Influencia de la Geopolítica de Inteligencia Artificial en el Enfoque Geoestratégico del Sistema de Defensa Colombiano.

Mayor (EJC) Edwin Hernán Franco Tarazona

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	**:**	EDWIN HERNAN FRANCO TARAZONA
Identificación	**:**	80797155
Programa académico	**:**	ESTRATEGIA Y GEOPOLITICA
Tutor metodológico	**:**	JUAN CAMILO ARISTIZABAL
Tutor temático	**:**	MY. R NELSON SANCHEZ MOLANO
Fecha de entrega	**:**	26 DE SEPTIEMBRE 2025
Extensión	**:**	7594 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

Influencia de la Geopolítica de Inteligencia Artificial en el Enfoque Geoestratégico del Sistema de Defensa Colombiano.

Influence of Artificial Intelligence Geopolitics on the Geostrategic Approach of the Colombian Defense System

MY Edwin Hernán Franco Tarazona [1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: La investigación analiza la influencia de la geopolítica de la inteligencia artificial (IA) en el enfoque geoestratégico del sistema de defensa colombiano. Metodológicamente, se emplearon revisiones científicas y matrices de análisis para identificar factores tecnológicos, económicos y políticos que condicionan la adopción de IA en defensa nacional. Los resultados evidencian que la dependencia tecnológica internacional limita la soberanía estratégica de Colombia, mientras que el rezago en investigación y desarrollo amplifica vulnerabilidades frente a ciberamenazas. Además, se observa un descalce entre las políticas públicas vigentes y las necesidades específicas del sector defensa. Se concluye que Colombia debe fortalecer su autonomía tecnológica mediante inversión en I+D+i+TT, cooperación internacional estratégica y producción científica aplicada. Esto permitirá optimizar la toma de decisiones, el control territorial y la respuesta ante amenazas emergentes en un entorno geopolítico altamente competitivo.

Palabras clave: inteligencia, artificial, geopolítica, defensa, Colombia y seguridad.

Abstract: This study examines the impact of artificial intelligence (AI) geopolitics on Colombia's defense system's geostrategic approach. Methodologically, scientific reviews and analytical matrices were used to identify technological, economic, and political factors influencing AI adoption in national defense. Results reveal that international technological dependence restricts Colombia's strategic sovereignty, while delays in research and development exacerbate vulnerabilities to cyber threats. Additionally, a mismatch exists between current public policies and specific defense sector needs. The study concludes that Colombia must enhance its technological autonomy through investment in R&D+i+TT, strategic international cooperation, and applied scientific production. These measures will improve decision-making processes, territorial control, and responses to emerging threats in a highly competitive geopolitical environment.

Keywords: Artificial Intelligence, Geopolitics, Defense, Colombia, Security.

[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/0009-0000-2033-2633- Contacto: edwin.franco@esdeg.edu.co.

Introducción

El desarrollo y la implementación de la inteligencia artificial (IA) han generado transformaciones profundas en el ámbito geopolítico y geoestratégico a nivel global, redefinido las capacidades de defensa y seguridad nacional, alterando los equilibrios de poder entre los Estados y planteando desafíos inéditos en contextos territoriales altamente conectados. Según Larsen (2022), la IA no solo fortalece las capacidades militares, sino que también introduce tensiones geopolíticas que afectan la estabilidad de las regiones.

En este contexto, Colombia enfrenta retos pues la incorporación de inteligencia artificial en el sistema de defensa nacional plantea interrogantes sobre la soberanía tecnológica y la dependencia de actores internacionales. En un mundo interconectado, la capacidad de adoptar y adaptar estas tecnologías se convierte en un factor crítico para prevenir amenazas complejas y garantizar la seguridad nacional.

Desde una perspectiva geoestratégica, la IA puede optimizar la toma de decisiones en la protección de fronteras, el combate contra el crimen organizado y la ciberseguridad. Sin embargo, también introduce riesgos, como vulnerabilidades frente a ciberataques y el uso indebido de algoritmos por parte de actores no estatales (Knox, 2020).

Las asimetrías tecnológicas entre países del norte y del sur globales son un factor determinante en la capacidad de Colombia para competir en el ámbito internacional. La concentración de recursos tecnológicos en potencias globales refuerza las brechas existentes, limitando el acceso a tecnologías críticas y perpetuando desigualdades en la formulación de políticas de defensa (Negrín, 2022). Además, los desafíos internos como la ralentización tecnológica, desactualización de sistemas de información y construcción de enfoques estratégicos basados en análisis de datos y tecnología estructural disminuyen la capacidad geoestratégica de los conceptos operacionales diseñados para hacerle frente a los 24 factores de inestabilidad planteados en el Plan de Campaña Plus.

En contexto nacional, el surgimiento de la inteligencia artificial desafía las estructuras clásicas de seguridad y defensa. Lo anterior por tres razones. Primero, porque la inteligencia artificial es un fenómeno tecnológico, cuyo uso en materia militar nacional no está claro. El número de investigaciones asociadas al empleo de la IA en contextos militares colombianos

es escaso, y por el contrario, las hipótesis que se configuren alrededor del problema se ciñen a la interpretación metodológica y teórica de fuentes de información predominantes, las cuales nacen de investigaciones asociadas con el campo tecnológico norteamericano, chino, británico, indio y japones[*].

Segundo, no hay entendimiento conceptual acerca del empleo de este tipo instrumentos por parte de sistemas militares que sí son legítimos o actores armados e insurgentes que encontraron en la inteligencia artificial, herramientas relevantes para analizar el terreno o para emplear aeronaves no tripuladas.

Tercero, desde una perspectiva estratégica – institucional, no hay fundamentos doctrinales que permitan incluir el empleo de IA, porque no hay conocimiento previo acerca de sus usos, métodos y medios para su inclusión en procedimientos de defensa transversales como el proceso militar para la toma de decisiones o el estudio de variables de contexto con las que plantear un escenario de naturaleza operacional.

Estas razones se reúnen en un mismo punto confluyente, el de los vacíos epistemológicos que reducen el entendimiento del sector defensa frente a un fenómeno tecnológico que evoluciona de manera secuencial en todas las áreas del conocimiento.

Ante este contexto, analizar la relación entre inteligencia artificial y seguridad y defensa se diversifica, no se queda únicamente en las perspectivas contemporáneas acerca del empleo de la IA para optimizar procesos. Por ello, el estudio de las categorías del problema debe darse en pro de una perspectiva interdisciplinar que se incline a un marco de estudio inicial: la geopolítica de la inteligencia artificial, tema que ya es discusión en modelos analíticos como el software de inteligencia estratégica del Foro Económico Mundial (Wolrd Economic Forum, 2025).

A partir de los argumentos expuestos, es notable entonces que la inteligencia artificial empieza a ocupar puestos estratégicos en el marco del diseño de conceptos operacionales, estrategia de seguridad nacional, pero especialmente: construcción internacional de enfoques geopolíticos direccionados al dominio explícito de la inteligencia artificial, ya sea en espectros intersectoriales o en campos orientados únicamente al tema militar.

[*] Esta afirmación se plantea con base en el análisis de sectores, áreas de publicación y países con mayor gestión y producción científica, que se llevó a cabo en Scopus y Web of Science con la técnica de triangulación.

Por lo anterior, esta investigación expone como pregunta del problema al siguiente interrogante: ¿Cómo influye la geopolítica de la inteligencia artificial en el enfoque geoestratégico del sistema de defensa colombiano?

Responder a este interrogante ameritó analizar los factores de influencia derivados de la inteligencia artificial que influyen en la construcción de enfoques geoestratégicos asociados al diseño de estrategias militares aplicadas (EMA). Para tal fin, se propusieron tres objetivos específicos. El primero, examinar los factores tecnológicos, económicos y políticos que determinan la adopción de inteligencia artificial en el sistema de defensa nacional.

