



Revista Perspectivas en Inteligencia

(Revista Científica en Ciencias Sociales e Interdisciplinaria)

Volumen 17, Número 26, enero - diciembre de 2025

ISSN: 2145-194X (impreso), 2745-1690 (en línea)

Página Web: <https://revistascedoc.com/index.php/pei>

Bogotá D.C., Colombia

Militarización de la Inteligencia Artificial: armas autónomas, equilibrio estratégico y gobernanza algorítmica

Autores

Germán Darío Corzo-Ussa

<https://orcid.org/0000-0001-7603-0896>

✉ german.corzo@esdeg.edu.co

Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia

Nathalie Tarazona-Rojas

<https://orcid.org/0000-0002-2113-4724>

✉ nathytr11@gmail.com

Escuela de Aviación del Ejército, Colombia

Carol Vanesa Quintero-Rosas

<https://orcid.org/0009-0004-9860-2081>

✉ carol.quintero@esdeg.edu.co

Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia

Citación APA: Corzo-Ussa, G. D., Quintero-Rosas, C. V. y Tarazona-Rojas, N. (2025). Militarización de la Inteligencia Artificial: armas autónomas, equilibrio estratégico y gobernanza algorítmica. *Perspectivas en Inteligencia*, 17(26), 83-96.

<http://doi.org/10.47961/2145194X.828>

Publicado en línea: 2025



Los artículos publicados por la Revista Científica Perspectivas en Inteligencia son de acceso abierto bajo una licencia **Creative Commons: Atribución - No Comercial – Sin Derivados**.

Para enviar un artículo:

<https://revistascedoc.com/index.php/pei/about/submissions>



*Esta página queda
intencionalmente
en blanco*

Militarización de la Inteligencia Artificial: armas autónomas, equilibrio estratégico y gobernanza algorítmica

Militarization of Artificial Intelligence: autonomous weapons, strategic balance, and algorithmic governance

Germán Darío Corzo-Ussa^{1*}, Carol Vanesa Quintero-Rosas² y Nathalie Tarazona-Rojas³

- (1) Escuela Superior de Guerra “General Rafael Reyes Prieto”, Bogotá, D. C., Colombia,
✉ german.corzo@esdeg.edu.co
(2) Escuela Superior de Guerra “General Rafael Reyes Prieto”, Bogotá, D. C., Colombia,
✉ carol.quintero@esdeg.edu.co
(3) Escuela de Aviación del Ejército, Bogotá, D. C., Colombia,
✉ nathytr11@gmail.com

* Autor a quien se dirige la correspondencia

Resumen

Este artículo analiza la militarización de la inteligencia artificial en la seguridad internacional mediante un enfoque bibliométrico con síntesis narrativa guiada por indicadores. Se consultó Scopus y aplicaron técnicas de coocurrencia, redes, clústeres y citación para delimitar empíricamente el campo y priorizar autores, conceptos y tendencias. Se definieron constructos analíticos (inteligencia artificial y tecnologías emergentes) y resultados de interés (poder geopolítico y soberanía tecnológica). Los hallazgos organizan cinco elementos clave: Proyección remota de capacidades, ventaja competitiva derivada del aprendizaje automatizado, desmaterialización del conflicto mediante integración digital, guerra híbrida con efectos cognitivo-informacionales y gobernanza orientada a regulación, verificación y salvaguardas. La evidencia muestra que la adopción algorítmica reconfigura balances de poder, incentiva nuevas dependencias tecnológicas y tensiona regímenes normativos, lo que exige marcos de contención y disuasión específicos. El estudio aporta un mapa estructural del campo y una ruta metodológica reproducible para orientar decisiones públicas y agenda de investigación.

Clasificación JEL: O33, O34.

Palabras clave: geopolítica algorítmica; inteligencia artificial; militarización; seguridad internacional; soberanía tecnológica; tecnologías emergentes.

Abstract

This article examines the militarization of artificial intelligence in international security through a bibliometric approach with an indicator-guided narrative synthesis. Scopus was consulted and techniques of cooccurrence, network analysis, clustering, and citation were applied to delimit the field empirically and prioritize authors, concepts, and trends. Analytical constructs were defined (artificial intelligence and emerging technologies) and outcomes of interest (geopolitical power and technological sovereignty). The findings organize five key elements: remote projection of capabilities, competitive advantage derived from automated learning, dematerialization of conflict through digital integration, hybrid warfare with cognitive-informational effects, and governance aimed at regulation, verification, and safeguards. The evidence shows that algorithmic adoption reshapes power balances, fosters new

technological dependencies, and strains regulatory regimes, demanding specific frameworks for containment and deterrence. The study provides a structural map of the field and a reproducible methodological path to guide public decision-making and the research agenda.

Keywords: algorithmic geopolitics; artificial intelligence; militarization; international security; technological sovereignty; emerging technologies.

Introducción

La militarización de la inteligencia artificial (IA) constituye un punto de inflexión en la transformación del poder global, reconfigurando las estructuras tradicionales de seguridad, conflicto y soberanía. En el panorama geopolítico actual, las potencias no solo compiten por la superioridad armamentística convencional, sino por la capacidad de integrar algoritmos, datos y autonomía tecnológica en sus sistemas de defensa (Dehghani-Firoozabadi y Chehrazad, 2024). Este fenómeno, identificado como “geopolítica algorítmica”, se ve impulsado por avances en sistemas autónomos, técnicas de aprendizaje automático (Machine Learning) y arquitecturas computacionales avanzadas, capaces de procesar y analizar información táctica en tiempos reducidos (Raska, 2021). Tales capacidades han dado lugar a modalidades de “guerra remota”, en las que drones, plataformas autónomas y software especializado redefinen el alcance y los límites de la intervención global (Biegon y Watts, 2022).

