Enfoques tecnológicos de quinta generación: vigilancia, identificación y monitoreo de amenazas sobre zonas estratégicas de intervención.

MY (EJC) Vanegas Melo Ronald

Artículo para optar al título profesional:

Magister en Seguridad y Defensa Nacional

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	**:**	Ronald Vanegas Melo
Identificación	**:**	80194816
Programa académico	**:**	Maestria en Seguridad y Defensa Nacional
Tutor metodológico	**:**	Juan Camilo Urazan Chinchilla
Tutor temático	**:**	Jose Manuel Jiménez Audor
Fecha de entrega	**:**	24 de Agosto de 2025
Extensión	**:**	7517 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

Enfoques tecnológicos de quinta generación: vigilancia, identificación y monitoreo de amenazas sobre zonas estratégicas de intervención.

Technological approaches of fifth generation: surveillance, identification, and monitoring of threats over strategic intervention zones.

My Ronald Vanegas Melo[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: La investigación aborda la integración de tecnologías de quinta generación en la defensa nacional de Colombia, enfocándose en la vigilancia, identificación y monitoreo de amenazas transversales en zonas críticas. Se utilizó un diseño cualitativo-descriptivo, con análisis multicriterio y vigilancia tecnológica para identificar brechas operativas y proponer soluciones estratégicas. Los resultados revelan un aumento del 26.3% en insurgencias post acuerdo y el tráfico del 70% de cocaína a través de fronteras vulnerables, destacando la urgencia de implementar drones, sensores avanzados y algoritmos predictivos. Además, se identificaron necesidades en protección de infraestructuras críticas y reducción de incertidumbre en escenarios estratégicos. La investigación concluye que la adopción de tecnologías disruptivas es esencial para modernizar las capacidades operativas de las Fuerzas Militares, optimizar la respuesta ante amenazas complejas y fortalecer la soberanía estatal en el marco del Plan de Transformación FFMM 2042.

Palabras clave: Tecnología, defensa, vigilancia, insurgencias, geoestrategia, infraestructura.

Abstract: The research examines the integration of fifth-generation technologies into Colombia's national defense, focusing on surveillance, identification, and monitoring of transversal threats in critical zones. A qualitative-descriptive design was employed, utilizing multicriteria analysis and technological surveillance to identify operational gaps and propose strategic solutions. Results show a 26.3% increase in post-agreement insurgencies and 70% cocaine trafficking through vulnerable borders, highlighting the urgency of implementing drones, advanced sensors, and predictive algorithms. Additionally, needs were identified in critical infrastructure protection and uncertainty reduction in strategic scenarios. The study concludes that adopting disruptive technologies is vital to modernizing military operational capabilities, optimizing responses to complex threats, and strengthening state sovereignty within the framework of the FFMM Transformation Plan 2042.

Keywords: technology, defense, surveillance, insurgencies, geostrategy, infrastructure.

[1] 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/ 0000-0003-1823-8714 - Contacto: ronald.vanegasj@esdeg.edu.co.

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

Introducción

La inclusión de tecnologías disruptivas al campo de la seguridad y defensa nacional configura un cambio estructural para el entendimiento de los contextos, así como para el pensamiento estratégico post funcionalista.

Desde esta perspectiva, el punto de discusión en teorías contemporáneas como la asimetría de conflicto y las nuevas guerras, la transformación tecnológica de los actores militares debe obedecer parámetros, fenómenos, variables y elementos de contexto que conlleven a una actualización de los métodos, modos y medios de protección securitista endógena (Ramírez, 2021).

El caso de las Fuerzas Militares de Colombia no es ajeno a la necesidad de adaptaciones tecnológicas si se tiene en cuenta que el Plan de Transformación de las Fuerzas Militares (2042) plantea como hoja de ruta la transformación estructural de los procesos requeridos en materia geoestratégica. Con base en esto, de frente a escenarios de futuro, la adopción de enfoques tecnológicos que conlleven a la materialización de objetivos geoestratégicos se convierte en un principio organizacional conexo a la optimización de los procesos de defensa; así como la integración y transformación de sistemas para la intervención y protección micro – territorial.

Ahora bien, aunque el Plan de Transformación de las FFMM – principal factor del enfoque geoestratégico – plantea la necesidad de innovación, desarrollo y transformación de sistemas de defensa, no hay aún en el marco de la estrategia cimentada en el Plan de Campaña Ayacucho 2.0, Política de Defensa y Convivencia Ciudadana o Metodología para el Diseño e Implementación de la Política de Ciencia y Tecnología para el Sistema de Defensa (MDIPCT) (Ministerio de Defensa Nacional, 2024), lineamientos estratégicos enfocados en la distinción de factores de inestabilidad comunes y/o transversales.

Es decir, si bien el MDN (2024) plantea un mapa de riesgos que guía el proceso de innovación, desarrollo e investigación, este no configura o conceptúa una línea de enfoques tecnológicos precisos que se adapte la característica primaria del sistema permanente de amenazas: su naturaleza transversal. No obstante, el desconocimiento de los enfoques tecnológicos de intervención, que de facto es un problema estructural de naturaleza geoestratégica, posee tres causas principales.

En primer lugar, como se evidencia en la MDIPCT, no hay especificaciones micro focalizadas en la distinción de tecnologías de disrupción con las cuales enfrentar dos fenomenologías de impacto: los daños ecosistémicos con afectación directa al enfoque de seguridad ambiental, y las problemáticas de seguridad territorial, cuyos factores son el tráfico internacional de narcóticos, la explotación ilícita de yacimientos mineros y la transgresión fronteriza de categoría territorial. Por otro lado, las investigaciones académicas enmarcadas en la seguridad y defensa con enfoques estratégicos son escazas, y su ausencia dificulta un proceso de co-creación de iniciativas estratégicas para: identificar retos comunes, identificar tecnológicas y concretar acciones asociadas con la producción de conocimiento científico colectivo. Es decir, empleo de metodologías de innovación organizacional como el Triple de Hélix.

Además, los ejercicios de vigilancia tecnológica en el marco de la defensa nacional no exploran a profundidad la concertación de tecnologías especializadas que, bajo el principio de flexibilidad, coadyuven al mejoramiento de la estrategia de defensa nacional conexa para el caso de las FFMM con el Plan de Campaña Ayacucho 2.0. Estas tres causas abordan problemáticas organizacionales cuyas consecuencias son la ralentización macro estratégica del Comando de las FF.MM en materia de defensa nacional, la desactualización de los métodos y medios para hacer la guerra, pero, sobre todo, la pérdida de capacidad geoestratégica centrada al tiempo en el concepto de la geopolítica de la tecnología.

Son las causas y posibles consecuencias las que llevan el trabajo de investigación a plantear como pregunta base lo siguiente: ¿Cuáles son los enfoques tecnológicos de quinta generación que se adaptan a la necesidad estratégica de vigilancia, identificación y monitoreo de amenazas ubicadas en zonas de intervención primaria?

Al responder este interrogante, la investigación busca analizar un parámetro estratégico conformado por enfoques de intervención en territorio, poco explorados en el marco de la tecnología adaptable al sistema de defensa nacional que se rige con los lineamientos de las FFMM por el Plan de Campaña Ayacucho Plus.

Identificar tecnologías propicias para la vigilancia y monitoreo de amenaza que por su naturaleza son transversales, y por su genealogía comunes, facilitaría a los actores militares del poder terrestre, interceptar e identificar fenomenologías criminales en constante evolución, así como analizar de forma predictiva su expansión y evolución.

El propósito de la pregunta de investigación es entonces subrayar desde las capacidades de poder terrestre qué se puede hacer en materia geoestratégica para contrarrestar el aumento exponencial de amenazas de tipología compleja, cuyas afectaciones, de acuerdo con el MDN (2024), son en su mayoría ambientales y territoriales.

En este contexto, se plantean tres factores de orden cualitativo que, ajustados al problema, justifican la investigación. En primer lugar, desde la perspectiva científica, encontrar los enfoques tecnológicos complementaría el diseño estratégico empleado para materializar objetivos estratégicos, sobre todo, el objetivo de protección civil propuesto por el Plan de Campaña Ayacucho 2.0.

En segundo lugar, desde la perspectiva académica, complementar las investigaciones que desde la técnica de vigilancia tecnológica se han presentado en pro de la protección territorial enmarcada en principios preventivos y disciplinas metódicas como la prospectiva.

En tercer lugar, desde la perspectiva militar, incluir análisis estructurales que conlleven a una consideración: inclusión de la dimensión tecnológica – geoestratégica al núcleo funcional de la seguridad multidimensional.

Metodología de la investigación

Para llevar a cabo esta investigación se adecúa un enfoque cualitativo con diseño descriptivo. Este enfoque facilita el análisis de diferentes fuentes de información, con las que se constituye una metodología dividida en tres partes.

La primera corresponde a la conceptualización (primer objetivo), y el propósito es caracterizar la relación que hay entre seguridad y defensa nacional, poder terrestre, factores de inestabilidad y tecnologías de quinta generación. Este punto relacionará los términos, y concertará el núcleo de amenazas que requiere de un enfoque tecnológico especial en caso colombiano.

La segunda parte hace alusión al estudio de las necesidades operacionales prioritarias que caracterizan los ecosistemas criminales conformados en zonas estratégicas de intervención especial. Este punto tiene por propósito la identificación de patrones comunes que conectan los ecosistemas criminales principales sobre territorio colombiano.

La tercera compete a un estudio de vigilancia tecnológica centrando en enfoques de defensa para la intervención temprana, tomando como punto de partida identificación de patentes técnicas ajustadas a la necesidad securitista del contexto.

Por último, la cuarta línea corresponde al **planteamiento de** la línea estratégica (teledetección) de proyección tecnológica por incluir en el Plan de Transformación de las FFMM 2042. El objetivo es contribuir al mejoramiento de las características del proceso de transformación, a partir de la proyección de capacidades tecnológicas para el poder terrestre.