Para tal fin, se realizó una revisión de contribuciones científicas sobre las posturas de Larsen (2022); Knox (2020); CDSE (2018); Arencibia (2021); Negrín (2022); Da Silva (2024); Bossio (2023); Saló y Galceran (2024); Salayer (2020); Slayer (2020); Horowitz, Allen, Saravalle, Frederick y Scharre (2022); Haney et al. (2020); Bistron y Piotrowski (2021); Araya y King (2022); Pătraşcu (2021); Taeihagh (2021).Del primer objetivo surgieron factores clave para estudiar como necesidad institucional la inclusión de inteligencia artificial al marco estratégico del campo de defensa nacional colombiano.

En el segundo objetivo se relacionó con la identificación de las implicaciones que tiene la dependencia tecnológica internacional frente al desarrollo de capacidades de defensa basadas en Inteligencia Artificial. En este objetivo se aplica una técnica de exploración de incidencias a partir de la exposición de vacíos frente a la creación y producción científica en el campo de la defensa, explícitamente, estudiando y explorando las versiones metodológicas y conceptuales desarrolladas por Fernández, Villalba, y Velandia (2024); Blackuvell (1993); Schmidt (2022); MINCIENCIAS (2022); Atencio, Zapata, Aguirre, Jiménez, y Paipa (2025); Ortíz y Fernández (2020); World Economic Forum (2025); Suárez (2023); Ospina & Sanabria (2020); Comando Conjunto Cibernético de las FFMM (CCOCI, 2024); Saló y Galceran (2024).

Una vez se conceptualizaron las categorías del problema, se pasó al desarrollo del tercer objetivo específico final el cual buscaba plantear el alcance que posee la inteligencia artificial en la formulación de enfoques estratégicos y acciones para garantizar. Este objetivo

implicó establecer el alcance que posee la inteligencia artificial en la formulación de enfoques geoestratégicos y acciones estratégicas para garantizar tanto el marco de defensa nacional.

Para tal fin se utilizó una matriz de análisis de alcance que se construyó con base en las contribuciones metodológica de Alizadeh (2012), Mortazavi, Mehrabanfar, Banaitis, y Banaitienė (2016) y Hecklau, Kidschun, Kohl, y Tominaj (2019).

Metodología

Enfoque y alcance de la investigación

Este artículo de investigación cuenta con un enfoque de tipología cualitativa. Para el desarrollo de los objetivos se utilizan las contribuciones metodológicas de Hernández, Fernández y baptista (2010), y por consiguiente el alcance de la investigación es exploratorio – descriptivo.

El alcance del artículo es la realización de un análisis estructural que permita establecer los elementos y factores de inteligencia artificial que a presente y sobre escenarios de futuro influyen e influirán en la formulación de decisiones asociadas con el marco de seguridad y defensa nacional. Cabe destacar que el alcance llega hasta la entrega del análisis, cuyo argumento conceptual está basado en 30 autores.

Diseño y proceso de la investigación

Para llevar a cabo esta investigación se plantearon cuatro fases específicas. La descripción de estas fases es la siguiente:

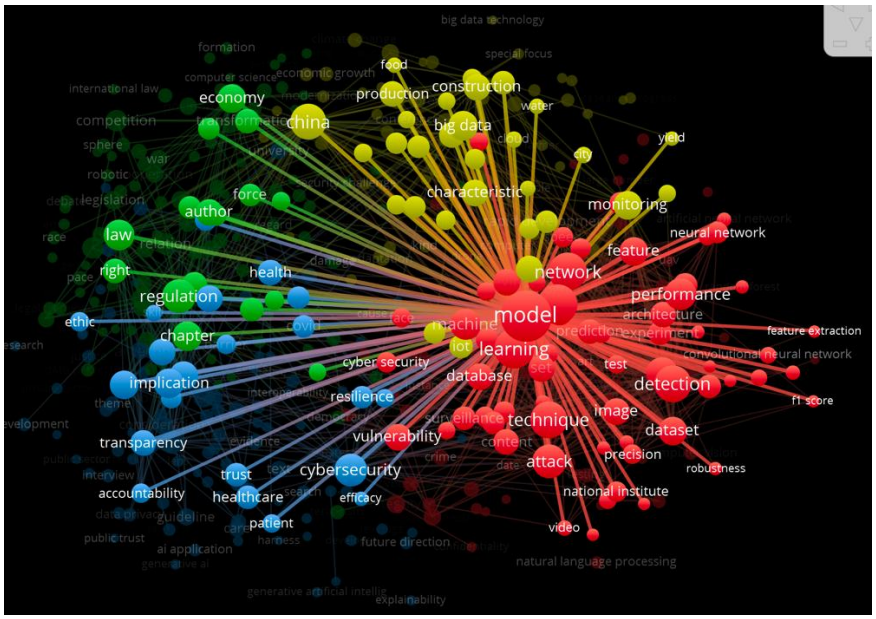
Primera parte – análisis conceptual. En este punto se realiza un estudio conceptual de 15 autores diferentes, cuyo objetivo principal es analizar ¿cómo la inteligencia artificial (IA) está transformando las dinámicas geopolíticas y geoestratégicas en el contexto colombiano, específicamente en el sistema de defensa nacional?.

A través de un enfoque interdisciplinario, se exploró el impacto de la IA en la soberanía tecnológica, la dependencia de actores externos, y la capacidad del país para enfrentar amenazas híbridas y transnacionales en un entorno globalizado e interconectado.

Para identificar los autores con mayor relación científica acerca de las características y categorías del problema, se empleó la técnica de identificación de términos concurrentes y autores relevantes.

El análisis se llevó a cabo con el software Vos Viewer, y el set de datos para la graficación de concurrencia se extrajo de SCOPUS. El proceso desarrollado fue el siguiente:

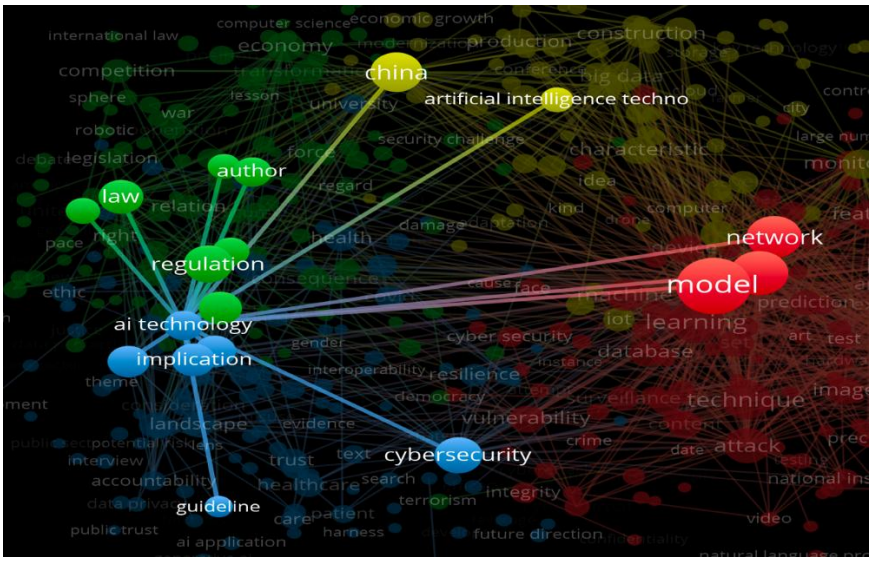
Figura 1. Núcleo con mayor concurrencia de términos I



Nota: elaboración propia con Vos Viewer

El término con mayor concurrencia y conectividad es Modelos Predictivos, Machine Learning y redes neuronales más tecnología y defensa nacional.

