Inteligencia artificial y amenazas híbridas en defensa y seguridad: un análisis bibliométrico y de clústeres en la literatura científica (2000–2025)

Artificial Intelligence and Hybrid Threats in Defense and Security: A Bibliometric and Cluster Analysis of the Scientific Literature (2000–2025)

Laura Janneth Delgado Nieto*
Julián Ricardo Romero Garibello**

Fecha de recepción: 21 de julio de 2025
Fecha de aprobación: 03 de octubre de 2025
Fecha de publicación: 15 de noviembre de 2025

DOI:https://doi.org/10.18041/1900-0642/criteriolibre.2025v23n43.13701

Resumen

La seguridad nacional enfrenta una problemática estratégica derivada de la compleja y acelerada convergencia entre la Inteligencia Artificial (IA) y las amenazas híbridas. Ante la necesidad de profundizar y sistematizar el conocimiento en este ámbito, se realizó un mapeo sistemático de un campo en rápida evolución, mediante la aplicación de una metodología cuantitativa basada en análisis bibliométrico y de clústeres. El estudio examinó 20.000 documentos extraídos de la base de datos Scopus durante el período 2000 – 2025. La coherencia del modelo jerárquico de agrupación se verificó mediante el índice de Calinski–Harabasz (1671.883), lo que garantiza una adecuada diferenciación entre los grupos. Los resultados evidencian una madurez temática caracterizada por un crecimiento exponencial, alcanzando su punto máximo en 2023, con cerca de 9.000 documentos en los que se identificó una estructura dominada por cuatro núcleos temáticos interconectados, que transitan

Citar como: Delgado, L. J. y Romero, J. R. (2025). Inteligencia artificial y amenazas híbridas en defensa y seguridad: un análisis bibliométrico y de clústeres en la literatura científica (2000–2025), 23 (43), 125-145. https://doi.org/10.18041/1900-0642/criteriolibre.2025v23n43.13701

*Docente de Cátedra Escuela Militar de Cadetes José María Córdova. Bogotá, Colombia. Magíster en Relaciones y Negocios Internacionales, Magister en Historia Militar. ORCID: https://orcid.org/0000-0003-4439-1747 Correo electrónico: laura.delgado@esmic.edu.co

**Magíster en Administración de Negocios MBA. Docente de Cátedra Escuela Militar de Cadetes José María Córdova. Bogotá, Colombia. ORCID: https://orcid.org/0000-0001-5873-1226 Correo electrónico: julian.romero@esmic.edu.co

desde la ciberseguridad y el *machine learning* tradicionales hacia la ética, la privacidad y las aplicaciones críticas (5G/IoT). El análisis de los diez clústeres confirmó una clara estructura núcleo-periferia del conocimiento, donde el núcleo clúster uno concentra la masa crítica de artículos en los que geográficamente, la producción está hegemónicamente concentrada en India, China y EE. UU. En conclusión, la investigación en IA y seguridad ha transitado hacia la multidisciplinariedad, evidenciando la urgencia de integrar consideraciones de gobernanza ética y resiliencia tecnológica en la formulación de políticas de defensa nacional frente a la automatización de las amenazas híbridas.

Palabras Clave: Inteligencia Artificial (IA), amenazas híbridas, análisis bibliométrico, clústers, aprendizaje de máquina.

Abstract

National security faces a strategic challenge arising from the complex and accelerated convergence between Artificial Intelligence (AI) and hybrid threats. In response to the need to deepen and systematize knowledge in this domain, a systematic mapping of a rapidly evolving field was conducted through the application of a quantitative methodology based on bibliometric and cluster analysis. The study examined 20,000 documents retrieved from the Scopus database over the period 2000-2025. The coherence of the hierarchical clustering model was validated using the Calinski-Harabasz index (1671,883), ensuring a clear differentiation between groups. The results reveal thematic maturity characterized by exponential growth, reaching its peak in 2023 with approximately 9,000 documents. A structure dominated by four interconnected cores was identified, envolving from traditional cybersecurity and machine learning towards ethics, privacy, and critical applications (5G/IoT). The analysis of the ten clusters confirmed a clear core-periphery structure of knowledge, where the primary cluster concentrates the critical mass of publications. Geographically, scientific output is hegemonically concentrated in India, China, and the United States. In conclusion, research on AI and security has envolved toward multidisciplinarity, highlighting the urgency of integrating ethical governance and technological resilience considerations into the formulation of national defense policies in the face of automation of hybrid threats.

Keywords: Artificial Intelligence (AI), hybrid threats, bibliometric analysis, clusters, machine learning.

1. Introducción

La seguridad y defensa de las naciones, en la actualidad y de cara al futuro, enfrentan una transformación sin precedentes marcada por la convergencia entre la Inteligencia Artificial (IA) y la proliferación de amenazas híbridas. Esta dinámica se configura en escenarios no lineales que combinan coerción militar con ciberataques, desinformación y manipulación tecnológica, lo que exige una comprensión profunda de su impacto en la defensa contemporánea.