Importancia geoestratégica de la incorporación de tecnologías de quinta generación al marco funcional de los sistemas de seguridad y defensa nacional.

La importancia estratégica de la inclusión de tecnologías de quinta generación en el marco de las estructuras de seguridad y defensa nacional se plantea con versiones asociadas al constructivismo de contexto.

Esto significa en el pensamiento clásico de Nance (1999), que el marco de seguridad y defensa debe ajustarse a enfoques contextuales que surgen a la par del campo tecnológico.

Pero, de acuerdo con Thee (2025), la relación entre seguridad, defensa nacional y tecnología a partir de una mirada funcionalista debe adoptar enfoques disruptivos que cambien los factores de planeación, integrando de manera tácita el concepto I+D+i+TT (Investigación, desarrollo, innovación y transferencias tecnológicas).

Eso significa, que el desarrollo tecnológico debe ser intrínseco al sistema de defensa, y por ello la necesidad primaria no solo está en las actualizaciones tecnológicas, sino también en las construcciones organizacionales de conocimiento colectivo.

El conocimiento se convierte en una variable estratégica para diseñar procesos de seguridad y defensa nacional. Esa es una discusión en el marco de la innovación para instituciones militares que exponen Jiménez, Villa y Bermúdez (2020), y que de facto encuentra en la explotación de conocimiento, una variable que también influye en las transformaciones tecnológicas.

Según estos autores, el conocimiento sumado a procesos de innovación interna conduce a la creación de factores tecnológicos centrados principalmente en la eficiencia operacional, la reducción de riesgos y anticipación temprana de amenazas.

De ahí, que otras posturas también hablen de la incorporación de tecnologías de quinta generación a las estructuras de seguridad y defensa nacional, aduciendo a la actualización de elementos doctrinales y organizacionales; especialmente aquellos relacionados con la vigilancia de amenazas conocidas e identificación de nuevas fenomenologías (Epstein, DiEuliis, y Urich, 2023).

Según Epstein *et al* (2023), son estas nuevas amenazas las que exigen a un sistema de seguridad y defensa nacional optimizar sus elementos operacionales, doctrinales y de intervención.

De hecho, su postura concertada en el artículo *Cómo las tecnologías emergentes se convierten en amenazas emergentes*, expone que la responsabilidad de los sistemas de defensa es entender el cambio en los ambientes operacionales a través de medidas de anticipación y prevención.

Dichas medidas, implican el análisis micro segmentado de factores de inestabilidad en presente y en futuro que ameriten la incorporación temprana de tecnologías disruptivas.

Frente a la contribución de Epstein *et al* (2023) surge un factor de análisis relevante: la seguridad como vector multidimensional y estructural, con direccionamientos ser claros y ajustados al entorno.

Ello significa, tal y como argumenta Corn (2021), que la creación o incorporación de tecnología a un sistema de defensa debe asumir, desde la postura del tomador de decisiones, un vector competitivo que supere el accionar, impacto o alcance geoestratégico de las amenazas ya identificadas e incluso de aquellas que se encuentran en transmutación.

La perspectiva de Corn (2021) se aleja de una versión realista de la seguridad nacional y se aproxima más a un entendimiento reflexivo, en el que el epicentro de securitización es el actor poblacional.

Ubicar a la población en el centro del sistema de seguridad implica aceptar que un modelo de defensa es multidimensional, y que la seguridad no es únicamente militar, sino también económica, ambiental y social (Ivančík, 2021). Siendo así, el alcance de las tecnologías a incorporar debe abarcar y retener factores de inestabilidad que, al materializarse, afecten el concepto de seguridad integral.

Para el caso de esta investigación, cuya categoría de seguridad recae en el poder terrestre, la adopción de tecnologías de quinta generación conlleva a una construcción multimodal de la estrategia.

Esto, en términos de Méndez (2022), se refiere al cambio de los enfoques geoestratégicos que cambian de manera paralela a la transformación de los ecosistemas criminales en las zonas de conflicto.

Entender esta problemática y concertar qué enfoques geoestratégicos deben ajustarse a dicho paralelismo, implica establecer en el marco de los factores de inestabilidad del Plan de Campaña Ayacucho 2.0, cuatro categorías de estudio. Su descripción y análisis ha sido objeto de investigación en perspectiva previas como las de Santoyo (2024) quien integra los

factores de inestabilidad como justificación para potenciar la inteligencia de señales o la Guía de Planeamiento Estratégico del Ejército Nacional, en la que se incluyen los factores desde el entendimiento de las dinámicas territoriales que poseen las guerras asimétricas (Ejército Nacional de Colombia, 2020). (Mírese la figura 1 para continuar):

Figura 1. Factores de inestabilidad agrupados por enfoques geoestratégicos

Nota: información recuperada de EJC (2020)

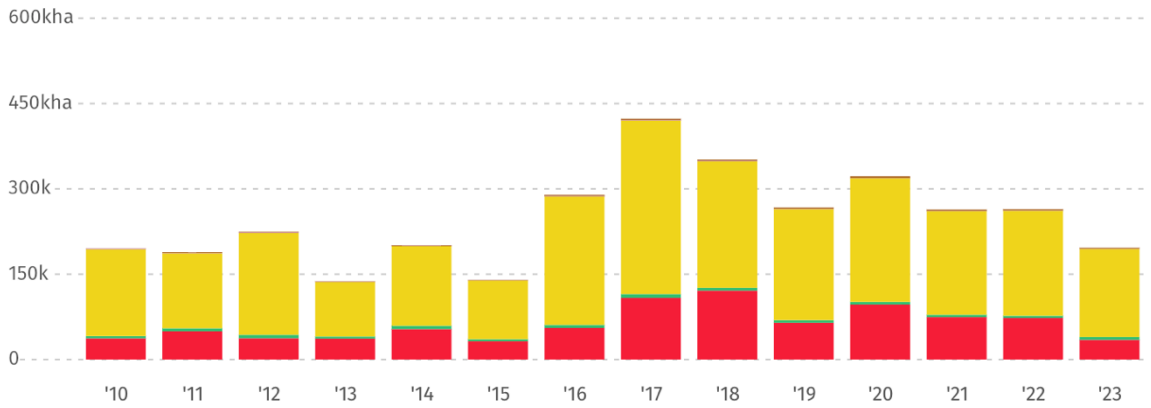
Los factores de inestabilidad para el poder terrestre, expuestos en la figura 1, constituyen un acercamiento al sistema general de amenazas persistentes y permanentes. Entender el núcleo de riesgos, diferenciando los vectores ambientales, económicos, sociales y territoriales, permite extender el análisis hacia la versión del Servicio de Investigación del Congreso de EEUU (2023), quien resalta el uso de tecnologías de quinta generación como un eje transversal para la efectividad de las acciones de defensa en puntos estratégicos como: espacios fronterizos, zonas geográficas complejas y centros de gravedad formados a partir de la explotación de vulnerabilidades socioeconómicas.

La postura del Servicio de Investigación del Congreso de EEUU se acerca al contexto colombiano porque conceptualiza con precisión espacios geográficos donde existen problemáticas relacionadas a factores como la geopolítica del narcotráfico, la transgresión de puntos fronterizos y la afectación medioambiental. Estos tres últimos elementos, vistos desde un escenario prospectivo por Rueda y Claros (2022), así como **por** Gonzáles **(2022)** y Gonzáles (2024), definen una categoría de análisis que integra a los factores de inestabilidad

relacionados con inseguridad ambiental, afectación geopolítica de las fronteras, terrorismo ambiental y afectaciones a las formas de desarrollo del actor poblacional. Este último fenómeno es producto de problemas asociados con el conflicto armado.

Las cuatro categorías señaladas tienen relación con el problema colombiano. En el caso de la inseguridad ambiental hay tres variables de afectación. Primero, un aumento de la deforestación de 2010 a 2023 que terminó con la pérdida de 1.45 millones de hectáreas de bosque primario (Global Forest Watch, 2024). Segundo, aumento en emisiones de CO_2 a 2.02 gigatoneladas, y tercero, pérdida del 24% de la masa forestal territorial total, tal y como se describe en la figura 2:

Figura 2. Aumento en emisiones de CO_2



Nota: información recuperada de Global Forest Watch (2024). Rojo: deforestación por materia prima; Amarillo: actividades de agricultura itinerante.

La segunda categoría, la geopolítica del narcotráfico, se presenta en el aumento exponencial del cultivo de hoja ilegal de coca que pasó de 48.000 hectáreas en 2013 a 251.000 en el 2023 (UNDOC, 2024). También, en el aumento del a producción de toneladas métricas de cocaína que pasó de 900 en 2015 a 2.700 en 2023.

Tercero, afectación exponencial territorial por el número de inmigrantes que atraviesan puntos fronterizos con poca gobernanza y gobernabilidad, siendo la subregión del Catatumbo y el Tapón del Darién con un tránsito de inmigrantes ilegales no menor a los 200.000 en 2023. Ambos ejemplos, problemáticas de tipología migratoria.

Cuarto, afectación al desarrollo en territorio, producto de la convergencia criminal que existe entre actores insurgentes, narcotráfico, explotación ilícita de yacimientos mineros y cercanía de los puntos fronterizos con los centros de hostilidad.

Las cuatro categorías representan actualmente un reto geoestratégico para el sistema de seguridad y defensa nacional. Eso significa que la incorporación de tecnologías de quinta generación al sistema de defensa que posee el poder terrestre, para el caso Ejército Nacional, debe dirigirse hacia la construcción de acciones estratégicas que permitan el monitoreo de afectaciones ambientales, la violación terrestre de puntos fronterizos, la conformación de ecosistemas criminales y el avance de las economías criminales.

Desde esta perspectiva, la exploración e identificación de tecnologías de quinta generación adaptables al sistema de defensa nacional debe comenzar con el reconocimiento de los patrones asimétricos que configuran el sistema de amenazas permanentes – persistentes, generando como deducción final el siguiente mapa de categorías tecnológicas que desde el análisis conceptual y de tendencias se asocia con el marco de seguridad con elementos estructurales de quinta generación:

Figura 3. Categorías y factores asociados a la inclusión de nuevas tecnologías al campo de defensa nacional.