No obstante, la integración de IA en entornos militares plantea desafíos significativos que van más allá de la capacidad tecnológica. La ausencia de marcos regulatorios internacionales consolidados, junto con la desigualdad en el acceso a tecnologías de frontera y de última generación, incrementa el riesgo de una carrera armamentista tecnológica y de empleos estratégicos desestabilizadores (Williams, 2021). En particular, las tecnologías de frontera impulsadas por Estados desarrolladores acentúan asimetrías respecto de países predominantemente usuarios, ampliando brechas de autonomía estratégica. Además, el desplazamiento progresivo de los conflictos hacia el ciberespacio y entornos virtuales crea dificultades para la atribución de ataques y la definición de reglas de enfrentamiento, lo que complica la gestión de la seguridad internacional (Bächle y Bareis, 2022). Estos vacíos normativos y operativos revelan la urgencia de una gobernanza tecnológica que equilibre el desarrollo y la responsabilidad.

En este contexto, Colombia ha comenzado a dar pasos hacia la adopción de capacidades militares inteligentes, siguiendo tendencias globales y regionales. Ejemplo de ello es el desarrollo de plataformas UAV equipadas con sensores multisensoriales para vigilancia y reconocimiento, que integran módulos de inteligencia de señales (SIGINT), inteligencia geoespacial (GEOINT) e inteligencia de medidas y firmas (MASINT), particularmente acústicas, e incorporan cómputo embarcado para análisis en tiempo real (Amézquita-Gómez et al., 2023). De manera complementaria, la exploración de metodologías para inteligencia de señales mediante radio definida por software (SDR) refuerza la infraestructura nacional de vigilancia espectral autónoma, potenciando su utilidad en tareas de contrainteligencia (Terán et al., 2021). Estos avances, aunque relevantes, evidencian la necesidad de articular políticas públicas, investigación científica y capacidades operativas para garantizar que la adopción de IA en defensa responda a criterios de autonomía estratégica y seguridad nacional.

El presente estudio tiene como objetivo analizar el impacto de la militarización de la inteligencia artificial en la configuración geopolítica contemporánea, identificando elementos clave que la caracterizan y evaluando su aplicabilidad en el caso colombiano. A través de un análisis bibliométrico con *Bibliometrix* sobre literatura indexada en Scopus, se examinan patrones conceptuales, autores influyentes y vacíos temáticos que permiten comprender el alcance y las implicaciones de este fenómeno.

La bibliometría añade un valor decisivo, pues delimita empíricamente el campo mediante indicadores reproducibles, coocurrencia, citación, redes y clústeres que priorizan autores, conceptos y tendencias, anclando las categorías analíticas en evidencia estructural. En particular, proyección remota, ventaja competitiva, desmaterialización, guerra híbrida y gobernanza se articulan con los grafos y clústeres identificados, lo que mitiga sesgos de selección y facilita una lectura acumulativa de la literatura. La exposición avanza, así, desde la relación entre IA y poder hacia los mecanismos cognitivo-informacionales de las arquitecturas híbridas, y concluye en su encuadre normativo y disuasivo, asegurando coherencia entre teoría, método y resultados.

Para el desarrollo metodológico, se definen los tres apartados siguientes, que corresponden al marco teórico fundamental, para orientar y dar trazabilidad a la búsqueda bibliométrica. Este marco operacionaliza los ejes de capacidad, integración humana, máquina y marco normativo con mecanismos de contención y disuasión, y guía la definición de descriptores y sinónimos de la estrategia de búsqueda. Asimismo, acota los criterios de inclusión y exclusión del corpus e ilumina la lectura de la estructura temática revelada por redes de coocurrencia y clústeres, de modo que la argumentación sustantiva se apoye en patrones observables y no solo en apreciaciones narrativas. Así, la investigación se desenvuelve hacia cinco elementos clave: proyección remota de poder, ventaja competitiva global, desmaterialización del conflicto, guerra híbrida y gobernanza de la IA, ofreciendo un marco de análisis útil para orientar la formulación de políticas de defensa y el debate internacional sobre el uso ético y responsable de estas tecnologías emergentes.

Inteligencia artificial y su transformación como instrumento geopolítico

La inteligencia artificial (IA) ha dejado de ser una innovación meramente técnica para convertirse en un activo geopolítico estratégico. Su militarización redefine el equilibrio de poder internacional al integrar algoritmos, datos y sistemas autónomos en doctrinas de defensa, control de territorios y proyección remota de fuerza (Biegon y Watts, 2022; Dehghani-Firoozabadi y Chehrazad, 2024). Este fenómeno, denominado por algunos como “geopolítica algorítmica”, ha llevado a potencias como Estados Unidos y China a invertir masivamente en el desarrollo de capacidades de inteligencia artificial con fines militares y diplomáticos (Rezapour, 2025).

A nivel regional, países como Colombia avanzan en esta dirección mediante el diseño de plataformas UAV multisensor equipadas con módulos de GEOINT, SIGINT y MASINT, lo cual constituye una arquitectura de Inteligencia, Vigilancia y Reconocimiento (ISR, por sus siglas en inglés) localmente desarrollada (Amézquita-Gómez et al., 2023). Estas iniciativas permiten a Estados emergentes mejorar su autonomía estratégica mediante el control del ciclo de inteligencia, desde la recolección hasta el análisis de datos en tiempo real. Así, la IA se consolida como un componente central de la política exterior y de defensa en un sistema internacional regido por el dominio informacional.

Arquitecturas híbridas de inteligencia y su papel en la guerra cognitiva

Los sistemas híbridos de inteligencia, que integran capacidades humanas con algoritmos de *machine learning*, emergen como herramientas clave en la anticipación de amenazas en entornos irregulares y asimétricos. Los sistemas de predicción basados en IA permiten pronosticar demandas logísticas o identificar amenazas emergentes en escenarios ambiguos, propios de las llamadas guerras en “zona gris” (Reep, 2024). Esta capacidad de anticipación confiere ventaja estratégica y reduce el margen de error operativo.

Asimismo, el uso de radio definido por software (SDR) para SIGINT y de redes neuronales apli-

cadadas a inteligencia acústica (MASINT) refuerzan la capacidad de vigilancia táctica y estratégica, especialmente en regiones con alta complejidad territorial o riesgo ambiental (Corzo-Ussa et al., 2023; Terán et al., 2021). Estas tecnologías no solo optimizan operaciones militares, sino que también forman parte del repertorio de herramientas usadas en conflictos de carácter cognitivo o informacional, donde el control de narrativas, datos y percepciones resulta decisivo. En conjunto, estas arquitecturas permiten a actores estatales diseñar sistemas inteligentes que no solo actúan de forma autónoma, sino que colaboran con operadores humanos para ejecutar decisiones informadas en tiempo real, consolidando una infraestructura cognitiva con valor táctico, político y simbólico.