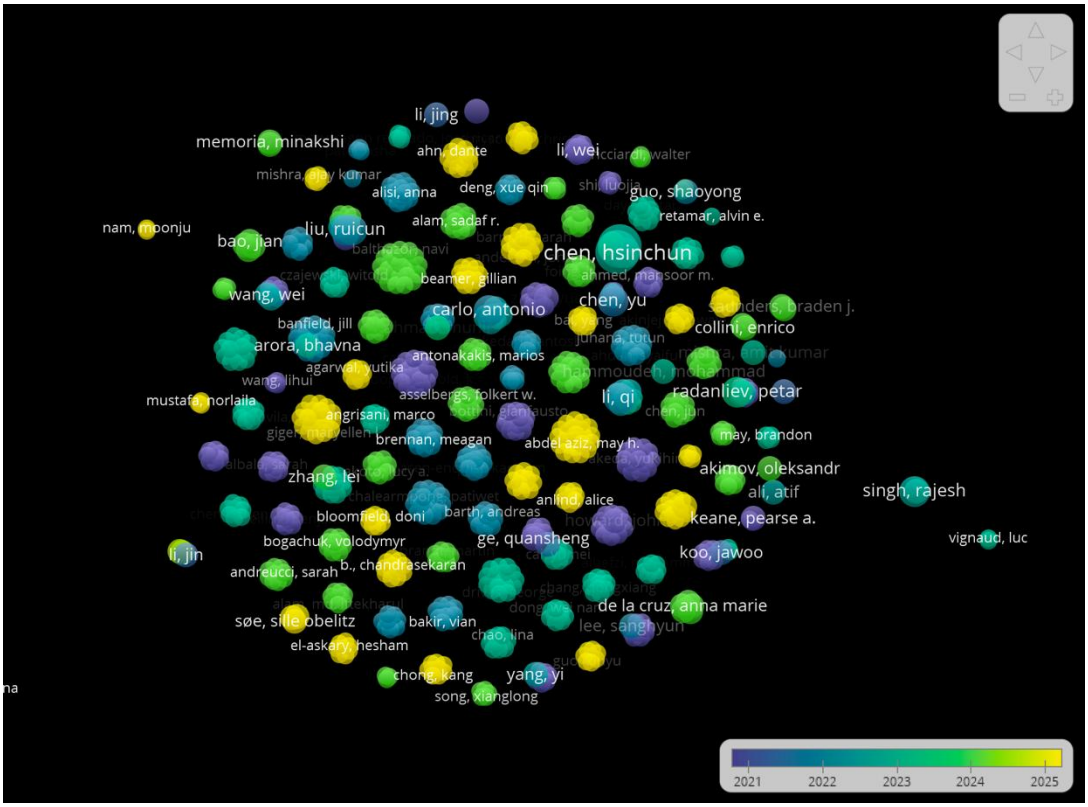
Figura 2. Núcleo con mayor concurrencia de términos II



Nota: elaboración propia con Vos Viewer

En cuanto al registro de autores y coautores, el análisis de convergencia de términos establece que las investigaciones pertinentes y ubicadas entre 2021 y 2025, pertenecen a Larsen (2022); Knox (2020); CDSE (2018); Arencibia (2021); Negrín (2022); Da Silva (2024); Bossio (2023); Saló y Galceran (2024); Salayer (2020); Slayer (2020); Horowitz, Allen, Saravalle, Frederick y Scharre (2022); Haney et al. (2020); Bistron y Piotrowski (2021); Araya y King (2022); Pătrașcu (2021); Taeihagh (2021).

Figura 3. Concurrencia por autores entre 2021 - 2023



Nota: elaboración propia con Vos Viewer

Segunda parte – análisis dependencia tecnológica. Explorar los diferentes conceptos que plantean la existencia de dependencia entre las capacidades militares basadas en inteligencia artificial y los factores de contexto que genera sujeción y dependencia. El

propósito es estructurar un proceso de análisis comparativo que permita concertar factores de discusión y análisis técnico.

Tercera parte – planteamiento de factores de influencia. Descripción y análisis correlacional cualitativa de las posturas científicas y la influencia de IA en seguridad y defensa nacional a la luz de una discusión exploratoria basada en la teoría clásica de seguridad y defensa nacional.

Factores Tecnológicos, Económicos y Políticos que Influyen en la Adopción de Inteligencia Artificial en el Sistema de Defensa Nacional Colombiano.

El desarrollo y la aplicación de la inteligencia artificial (IA) han transformado las dinámicas geopolíticas y geoestratégicas del escenario internacional, generando retos únicos en contextos territoriales ampliamente influenciados por tecnología con constante conectividad.

Según Larsen (2022), la IA no solo concreta las capacidades militares y de defensa, sino que también genera desbalance en el equilibrio de poder entre Estados, actores y regiones con tensiones geopolíticas en transmutación constante.

En el contexto colombiano, frente al conflicto armado y amenazas híbridas y trasnacionales, la incorporación de tecnologías de IA en el sistema de defensa nacional trae consigo interrogantes acerca de la soberanía tecnológica, la dependencia de actores foráneos y la capacidad para prevenir amenazas complejas en un entorno globalizado e interconectado.

Desde una perspectiva geoestratégica, la IA influye en la toma de decisiones relacionadas con la seguridad nacional y defensa territorial. Al respecto, Knox (2020) argumenta que la implementación de sistemas de análisis de datos, vigilancia tecnológica y ciberseguridad basada en IA plantea ventajas geo tecnológicas para la protección de fronteras y la lucha contra el crimen estructural organizado.

Sin embargo, estas tecnologías también presentan riesgos inherentes, como la vulnerabilidad a ciberataques, la manipulación de algoritmos y la posibilidad de un uso indebido por parte de actores no estatales (CDSE, 2018).

En este sentido, surge la necesidad de evaluar cómo los elementos de la geopolítica de IA están configurando las prioridades estratégicas del país y qué implicaciones tienen para su autonomía en materia de defensa.

Por otro lado, la concentración de recursos tecnológicos y de conocimiento en potencias globales crea dependencias que impactan directamente en las capacidades territoriales para establecer y aplicar tecnologías de IA con fines defensivos.

Por otra parte, Arencibia (2021) exponen que dicha dependencia limita la capacidad del país para competir en el ámbito internacional, posicionándolo en desventaja frente a actores con mayores recursos tecnológicos.

Además, esta dinámica refuerza las brechas existentes entre los países del norte y el sur globales, perpetuando desigualdades en el acceso a tecnologías críticas y en la capacidad de respuesta ante amenazas emergentes (Negrín, 2022). Por ello, es imperativo analizar cómo las asimetrías tecnológicas afectan la formulación de políticas de defensa en Colombia.

En contexto colombiano, la geopolítica de la IA también está influenciada por factores internos, como la fragmentación institucional, la corrupción y la falta de inversión en investigación y desarrollo.

Da Silva (2024), sostiene que estos desafíos estructurales dificultan la integración efectiva de tecnologías avanzadas en el sistema de defensa nacional, lo que a su vez compromete la capacidad del país para adaptarse a las demandas del entorno geoestratégico contemporáneo.

Asimismo, la ausencia de una estrategia coordinada para el desarrollo de IA en el ámbito militar pone en riesgo la seguridad nacional y limita las posibilidades de cooperación internacional en este campo (Bossio, 2023).

Por lo anterior, es importante considerar las implicaciones éticas y legales asociadas al uso de la IA en la defensa nacional. Saló y Galceran (2024) argumenta que la falta de marcos regulatorios específicos en Colombia para el uso de sistemas autónomos y algoritmos de IA en operaciones militares genera incertidumbre sobre su implementación y posibles abusos.