Nota: elaboración propia

Análisis de las necesidades operacionales prioritarias que caracterizan los ecosistemas criminales conformados en zonas estratégicas de intervención especial: exploración a partir de análisis de datos.

El análisis de la importancia geoestratégicas que contrae la inclusión de tecnologías con características 5G a la estructura de defensa nacional, constituye un primer factor de estudio que se conecta con el análisis de las necesidades operacionales prioritarias.

Es así, que en esta parte de la investigación se llevó a cabo un ejercicio de exploración estadística, a partir de una técnica de relacionamiento de factores de inestabilidad centrados en las cuatro categorías identificadas. Para tal fin, se desarrollará un análisis del sistema de amenaza permanente y persistente diseñando un modelo metodológico basado en las contribuciones de Bojanić (2022) quien propone el estudio de la amenaza a través de la teoría de la seguridad nacional, en el que se incluyen variables matemáticas, modelos multicriterio, y escala intervalar. También con las contribuciones de Fingar (2020) y su análisis compuesto por recolección de datos y reducción de incertidumbre a través de relacionamiento de variables y el Director Oficial de Inteligencia Norteamericana (2025), de donde sale el concepto de análisis metódico BIRP (Desafíos, riesgos y amenazas).

La configuración de esa matriz de análisis se exponer de la siguiente manera:

Tabla 1. Elementos de análisis y descripción

Elemento	Descripción
Enfoque del Marco Sectorial	Divide las amenazas en categorías como político, militar, económico, social, ecológico e informacional.
Metodología Basada en el Riesgo	Evalúa desafíos, riesgos y amenazas de manera objetiva y medible.
Modelo Multicriterio Matemático	Clasifica las amenazas según su nivel de peligro utilizando criterios matemáticos.
Análisis Comparativo y Definición de Categorías	Diferencia entre desafío, riesgo y amenaza según su impacto.
Evaluación Intuitiva y Escala Intervalar	Mide intensidad, dirección y probabilidad de amenazas.
Reducción de la Incertidumbre	Estandariza análisis para mejorar decisiones estratégicas.

Elemento	Descripción
Separación de Categorías de Amenazas	Propone distinguir entre desafíos, riesgos y amenazas para estrategias más claras.

Nota: elaboración propia con información recuperada de Bojanić (2022), Fingar (2020) y Director Oficial de Inteligencia Norteamericana (2025)

Esta matriz de análisis se refina con la integración de las contribuciones metodológicas del MCE 5-0 Planeamiento y producción de órdenes; MCE – 3-24 Guerra irregular, MCE 3-24-1 Contrainsurgencia, y MFRE 5-0 Proceso de operaciones.

Asimismo, se integraron los principales indicadores de análisis de acuerdo con las contribuciones plasmadas en cinco fuentes de investigación: (UNDOC, 2024) (UNDOC, 2022), (UNDOC, 2022); (ONU, 2025); (OCHA, 2025)

Tabla 2. Matriz de análsis de amenaza refinada – contexto colombiano

Elemento	Descripción	Indicador Cuantitativo		Valor (impacto geoestratégico)	Ralentización operacional	Ralentización estratégica (dominio terrestre)
Planeamiento Operacional	Evalúa la capacidad de planificación estratégica para misiones específicas.	Factores para el planeamiento	Tecnologías para la reducción de incertidumbres y proceso para la toma de decisiones	1	0,9	0,9
			Tecnología para el análisis georreferencial del territorio	0,5	0,4	0,4
			Tecnologías para la delimitación de escenarios de convergencia criminal en zonas de intervención estratégica	0,5	0,7	0,7
Gestión de Amenazas Irregulares	Analiza la efectividad en la identificación y neutralización de amenazas no convencionales.	Número de amenazas mitigadas	Crecimiento de nuevas insurgencias post acuerdo. Aumento del 26,3% desde 2016 en zonas como Catatumbo, Putumayo y Cauca.	0,3	0,4	0,4
			Inclusión de nuevas metodologías asimétricas de afectación como la utilización de drones en 12 eventos reportados por MDN hasta 2024.	0,7	0,8	0,8
			Configuración de nuevas capacidades por parte de grupos insurgentes que poseen relación con grupos de delincuencia organizada transnacional, específicamente en zonas fronterizas como Venezuela, Brasil y zona pacífico. Se estima que por esas tres fronteras, debido a su porosidad y ausencia de institucionalidad estatal, sale el 70% de clorhidrato de cocaína a nivel nacional.	1	0,9	0,9
Capacidades de Contrainsurgencia	Mide la inclusión de tendencias de rápida	Tendencias de instrumentalización	Alta capacidad financiera por la participación territorial en los dos eslabones de la cadena del narcotráfico: cultivo de hoja de coca y producción de narcóticos (los cultivos	0,8	0,7	0,7

	afectación a la fuerza pública		aumentaron un 14% sobre territorio nacional) y explotación ilícita de yacimientos mineros (aumentó en un 12% de 2018 a 2022).			
			Instrumentalización de población civil para generar acciones violentas en contra de la fuerza pública, incurriendo en conductas penales como asonada y secuestro simple.	1,2	1,1	1,1
Eficiencia en Producción de Órdenes	Mide la rapidez y precisión en la generación de órdenes con impacto operacional	Eficiencia en la gestión operacional	Necesidades de tecnificación en PMTD, debido a la rápida evolución que hay entre las variables crimen transnacional y tecnologías de disrupción.	2	1,9	1,9
Impacto en Seguridad Nacional	Analiza el efecto de las operaciones en la seguridad y estabilidad del territorio.	Reducción de incidentes (%)	Transgresión medio ambiental	0,45	0,44	0,44
			Transgresión geopolítica territorial	0,35	0,43	0,43
			Transgresión sistemática en contra del dominio cibernético	0,38	0,37	0,37
			Disrupción sistemática por afectación a infraestructura crítica	1	0,9	0,9
			Utilización de redes sociales y otras tecnologías para el reclutamiento de menores en zonas con vulnerabilidad socioeconómica. En Catatumbo el reclutamiento aumentó un 8%, con incidencia de un 18% sobre migrantes venezolanos.	1	0,9	0,9

Nota: elaboración propia con información recuperada de (UNDOC, 2024) (UNDOC, 2022), (UNDOC, 2022); ((ONU), 2025); (OCHA, 2025)

El análisis desarrollado con la matriz, incluyó variables conexas a los factores de inestabilidad registrados en el plan de campaña Ayacucho plus, pero también un análisis categórico tomando como base conceptual las funciones para la conducción de la guerra (FCG). De esta forma, los elementos incluidos en la matriz cuentan con un factor de análisis doctrinal, pero también geoestratégico y centrado en la necesidad real de un contexto operacional cambiante.

Frente a la **FCG de movimiento y maniobra**, que abarca actividades como la proyección de la fuerza y la maniobra táctica, se ve impactada por la necesidad de tecnologías avanzadas para el planeamiento operacional. Los valores obtenidos (1, 0.9 y 0.9) reflejan una dependencia significativa de herramientas disruptivas para mejorar la precisión en la toma de decisiones. Sin embargo, los resultados asociados al análisis georreferencial del territorio (0.5, 0.4 y 0.4) y la delimitación de escenarios estratégicos (0.5, 0.7 y 0.7) evidencian brechas en la implementación de tecnologías que permitan identificar y neutralizar áreas de convergencia criminal.

La **FCG de inteligencia**, esencial para apoyar el entendimiento del ambiente operacional, también enfrenta retos significativos. La **gestión de amenazas irregulares**, por ejemplo, destaca el crecimiento de insurgencias post acuerdo, con un aumento del 26.3% en regiones críticas como Catatumbo, Putumayo y Cauca. Este incremento se refleja en valores como 0.3, 0.4 y 0.4, que subrayan la necesidad de fortalecer las capacidades de recolección y análisis de información. Además, la inclusión de metodologías asimétricas, como el uso de drones (0.7, 0.8 y 0.8), resalta la urgencia de integrar tecnologías de vigilancia más sofisticadas para contrarrestar estas amenazas.

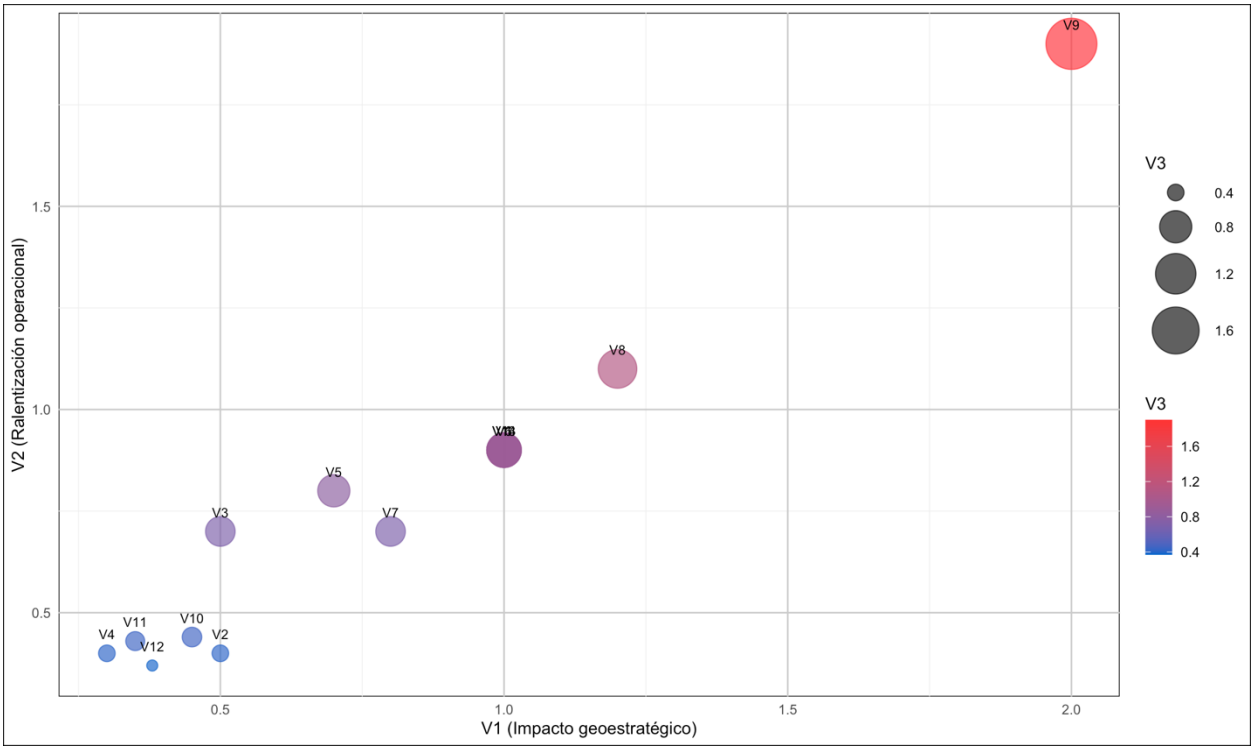
En cuanto a la **FCG de fuegos**, que incluye la integración de todas las formas de fuegos y el apoyo a la selección y priorización de blancos, es evidente que los grupos insurgentes han desarrollado capacidades avanzadas que desafían las operaciones militares. Esto se refleja en la configuración de nuevas capacidades insurgentes vinculadas al crimen transnacional (1, 0.9 y 0.9), lo que exige una mayor precisión en la identificación y neutralización de objetivos estratégicos.