Seguridad ambiental, ciberespacio y normativas emergentes en la era de la IA

La expansión de la inteligencia artificial ha ampliado el concepto de seguridad más allá del ámbito militar, integrando dimensiones ambientales, digitales y normativas. La aplicación de IA a la vigilancia de incendios, deforestación o actividades ilegales en zonas rurales refuerza la noción de una seguridad humana y ecológica interdependiente (Francisco, 2023). En este marco, la IA se convierte en una herramienta dual, útil tanto para operaciones militares como para la protección del medio ambiente, como lo demuestra el uso de redes neuronales en sensores acústicos diseñados para monitorear detonaciones, actividad sísmica o desplazamientos no autorizados (Corzo-Ussa et al., 2023).

Esta transformación funcional plantea desafíos jurídicos y éticos en el ámbito internacional. La creciente sofisticación de sistemas autónomos de armas y de plataformas de vigilancia algorítmica ha generado debates sobre el derecho internacional humanitario, la responsabilidad en conflictos automatizados y la soberanía digital. Aunque aún sin marco regulatorio consolidado, se evidencia la necesidad de infraestructuras jurídicas globales que acompañen el avance tecnológico (Dehghani-Firoozabadi y Chehrazad, 2024).

La convergencia entre IA, ciberespacio y medio ambiente obliga a repensar la arquitectura de seguridad desde una lógica integrada, donde la defensa del territorio incluye la gestión de datos, recursos naturales y flujos de información estratégicos.

Metodología

Esta investigación adopta un enfoque bibliométrico con síntesis narrativa guiada por indicadores. Los patrones estructurales del corpus (coocurrencia, redes, clústeres y citación) se emplean como criterios de codificación temática a priori para interpretar tendencias y articular categorías analíticas. Su objetivo es identificar los elementos clave que configuran la militarización de la inteligencia artificial y su impacto geopolítico, desde la literatura científica especializada en defensa, tecnología y relaciones internacionales. Con este enfoque metodológico se logra organizar y comprender el campo de estudio, fundamentando un marco interpretativo sólido (Díez-Gómez et al., 2019), con el fin de contribuir a propuestas responsables y estratégicas para el desarrollo de tecnologías emergentes aplicadas a la seguridad y la defensa.

El análisis se realizó utilizando *Bibliometrix*, un paquete en R diseñado para ejecutar análisis bibliométricos integrales, incluyendo visualización, mapeo temático y análisis de redes (Aria y Cuccurullo, 2017). Se seleccionó la base de datos *Scopus*, por su cobertura multidisciplinaria y actualizada.

Se procedió a la recolección de registros bibliográficos mediante una estrategia de búsqueda con palabras clave relacionadas con inteligencia artificial, seguridad, autonomía tecnológica y conflicto híbrido, aplicando filtros temáticos, temporales y lingüísticos. Los datos obtenidos permitieron apli-

car técnicas como coocurrencia de términos, redes de colaboración y acoplamiento bibliográfico, lo cual facilitó la identificación de enfoques dominantes, autores clave y vacíos teóricos.

Así las cosas, para el desarrollo de la investigación se partió con un conjunto amplio de palabras que cubriera los parámetros de búsqueda, estas son: Artificial Intelligence (AI), Military applications, Military strategy, Lethal Autonomous Weapons Systems (LAWS), Autonomous weapons, Geopolitics, International relations, Security Strategic stability, Arms race, Deterrence, Ethics, Regulation y Governance. Luego se agruparon en conectores booleanos para seleccionar artículos relevantes y ampliamente relacionados con el objeto de investigación; la ecuación avanzada de búsqueda ingresada a *Scopus* fue la siguiente:

(TITLE-ABS-KEY ((“artificial intelligence” AND military AND geopolitics)) OR TITLE-ABS-KEY ((“military applications” AND “machine learning”) AND (conflict OR escalation) AND (global OR international)) OR TITLE-ABS-KEY ((“AI in warfare” OR “artificial intelligence in military”) AND (arms AND race OR deterrence) AND “strategic stability”) OR TITLE-ABS-KEY ((“autonomous weapons” OR “lethal autonomous weapons systems”) AND (regulation OR ethics) AND “international security”) OR TITLE-ABS-KEY ((“geopolitics” AND “artificial intelligence”) AND (“national security” OR “defense policy”) AND (China OR USA OR Russia)))

La búsqueda en *Scopus* se ejecutó para el periodo 1997 - 2025 con última consulta el 25 agosto de 2025. Se obtuvo un archivo bibliométrico de veinticinco documentos, los cuales se cargan completamente en *Bibliometrix*. Luego se realiza la búsqueda para identificar los elementos clave que configuran la militarización de la inteligencia artificial y su impacto geopolítico, los resultados de estos documentos están distribuidos como se muestra en la Tabla 1.

Tabla 1. Resultado de búsqueda de documentos en *Scopus*

Descripción	Resultados
Periodo de tiempo	1997:2025
Fuentes (revistas, libros, etc.)	24
Documentos	25
Palabras clave Plus	66
Palabras clave del autor	90
Autores	39

Fuente: elaboración propia, a partir del software *Bibliometrix*

Con base en los documentos encontrados, donde todos aportan información relevante y coherente al tema de información gracias a los filtros aplicados, se realiza el análisis documental sin limitar el periodo de publicación y se procede a priorizar los documentos más citados en la base de datos obtenida; los resultados de *Bibliometrix* en este aspecto se muestran en la Tabla 2.