Otro punto de vista para entender el rol de la inteligencia artificial en el marco de los aportes al enfoque geoestratégico se observa en la investigación de Salayer (2020) quien explica que la inteligencia artificial (IA) transforma el panorama de la seguridad nacional, ya que su dominio forma capacidades estratégicas ligadas al análisis de entorno y toma de decisiones.

La investigación de Slayer (2020) permite entender a partir de una metodología descriptiva, que la inteligencia artificial cambia el ritmo de batalla para los actores involucrados en un núcleo conflictual.

Como Slayer (2020), Horowitz, Allen, Saravalle, Frederick y Scharre (2022) entran a la discusión para explicar que la inteligencia artificial es un proceso de optimización interno que permite el mejoramiento de los sistemas de defensa nacional, al mismo tiempo que presenta desafíos complejos para el sistema de defensa nacional.

De hecho, Haney *et al* (2020) discute como Horowitz et al (2022), que la inteligencia artificial moldea el futuro de las Fuerzas Militares, pero ello ocurre desde una perspectiva holística, en la que el marco IA no representa militarización sino aplicación de sus funciones para mejorar la toma de decisiones.

Seguido a Haney *et al* (2020), Bistron y Piotrowski (2021), desde una perspectiva ligada a la ciber seguridad, explican que la inteligencia artificial aumenta el espectro de impacto de las amenazas. La inclusión de la IA aumenta esos impactos ya que facilita a los ciber atacantes el desarrollo de código para la inyección de datos u otro tipo de disrupción digital.

Las versiones de Haney *et al* (2020) y Bistron y Piotrowski (2021), se evidencian en la postura técnica de Araya y King (2022), quienes exponen el núcleo de riesgos que produce la inteligencia artificial en el marco del sector defensa.

De acuerdo con Araya y King (2022), la inclusión de IA al sector defensa genera riesgo estructural sobre: disparidades tecnológicas (creación), impactos sociales debido al acceso masivo a la información y configuración de nuevas amenazas basadas en el dominio cibernético.

Asimismo, Pătrașcu (2021) ofrece desde el enfoque del Internet de las Cosas una versión acerca de la inteligencia artificial, y en su versión explica que esta dinamiza el desarrollo de procesos estratégicos, operacionales y de producción tecnológica.

Las versiones expuestas hasta este punto concretan una idea acerca del rol de la inteligencia artificial en el marco de la defensa nacional. Ese rol puede darse desde las necesidades de optimización o creación de amenazas con naturalezas desconocidas.

Precisamente, frente a ese entendimiento, Taeihagh (2021) entra a este debate para explicar que las categorías asociadas al entendimiento del rol de la inteligencia artificial son la optimización y creación, pero también la innovación organizacional, y producción científica que permita buscar soluciones institucionales ajustadas a la necesidad real.

En este contexto, es posible concluir que la inteligencia artificial no solo transforma las capacidades defensivas de los Estados, sino que también redefine las dinámicas geoestratégicas al introducir tanto oportunidades como riesgos en el ámbito de la seguridad nacional.

Por un lado, la IA optimiza procesos clave como la vigilancia, el análisis de datos y la ciberseguridad, lo que fortalece la capacidad de los Estados para responder a amenazas emergentes. Sin embargo, esta misma tecnología expone a los sistemas de defensa a vulnerabilidades significativas, como ciberataques y la manipulación de algoritmos, especialmente en contextos donde la infraestructura tecnológica y los marcos regulatorios son débiles o inexistentes.

Además, la dependencia tecnológica de potencias globales refuerza las desigualdades existentes entre países desarrollados y en desarrollo, afectando directamente la soberanía tecnológica y la capacidad de los Estados menos avanzados para implementar soluciones autónomas en defensa.

En el caso de Colombia, estas asimetrías limitan su competitividad y autonomía estratégica, perpetuando brechas tecnológicas que dificultan la formulación de políticas efectivas en un entorno internacional cada vez más interconectado y competitivo.

Implicaciones de la dependencia tecnológica internacional en el desarrollo de capacidades de defensa basadas en inteligencia artificial: contexto colombiano.

La dependencia tecnológica internacional en el desarrollo de capacidades de defensa basadas en inteligencia artificial (IA) para Colombia genera una serie de implicaciones que afectan tanto la soberanía tecnológica como la capacidad del país para adaptarse a los desafíos del entorno global (Fernández, Villalba, y Velandia, 2024).

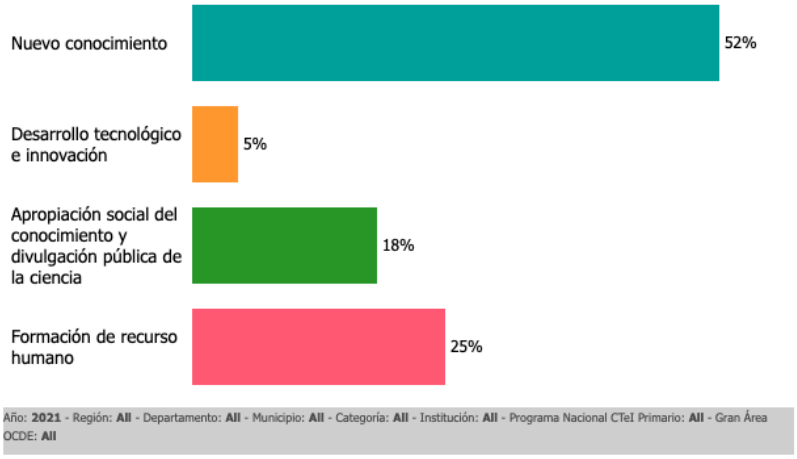
En primer lugar, dicha dependencia limita la autonomía estratégica de Colombia, ya que la adquisición de tecnologías avanzadas suele estar condicionada por intereses geopolíticos de los países proveedores. Esta es una afirmación hallada en dos versiones relevantes. Una, de tipología clásica, conceptúa que la dependencia tecnológica debilita el alcance estratégico de las acciones para garantizar la seguridad nacional (Blackuvell, 1993).

Otra moderna que halla en la dependencia tecnológica internacional un vacío estratégico para la estructura de defensa nacional (Schmidt, AI, great power competition & national security., 2022).

Ambos vacíos restringen la capacidad del Estado para tomar decisiones independientes en materia de defensa, especialmente en contextos de tensiones internacionales donde los intereses de los países desarrollados pueden no alinearse con los de Colombia.

Una de las causas que ralentizan el desarrollo tecnológico a nivel nacional y que genera dependencia internacional, es el reducido margen de investigación científica centrada en producción de conocimiento y transferencias tecnológicas. Esta afirmación encuentra un respaldo investigativo en la ausencia de grupos de investigación públicos formados para llevar a cabo experimentación técnica en materia militar:

Figura 4. Producción científica de los grupos de investigación reconocidos



Nota: información recuperada de MINCIENCIAS (2022)

Figura 5. Producción científica en desarrollo tecnológico e innovación

Nota: información recuperada de MINCIENCIAS (2022)

Como se puede observar en las figuras 4 y 5, la producción científica nacional relacionada con desarrollo tecnológico e innovación es de solo el 5%. Eso se traduce en solo 3.800 investigaciones relacionadas con creación de software y 6.080 investigaciones conexas a diseño de prototipo industrial.

Las cifras expuestas permiten concertar que en Colombia la dependencia tecnológica sitúa una parte de su génesis en la ausencia de modelos y procesos de investigación centrados en producción de I+D+i+TT en el sector defensa.

De hecho, esa es una postura que comparten Atencio, Zapata, Aguirre, Jiménez, y Paipa (2025).

De acuerdo con Atencio *et al* (2025), los desafíos en el sector defensa relacionados con la gestión de ciencia, tecnología e innovación (CTeI) abarcan múltiples dimensiones críticas. Entre ellos, destaca la necesidad de integrar tecnologías avanzadas como la inteligencia artificial y el Internet de las cosas, enfrentando limitaciones presupuestarias que dificultan la ejecución de proyectos estratégicos.