La **FCG de sostenimiento**, que abarca logística, mantenimiento y apoyo de ingeniería, también se ve afectada por la rápida evolución del crimen transnacional y las tecnologías de disrupción. Los valores obtenidos en la eficiencia en la producción de órdenes (2, 1.9 y 1.9) evidencian una necesidad crítica de actualizar los procesos de planeamiento y toma de decisiones para garantizar una respuesta ágil y efectiva ante amenazas emergentes.

Por último, la **FCG de mando tipo misión**, que incluye el proceso de operaciones, la gestión del conocimiento y la sincronización de capacidades, se enfrenta a desafíos relacionados con la coordinación y la integración de tecnologías avanzadas. Los valores asociados a la transgresión medioambiental (0.45, 0.44 y 0.44), geopolítica territorial (0.35, 0.43 y 0.43) y cibernética (0.38, 0.37 y 0.37) reflejan afectaciones moderadas, mientras que la disrupción en infraestructura crítica (1, 0.9 y 0.9) y el reclutamiento de menores (1, 0.9 y 0.9) subrayan la necesidad de estrategias más robustas y coordinadas.

Con base en lo anterior, los resultados presentados en la Tabla 1 Matriz de análsis de amenaza refinada – contexto colombiano, en conjunto con las funciones de conducción de la guerra descritas en el MFRE 1-03, evidencian que las tecnologías necesarias para abordar las dinámicas complejas de amenazas con rápida capacidad de cambio y/o evolución se centran en mejorar el planeamiento operacional y en el impacto sobre la seguridad nacional. Véase la figura 4 para continuar:

Figura 4. Medición de variables con impacto estratégico y ralentización operacional



Nota: elaboración propia con Rstudio

Con esas dos categorías alineadas entre el planeamiento Operacional e impacto en Seguridad Nacional y las funciones para la conducción dela guerra, se establecen como factores de atención primaria para el estudio del proceso consiguiente (vigilancia tecnológica), las variables cualitativas que se exponen a continuación:

- **VC1[2]:** Tecnologías para la reducción de incertidumbres y proceso para la toma de decisiones
- **VC2:** Tecnología de detección de amenazas en zonas de difícil acceso.
- **VC3:** Protección para reducir afectación a infraestructura crítica
- **VC4:** Estrategias ligadas a operaciones de información.

Vigilancia tecnológica para la identificación de enfoques de defensa y concertación de acciones de intervención temprana.

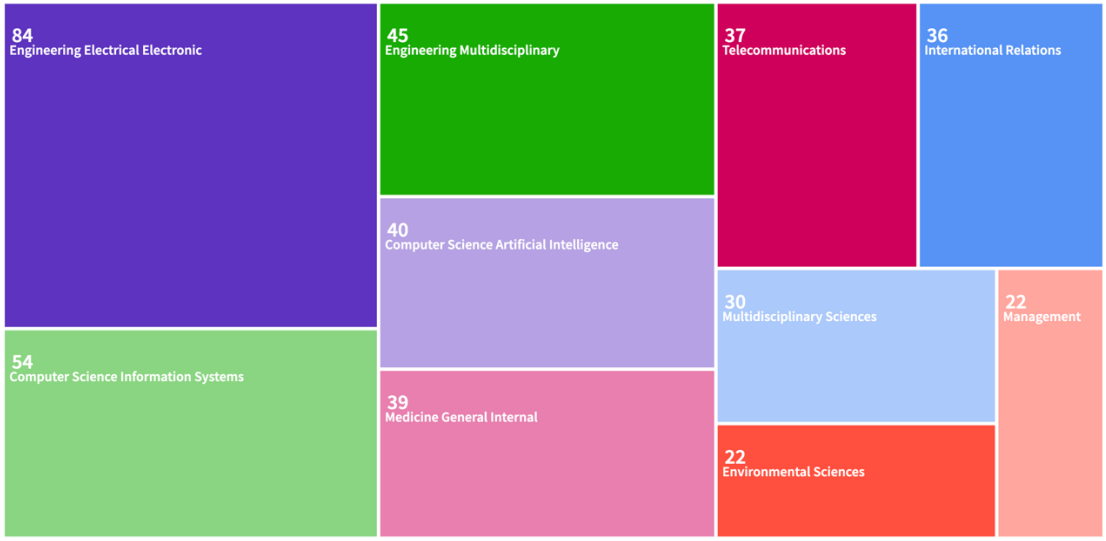
Las variables cualitativas que se plantearon a partir del análisis con la matriz de amenazas, conducen y/o direccionan el trabajo de investigación a una fase de construcción de conocimiento basada en dos técnicas diferentes: el análisis cienciométrico sobre los elementos que tecnológicos que mayor concurrencia tienen en un set de datos conformado por 612 artículos extraídos de Web of Science[3] y una matriz de análisis de patentes alineada con las **VC** y **FCG**.

Para el análisis cienciométrico se utilizó como ecuación de búsqueda: * military*strategy*security*protection*technology*defense. Los resultados se exponen a continuación:

Figura 5. Campos de investigación con mayor publicación multidisciplinar conexos con defensa nacional.

[2] Variable cualitativa

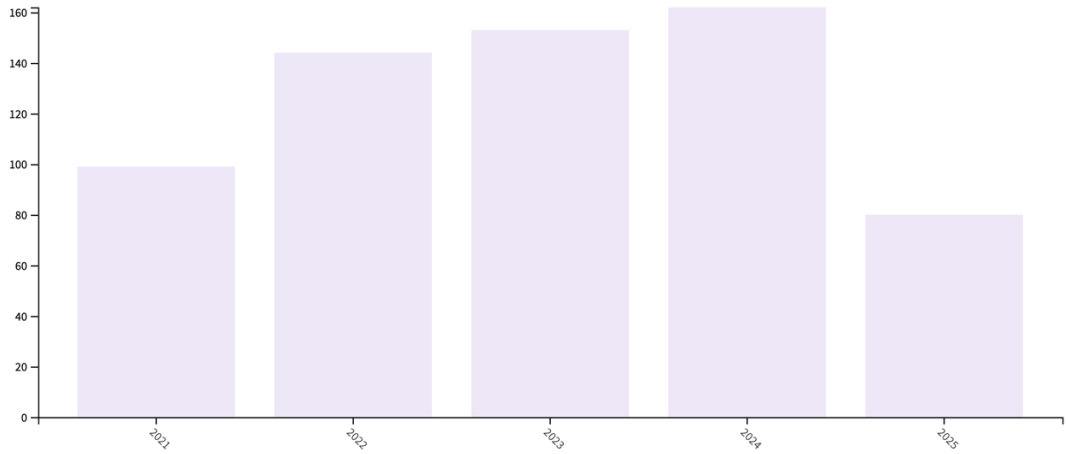
[3] Los 612 artículos se presentan en el Anexo 1_Texto plano_WOS



Nota: información recuperada de WOS (2025)

El resultado estadístico de WOS (2025) permite ver que los campos de la ingeniería electrónica, las ciencias computacionales y los sistemas de información, así como las ciencias asociadas con inteligencia artificial y ciencias multidisciplinares, son los campos con mayor investigación centrada en ejes transversales multidisciplinares correlacionados con defensa nacional.