Tabla 2. Documentos más citados

Título del Documento	Citaciones
Robot Wars: US Empire and geopolitics in the robotic age (Shaw, 2017)	40
The sixth RMA wave: Disruption in Military Affairs? (Raska, 2021)	29

Artificial intelligence for environmental security: national, international, human and ecological perspectives (Francisco, 2023)	22
Remote Warfare and the Retooling of American Primacy (Biegon y Watts, 2022)	18
Knowledge discovery in international conflict databases (Förnkrantz et al., 1997)	16
Operations of power in autonomous weapon systems: ethical conditions and socio-political prospects (Hynek y Solovyeva, 2021)	12
“Autonomous weapons” as a geopolitical signifier in a national power play: analysing AI imaginaries in Chinese and US military policies (Bächle y Bareis, 2022)	12
Locating LAWS: Lethal Autonomous Weapons, Epistemic Space, and “Meaningful Human” Control (Williams, 2021)	8
Geopolitics of Technological Futures: Warfare Technologies and Future Battlefields in German Security Debates (Ruppert, 2024)	3
Artificial intelligence: The new tool for cyber diplomacy (Bângăoanu y Cheregi, 2021)	2

Fuente: elaboración propia, a partir del software *Bibliometrix*

El estudio combina análisis bibliométrico (coocurrencia, redes y citas) con una síntesis narrativa guiada por indicadores; los patrones estructurales del corpus (nodos, aristas y clústeres) se emplean como criterios de codificación temática a priori para interpretar tendencias y articular categorías analíticas. Se parte con un estudio de los documentos disponibles, luego, los conceptos y palabras clave previamente identificados emergen de los indicadores bibliométricos (Keywords Plus, coocurrencia y documentos más citados) y se integran mediante síntesis narrativa, lo que permite pasar de la estructura del campo a cinco categorías interpretativas con trazabilidad metodológica.

Resultados

Los conceptos y palabras clave estudiadas anteriormente son esenciales para comprender cómo la militarización de la IA redefine los equilibrios estratégicos y las capacidades operativas de los Estados. La combinación de IA con tecnologías relacionadas con la cuarta revolución industrial, como el blockchain (cadena de bloques) y el internet de las cosas (IoT), fortalece la conectividad, integridad de datos y la ciberseguridad, aspectos críticos para entornos militares y de inteligencia (Corzo-Ussa et al., 2022; Jyothi et al., 2025; Wasserman, 2025). Asimismo, la integración de sistemas autónomos en contextos híbridos y desmaterializados refleja una tendencia hacia conflictos multidominio, donde la superioridad tecnológica es tan determinante como la física (Biegon y Watts, 2022; Raska, 2021). Estos enfoques teóricos constituyen la base para interpretar y valorar los elementos clave identificados en la investigación.

La Tabla 3 sintetiza los principales elementos clave que estructuran la militarización de la inteligencia artificial, derivados del análisis bibliográfico y conceptual desarrollado, a su vez, en el análisis de los documentos consultados. Cada elemento describe un aspecto crítico de la integración de la IA en el ámbito militar, desde su papel en la proyección remota y la ventaja competitiva global, hasta su influencia en la desmaterialización del conflicto, la guerra híbrida y los desafíos normativos. La tabla vincula estos componentes con las referencias académicas que los sustentan, ofreciendo una visión consolidada que conecta la teoría con los hallazgos empíricos de la investigación.

Tabla 3. Elementos clave de la militarización de la IA

Elemento clave	Descripción	Artículos que lo sustentan
IA y proyección remota	La IA facilita la proyección remota de poder militar y político mediante el uso de sistemas autónomos, como drones y armas letales autónomas, permitiendo realizar operaciones a distancia con mínima intervención humana. Esta capacidad redefine los escenarios de conflicto al extender el alcance estratégico sin necesidad de despliegues tradicionales.	(Biegon y Watts, 2022; Dehghani-Firoozabadi y Chehrazad, 2024; Corzo-Ussa et al., 2023; Hynek y Solovyeva, 2021; Shaw, 2017; Williams, 2021)
IA como ventaja competitiva global	La IA se ha convertido en un motor crucial de competencia entre grandes potencias, que invierten en su desarrollo para alcanzar o mantener la hegemonía tecnológica. Esta rivalidad impulsa innovaciones estratégicas que redefinen la superioridad en los ámbitos militar, económico y geopolítico, afectando el balance global de poder.	(Bächle y Bareis, 2022; Dehghani-Firoozabadi y Chehrazad, 2024; Hynek y Solovyeva, 2021; Raska, 2021; Shaw, 2017)
Desmaterialización del conflicto	La IA transforma la naturaleza de los conflictos al trasladar las operaciones bélicas del dominio físico al digital. Los conflictos desmaterializados son librados en redes, algoritmos y bases de datos, reduciendo la necesidad de presencia humana directa. Este cambio plantea nuevos desafíos en la identificación y control de actores beligerantes.	(Dehghani-Firoozabadi y Chehrazad, 2024; Corzo-Ussa et al., 2023; Raska, 2021; Shaw, 2017; Williams, 2021)
IA y guerra híbrida/líquida	La IA es catalizadora de nuevas formas de guerra híbrida y líquida, combinando acciones militares convencionales con operaciones cibernéticas, espaciales e informativas. Esta evolución estratégica crea conflictos flexibles y difíciles de delimitar, donde los ataques pueden ocurrir simultáneamente en múltiples dominios, afectando tanto infraestructura física como cognitiva.	(Dehghani-Firoozabadi y Chehrazad, 2024; Corzo-Ussa et al., 2023; Hynek y Solovyeva, 2021; Raska, 2021; Shaw, 2017)
Normativas y gobernanza de la IA	La creciente militarización de la IA genera serios desafíos normativos y éticos, exigiendo el establecimiento de nuevas reglas de gobernanza global. La falta de marcos regulatorios claros incrementa el riesgo de carreras armamentistas tecnológicas, desigualdades en el acceso a tecnologías avanzadas y vulnerabilidad en la seguridad internacional.	(Bächle y Bareis, 2022; Dehghani-Firoozabadi y Chehrazad, 2024; Fürnkranz et al., 1997; Williams, 2021)

Fuente: elaboración propia

El análisis de la Tabla 3 revela que los cinco elementos clave identificados, como lo son: proyección remota de poder, ventaja competitiva global, desmaterialización del conflicto, guerra híbrida y gobernanza de la IA, no solo sintetizan tendencias conceptuales, sino que reflejan transformaciones operativas en los entornos estratégicos contemporáneos. La proyección remota, impulsada por sistemas autónomos y capacidades ISR avanzadas, permite intervenciones precisas sin presencia física directa (Amézquita-Gómez et al., 2023).