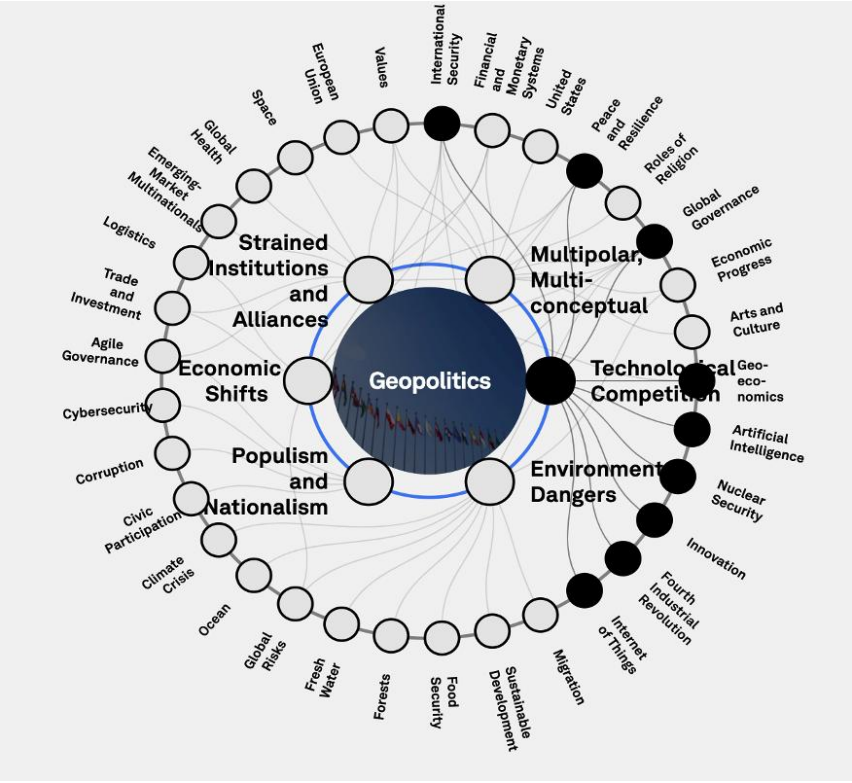
Asimismo, la ciberseguridad emerge como un reto crucial, dada la creciente sofisticación de las amenazas cibernéticas transnacionales. A esto se suma la falta de mecanismos efectivos para la gestión del conocimiento, lo que limita la transferencia tecnológica y la innovación (Atencio *et al*, 2025).

En segundo lugar, la dependencia tecnológica internacional perpetúa desigualdades estructurales en el acceso a tecnologías críticas. Las potencias globales concentran los

recursos necesarios para la investigación y el desarrollo de IA, mientras que países como Colombia deben recurrir a la importación de soluciones tecnológicas, lo que incrementa los costos y reduce la capacidad de adaptación a las necesidades locales. Este fenómeno, genera inequidad en la competencia tecnológica que exige el proceso de configuración y construcción de nuevos enfoques orientados a la integración de inteligencia artificial; esta última, herramienta necesaria para diseñar estrategias de seguridad ajustadas a contexto nacional (Ortíz y Fernández, 2020).

En un marco geopolítico internacional, la competencia tecnológica orientada a la construcción de hegemonías basadas en I+D+i+TT, es en sí una tendencia interconectada con enfoques específicos: uno de esos es la competencia tecnológica y su relación con la seguridad internacional. (Ver figura 6):

Figura 6. Conexión entre geopolítica y competencia tecnológica



Fuente: información recuperada de World Economic Forum (2025)

Establecer mecanismos de cooperación más que acuerdos con inequidad en condiciones es imperativo para proyectar el desarrollo tecnológico autónomo del sector defensa colombiano. Dicha autonomía es necesaria para diseñar estrategias basadas en tecnología que apunten a la restricción de acceso o surgimiento en nuevas amenazas; sobre todo de carácter cibernético (Suárez, 2023).

Por lo anterior, una tercera implicación por exponer está relacionada con la vulnerabilidad frente a ciberataques. Al depender de tecnologías desarrolladas por terceros, Colombia se expone a riesgos asociados a la manipulación de algoritmos y al acceso no autorizado a sistemas críticos, así como también a desafíos estructurales que surgen por la rápida intervención e influencia funcional que produce la inteligencia artificial (Ospina & Sanabria, 2020).

Además, la falta de control total sobre el diseño y funcionamiento de estas tecnologías limita la capacidad del país para implementar medidas de seguridad que se ajusten a su contexto específico, el cual, a 2025, es exponencialmente vulnerable según las Estadísticas presentadas por el Comando Conjunto Cibernético de las FFMM (CCOCI, 2024), ya que:

- **Primero**, entre el 12 de noviembre y el 10 de diciembre, los ataques de ransomware en Colombia mostraron un aumento significativo, alcanzando su punto máximo con más de 550 detecciones en noviembre. La amenaza más prevalente fue *Trojan-Ransom.Win32.Crypren.gen*, representando el 56.64% de los casos.
- **Segundo**, los ataques relacionados con correos electrónicos maliciosos experimentaron fluctuaciones constantes, con picos de hasta 5,500 detecciones. Las amenazas principales incluyeron *Trojan.OLE2.UrcBadur.gen* (12.30%) y *Trojan.Script.Generic* (10.93%), destacando la diversidad de vectores de ataque.
- **Tercero**, los ataques de red en el mismo periodo superaron las 120,000 detecciones en su máximo. *Bruteforce.Generic.Rdp.a* fue el vector dominante, representando el 60.07% de los casos, seguido de *DoS.Generic.Flood.ICMP* (6.87%), evidenciando la prevalencia de ataques de fuerza bruta.

La cuarta implicación es la dificultad para adaptar las tecnologías importadas a las necesidades locales. Muchas de las soluciones basadas en IA están diseñadas para contextos específicos y no siempre se ajustan a las realidades operativas de Colombia, como las amenazas híbridas y transnacionales que enfrenta. Esto genera ineficiencias en la implementación de estas tecnologías y reduce su efectividad en la protección de la seguridad nacional.

En quinto lugar, la dependencia tecnológica internacional afecta la sostenibilidad económica del sistema de defensa colombiano. La adquisición y mantenimiento de tecnologías avanzadas implica altos costos que pueden desviar recursos de otras áreas críticas, como la inversión en investigación y desarrollo local. Esto perpetúa un ciclo de dependencia en el que el país no logra desarrollar sus propias capacidades tecnológicas y sigue dependiendo de actores externos para garantizar su seguridad.

Otra implicación importante es la limitación en la transferencia de conocimiento. Los acuerdos de adquisición de tecnologías suelen incluir restricciones sobre el acceso a los procesos de diseño y desarrollo, lo que dificulta la formación de capacidades locales en el uso y mejora de estas tecnologías. Esto afecta directamente la capacidad de Colombia para construir una base tecnológica sólida que le permita avanzar hacia la autosuficiencia en el ámbito de la defensa.

La séptima implicación se refiere al impacto en la cooperación internacional. Aunque la dependencia tecnológica puede facilitar alianzas estratégicas con países desarrollados, también puede generar tensiones si los intereses de estos actores entran en conflicto con los de Colombia. Esto podría limitar las oportunidades de colaboración en áreas clave, como la lucha contra el crimen organizado y la protección de fronteras, donde la IA tiene un papel fundamental.

En octavo lugar, la dependencia tecnológica internacional plantea desafíos éticos y legales. La falta de control sobre las tecnologías adquiridas puede generar incertidumbre sobre su uso responsable, especialmente en contextos de operaciones militares. Como señalan Saló y Galceran (2024), es necesario establecer marcos regulatorios que garanticen el uso ético de la IA en la defensa, pero esto se complica cuando las tecnologías provienen de actores externos con diferentes estándares éticos y legales.