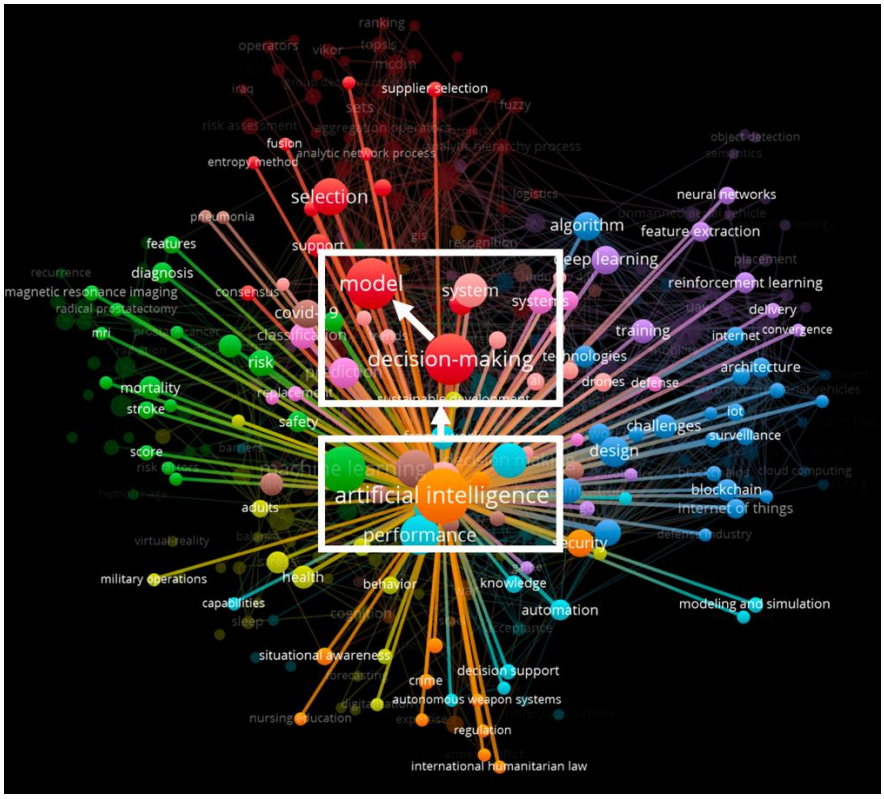
Figura 6. Publicación por años



Nota: información recuperada de WOS (2025)

En cuanto a la producción de conocimiento científico – tecnológico relacionado con el sector defensa, los años 2022 y 2024 son los que mayor contribución científica y cuantitativa registran en el marco de investigación indexadle. Los temas y términos concurrentes con tecnología y defensa y/o seguridad nacional son:

Figura 7. Clúster de concurrencia de términos nº 1

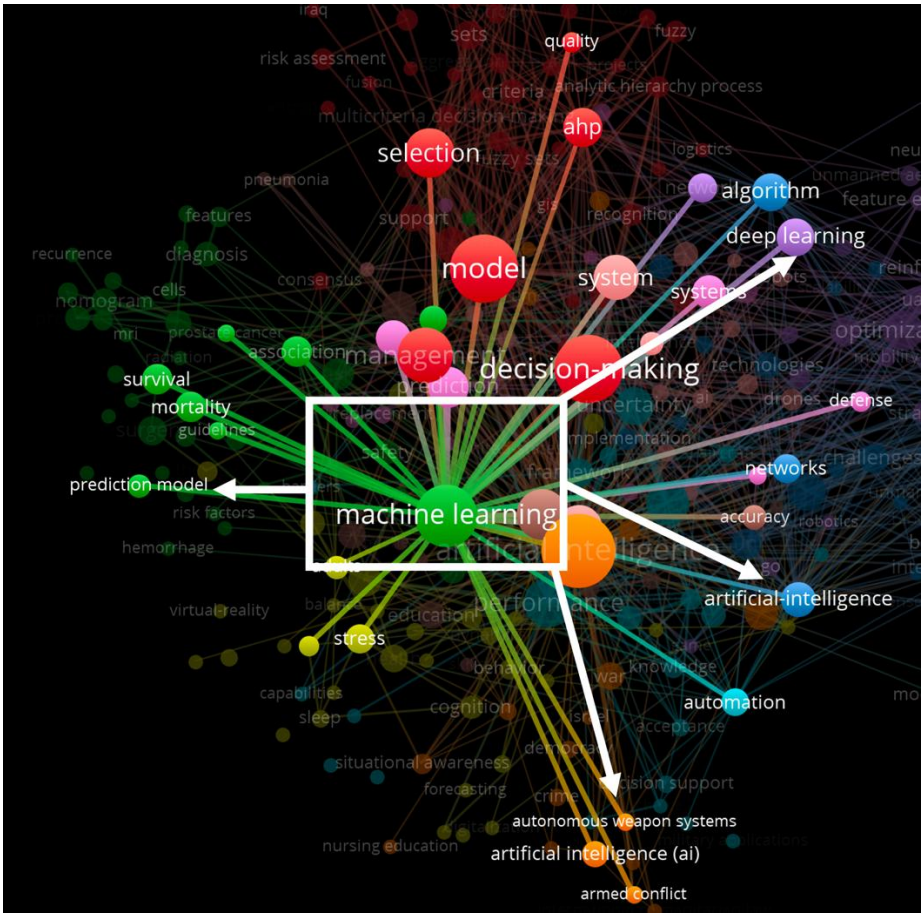


Nota: elaboración propia con software Vos Viewer

El análisis de datos por concurrencia de términos al que se someten los 612 artículos encontrados en WOS arroja tres clúster con mayor concentración para los términos defensa y/o seguridad nacional y tecnología tendencia.

El clúster más fuerte (Figura 7) representa la relación conceptual creada entre inteligencia artificial y modelos para la toma de decisiones.

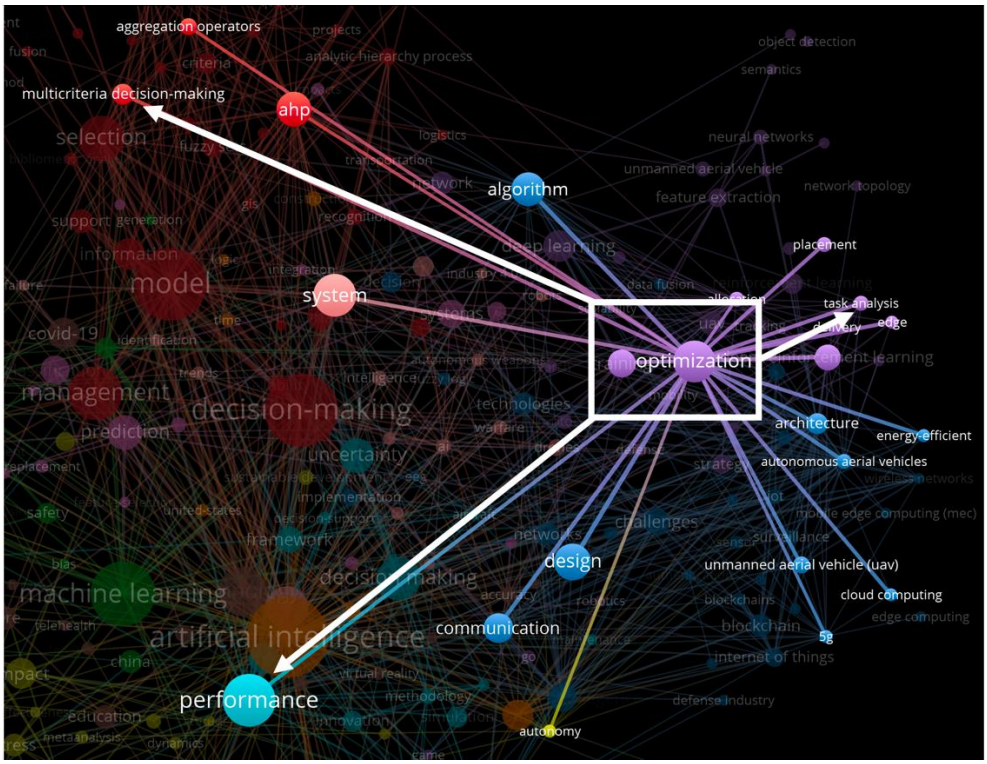
Figura 8. Clúster de concurrencia de términos nº 2



Nota: elaboración propia con software Vos Viewer

En el clúster nº 2, el tema concurrente es el machine learning, el cual se agrupa con modelos predictivos para la toma de decisiones y los procesos de aprendizaje profundo (Deep learning), cuya relación directa se da con las subvariables de inteligencia artificial, sistemas de armas autónomos y conflicto armado convencional.

Figura 9. Clúster de concurrencia de términos nº 3



Nota: elaboración propia con software Vos Viewer

En cuanto al clúster nº 3, el término concurrente es la optimización, cuya conexión se da con el rendimiento organizacional, el análisis y cumplimiento de misión por tareas, y al análisis multicriterio.

Los tres clústeres presentados abordan elementos tecnológicos que van desde la inclusión de inteligencia artificial y su relación con la toma de decisiones, así como la implementación de modelos predictivos con machine learning y optimización de procesos y decisiones con base en el análisis de tareas y decisión militar multicriterio.

Estos tres hallazgos se alinean con el núcleo de las variables cualitativas porque:

- Primero, **VC1** es igual a reducción de incertidumbre, y para la intervención de zonas estratégicas afectadas por sub variables con incidentes a la seguridad nacional. En este caso, incorporación de inteligencia artificial para analizar amenazas en puntos geográficos afectados por la convergencia de factores criminales como narcotráfico, violación de derechos humanos, explotación ilícita de yacimientos mineros, desforestación y delitos ambientales, narcotráfico en sus tres eslabones, transgresiones fronterizas y condiciones de pobreza multidimensional. Lo anterior, una ecuación para el aumento de violencia según

deducciones científicas interpretables en Hulme y Weir (2021), y Mueller y Techasunthornwat (2020).