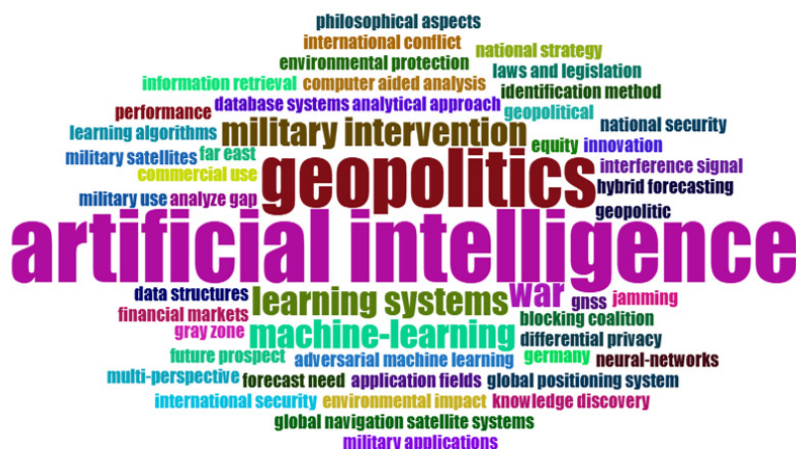
La ventaja competitiva global, en cambio, se relaciona con la capacidad de dominar la infraestructura algorítmica y de datos, como señala la geopolítica algorítmica descrita por Bächle y Bareis (2022). La desmaterialización del conflicto, en la que operaciones cibernéticas y ataques a infraestructuras críticas reemplazan enfrentamientos convencionales, coincide con el enfoque de ciberseguridad adaptativa planteado por Jyothi et al. (2025). La guerra híbrida combina estas dinámicas con operaciones de influencia y manipulación informativa, destacando el rol de tecnologías, como blockchain, para preservar la integridad de datos (Wasserman, 2025). Finalmente, la gobernanza de la IA se erige como el marco necesario para asegurar control humano significativo y prevenir escaladas no in-

tencionales, cuestión enfatizada por Williams (2021). En conjunto, estos resultados ofrecen un marco integral para comprender cómo la IA reconfigura el poder y la seguridad en escenarios multidominio.

Análisis de palabras clave y redes de coocurrencia

Las *Keywords Plus* son términos generados automáticamente a partir de las palabras y frases presentes en los títulos de las referencias citadas por los artículos, lo que permite ampliar el alcance del análisis bibliométrico más allá de las palabras clave proporcionadas por los autores. Este enfoque ofrece una visión enriquecida del campo de estudio, ya que identifica conceptos relevantes que pueden no haberse declarado explícitamente, pero que forman parte del contexto intelectual de la literatura analizada (Aria y Cuccurullo, 2017). En el caso de la investigación sobre militarización de la inteligencia artificial, el análisis de *Keywords Plus* resulta valioso para detectar marcos teóricos, tendencias emergentes y áreas temáticas relacionadas como ciberseguridad, ética, sistemas autónomos o derecho internacional. Además, permite establecer conexiones entre los elementos clave del marco teórico y el universo conceptual más amplio del que forman parte, fortaleciendo así la interpretación y la relevancia de los resultados obtenidos. La Figura 1 muestra el resultado con cincuenta palabras clave plus generada por *Bibliometrix*.

Figura 1. Nube de palabras clave plus sobre militarización de la IA



Fuente: elaboración propia, a partir del software *Bibliometrix*

La nube de palabras obtenida a partir del análisis de *Keywords Plus* evidencia la centralidad de conceptos, como *artificial intelligence*, *geopolitics* y *military intervention*, los cuales se corresponden con los ejes temáticos descritos anteriormente. Estos términos confirman que la militarización de la IA se articula en torno a la convergencia entre innovación tecnológica, estrategia geopolítica y despliegue operativo, tal como se expone en los elementos clave de proyección remota, ventaja competitiva global y guerra híbrida.

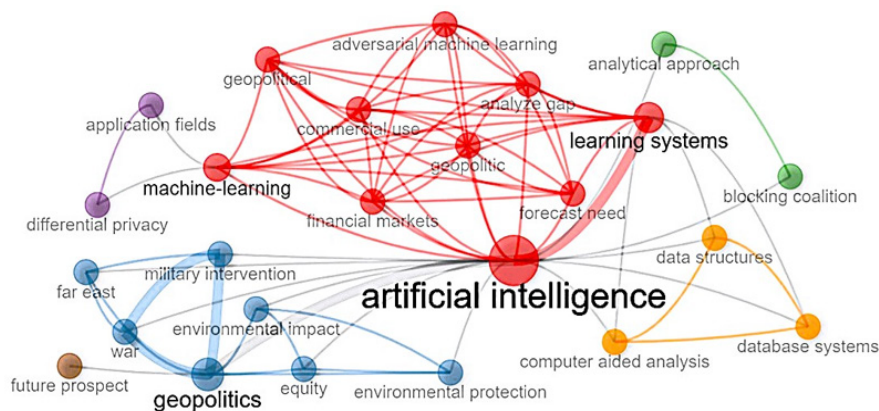
La presencia de expresiones como *machine-learning*, *learning systems* y *neural-networks* refuerza la importancia de las arquitecturas avanzadas de IA en la configuración de entornos multidominio, donde la capacidad algorítmica es tan determinante como la fuerza física (Korteling et al., 2021). Asimismo, referencias a *national security*, *laws and legislation* e *international security* reflejan la creciente necesidad de marcos normativos y éticos, vinculados al elemento de gobernanza de la IA (Eaton, 2025).

Conceptos como *jamming*, adversarial *machine learning* y *environmental protection* amplían el espectro hacia amenazas híbridas y seguridad ambiental, aspectos destacados en estudios sobre ciberseguridad y operaciones autónomas (Dehghani-Firoozabadi y Chehrazad, 2024; Jyothi et al., 2025). En conjunto, este patrón semántico respalda la interpretación de que los cinco elementos clave identificados no solo son coherentes con la literatura, sino que se insertan en un marco global de alta complejidad tecnológica y estratégica.

