a las Fuerzas Militares, sino que debe

integrar a actores civiles, académicos y tecnológicos, bajo un esquema de gobernanza de defensa tecnológica, tal cual como lo sugiere Cárdenas et al,. (2022) en este sentido, el Ministerio de Defensa Nacional tiene el rol rector de convocar a instituciones como el Comando Conjunto Cibernético, el Ministerio de Ciencia y Tecnología, universidades con centros de investigación en IA, y aliados del sector privado con experiencia en análisis de datos, criptografía y ciberinteligencia (MINTIC, 2024).

Asimismo, uno de los pilares de esta doctrina debe ser la integración sistemática de escenarios basados en IA dentro de los ejercicios de entrenamiento militar y de planificación operacional. Esto se traduce en incorporar simulaciones con algoritmos adversarios, detección de patrones digitales hostiles, manipulación de entornos virtuales y anticipación de escenarios no lineales mediante inteligencia artificial predictiva. Según Guzmán (2024) (2024), es necesario comprender que los conflictos del siglo XXI no se desarrollan exclusivamente en el terreno físico, sino que también transcurren en entornos intangibles como el ciberespacio, los sistemas de información y la percepción pública, todos ellos directamente influenciables por tecnologías de IA.

Otro componente central de esta doctrina debe ser la formulación de protocolos de actuación en caso de amenaza tecnológica. Tal como lo plantea Mier (2019), las doctrinas modernas deben contener respuestas a escenarios como: interferencia de drones autónomos sobre instalaciones estratégicas, sabotaje digital a centros de comando, uso de redes neuronales para ocultamiento de rutas de narcotráfico o campañas de desinformación a través de redes sociales. La ausencia de lineamientos claros frente a estos desafíos deja al personal militar sin herramientas conceptuales para actuar de forma eficaz, lo que limita la proyección de fuerza y expone al Estado a daños irreversibles.

La doctrina, además, debe incorporar una visión diferencial del riesgo tecnológico en zonas de frontera, particularmente en regiones como el Putumayo. Allí, la combinación entre baja presencia institucional, acceso limitado a tecnología estatal, y dominio de actores armados facilita que las capacidades de IA se desarrollen por parte de disidencias sin resistencia significativa. Por ello, la doctrina debe contemplar el refuerzo de las capacidades de defensa en regiones periféricas, mediante tecnología portátil, acceso a redes seguras y despliegue de unidades especializadas en neutralización tecnológica (Jaime, 2023).

Desde una perspectiva geopolítica, esta doctrina permitiría también el fortalecimiento del posicionamiento internacional de Colombia como un país que reconoce y enfrenta de manera proactiva los desafíos de la inteligencia artificial en el campo de la seguridad. Así, el país podría liderar iniciativas de cooperación multilateral sobre defensa digital, participar en el desarrollo de estándares éticos de IA aplicados a contextos de conflicto armado, y consolidar alianzas técnicas con actores internacionales estratégicos (Luhmann, 1991). Como lo plantea Acerbi (2020), los Estados que asumen un liderazgo en la comprensión y regulación de la IA en entornos de seguridad tenderán a proyectar mayor influencia global.

Así las cosas, una doctrina nacional sobre tecnologías emergentes no puede ser un documento técnico aislado, sino una herramienta estratégica de primer orden, orientada a anticipar amenazas, orientar decisiones tácticas y fortalecer la resiliencia institucional. Enfrentar el uso de IA por parte de actores armados no estatales no es solo una cuestión operativa, sino una decisión política y doctrinal que definirá el rumbo de la defensa nacional en la próxima década (Osorio & Pulido, 2022).

Fortalecimiento de las capacidades de inteligencia técnica y cibernética

En el nuevo contexto de amenazas tecnológicas, el éxito de la respuesta militar no depende exclusivamente de la capacidad de fuego, sino de la superioridad en el manejo de la información y del entorno digital (Porcelli, 2020). Las disidencias armadas han demostrado una creciente habilidad para manipular datos, vulnerar redes, burlar sistemas de vigilancia y operar de manera descentralizada gracias a herramientas como la inteligencia artificial, la criptografía avanzada y la georreferenciación automatizada. Esto ha generado un desequilibrio operacional que exige una transformación profunda de las capacidades de inteligencia técnica (TECHINT), señales (SIGINT) y ciberinteligencia, no como unidades de apoyo, sino como ejes centrales de la estructura defensiva (Prieto, 2023).