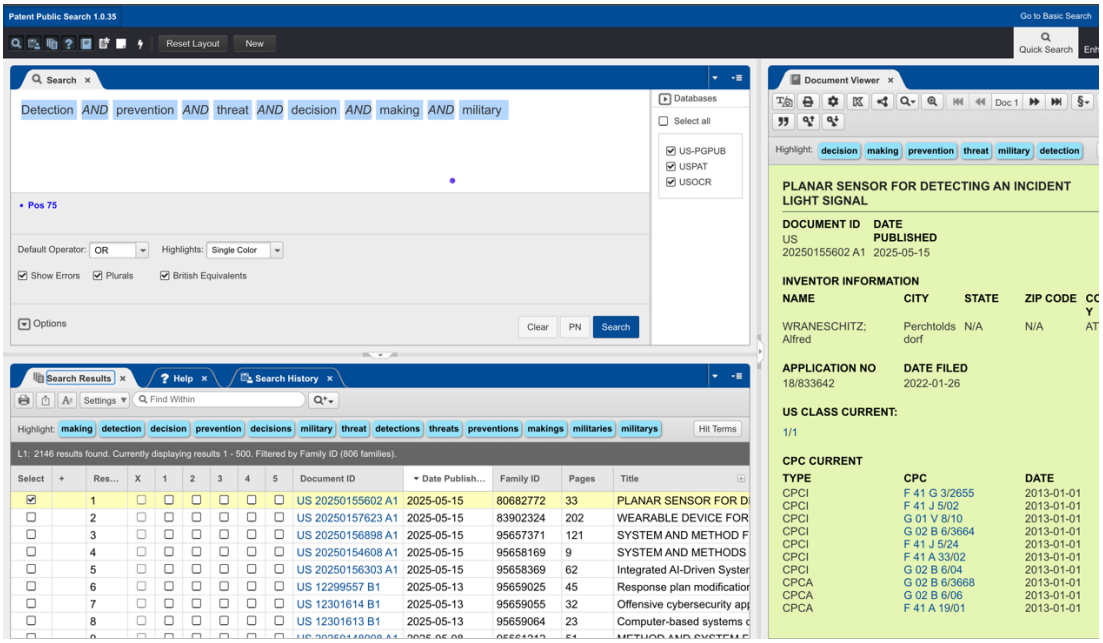
- Segundo, **VC2** es igual a tecnologías de detección en zonas de difícil acceso. En el clúster 2 se habla de conexión científica entre machine learning, aprendizaje profundo, modelos de predicción y arma autónomas, así como aeronaves no tripuladas (cluster nº3). Eso significa que la impelementación de modelos preventivos es una capacidad para la detección temprana de amenazas o nuevos factores de inestabilidad.
- Tercero, **VC3** es igual a reducción de afectación a infraestructura crítica, lo que ameritaría una optimización de procesos para el análisis y determinación de tareas propicias en el teatro operacional con mayor riesgo de afectación a partir de análisis de datos y modelos predictivos sobre hechos y posibles ocurrencias.
- Cuarto, **VC4** es igual a operaciones de información lo cual hace alusión a la utilización de inteligencia artificial para construir modelos algorítimos para la rápida difusión de información.

Con la identificación de las necesidades tecnológicas a partir del estudio cienciométrico se pasa a la búsqueda de patentes con la ecuación de búsqueda extraída de la explicación de VC 1, 2, 3 y 4:

- **E1:** *Detection*prevention* threat * decision* making*military*
- **E2**: *Environment *threat * prevention* system* trend* method* outcome* military*
- **E3**: *New* threat*prevention * system* strategy* technology* test* approved* technique*

Las ecuaciones de búsqueda se incorporaron en la base de datos de patentes públicas USPTO, y con **E1** se encontraron 2600 patentes, tal y como se registra en la figura 10:

Figura 10. Patentes halladas con **E1**



Nota: información recuperada de USPTO (2025)

Para la delimitación y selección de patentes se utilizan los siguientes criterios: inteligencia artificial, análisis de datos y tecnologías para interpretar y reducir incertidumbre en escenarios estratégicos afectados por factores criminales, como narcotráfico, violaciones de derechos humanos, explotación ilícita de recursos, entre otros.

Las patentes seleccionadas se exponen y explican en la tabla del Anexo 1, y desde su alineación con las VC se plantean las deducciones consiguientes:

El Anexo 1 presentada una visión integral de cómo las patentes seleccionadas abordan las variables críticas y su relación con las funciones para la conducción de la guerra. Cada una de estas tecnologías se alinea con las necesidades operacionales en escenarios estratégicos, aportando capacidades innovadoras que fortalecen la respuesta ante desafíos complejos. Por ejemplo, la reducción de incertidumbre, representada en la primera variable crítica, encuentra en patentes como *US 12299557 B1* y *US 20240111305 A1* soluciones que aprovechan la inteligencia artificial y el uso de drones para recopilar y analizar datos en tiempo real.

Estas herramientas identifican patrones y amenazas en zonas estratégicas afectadas por factores como el narcotráfico o la explotación ilícita de recursos, lo que resulta esencial para mejorar la toma de decisiones en entornos operacionales dinámicos.

Por otro lado, las tecnologías de detección en zonas de difícil acceso, asociadas a la segunda variable crítica, son fundamentales para apoyar la proyección de fuerzas y la maniobra táctica, componentes esenciales dentro de las funciones de movimiento y maniobra.

Patentes como *US 20250155602 A1* y *US 20240111305 A1* resaltan su capacidad de empleo de sensores avanzados y aeronaves no tripuladas, facilitando la detección temprana de amenazas en áreas remotas. Esto no solo mejora la capacidad de respuesta táctica, sino que también optimiza el planeamiento operacional al proporcionar información oportuna sobre el contexto operacional.

De la misma manera, la protección de infraestructuras críticas, conectadas a la tercera variable crítica, tiene un impacto en las funciones de sostenimiento y fuegos. Tecnologías como las diseñadas en *US 12261822 B2* y *US 20250112988 A1* ofrecen soluciones para prevenir el surgimiento de amenazas cibernéticas y coordinar respuestas ante posibles afectaciones a activos estratégicos.

Es así, como la implementación de modelos predictivos y algoritmos de aprendizaje profundo no solo protegen infraestructuras, sino que también producen mayor precisión en la selección de blancos estratégicos, reduciendo la capacidad operativa de actores hostiles y minimizando riesgos en escenarios con afectación histórica.

En cuanto a las operaciones de información, representadas en la cuarta variable crítica, la rapidez y efectividad en la difusión de datos son esenciales para las funciones de mando tipo misión. Patentes como *US 12299557 B1* y *US 20250112988 A1* destacan por la configuración de modelos algorítmicos que priorizan la transmisión de información clave.

Ello sincroniza capacidades, mejorando la gestión operacional y la articulación geo estratégica en tiempo real, especialmente en contextos donde hay condiciones de conflicto en constante cambio, requiriendo un método de respuesta ágil y preciso.

El análisis de estas patentes, desde una perspectiva doctrinal y geoestratégica, evidencia cómo las tecnologías seleccionadas impactan directamente en las funciones esenciales para la conducción de la guerra.

Herramientas disruptivas como drones, sensores avanzados y algoritmos predictivos fortalecen la movilidad táctica, la recolección de inteligencia y la protección de infraestructuras críticas, mientras que modelos algorítmicos aseguran una gestión eficiente del conocimiento y una mejor coordinación operativa.

Estas capacidades no solo fortalecen el marco estratégico y operacional para afrontar desafíos actuales (CGFM, 2023), sino que también preparan el terreno para responder a amenazas emergentes de manera más efectiva y adaptada a las necesidades cambiantes del entorno estratégico. La integración de estas tecnologías representa una fase transitoria hacia la modernización de las capacidades operativas en escenarios de alta complejidad.

Líneas estratégicas de proyección tecnológica por incluir en el Plan de Transformación de las FFMM 2042.

El estudio de vigilancia tecnológica desarrollado demostró que las tendencias contextuales giran en torno a una integración gradual de enfoques asociados con la estrategia militar influenciada por factores conectados con el análisis de terreno, la reducción de incertidumbre y la toma de decisiones.

Bajo el anterior concepto, la evolución tecnológica y su impacto en las estrategias de seguridad y defensa nacional han transformado los paradigmas tradicionales de planeación militar. En este contexto, la incorporación de tecnologías de quinta generación (5G) al marco funcional las fuerzas de dominio y poder terrestre se posiciona como un eje estratégico para responder a amenazas persistentes y emergentes en zonas de intervención primaria.

Estas tecnologías no solo amplían las capacidades operativas, sino que también redefinen los enfoques geoestratégicos necesarios para enfrentar fenómenos como la convergencia criminal, el narcotráfico, la explotación ilícita de recursos, la transgresión fronteriza y el deterioro ambiental.

El análisis desarrollado hasta este punto articula elementos doctrinales, geoestratégicos y tecnológicos para plantear líneas estratégicas de proyección tecnológica que puedan ser incluidas en el Plan de Transformación de las FFMM 2042.

A partir de un enfoque multidimensional, se exponen las tecnologías disruptivas que optimicen el monitoreo, la identificación y la neutralización de amenazas en contextos operacionales complejos, asegurando una respuesta integral y adaptada a las necesidades del entorno estratégico.

Para configurar las líneas, se plantea la matriz relacionada en la tabla:

Tabla 3. Líneas estratégicas

Línea Estratégica	Descripción	Objetivos	Indicadores	Contribución Geoestratégica
Inteligencia Artificial para la Reducción de Incertidumbre	Implementación de sistemas basados en inteligencia artificial (IA) para el análisis geoestratégico en tiempo real, integrando datos operacionales, ambientales y sociales.	- Mejorar la capacidad de análisis predictivo para la toma de decisiones.	- Porcentaje de reducción en el tiempo de toma de decisiones estratégicas.	- Fortalecimiento del planeamiento operacional en zonas de convergencia criminal.
		- Reducir la incertidumbre en escenarios estratégicos con múltiples factores de inestabilidad.	- Número de escenarios de riesgo identificados con precisión mediante IA.	- Incremento en la capacidad de anticipación y prevención de amenazas en puntos críticos como fronteras y ecosistemas vulnerables.
Sistemas de Detección en Zonas de Difícil Acceso	Desarrollo e integración de tecnologías como drones, sensores avanzados y modelos predictivos para la vigilancia y monitoreo en áreas remotas o de difícil acceso.	- Aumentar la capacidad de detección temprana de amenazas.	- Número de amenazas detectadas en zonas remotas.	- Mejora de la cobertura operativa en áreas de alta complejidad geográfica.
		- Optimizar el monitoreo en zonas críticas afectadas por factores criminales.	- Reducción del tiempo de respuesta ante incidentes en áreas de difícil acceso.	- Reducción de la actividad criminal en zonas estratégicas como el Catatumbo, el Tapón del Darién y la región amazónica.
Protección de Infraestructura Crítica	Implementación de sistemas de ciberseguridad, análisis de datos y algoritmos predictivos para proteger infraestructura clave frente a amenazas físicas y cibernéticas.	- Garantizar la continuidad operativa de infraestructuras críticas.	- Número de incidentes mitigados en infraestructuras críticas.	- Aseguramiento de activos estratégicos como redes de comunicación, instalaciones militares y sistemas de transporte.
		- Prevenir ataques cibernéticos y físicos mediante tecnologías avanzadas.	- Porcentaje de reducción de vulnerabilidades detectadas en sistemas operativos y redes de comunicación.	- Incremento en la resiliencia operativa frente a amenazas cibernéticas y físicas.