Continuando con el análisis, la herramienta *cooccurrence network* de *Bibliometrix* permite identificar y representar gráficamente las relaciones entre términos clave en un conjunto de documentos, ya sean *author keywords* o *Keywords Plus*. Este análisis revela patrones de coocurrencia, mostrando cómo los conceptos se agrupan y conectan dentro del corpus bibliográfico. En la red, cada nodo representa una palabra clave y su tamaño refleja la frecuencia de aparición; las aristas indican la fuerza de la relación, según el número de veces en que los términos coexisten en los mismos artículos.

Mediante algoritmos de *clustering* (agrupamiento), como *Edge betweenness*, es posible detectar comunidades temáticas, cada una representada con un color distinto. Este tipo de visualización es relevante porque facilita la identificación de núcleos conceptuales, la detección de subtemas emergentes y la verificación de coherencia entre los hallazgos bibliométricos y el marco teórico. Según Aria y Cuccurullo (2017), este enfoque proporciona una base metodológica sólida para el mapeo de la ciencia y el análisis estructural de campos de investigación complejos. La Figura 2 muestra la red de coocurrencia con las palabras clave plus obtenida con *Bibliometrix*.

Figura 2. Red de coocurrencia con palabras clave plus



Fuente: elaboración propia, a partir del software *Bibliometrix*

La red de coocurrencia obtenida a partir de las *Keywords Plus* muestra una estructura conceptual en la que destacan nodos centrales como *artificial intelligence* y *geopolitics*, interconectados de forma directa y con un alto peso en el grafo. Esta relación confirma que el campo de estudio se articula principalmente en torno a la convergencia entre avances tecnológicos en IA y su proyección en el ámbito geopolítico, tal como se expone en los elementos de proyección remota y ventaja competitiva global, como elementos clave de la militarización de la IA (Bächle y Bareis, 2022; Dehghani-Firoozabadi y Chehrazad, 2024).

En el clúster rojo, además de estos conceptos centrales, se observa la conexión a términos como *military intervention*, *war* y *environmental protection* en el cluster azul, lo que evidencia el vínculo entre la IA y la formulación de estrategias de defensa que incluyen la protección ambiental. Este patrón es coherente con lo identificado en la nube de palabras, donde varios términos asociados con la

formulación de estrategias de defensa ocupan posiciones dominantes, reforzando la idea de que la IA se ha convertido en un activo geopolítico estratégico capaz de redefinir el equilibrio de poder global (Raska, 2021; Shaw, 2017).

Otros términos, como *machine learning* y *learning systems*, destacan por su asociación con el desarrollo de arquitecturas avanzadas de IA, las cuales, son fundamentales para la ejecución de operaciones en entornos híbridos y desmaterializados. Estos hallazgos coinciden con los elementos de guerra híbrida y desmaterialización del conflicto, destacando cómo la capacidad algorítmica complementa la dimensión física en escenarios multidominio (Jyothi et al., 2025; Korteling et al., 2021).

Finalmente, clústeres menores agrupan términos emergentes, como *future prospect* unido con *equity*, así como *differential privacy* con *application fields*, resaltando algunas conexiones de IA y geopolítica con palabras como *equity*, *environmental protection* y *war*, evidenciando que la militarización de la IA también abarca aspectos normativos y éticos, así como dimensiones de seguridad ambiental. Esta diversidad temática refuerza el elemento de gobernanza de la IA, identificado en los elementos clave, y confirma que su desarrollo debe abordarse desde un enfoque integral que considere implicaciones técnicas, políticas y sociales (Eaton, 2025; Wasserman, 2025).

Estas agrupaciones fortalecen los cinco elementos clave identificados: proyección remota, ventaja competitiva, desmaterialización del conflicto, guerra híbrida y líquida, y gobernanza de la inteligencia artificial. En conjunto, los resultados evidencian cómo la inteligencia artificial está transformando la naturaleza del poder en el sistema internacional, consolidándose como una herramienta estratégica en los ámbitos militar, político, normativo y ambiental.

Discusión

Los resultados obtenidos confirman que la inteligencia artificial (IA) ha emergido como un eje estratégico de transformación en las dinámicas de poder global, redefiniendo los escenarios de seguridad, defensa y soberanía en el siglo XXI. A nivel internacional, la militarización de la IA ha impulsado nuevas formas de proyección remota, desmaterialización del conflicto, guerra híbrida y retos normativos, elementos clave que también encuentran expresión en el caso colombiano (Dehghani-Firoozabadi y Chehrazad, 2024; Raska, 2021). Este fenómeno, enmarcado en la denominada “geopolítica algorítmica” (Bächle y Bareis, 2022; Shaw, 2017), otorga ventaja estratégica a los Estados capaces de integrar sistemas autónomos, machine learning y ciberseguridad en sus doctrinas de defensa, reforzando la ventaja competitiva global como otro componente esencial de este proceso.

Colombia, consciente de los desafíos geopolíticos y de defensa contemporáneos, ha iniciado procesos de modernización militar en los que la IA desempeña un papel clave. El desarrollo de plataformas UAV multisensoriales, equipadas con capacidades SIGINT, GEOINT y MASINT, representa un avance significativo en la proyección remota y la capacidad autónoma de inteligencia y vigilancia estratégica (Amézquita-Gómez et al., 2023). De forma complementaria, la implementación de sistemas de geoposicionamiento mediante radiofrecuencia en zonas de difícil acceso (Guzmán-Castañeda et al., 2020) y el uso de inteligencia acústica en escenarios sostenibles (Corzo-Ussa et al., 2023) refuerzan el enfoque de defensa multidimensional, alineado con la guerra híbrida y su capacidad de operar en múltiples dominios.

La ciberseguridad, reconocida como un desafío crucial para las Fuerzas Militares (Peña-Suarez, 2023), impulsa la adopción de IA en la protección de infraestructuras críticas y soberanía digital. La incorporación de sistemas de radio definida por software (SDR) para inteligencia de señales (Terán et al., 2021; Torres-Garzón et al., 2022) y los avances en UAVs dotados con sensores IR-FLIR (Beltrán-Bejarano y Alfonso-Sandoval, 2021) demuestran un interés creciente por tecnologías duales,

aplicables tanto a defensa convencional como a protección ambiental, fortaleciendo los ámbitos de desmaterialización del conflicto y guerra híbrida.