De igual modo, la inteligencia técnica es hoy una prioridad estratégica. Según Cuenca (2023), gran parte de los sistemas de IA utilizados por actores armados irregulares son construidos a partir de software de libre acceso, plataformas de código abierto, hardware comercial adaptado y datos obtenidos de redes sociales. Esto significa que la barrera tecnológica entre el Estado y los grupos criminales se ha reducido peligrosamente. Para revertir esta tendencia, el Ejército Nacional debe adoptar una política sostenida de inversión en capacidades tecnológicas propias, que incluya laboratorios de ciberinteligencia, unidades móviles de guerra electrónica, y plataformas de análisis de big data con capacidad predictiva (Velasco, Periche, Gómez, & Benedí, 2024).

Dicha inversión debe articularse con un ecosistema nacional de innovación en defensa, donde universidades, centros de investigación y empresas del sector TIC aporten al desarrollo de soluciones duales, es decir, tecnologías aplicables tanto en el ámbito militar como civil. El modelo israelí del Talpiot Program o el británico Centre for Data Ethics and

Innovation ofrecen ejemplos de cómo consolidar alianzas estratégicas entre las Fuerzas Armadas y el sector tecnológico para crear una base industrial y científica de defensa nacional (Ramírez & Jiménez, 2017). En el caso colombiano, entidades como el MINTIC (2024) y Colciencias deben participar activamente en la construcción de un sistema de innovación para la seguridad, enfocado en el desarrollo de capacidades autónomas en inteligencia artificial, visión computacional y aprendizaje automático.

Además de los recursos materiales, es fundamental el *entrenamiento especializado del recurso humano militar*. Las tropas que operan en zonas de alta amenaza tecnológica, como el Putumayo o el Catatumbo, deben ser formadas en temas como análisis de metadatos, lectura de redes sociales, ciberseguridad operativa, uso de software de análisis forense y reconocimiento de dispositivos electrónicos alterados (Vigevano, 2021). Esto requiere una revisión profunda de los currículos en las escuelas de formación militar y la creación de cursos avanzados en colaboración con universidades y expertos internacionales. El conocimiento técnico ya no puede ser exclusivo del personal de inteligencia; debe extenderse a todos los niveles de mando, desde el comandante de pelotón hasta el oficial de Estado Mayor.

Por otro lado, se deben consolidar *equipos de respuesta rápida ante incidentes tecnológicos*, capaces de identificar y neutralizar amenazas emergentes en tiempo real. Estas unidades inspiradas en los CSIRT (Computer Security Incident Response Teams) pueden desplegarse en escenarios críticos, analizar dispositivos capturados a disidencias, interceptar comunicaciones cifradas y prevenir ciberataques a infraestructuras militares (TechTarget, 2012). Heras (2023) destaca que, en escenarios de guerra híbrida, la capacidad de respuesta

rápida frente a anomalías tecnológicas es determinante para mantener la iniciativa táctica y garantizar la superioridad informacional.

Una dimensión aún poco explorada pero crucial es el uso *ofensivo y defensivo de inteligencia artificial por parte del Estado*, no solo para vigilar, sino para prevenir, persuadir y disuadir. Como lo plantea Guzmán (2024), la IA puede ser utilizada éticamente para modelar escenarios, anticipar rutas de repliegue de grupos armados, identificar patrones de reclutamiento juvenil en redes sociales y crear alertas tempranas de desplazamiento forzado o consolidación criminal. Este enfoque proactivo requiere marcos normativos claros, pero también una apertura institucional hacia nuevas formas de pensar y actuar en seguridad nacional.