Operaciones de Información Basadas en IA	Uso de inteligencia artificial para desarrollar modelos algorítmicos que permitan la difusión rápida y precisa de información estratégica en operaciones de mando.	- Mejorar la coordinación y sincronización de capacidades operativas.	- Tiempo promedio de difusión de órdenes estratégicas.	- Fortalecimiento de las capacidades de mando y control en entornos operativos dinámicos.
		- Incrementar la eficacia en la gestión de información crítica durante operaciones militares.	- Número de operaciones exitosas con soporte de modelos algorítmicos.	- Mejora de la articulación geoestratégica en tiempo real, especialmente en escenarios de conflicto asimétrico.

Fuente: elaboración propia

El análisis de la contribución geoestratégica de las líneas estratégicas propuestas se encuentra profundamente arraigado en los principios de la teoría clásica de defensa nacional, particularmente desde la perspectiva de la escuela realista de Copenhague. Este enfoque resalta la centralidad del Estado como el principal actor en la preservación de la seguridad nacional, enfatizando la importancia de las capacidades materiales, tecnológicas y operativas como elementos esenciales para garantizar la estabilidad frente a amenazas externas e internas. En este sentido, las tecnologías de quinta generación no solo representan una herramienta instrumental para la defensa, sino que también se convierten en un pilar estructural para consolidar la soberanía en territorios estratégicos, especialmente en contextos donde la convergencia criminal y los conflictos asimétricos desafían la capacidad estatal.

Desde la perspectiva realista, la seguridad se entiende como un fenómeno multidimensional, donde cada amenaza debe ser abordada con una respuesta proporcional basada en la acumulación y optimización de recursos estratégicos. Los hallazgos de esta investigación evidencian que la implementación de inteligencia artificial para reducir incertidumbres en escenarios operacionales no solo mejora la capacidad de toma de decisiones, sino que también refuerza la posición del Estado frente a actores no estatales que operan en zonas críticas como el Catatumbo o el Tapón del Darién. Por ejemplo, el uso de tecnologías predictivas basadas en IA permitiría anticipar el comportamiento de grupos insurgentes que, según las estadísticas, han incrementado su capacidad operativa en un 26.3% desde 2016 en regiones clave, lo que subraya la necesidad de herramientas avanzadas para contrarrestar su impacto.

Asimismo, la teoría realista enfatiza la importancia de la defensa territorial como un componente esencial de la seguridad nacional. En este contexto, las tecnologías de detección en zonas de difícil acceso adquieren un valor estratégico incuestionable, ya que facilitan la vigilancia y el monitoreo en áreas donde la presencia estatal es limitada o inexistente. Este enfoque se alinea con los principios de la escuela de Copenhague, que destaca la necesidad de proteger los puntos geoestratégicos como un medio para evitar la transgresión de fronteras y la explotación de vulnerabilidades territoriales. Los datos presentados en este análisis revelan que, en 2023, el 70% del clorhidrato de cocaína producido en Colombia se trafica a través de fronteras porosas, lo que evidencia la urgencia de fortalecer las capacidades de detección y control en estas áreas mediante el uso de drones y sensores avanzados.

Otro aspecto central de la teoría clásica de defensa nacional es la protección de infraestructura crítica, entendida como un elemento clave para garantizar la continuidad operativa del Estado en situaciones de crisis. En este sentido, las tecnologías avanzadas de ciberseguridad y los algoritmos predictivos no solo contribuyen a prevenir ataques físicos y cibernéticos, sino que también refuerzan la resiliencia de los sistemas estratégicos frente a amenazas emergentes. Este enfoque es particularmente relevante en un contexto donde las transgresiones cibernéticas y las disrupciones a infraestructuras críticas representan riesgos significativos para la estabilidad nacional. Por ejemplo, la afectación a redes de comunicación y sistemas operativos podría tener un impacto directo en la capacidad del Estado para responder a incidentes en tiempo real, lo que subraya la importancia de priorizar la inversión en estas tecnologías.

Finalmente, las operaciones de información basadas en inteligencia artificial refuerzan la capacidad del Estado para coordinar y sincronizar sus esfuerzos en entornos operativos dinámicos. Desde la perspectiva de la escuela realista, la gestión del conocimiento y la difusión eficiente de información estratégica son fundamentales para consolidar la autoridad estatal en escenarios de conflicto. Las tecnologías que permiten la rápida transmisión de datos críticos no solo mejoran la eficacia operativa, sino que también fortalecen la cohesión interna del aparato militar, asegurando una respuesta coordinada y adaptada a las necesidades del entorno. Este enfoque es especialmente relevante en contextos donde las dinámicas del conflicto cambian rápidamente, como lo demuestra el aumento del 8% en el reclutamiento de menores en el Catatumbo, con una incidencia del 18% sobre migrantes venezolanos, lo que evidencia la necesidad de estrategias más robustas para contrarrestar estas prácticas.

Así las cosas, el análisis de la contribución geoestratégica de las tecnologías de quinta generación desde la perspectiva de la teoría clásica de defensa nacional resalta la importancia de estas herramientas como un medio para fortalecer la soberanía estatal y garantizar la seguridad en un entorno cada vez más complejo. Las cifras presentadas, como el incremento del 26.3% en las insurgencias post acuerdo y el tráfico del 70% de cocaína a través de fronteras porosas, subrayan la urgencia de adoptar soluciones tecnológicas disruptivas que permitan al Estado mantener su ventaja estratégica frente a actores hostiles. Además, la integración de inteligencia artificial, sistemas de detección avanzada y algoritmos predictivos no solo optimiza la capacidad operativa de las Fuerzas Militares, sino que también refuerza la posición del Estado como garante de la seguridad y el bienestar de su población. Este enfoque multidimensional, alineado con los

principios de la escuela realista de Copenhague, proporciona un marco sólido para la modernización de las capacidades de defensa nacional en el contexto del Plan de Transformación de las FFMM 2042.

Conclusiones

Las conclusiones de esta investigación surgen como una síntesis integral de los hallazgos obtenidos a través del análisis de necesidades estratégicas, la aplicación de metodologías avanzadas y el estudio de tecnologías de quinta generación. Estas conclusiones responden a la pregunta de investigación planteada, destacando cómo los enfoques tecnológicos pueden adaptarse para fortalecer las capacidades de vigilancia, identificación y monitoreo en zonas de intervención primaria. Cada apartado del estudio se conecta con las variables críticas y los elementos geoestratégicos que configuran el marco de acción para las Fuerzas Militares, abordando tanto los desafíos actuales como las proyecciones futuras de modernización operativa.

Desde la perspectiva metodológica, el diseño de la matriz de análisis refinada permitió estructurar un marco evaluativo basado en modelos multicriterio, análisis intervalar y reducción de incertidumbre. Este enfoque metodológico, fundamentado en las contribuciones de Bojanić (2022), Fingar (2020) y el Director Oficial de Inteligencia Norteamericana (2025), integró elementos doctrinales como las funciones para la conducción de la guerra (FCG) y datos contextuales específicos del entorno colombiano. Los resultados obtenidos reflejan una dependencia significativa de tecnologías disruptivas para optimizar el planeamiento operacional, evidenciada en valores como 1.0 y 0.9 en las categorías de reducción de incertidumbre y delimitación de escenarios estratégicos. Este marco metodológico no solo facilitó la identificación de brechas tecnológicas, sino que también estableció un vínculo directo entre las necesidades operacionales y las capacidades tecnológicas requeridas.

En cuanto a los resultados relacionados con las amenazas irregulares, el análisis evidenció un crecimiento del 26.3% en las insurgencias post acuerdo desde 2016, concentrado en regiones como Catatumbo, Putumayo y Cauca. Este fenómeno, combinado con el uso de metodologías asimétricas como drones, destacó la urgencia de integrar tecnologías avanzadas de detección y monitoreo. Por ejemplo, los valores de 0.7 y 0.8 asociados a estas metodologías subrayan la necesidad de sistemas que permitan una respuesta ágil y efectiva en zonas de difícil acceso. Además, la relación entre crimen transnacional y vulnerabilidades territoriales, como el tráfico del 70% de cocaína a través de fronteras porosas, refuerza la importancia de fortalecer las capacidades de vigilancia en áreas críticas mediante el uso de sensores avanzados y aeronaves no tripuladas.

Otro hallazgo clave se relaciona con la protección de infraestructuras críticas, donde la implementación de algoritmos predictivos y sistemas de ciberseguridad demostró ser esencial para

garantizar la continuidad operativa frente a amenazas emergentes. Los valores de 1.0 y 0.9 en la categoría de disrupción en infraestructura crítica reflejan una alta prioridad en este ámbito, especialmente en un contexto donde las transgresiones cibernéticas representan riesgos significativos. Asimismo, el análisis de datos reveló que el aumento del 14% en los cultivos de cocaína y el 12% en la explotación ilícita de yacimientos mineros desde 2018 subrayan la necesidad de optimizar los procesos de sostenimiento y fuegos, asegurando una respuesta coordinada y eficiente ante estas amenazas.

Esta investigación demuestra que la integración de tecnologías de quinta generación, como la inteligencia artificial, los drones y los algoritmos predictivos, constituye un pilar fundamental para modernizar las capacidades operativas de las Fuerzas Militares en el contexto del Plan de Transformación FFMM 2042. Los hallazgos, respaldados por cifras como el aumento del 26.3% en insurgencias y el tráfico del 70% de cocaína a través de fronteras vulnerables, subrayan la necesidad de adoptar soluciones tecnológicas que fortalezcan la soberanía estatal y la seguridad nacional. Este enfoque, alineado con los principios de la teoría clásica de defensa nacional, proporciona un marco estratégico para enfrentar las amenazas persistentes y emergentes en un entorno cada vez más complejo y dinámico.