Además, con los aportes desde la Cuarta Revolución Industrial, con la integración de IA, Big Data, internet de las cosas, blockchain y, potencialmente, computación cuántica, se abren oportunidades para que Colombia reduzca brechas tecnológicas históricas en su estructura de defensa (Corzo-Ussa et al., 2022; Jyothi et al., 2025). Esta convergencia tecnológica no solo fortalece la ventaja competitiva global, sino que también demanda el desarrollo de marcos de gobernanza de la IA que garanticen su uso ético y seguro (Eaton, 2025; Williams, 2021).

Este proceso, aunque incipiente, posiciona al país como un actor regional en el uso estratégico de tecnologías emergentes aplicadas a la seguridad, la defensa y la proyección de poder en un entorno internacional cada vez más competitivo y algorítmico. Sin embargo, para consolidar estos avances, es necesario fortalecer la soberanía tecnológica, la gobernanza ética de la IA y la interoperabilidad de sistemas con aliados estratégicos.

Como línea de investigación futura, se propone ampliar el análisis a otras bases de datos y periodos de tiempo para captar tendencias emergentes y evaluar comparativamente las capacidades nacionales frente a potencias y actores regionales. Asimismo, resultaría valioso profundizar en la medición de la resiliencia de las infraestructuras críticas y en el impacto de la dependencia tecnológica externa. Esto permitiría superar las limitaciones de la presente investigación, centrada en un corpus acotado y en un análisis que, si bien sólido, se enfoca principalmente en la perspectiva documental y no en métricas operativas de desempeño.

Conclusiones

La inteligencia artificial redefine las dinámicas de poder global al introducir nuevas formas de proyección remota, competencia estratégica, desmaterialización de conflictos, guerras híbridas y desafíos normativos. Estos elementos delinean un entorno geopolítico algorítmico, en el que el control de datos y sistemas autónomos reconfigura la soberanía y la seguridad internacional. Según Shaw, la proliferación de tecnologías robóticas está transformando el campo de batalla en espacios automatizados de poder, lo que él denomina un “imperio robótico”, redefiniendo el alcance de las intervenciones militares y su impacto en las democracias contemporáneas.

En este escenario, Colombia ha iniciado procesos de modernización que reflejan estas tendencias globales. El desarrollo de plataformas UAV multisensoriales, la implementación de sistemas de inteligencia de señales (SIGINT) y el fortalecimiento de capacidades en ciberseguridad demuestran un interés estratégico por adaptar la defensa nacional a las dinámicas de la geopolítica algorítmica. Además, la incorporación de tecnologías de la Industria 4.0 en aplicaciones militares permite al país cerrar brechas tecnológicas históricas y posicionarse como actor emergente en la región.

Si bien estos avances son significativos, también plantean desafíos en términos de soberanía tecnológica, gobernanza de la IA y dependencia estratégica. Colombia debe consolidar políticas públicas que garanticen un desarrollo ético y autónomo de estas capacidades, alineadas con un enfoque de defensa integral y sostenible frente a las nuevas amenazas globales.

Referencias

- Amézquita-Gómez, N., González-Bautista, S. R., Terán, M., Salazar, C., Corredor, J. y Corzo, G. D. (2023). Preliminary Approach for UAV-Based Multi-Sensor Platforms for Reconnaissance and Surveillance applications. *Ingeniería*, 28(3), e21035. <https://doi.org/10.14483/23448393.21035>
- Aria, M. y Cuccurullo, C. (2017). Bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics*, 11(4), 959-975. <https://doi.org/10.1016/j.joi.2017.08.007>
- Bächle, T. C. y 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). <https://doi.org/10.1186/s40309-022-00202-w>
- Bârgăoanu, A. y Cheregi, B. F. (2021). Artificial intelligence: The new tool for cyber diplomacy en F. Roumate (Ed.), *Artificial Intelligence and Digital Diplomacy: Challenges and Opportunities* (pp. 115-130). Springer. https://doi.org/10.1007/978-3-030-68647-5_9
- Beltrán-Bejarano, Ó. L. y Alfonso-Sandoval, J. D. (2021). Inteligencia, vigilancia y reconocimiento IR-FLIR en los vehículos aéreos no tripulados de la Inteligencia Militar. *Perspectivas en Inteligencia*, 13(22), 203-225. <https://doi.org/10.47961/2145194x.278>
- Biegon, R. y Watts, T. F. A. (2022). Remote Warfare and the Retooling of American Primacy. *Geopolitics*, 27(3), 948-971. <https://doi.org/10.1080/14650045.2020.1850442>
- Corzo-Ussa, G. D., Álvarez-Aros, E. L. y Chavarro, F. (2022). La industria 4.0 y sus aplicaciones en el ámbito militar: oportunidad estratégica para Latinoamérica. *Revista Científica General José María Córdova*, 20(39), 717-736. <https://doi.org/10.21830/19006586.882>
- Corzo-Ussa, G. D., Álvarez-Aros, E. L., Mariño, J. P. y Amézquita-Gómez, N. (2023). Military artificial intelligence applied to sustainable development projects: sound environmental scenarios. *DYNA (Colombia)*, 90(228), 115-122. <https://doi.org/10.15446/dyna.v90n228.108639>
- Dehghani-Firoozabadi, S. J. y Chehrazad, S. (2024). Geopolitics of artificial intelligence; Theoretical roadmap for algorithmic competitions of world actors. *Geopolitics Quarterly*, 20(3), 270-313. <https://doi.org/10.22034/igq.2024.143237>
- Díez-Gómez, D. A., Guillén, M. y Rodríguez, M. del P. (2019). Revisión de la literatura sobre la toma de decisiones éticas en organizaciones. *Información Tecnológica*, 30(3), 25-38. <https://doi.org/10.4067/s0718-07642019000300025>
- Eaton, S. E. (2025). Global trends in education: artificial intelligence, postplagiarism, and future-focused learning for 2025 and beyond – 2024–2025 werkund distinguished research lecture. *International Journal for Educational Integrity*, 21(1). <https://doi.org/10.1007/s40979-025-00187-6>
- Francisco, M. (2023). Artificial intelligence for environmental security: national, international, human and ecological perspectives. *Current Opinion in Environmental Sustainability*, 61. <https://doi.org/10.1016/j.cosust.2022.101250>