La novena implicación está relacionada con la capacidad de respuesta ante amenazas emergentes. La dependencia de tecnologías externas puede retrasar la implementación de soluciones necesarias para enfrentar nuevas amenazas, ya que el país debe esperar la disponibilidad de estas tecnologías en el mercado internacional. Esto reduce la capacidad de Colombia para adaptarse rápidamente a un entorno de seguridad en constante evolución.

Por último, la décima implicación es el impacto en la percepción de la soberanía nacional. La dependencia tecnológica puede ser vista como una forma de subordinación a los intereses de potencias extranjeras, lo que afecta la imagen del país tanto a nivel interno como externo. Esto podría debilitar la confianza en las instituciones de defensa y generar cuestionamientos sobre la capacidad del Estado para garantizar la seguridad de su población.

Con base en las contribuciones expuestas, es corrector debatir que la dependencia tecnológica internacional en el desarrollo de capacidades de defensa basadas en IA tiene implicaciones para Colombia, pues afecta tres vectores transversales en la creación de una estrategia militar aplicada: autonomía en el diseño, diminución de las variables que producen incertidumbre en la toma de decisiones y optimización en la precisión y exactitud de los métodos de planeamiento utilizados para desarticular ecosistemas criminales.

Alcances y factores de influencia que presenta la IA en la construcción de enfoques geoestratégicos: análisis sobre contexto colombiano.

Una vez analizadas las categorías del problema, se construye en este acápite una fase de investigación que busca establecer alcances y factores de influencia que, desde el Marco de la inteligencia artificial, pueden influir en la construcción de enfoques estratégicos de seguridad y defensa nacional.

Es decir, en este punto, a partir de una matriz de análisis comparativo se exponen seis elementos de valor que constituyen el núcleo influencias, mientras que se exponen dos alcances funcionales y estructurales correlacionados al diseño de conceptos operacionales altamente influenciados por la inteligencia artificial.

En tal sentido, y trayendo a colación el contexto colombiano y la literatura pertinente, es necesario discutir que a 2025 sólo hay una política pública direccionada a trazar un marco

estratégico de dominio y función para la inclusión de inteligencia artificial en los estamentos del Estado. Esa política se encuentra en el documento CONPES 4144 (DNP, 2025).

El documento CONPES 4144 resalta cómo la inteligencia artificial (IA) puede influir significativamente en la toma de decisiones al ofrecer herramientas avanzadas para analizar grandes volúmenes de datos, identificar patrones y generar recomendaciones (CONPES, 4144).

Esto permite a los tomadores de decisiones analizar problemas complejos con mayor precisión y eficiencia, optimizando recursos y maximizando resultados en sectores como la salud, la educación y la gestión pública. Además, la IA facilita la anticipación de escenarios futuros, promoviendo decisiones informadas y estratégicas que contribuyen al desarrollo sostenible del país.

Ahora, aunque el CONPES exhibe como necesidad estatal conexa a la inclusión de inteligencia artificial para mejorar marcos político - sociales como la gobernanza en territorio o la gobernabilidad a nivel nacional, el direccionamiento hacia los enfoques de seguridad y defensa nacional o el mismo campo militar son nulos; es decir, este es un documento de política social que hasta el momento va incluido el principio de necesidad militar como línea estratégica necesaria para contrarrestar desafíos que transmutan del sector civil, público organizacional o privado empresarial al campo militar. Esos desafíos si están reflejados en el CONPES 4144y su descripción es la siguiente:

Tabla 1. Desafíos que contrae la inteligencia artificial a campos intersectoriales colombianos.

Desafío	Explicación
Brechas en talento e infraestructura	Colombia enfrenta una carencia de profesionales especializados en inteligencia artificial y una infraestructura tecnológica insuficiente, lo que limita su capacidad para competir en el ámbito global.
Riesgos legales y éticos	La falta de regulación clara para la IA genera incertidumbre sobre cómo manejar problemas como el uso indebido de datos personales o errores algorítmicos que afectan derechos fundamentales.

Desafío	Explicación
Dependencia tecnológica	La alta dependencia de proveedores externos para el desarrollo y mantenimiento de sistemas de IA debilita la soberanía digital del país y limita su autonomía tecnológica.
Impactos sociales y ambientales	La adopción de IA puede provocar problemas como sesgos en algoritmos, afectaciones psicológicas en usuarios, y un alto consumo energético que impacta el medio ambiente.
Conectividad y calidad de datos	La falta de acceso a Internet en zonas rurales y la escasez de datos confiables dificultan la implementación efectiva de tecnologías de inteligencia artificial.

Nota: elaboración propia con información recuperada del CONPES 4144 de 2025

Los desafíos subrayados en la tabla 1 son parte del problema desde la óptica del campo de desarrollo intersectorial nacional. Sin embargo, sólo dos de estos desafíos se ajusta el problema militar: la dependencia tecnológica y las brechas en talento humano. Éstos desafíos, son al mismo tiempo factores de influencia si se tienen cuenta que de acuerdo con García (2024), la inteligencia artificial aplicada al campo militar puede mejorar los procesos militares para la toma decisiones, optimizar recursos económicos y mejorar los enfoques tácticos orientados a la intervención en territorio.

Pero, a la versión de García (2024) y a la tabla desafíos que impone esta política es necesario agregar 10 factores de influencia más, los cuales surgen de la matriz de relación que se anexa en el archivo Excel constituido con el nombre de ANEXO_FACTORES_INFLUENCIA.

Esta matriz permitió al investigador correlacionar factores de influencia para, al finalizar, ponderar los impactos geo estratégicos e impacto sistemáticos, y así establecer un parámetro de análisis metodológico, técnico y de rigor científico.

El primer factor que deriva del ejercicio desarrollado, es el dominio epistemológico de la inteligencia artificial. En tal aspecto Rashid, Kausik, Al Hassan, y Bappy (2023), han enfatizado que la inteligencia artificial requiere como eje transversal el dominio conceptual por parte de los actores militares.

Es decir, antes que su funcionamiento, alcance o capacidad de impacto, la inteligencia artificial tiene que medirse en pro de los avances tecnológicos demostrados en el sector defensa.

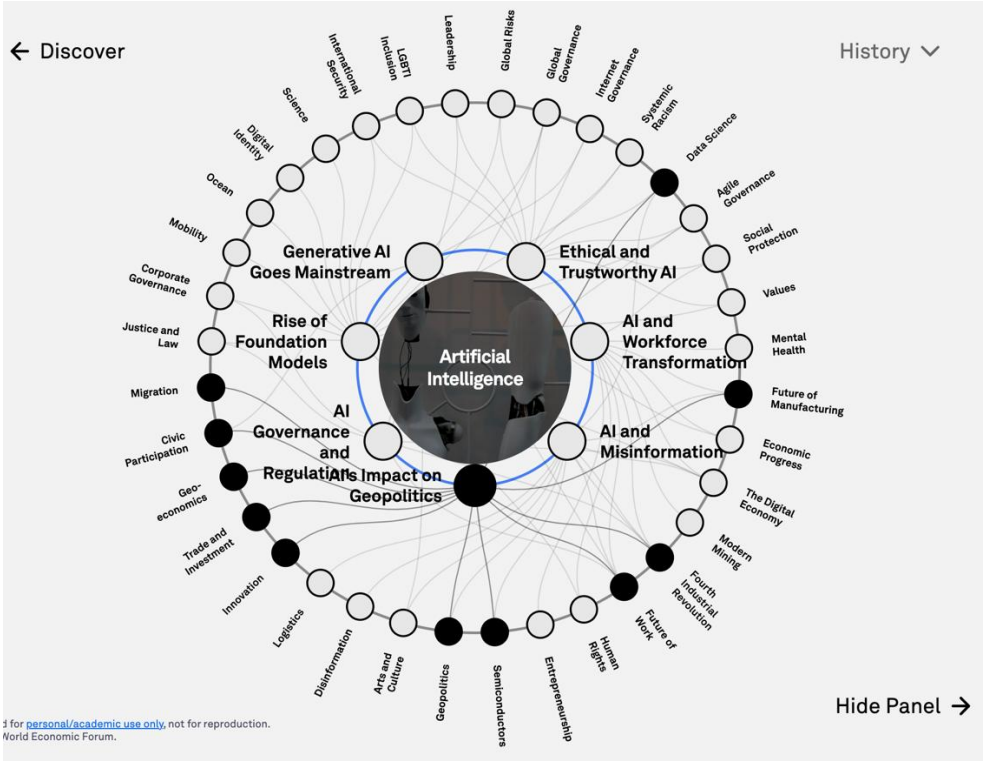
Por ende, a mayor dominio conceptual, mayor dominio tecnológico y por consiguiente, mayores los efectos operacionales y estratégicos de éste tipo de instrumentos en la configuración de conceptos operacionales (Szabadföldi, 2021).