De ese modo, *la inteligencia técnica y cibernética debe convertirse en un pilar central del poder militar colombiano*, no como un componente aislado, sino como una capacidad transversal que potencie el análisis, la planificación y la ejecución de las operaciones en entornos de alta complejidad. La inteligencia artificial no solo ha transformado el rostro del enemigo: también ofrece al Estado una oportunidad para reinventarse, ganar eficiencia y recuperar la ventaja estratégica perdida en zonas disputadas.

Conclusiones

La inteligencia artificial se ha convertido en un factor decisivo dentro del nuevo entorno estratégico de seguridad en Colombia, particularmente en zonas como la frontera colombo-ecuatoriana del Putumayo, donde confluyen debilidad institucional, economías ilícitas y estructuras armadas con alta capacidad de adaptación. Este artículo ha demostrado que las disidencias de las FARC han incorporado diversas tecnologías basadas en IA como drones autónomos, vigilancia predictiva, comunicaciones cifradas y campañas de desinformación que alteran profundamente las condiciones tradicionales del conflicto armado y superan las capacidades convencionales de respuesta del Estado.

Desde el ámbito operacional, estas herramientas han permitido a los actores ilegales ganar ventaja táctica mediante la evasión de patrullajes, la anticipación de operaciones militares y el control simbólico de territorios por medio de vigilancia y propaganda. El uso de sistemas algorítmicos por parte de las disidencias transforma la dinámica del conflicto, desdibujando las fronteras entre lo militar, lo tecnológico y lo psicológico, y situando al Estado ante una amenaza híbrida de nueva generación.

El análisis también evidenció que el aparato de defensa colombiano no cuenta aún con una doctrina nacional consolidada para enfrentar este tipo de amenazas emergentes. La ausencia de protocolos específicos, capacidades técnicas integradas y entrenamiento especializado limita la capacidad de anticipación, interdicción y contención. Esta brecha no solo compromete la eficacia operativa de las Fuerzas Militares, sino que pone en riesgo la legitimidad del Estado en regiones fronterizas donde la autoridad está en disputa.

Como respuesta a este panorama, se propusieron cinco líneas estratégicas de acción: (1) la formulación de una doctrina nacional para la defensa frente a tecnologías emergentes; (2) el fortalecimiento de las capacidades de inteligencia técnica y cibernética; (3) la integración del componente ético y jurídico en el uso defensivo de IA; (4) el desarrollo de mecanismos de cooperación binacional con Ecuador; y (5) la generación de conocimiento desde la experiencia operativa en terreno. Estas propuestas buscan no solo contener el uso ilegal de IA, sino también dotar al Estado de una ventaja adaptativa sostenida.

El estudio se apoyó en la teoría del riesgo social de Niklas Luhmann, permitiendo interpretar el uso de IA no únicamente como una amenaza puntual, sino como un fenómeno estructural que incrementa la complejidad del sistema de seguridad y obliga a repensar los fundamentos de la acción estatal en contextos periféricos. Bajo esta óptica, la inteligencia artificial no es solo un desafío técnico, sino un generador de riesgo sistémico que tensiona las fronteras entre legalidad e ilegalidad, visibilidad e invisibilidad, control y autonomía.

En definitiva, el futuro de la defensa nacional frente a amenazas como la IA no dependerá únicamente de la adquisición de nuevas tecnologías, sino de la capacidad del Estado para *integrarlas con visión estratégica, sentido ético y legitimidad institucional*. La frontera ya no se defiende solamente con soldados en tierra, sino también con algoritmos, información precisa, marcos legales robustos y comunidades que confíen en su gobierno. El reto, entonces, no es solo técnico ni militar: es político, doctrinal y profundamente humano.