La implementación de estas tecnologías no solo optimiza la capacidad de respuesta operativa, sino que también posiciona al Estado como un actor resiliente y preparado para los desafíos del futuro.

Referencias

(ONU), O. d. (11 de mayo de 2025). *ONU Derechos Humanos expresa su alarma por el reclutamiento de niñas, niños y adolescentes en Catatumbo, y por la situación de riesgo que siguen viviendo las comunidades y personas defensoras en esta región de Colombia*. Obtenido de https://www.hchr.org.co/historias_destacadas/onu-derechos-humanos-expresa-su-alarma-por-el-reclutamiento-de-ninas-ninos-y-adolescentes-en-catatumbo-y-por-la-situacion-de-riesgo-que-siguen-viviendo-las-comunidades-y-personas-defensoras-en-esta/

Bojanić, D. (2022). The theoretical and methodological analysis of challenges, risks and threats in modern theory of national security. *Vojno delo, 7*(2), 1-17.

CGFM. (2023). *MANUAL FUNDAMENTAL CONJUNTO- MFC 3-0 OPERACIONES CONJUNTA.* Bogotá D.C.: Pub. CGFF.

Corn, G. (2021). National Security Decision-Making in the Age of Technology: Delivering Outcomes On Time and On Target. (W. C. American University, Ed.) *Joournal of National Secuirity Law y Policy, 61*, 1-10.

DANE. (12 de diciembre de 2022). *Geovisor Indicadores Regionales*. Obtenido de https://geoportal.dane.gov.co/geovisores/sociedad/indicadores-regionales/

Defensoría del Pueblo. (20 de enero de 2025). Obtenido de Se agrava la crisis humanitaria en el Catatumbo: más de 36.000 personas desplazadas: https://www.defensoria.gov.co/-/se-agrava-la-crisis-humanitaria-en-el-catatumbo-36.000-personas-desplazadas?redirect=%2Fen%2Fweb%2Fguest%2Fhome

Ejército Nacional de Colombia. (2020). Guía de Planeamiento Estratégico. *Informe Técnico*. Colombia: Publicación EJC.

Epstein, G., DiEuliis, D., & Urich, Q. (2023). How Emerging Technologies Become Emerging Threats: Workshop Report. *Center for the Study of Weapons of Mass Destruction*, 1-7.

Fingar, T. (2020). Reducing uncertainty: Intelligence analysis and national security. *Stanford University Press.*, 1-10.

Global Forest Watch. (2024). *Deforestación - Colombia*. Obtenido de Dashboard de control: https://www.globalforestwatch.org/dashboards/country/COL/?map=eyJjYW5Cb3VuZCI6dHJ1ZX0%3D

Gonzáles, J. (2024). Geopolítica del narcotráfico en la zona ZEII Pacífico Nariñense: análisis estructural y líneas estratégicas. *Trabajo de investigación de maestría*. Repositorio ESDEGUE: https://www.esdegrepositorio.edu.co/handle/20.500.14205/11011.

Gonzáles, J. (2024). Geopolítica del narcotráfico en la zona ZEII Pacífico Nariñense: análisis estructural y líneas estratégicas. *Trabajo de investigación de maestría*. Repositorio ESDEGUE: https://www.esdegrepositorio.edu.co/handle/20.500.14205/11011.

González, E. (2022). Geopolítica del narcotráfico, un análisis cualitativo de la relación que hay entre geografía, territorio, tráfico de narcóticos y factores de tipología poblacional. *Artículo de investigación - trabajo de maestría*. Bogotá D.C.: Respositorio ESDEGUE: https://esdegrepositorio.edu.co/handle/20.500.14205/11124.

Hulme, K., & Weir, D. (2021). Environmental protection in armed conflict. . *Research handbook on international environmental law - Edward Elgar Publishing.*, 392-411.

Ivančík, R. (2021). Security theory: security as a multidimensional phenomenon. *Vojenské Reflexie*, *3*(32-45), 32-53.

Jiménez, B., Villa, E., & Bermúdez, J. (. (2020). La gestión de la tecnología y la innovación en el sector defensa: resultados desde un análisis bibliométrico. *Revista Virtual Universidad Católica del Norte*, *59*, 45-70.

Méndez, L. (2022). La política de seguridad y defensa como estrategia principal para ejercer el control efectivo en el Catatumbo. *Estrategia Poder y Desarrollo*, *1*(1), 75-82.

Mueller, H., & Techasunthornwat, C. (2020). *Conflict and poverty*. Washington: World Bank.

Nance, B. (1999). An update on national missile defense. *Comparative Strategy*, *18*(3), 239-243.

OCHA. (marzo de 2025). *Colombia: Informe de situación humanitaria 2025 - enero a febrero de 2025 (publicado el 21 de marzo de 2025)*. Obtenido de https://www.unocha.org/publications/report/colombia/colombia-informe-de-situacion-humanitaria-2025-enero-febrero-de-2025-publicado-el-21-de-marzo-de-2025

Oficina de las Naciones Unidas en contra de la Droga y el Delito. (2024). *Monitoreo de Territorios con Presencia de Cultivos de Coca*. Obtenido de https://www.unodc.org/documents/crop-monitoring/Colombia/Colombia_monitoreo_2023.pdf

ONU (11 de mayo de 2025). *ONU Derechos Humanos expresa su alarma por el reclutamiento de niñas, niños y adolescentes en Catatumbo, y por la situación de riesgo que siguen viviendo las comunidades y personas defensoras en esta región de Colombia*. Obtenido de

https://www.hchr.org.co/historias_destacadas/onu-derechos-humanos-expresa-su-alarma-por-el-reclutamiento-de-ninas-ninos-y-adolescentes-en-catatumbo-y-por-la-situacion-de-riesgo-que-siguen-viviendo-las-comunidades-y-personas-defensoras-en-esta/

Rueda, T., & J., C. (2022). Estudio prospectivo para diseñar la estrategia de defensa nacional sobre la región del Catatumbo a 2042. *Trabajo de investigación de maestría*. Bogotá D.C.: Repositorio de la Universidad de Externado de Colombia.

Santoyo, W. J. (2024). Potencial de las capacidades de inteligencia de señales del Ejército Nacional para anticipar y responder a desastres naturales. *Trabajo de grado - artículo de maestría*. Bogotá D.C.: Repositorio de ESDEGUE: https://esdegrepositorio.edu.co/handle/20.500.14205/10995.

Servicio de Investigación del Congreso. (2023). National Security Implications of Fifth Generation (5G) Mobile Technologies. *Análisis técnico*. Publciación Congreso EEUU: https://crsreports.congress.gov | IF11251 · VERSION 19.

Thee, M. (2025). *Military technology, military strategy and the arms race.* . Bogotá D.C.: Taylor & Francis.

UNDOC. (2022). Informe de Explotación Ilícita de Yacimientos Mineros . *UNDOC PUB.*, 1-48.

UNDOC. (2022). *Informe de Monitoreo de Cultivos de Hoja Ilegal de Coca* . Bogotá : Pub. UNDOC.

Anexos

Anexo 1. Patentes seleccionadas

Patente	Título	VC1: Reducción de incertidumbre	VC2: Tecnologías de detección	VC3: Reducción de afectación a infraestructura crítica	VC4: Operaciones de información
US 12299557 B1	*Response plan modification through artificial intelligence applied to ambient data communicated to an incident commander*	Utiliza inteligencia artificial para analizar datos ambientales y reducir incertidumbre en escenarios estratégicos complejos.	Incorpora modelos predictivos en tiempo real para detectar amenazas emergentes en zonas críticas.	Optimiza planes de acción mediante análisis avanzado, reduciendo riesgos en infraestructuras críticas.	Facilita la toma de decisiones rápidas a través de modelos algorítmicos que priorizan la difusión de información clave.
US 20250155602 A1	*Planar sensor for detecting an incident light signal*	Permite identificar patrones de luz asociados a actividades ilícitas, contribuyendo al análisis de amenazas en territorios sensibles.	Sensores avanzados para la detección en áreas de difícil acceso, adaptados a condiciones geográficas adversas.	Mejora la vigilancia de infraestructuras críticas mediante sensores de alta precisión que detectan anomalías en tiempo real.	Genera datos procesables que pueden ser utilizados para informar y coordinar respuestas rápidas.
US 20250112988 A1	*A method for detecting synthetic voice and video calls*	Reduce la incertidumbre al identificar comunicaciones falsas que podrían ser utilizadas para actividades criminales.	Emplea machine learning para detectar patrones en comunicaciones sintéticas, incluso en zonas remotas.	Protege infraestructuras críticas al prevenir el uso de comunicaciones falsas para coordinar ataques.	Apoya operaciones de información al validar la autenticidad de las comunicaciones en tiempo real.

US 12261822 B2	*Network threat prediction and blocking*	Analiza datos de red para anticipar amenazas cibernéticas que podrían impactar la seguridad nacional.	Implementa tecnologías de aprendizaje profundo para predecir y bloquear amenazas en redes complejas.	Protege infraestructuras digitales críticas mediante la prevención de ciberataques.	Proporciona información estratégica sobre amenazas cibernéticas para la toma de decisiones rápidas y efectivas.
US 20240111305 A1	*Unmanned aerial vehicle event response system and method*	Reduce la incertidumbre al emplear drones para recopilar datos en tiempo real en zonas estratégicas afectadas por amenazas.	Utiliza aeronaves no tripuladas para acceder a áreas de difícil acceso, mejorando la capacidad de detección temprana.	Minimiza riesgos para infraestructuras críticas mediante el monitoreo constante desde el aire.	Permite la transmisión inmediata de datos recolectados por drones para coordinar respuestas operativas.

Fuente: elaboración propia con información recuperada de USTPO (2025)