Tal entendimiento se suma a otro factor (segundo): la generación de doctrinas integradas. En este factor, (Vestner, 2024) describe que la alineación dogmática, funcional, estratégica y multidimensional de un sistema militar es fundamental para desarrollar fases orientadas a la transición y migración a sistemas tecnológicos y de información.

La inteligencia artificial, es uno de los campos de rigor en donde los sistemas miliares transitan de manera secuencial. Llama la atención, que la migración puede empezar con la inclusión de inteligencia artificial para la reducción de incertidumbre en la toma decisiones, pero también en la utilización de nuevas técnicas y métodos de guerra asociados a la incorporación de *remote sensing* y *machine learning* a procesos esenciales como los análisis sobre el terreno.

El tercer factor tiene relación con nuevas facetas geopolíticas que estudian el concepto de la inteligencia artificial a través de acuerdos de cooperación y otras características conectadas a la relaciones internacionales. En tal sentido, Bächle y Bareis (2022) interpretan que la producción de conocimiento científico alrededor del desarrollo de la inteligencia artificial amerita la concertación de acuerdos y tratados de cooperación y colaboración enfocados sobre la variable I+D+i+ TT. (Ver figura 6):

Figura 6. Conexión entre geopolítica e inteligencia militar



Fuente: información recuperada de World Economic Forum (2025)

Al respecto, se puede observar en la figura 6 que la inteligencia artificial se asocia con los impactos geopolíticos a través de vectores de cooperación que buscan construir primeramente, conocimiento científico y experimental ajustado a la necesidad del sistema militar que desarrolla la investigación (Schmidt, 2023).

Pero también, se relaciona con otros vectores como la ciencia de datos, la geoeconomía, la lucha en contra de la desinformación, el trabajo del futuro y hasta los derechos humanos. Frente a este último aspecto, es importante resaltar que la inteligencia artificial conlleva incluso al diseño de estrategias militares que, al aplicar algoritmos, reduce la probabilidad de impacto militar y hostil sobre el actor poblacional, favoreciendo el marco activo y de protección que requieren los derechos humanos en el escenario que regula la acción bélica y militar, también conectada al espectro del derecho internacional humanitario.

El cuarto factor se relaciona con la creación de modelos IA ajustados a la necesidad explícita y militar. En este campo, se entiende de (Gaire, 2023), que como herramienta, la

inteligencia artificial simplifica la complejidad de procesos militares orientados a la protección del medio ambiente, innovación y creación de ciencia.

Es por tal razón, que el diseño de modelos apropiados hace parte de la fase de transición y migración. No obstante, como se ha descrito, su dominio depende capacidades cognoscitivas, desarrolladas de manera temporal en la instituciones.

Así los términos, esta investigación es relevante en el campo de la defensa nacional, pues entrega un acercamiento inicial y cualitativo que permite establecer qué necesidades, de frente a un nuevo núcleo de amenazas, tienen que abordarse y/o cubrirse con modelos específicos, conexos con machine learning y análisis de datos para procesos predictivos. Cabe resaltar que en las investigaciones consultadas por categorías, la inclusión de aprendizaje automático y ciencia para el estudio de datos ocupa puestos relevantes en los estudios de rigor acerca de la inteligencia artificial aplicada al campo de las ciencias militares.

La geopolítica de la inteligencia artificial influye significativamente en el enfoque geoestratégico de defensa colombiano a través de múltiples dimensiones interconectadas. El análisis expone que el impacto de la IA trasciende aspectos como la implementación tecnológica, moldeando la doctrina militar, los conceptos operacionales y los procesos de toma de decisiones estratégicas.

El sistema de defensa colombiano enfrenta el doble desafío de la dependencia tecnológica y las brechas en talento humano, mientras simultáneamente necesita desarrollar capacidades autónomas en áreas críticas como ciberseguridad, sistemas no tripulados y análisis predictivo. La intersección entre marcos de cooperación internacional, iniciativas de política interna como el CONPES 4144 y los requerimientos de modernización militar demuestra que la influencia de la IA en la estrategia de defensa colombiana es transformadora, requiriendo un enfoque equilibrado entre adopción tecnológica y autonomía estratégica.

Esta influencia se manifiesta particularmente en tres áreas críticas: capacidades mejoradas de toma de decisiones, sistemas avanzados de control territorial y modelos de predicción de amenazas, todos los cuales están reconfigurando el posicionamiento geoestratégico de Colombia en el panorama de seguridad regional.

Conclusiones

La investigación desarrollada permitió entender que la dependencia tecnológica internacional en IA condiciona la arquitectura estratégica de defensa de Colombia y tensiona su soberanía decisional en un entorno de competencia geopolítica acelerada. Las cifras de base científica y de ciberamenazas muestran, además, que el rezago interno en I+D+i+TT y las limitaciones de talento e infraestructura amplifican el riesgo operativo justo cuando la IA redefine doctrinas, capacidades y ciclos de decisión.

En ese marco, las conclusiones que siguen se entrelazan con el diagnóstico y con los imperativos de política y cooperación que el país debe equilibrar para ganar autonomía sin aislarse de los flujos globales de conocimiento.

Primero, la autonomía estratégica está hoy erosionada por una combinación de dependencia tecnológica e insuficiencia de investigación aplicada local. La producción científica nacional vinculada a desarrollo tecnológico e innovación alcanza apenas el 5%, lo que se traduce en cerca de 3.800 trabajos en creación de software y 6.080 en diseño de prototipos industriales; este bajo volumen limita la masa crítica para generar modelos propios de IA en defensa y sostiene el ciclo de importación tecnológica.

Esta fragilidad encaja con los planteamientos que, desde visiones clásicas y contemporáneas, advierten que la dependencia reduce el margen para decisiones soberanas en seguridad; en consecuencia, la ruta de salida exige escalar inversión y transferencia de conocimiento orientadas a defensa, a la vez que alinear doctrinas y cooperación para transformar ese 5% en capacidades efectivas de I+D+i+TT con aplicación operacional.

Segundo, la exposición a amenazas cibernéticas confirma que la dependencia tecnológica no es un problema abstracto, sino un vector de riesgo inmediato que presiona la adaptación de la seguridad nacional. Entre el 12 de noviembre y el 10 de diciembre recientes, los ataques de ransomware en Colombia superaron las 550 detecciones con una variante predominante que concentró el 56,64% de los casos; en paralelo, los incidentes asociados a correos maliciosos tuvieron picos de hasta 5.500 detecciones y, en redes, los ataques alcanzaron más de 120.000 eventos, con el 60,07% atribuido a fuerza bruta RDP.