- Fürnkranz, J., Petrak, J. y Trappl, R. (1997). Knowledge discovery in international conflict databases. *Applied Artificial Intelligence*, 11(2), 91-118. <https://doi.org/10.1080/088395197118262>
- Guzmán-Castañeda, Á. A., Pinto-Urbe, J. W. y Velosa-Castañeda, D. A. (2020). Implementación de un sistema de geoposicionamiento con transmisión de coordenadas por radiofrecuencia. *Perspectivas en Inteligencia*, 12(21), 275-291. <https://doi.org/10.47961/2145194x.227>
- Hynek, N. y Solovyeva, A. (2021). Operations of power in autonomous weapon systems: ethical conditions and socio-political prospects. *AI and Society*, 36(1), 79-99. <https://doi.org/10.1007/s00146-020-01048-1>
- Jyothi, D., Vijay, P. J., Kumar, M. K. y Lakshmi, R. V. (2025). Design of an improved method for intrusion detection using CNN, LSTM, and Block chain. *Journal of Theoretical and Applied Information Technology*, 103(1), 1-21. <https://www.jatit.org/volumes/hundredthree1.php>
- Korteling, J. E., Van de Boer-Visschedijk, G. C., Blankendaal, R. A. M., Boonekamp, R. C. y Eikelboom, A. R. (2021). Human - versus Artificial Intelligence. *Frontiers in Artificial Intelligence*, 4. <https://doi.org/10.3389/frai.2021.622364> PMID:33981990 PMCID:PMC8108480
- Peña-Suárez, J. S. (2023). Ciberseguridad, un desafío para las Fuerzas Militares colombianas en la era digital. *Perspectivas en Inteligencia*, 15(24), 333-359. <https://doi.org/10.47961/2145194X.628>
- Raska, M. (2021). The sixth RMA wave: Disruption in Military Affairs? *Journal of Strategic Studies*, 44(4), 456-479. <https://doi.org/10.1080/01402390.2020.1848818>
- Reep, M. J. (2024). Leveraging Hybrid Systems to Forecast Needs and Analyze Gaps for Dual Commercial and Military Use. *2024 19th Annual System of Systems Engineering Conference, SoSE*, 124-129. <https://doi.org/10.1109/SOSE62659.2024.10620960>
- Rezapour, D. (2025). China's Cooperation with Central Asia with an Emphasis on Artificial Intelligence. *Journal of Central Eurasia Studies*, 17(35), 157-187. <https://magiran.com/p2835093>
- Ruppert, L. (2024). Geopolitics of Technological Futures: Warfare Technologies and Future Battlefields in German Security Debates. *Geopolitics*, 29(2), 581-606. <https://doi.org/10.1080/14650045.2023.2174431>
- Shaw, I. G. (2017). Robot wars: US empire and geopolitics in the robotic age. *Security Dialogue*, 48(5), 451-470. <https://doi.org/10.1177/0967010617713157> PMID:29081605 PMCID:PMC5639954
- Terán, M., Aranda, J., Marín, J., Uchamocha, E. y Corzo-Ussa, G. D. (2021). A methodology for signals intelligence using non-conventional techniques and software-defined radio. *2021 IEEE Colombian Conference on Communications and Computing, COLCOM*, 1-6. <https://doi.org/10.1109/COLCOM52710.2021.9486297>
- Torres-Garzón, E. A., Guevara-Cardona, J. C. y Mendoza-Prieto, Y. O. (2022). Estudio sobre el desarrollo de un prototipo para monitoreo del espectro radioelectrónico utilizando SDR. *Perspectivas en Inteligencia*, 14(23), 303-323. <https://doi.org/10.47961/2145194x.344>

- Wasserman, N. H. (2025). Untrustworthy AI: Blockchain as Inhibitor to the Propagation of Disinformation. *Lecture Notes in Networks and Systems*, 1284, 438-453. https://doi.org/10.1007/978-3-031-85363-0_28
- Williams, J. (2021). Locating LAWS: lethal autonomous weapons, epistemic space, and “meaningful human” control. *Journal of Global Security Studies*, 6(4). <https://doi.org/10.1093/jogss/ogab015>



Revista Perspectivas en Inteligencia

(Revista Científica en Ciencias Sociales e Interdisciplinaria)

Volumen 17, Número 26, enero - diciembre de 2025

ISSN: 2145-194X (impreso), 2745-1690 (en línea)

Página Web: <https://revistascedoc.com/index.php/pei>

Bogotá D.C., Colombia

Militarización de la Inteligencia Artificial: armas autónomas, equilibrio estratégico y gobernanza algorítmica

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo.

Financiamiento

Los autores no declaran fuente de financiamiento para la realización de este artículo.

Sobre el/los autor(es)

Germán Darío Corzo-Ussa es PhD en Planeación Estratégica y Dirección de Tecnología de la Universidad Popular Autónoma del Estado de Puebla (México), es Magister en Ingeniería Electrónica de la Pontificia Universidad Javeriana (Colombia), es Ingeniero Electrónico de la Universidad Distrital Francisco José de Caldas (Colombia), docente universitario e Investigador Senior del Sistema Nacional de Ciencia Tecnología e Innovación, Ejército Nacional de Colombia.

<https://orcid.org/0000-0001-7603-0896> - Contacto: german.corzo@esdeg.edu.co

Carol Vanesa Quintero-Rosas es Magister en Contratación Estatal de la Universidad de la Sabana (Colombia), Especialista en Derecho Procesal Penal, Constitucional y Justicia Penal Militar de la Universidad Militar Nueva Granada (Colombia), Abogada de la Universidad Libre (Colombia).

<https://orcid.org/0009-0004-9860-2081> - Contacto: carol.quintero@esdeg.edu.co

Nathalie Tarazona-Rojas es Magister en Innovación y Tecnologías para la Educación de la Universidad El Bosque (Colombia), Especialista en Gerencia de Proyectos de la Universidad Piloto de Colombia, es Ingeniera Eléctrica de la Universidad Industrial de Santander (Colombia).

<https://orcid.org/0000-0002-2113-4724> - Contacto: nathytr11@gmail.com