Referencias

Acerbi, J. (2020). *Terrorismo, tecnología y sociedad en el siglo XXI*. Obtenido de https://www.redalyc.org/journal/924/92471540002/html/

Arce, J. (2025). *Alerta en la frontera: Ecuador envió un escuadrón de 1500 militares a zona colindante con Perú y Colombia.* Obtenido de https://www.infobae.com/peru/2025/05/15/alerta-en-la-frontera-ecuador-envio-un-escuadron-de-1500-militares-a-zona-colindante-con-peru-y-colombia/

BBC. (2024). *Qué poder tienen las bandas que Ecuador califica como "organizaciones terroristas"*. Obtenido de https://www.bbc.com/mundo/articles/c1vy2ylnz5go

Bonilla, L. (2025). *Asesinato de militares en Ecuador: la historia desconocida de Comandos de Frontera.* Obtenido de https://www.elespectador.com/colombia-20/analistas/asesinato-de-11-militares-en-ecuador-por-comandos-de-frontera-muestra-crisis-de-triple-frontera/

Cárdenas, J., Downing, C., Johnson, K., Olaya, Á., & Vélez, J. (2022). *Percepciones sobre los Grupos Disidentes de las FARC en Colombia: Implicaciones para la futura construcción de paz*. Obtenido de https://bit.ly/4gtKJ4A

Conde, M. F., & Orbe, M. (2020). *Grupos irregulares armados en el conflicto de la frontera colombo-ecuatoriana y su relación con el narcotráfico*. Obtenido de https://www.armyupress.army.mil/Journals/Edicion-Hispanoamericana/Archivos/Segundo-Trimestre-2020/Grupos-irregulares-armados-en-el-conflicto-de-la-frontera-colombo-ecuatoriana-y-su-relacion-con-el-narcotrafico/

Cuenca, D. P. (2023). *IA en la seguridad y delincuencia. Implicaciones político-criminales para el futuro*. Obtenido de https://bit.ly/3WN3NE0

Cuevas, D. F. (2023). *La inteligencia artificial en el pos-acuerdo colombiano : el caso de los drones de combate para operaciones sostenidas contra grupos armados organizados*. Obtenido de https://bdigital.uexternado.edu.co/entities/publication/bcf16cfa-693f-4938-9251-39a1b0fad0a6

Defesnsoría del Pueblo. (2024). *Defensoría presentó informe estructural sobre el Putumayo*. Obtenido de https://www.defensoria.gov.co/-/defensor%C3%ADa-present%C3%B3-informe-estructural-sobre-el-putumayo

Guzmán, C. A. (2024). *Inteligencia artificial y crímenes de guerra*. Obtenido de https://blogpenal.uexternado.edu.co/inteligencia-artificial-y-crimenes-de-guerra/

Heras, P. L. (2023). *El reto de la inteligencia artificial para la seguridad y defensa*. Obtenido de https://www.unav.edu/web/global-affairs/el-reto-de-la-inteligencia-artificial-para-la-seguridad-y-defensa

Huamán, H. Y., Cataño, K., Sevincha, M., & Vargas, O. (2022). *La inteligencia artificial y la video-vigilancia en la predicción y detección de delitos en espacio-tiempo: una revisión sistemática*. Obtenido de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082023000100011

Jaime, Ó. (2023). *El futuro del terrorismo y su prevención*. Obtenido de https://seguridadinternacional.es/resi/html/el-futuro-del-terrorismo-y-su-prevencion/

Luhmann, N. (1991). *Sociología del riesgo*. Obtenido de https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://analisisinstitucionaluba.wordpress.com/wp-content/uploads/2013/08/sociologia-del-riesgo-niklas-luhmann.pdf&ved=2ahUKEwjLkaak7ayLAxW-SzABHTi-H88QFnoECCoQAQ&usg=AOvVaw1oGt032rMxpnvaJQ

Matiz, A. H., & Fernández, J. (2023). *Del uso de la inteligencia artificial como medio y método en los conflictos armados*. Obtenido de https://www.redalyc.org/journal/4762/476277508010/html/

Mier, S. G. (2019). *Inteligencia artificial como herramienta de estrategia y seguridad para defensa de los Estados*. Obtenido de https://portal.amelica.org/ameli/journal/262/2621457007/html/index.html

MINTIC. (2024). *El país consolida estrategias para robustecer la seguridad informática en el sector financiero*. Obtenido de https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/397918:El-pais-consolida-estrategias-para-robustecer-la-seguridad-informatica-en-el-sector-financiero