Este panorama confirma la urgencia de capacidades propias para auditar algoritmos, endurecer arquitecturas y ajustar medidas al contexto local, pues depender de soluciones

externas vuelve más lenta la respuesta ante amenazas emergentes y menos granular el control sobre salvaguardas críticas.

Tercero, la brecha entre el marco público de IA vigente y las necesidades del sector defensa mantiene un descalce funcional que reproduce la dependencia y posterga la autonomía. A 2025, el CONPES 4144 es la única política de IA y prioriza impactos sociales y económicos, mientras que para defensa los desafíos que efectivamente aplican —dependencia tecnológica y déficit de talento— quedan sin un carril operativo claro; así, el sistema de defensa debe competir por recursos y capacidades en un entorno donde la cooperación internacional es necesaria pero puede introducir asimetrías.

En este contexto, avanzar hacia modelos y doctrinas propias exige integrar formación y dominio conceptual, estandarización doctrinal y acuerdos de cooperación con cláusulas de transferencia, a fin de que los bajos porcentajes de producción tecnológica (ese 5% y sus 3.800/6.080 productos) se traduzcan en prototipos, algoritmos y procedimientos que fortalezcan la toma de decisiones, los sistemas de control territorial y la predicción de amenazas, cerrando el ciclo entre conocimiento local y resiliencia frente a vectores de ataque que hoy ya se cuentan por decenas de miles.

Referencias

Alizadeh, Y. (2012). Firm-level technological capability assessment; a literature review. . *International Technology Management Conference* , 398-404.

Araya, D., & King, M. (2022). *The impact of artificial intelligence on military defense and security* (No. 263). CIGI Papers.

Arencibia, M. (2021). Inteligencia artificial y big data como nuevas herramientas de la geopolítica: su impacto en América Latina y el Caribe. *Serie Científica de la Universidad de las Ciencias Informáticas, 14*(1), 146-177.

Atencio, L. S., Zapata, J., Aguirre, Y., Jiménez, B., & Paipa, E. G. (2025). Revisión de mecanismos de gestión de ciencia, tecnología e innovación en el sector defensa. *Revista Logos Ciencia & Tecnología, 103*, 1-10.

Bächle, T., & Bareis, J. (2022). "Autonomous weapons" as a geopolitical signifier in a national power play: analysing AI imaginaries in Chinese and US military policies. *European Journal of Futures Research, 10*(1), 1-10.

Bistron, M., & Piotrowski, Z. (2021). Artificial intelligence applications in military systems and their influence on sense of security of citizens. *Electronics*, *10*(7), 871.

Blackuvell, J. (1993). Prospects and Risks of Technological Dependency. En *Superioridad tecnológica.* JBA.

CCOCI. (2024). Boletín CCOCI - 2024. Repositorio CCOCI: https://drive.google.com/file/d/1sMT1D2WRDP7kwWaPCnVVIQG94RJkplVg/view.

CDSE. (2018). Common Cyber Threats: Indicators and Countermeasures. *Course Library: Common Cyber Threat Indicators and Countermeasures*, 1-10.

Da Silva, E. (2024). A Inteligência Artificial e a Competição Global pela Hegemonia entre as Grandes Potências: China e Estados Unidos. *Revista de Geopolítica, 15*(2), 1-15.

DNP. (2025). Política Nacional de Inteligencia Artificial. *Documento CONPES 4144. Bogotá, Colombia.* , 1-50.

Fernández, A. E., Villalba, L., & Velandia, E. F. (2024). Gobernanza policéntrica, big data e inteligencia artificial: herramientas para la seguridad ciudadana en Colombia. *Revista Criminalidad, 66*(3), 11-25.

Gaire, U. S. (2023). Application of artificial intelligence in the military: An overview. *Unity Journal, 4*(01), 161-174.

Garcia, D. (2024). Algorithms and decision-making in military artificial intelligence. *Global Society, 38*(1), 24-33.

Haney, B. S. (2020). Applied artificial intelligence in modern warfare and national security policy. *Hastings Sci. & Tech. LJ*, *11*, 61.

Hecklau, F., Kidschun, F., Kohl, H., & Tominaj, S. (2019). Requirements for a Methodology for the Analysis and Assessment of Technological Capability in Research and Technology Organizations. *Proceedings of the 15th European Conference on Management, Leadership and Governance ECMLG*, 159-168.

Hernández, L., Fernández, D., & Baptista, L. (2010). *Metodología de la investigación.* México D.F.: Mc Graw Hill.

Horowitz, M. C., Allen, G. C., Saravalle, E., Cho, A., Frederick, K., & Scharre, P. (2022). *Artificial intelligence and international security*. Center for a New American Security..

Knox, J. (2020). Artificial intelligence and education in China. *Learning, Media and Technology, 45*(3), 298-311.

Larsen, B. C. (2022). *The geopolitics of AI and the rise of digital sovereignty.* Brookings.

MINCIENCIAS. (2022). *GRUPOS DE INVESTIGACIÓN RECONOCIDOS*. Obtenido de https://minciencias.gov.co/la-ciencia-en-cifras/grupos

Mortazavi, S., Mehrabanfar, E., Banaitis, A., & Banaitienė, N. (2016). Framework for assessing technological innovation capability in research and technology organizations. *Journal of Business Economics and Management, 17*(6), 825-847.

Negrín, F. (2022). *Dependencia tecnológica y soberanía en América Latina: Un análisis crítico*. Buenos Aires: Ediciones Políticas.

Negrín, M. (2022). Tecnología, inteligencia artificial y la desestabilización de la hegemonía global: China y Estados Unidos ante su dominio. . *Boletín IEEE*, 1-10

Ortíz, A., & Fernández, A. (2020). La inteligencia artificial en el contexto militar internacional y sus posibles aplicaciones en el Ejército Nacional de Colombia.

Trabajo de grado . Bogotá D.C.: Rep. ESDEGUE:https://www.esdegrepositorio.edu.co/handle/20.500.14205/4514.

Ospina, M., & Sanabria, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista criminalidad, 62*(2), 199-217.

Pătraşcu, P. (2021). Emerging technologies and National Security: The impact of IoT in critical infrastructures protection and defence sector. *Land Forces Academy Review*, *26*(4), 423-429.

Rashid, A., Kausik, A., Al Hassan, A., & Bappy, M. H. (2023). Artificial intelligence in the military: An overview of the capabilities, applications, and challenges. . *International journal of intelligent systems*, 1-10.

Saló, P., & Galceran, L. (2024). *Ética y regulación en el uso de la inteligencia artificial en defensa*. Madrid: Ética y Tecnología Editorial.

Sayler, K. M. (2020). Artificial intelligence and national security. *Congressional Research Service*, *45178*.

Schmidt, E. (2022). AI, great power competition & national security. *Daedalus, 151*(2), 288-298.

Slayer, T. (2020). *Transformación digital en defensa: El papel de la inteligencia artificial*. Berlín: Military Innovations Press.

Suárez, J. (2023). Ciberseguridad, un desafío para las Fuerzas Militares colombianas en la era digital. *Revista Científica Perspectivas en Inteligencia, 15*(24), 333-359.

Szabadföldi, I. (2021). Artificial intelligence in military application–opportunities and challenges. *Land Forces Academy Review, 26*(2), 157-165.

Vestner, T. (2024). From strategy to orders: preparing and conducting military operations with artificial intelligence. In Research Handbook on Warfare and Artificial Intelligence. *Research Handbook on Warfare and Artificial Intelligence*, 116-134.

Wolrd Economic Forum. (2025). Obtenido de https://intelligence.weforum.org/topics/a1Gb0000000pTDREA2/key-issues/a1Gb00000017L8jEAE