Newton, C. (2024). *Cuatro formas en que la IA está transformando el crimen organizado en América Latina*. Obtenido de https://insightcrime.org/es/noticias/cuatro-formas-inteligencia-artificial-transformando-crimen-organizado-america-latina/

Olaya, A. Y. (2019). *La frontera entre Colombia y Ecuador: Movilidades de comunidades afrocolombianas en escenarios del narcotráfico*. Obtenido de https://www.redalyc.org/journal/2110/211062829004/html/

Orgaz, C. J. (2024). *6 maneras en que grupos criminales de América Latina usan la inteligencia artificial para delinquir*. Obtenido de https://www.bbc.com/mundo/articles/crej5gwllvlo

Osorio, J. F., & Pulido, Ó. (2022). *Caracterización de las disidencias de las FARC, un análisis desde el Derecho Internacional Humanitario.* Obtenido de https://bit.ly/3ErA9hu

Ownby, J. (2024). *Drones que lanzan bombas: la nueva etapa del conflicto colombiano*. Obtenido de https://elpais.com/america-colombia/2024-06-19/drones-que-lanzan-bombas-la-nueva-etapa-del-conflicto-colombiano.html

Parada, V. (2024). *Los grupos narcotraficantes de Colombia y Ecuador se enfrentan en la frontera amazónica por el negocio de la coca*. Obtenido de https://elpais.com/america/amazonia-sin-fronteras/2024-11-29/los-grupos-narcotraficantes-de-colombia-y-ecuador-se-enfrentan-en-la-frontera-amazonica-por-el-negocio-de-la-coca.html

Porcelli, A. M. (2020). *La inteligencia artificial y la robótica: sus dilemas sociales, éticos y jurídicos*. Obtenido de https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2448-51362020000300049

Prieto, J. V. (2023). *Nuevas formas de financiación del terrorismo: retos y soluciones para combatirla utilizando sistemas inteligentes.* Obtenido de https://digibug.ugr.es/handle/10481/87681

Ramírez, E. P., & Jiménez, J. (2017). *Israel: la transformación estratégica - militar frente a nuevas amenazas*. Obtenido de https://esdegrevistas.edu.co/index.php/resd/article/view/254/582

Rodriguez, L. A. (2024). *La inteligencia artificial y el crimen organizado.* Obtenido de https://es.linkedin.com/pulse/la-inteligencia-artificial-y-el-crimen-organizado-rojas-rodriguez-kzote

Rojas, A. H., & Camargo, J. (2023). *Del uso de la inteligencia artificial como medio y método en los conflictos armados* . Obtenido de https://dx.doi.org/10.21830/19006586.1151

Ruiz, Ó. (2024). *Terrorismo e inteligencia artificial, un tándem mortal*. Obtenido de https://thediplomatinspain.com/2024/10/28/terrorismo-e-inteligencia-artificial-un-tandem-mortal/

Saavedra, F. (2024). *Con ayuda de la inteligencia artificial, descubrieron red de reclutadores de las disidencias de las Farc, ELN y el Clan del Golfo.* Obtenido de https://www.infobae.com/colombia/2024/09/26/con-ayuda-de-la-inteligencia-artificial-lograron-descubrir-red-de-reclutadores-de-las-disidencias-de-las-farc-eln-y-clan-del-golfo/

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

Sánchez, C. C. (2014). *Procesos de resistencia en la frontera colombo-ecuatoriana*. Obtenido de https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1665-85742014000100005

TechTarget. (2012). *Equipo de Respuesta frente a Incidencias de Seguridad Informática (CSIRT)*. Obtenido de https://www.computerweekly.com/es/definicion/Equipo-de-Respuesta-frente-a-Incidencias-de-Seguridad-Informatica-CSIRT

Velasco, C., Periche, J., Gómez, J., & Benedí, M. (2024). *Inteligencia artificial y el crimen organizado*. Obtenido de https://bit.ly/40MsDVP

Vigevano, M. (2021). *Inteligencia Artificial aplicable a los conflictos armados: Límites jurídicos y éticos*. Obtenido de https://arbor.revistas.csic.es/index.php/arbor/article/view/2417/3638