La naturaleza interdisciplinaria y la rápida evolución de este fenómeno han generado un volumen creciente y complejo de literatura académica. Sin embargo, la identificación de la estructura temática subyacente y de las tendencias futuras del campo permanece fragmentada en las revisiones narrativas tradicionales. En este contexto, surge la siguiente pregunta de investigación: ¿de qué manera ha evolucionado la estructura del conocimiento científico y cuáles son las tendencias emergentes en la intersección entre la inteligencia artificial y las amenazas híbridas dentro de la literatura académica global entre 2000 y 2025?

Para abordar esta brecha y ofrecer una visión sistemática, el presente artículo aplica un riguroso análisis bibliométrico y de clústeres, a partir de la cartografía de la producción científica global en el período 2000-2025. El objetivo principal es identificar los núcleos de conocimiento, los países líderes y la dinámica de las líneas de investigación que configuran la interrelación entre la IA, las amenazas híbridas y la seguridad.

2. Revisión de Literatura

La naturaleza interdisciplinaria y el acelerado desarrollo de la Inteligencia Artificial (IA) aplicada a la seguridad demandan un enfoque de revisión de literatura que trascienda las aproximaciones narrativas tradicionales. En este contexto, la bibliometría se consolida como una herramienta cuantitativa esencial para analizar grandes volúmenes de producción científica y revelar la estructura de conocimiento en un campo determinado. Este enfoque supera la mera contabilización de documentos, al ofrecer un mapeo objetivo de las dinámicas de investigación, las tendencias temáticas y las redes de colaboración institucional (Romero et al., 2025a).

La ruta metodológica de este estudio se fundamenta en los principios del mapeo científico propuestos por Zupic y Čater (2015), quienes sostienen que los métodos bibliométricos introducen rigor y objetividad en el proceso de revisión de literatura, mitigando el sesgo subjetivo del investigador.

El uso de metodologías bibliométricas, —incluidas las técnicas de análisis de clústeres y coocurrencia de palabras clave —resulta especialmente pertinente en dominios tecnológicos emergentes y en constante evolución. Estas herramientas permiten desvelar la estructura de campos con alto impacto socioeconómico y rápido cambio, como lo evidencia su aplicación en el análisis de tendencias e innovación en el sector bancario y *fintech* (Romero et al., 2025b). En consecuencia, su empleo en el presente estudio se justifica como un medio para ofrecer un diágnostico

riguroso y sistemático del estado del arte en la interrelación entre la IA, la defensa y las amenazas híbridas.

La Inteligencia Artificial (IA) se define operacionalmente como el conjunto de sistemas y máquinas que emulan capacidades cognitivas humanas, tales como el aprendizaje, la percepción y la toma de decisiones (Gandomi & Haider, 2015). En el ámbito de la defensa y la seguridad, la IA ha pasado de ser una promesa futurista a constituirse en un catalizador de transformación militar y estratégica (Scharre, 2019).

Por su parte, el concepto de amenaza híbrida alude a la combinación de métodos de guerra convencionales y no convencionales, integrando coerción militar con estrategias subversivas no militares, como la desinformación, la guerra cibernética, la presión económica y la manipulación de la opinión pública (Galeotti, 2018). En este sentido, la hibridez no implica necesariamente la creación de nuevas tácticas, sino la sincronización estratégica de herramientas existentes con el fin de explotar vulnerabilidades políticas, sociales y tecnológicas del adversario sin cruzar el umbral de un conflicto abierto; una dinámica, de medios que es vista como una forma de desafío sistémico, diseñada para crear ambigüedad y evitar la escalada directa (Renz, 2016).

En la actualidad, las amenazas híbridas emergen de la articulación de instrumentos militares, cibernéticos, económicos e informacionales orientados a explotar vulnerabilidades sociopolíticas y tecnológicas de los estados, obligando a repensar los marcos teóricos tradicionales de las relaciones internacionales (Danyk & Briggs, 2023). Desde esta perspectiva, la hibridación de los conflictos desplaza el foco desde la capacidad bélica hacia la gestión de la percepción pública, la resiliencia societal y la gobernanza de infraestructuras críticas.

En este contexto, la Inteligencia Artificial potencia tanto la sofisticación —por ejemplo, mediante la automatización de operaciones de influencia y guerra cognitiva— como la velocidad de las acciones híbridas, lo que exige marcos analíticos capaces de integrar dinámicas tecnológicas, asimetrías de poder y procesos normativos transnacionales para diseñar respuestas políticas y estratégicas efectivas.

La característica principal en el marco de las amenazas híbridas es la integración de la coerción a través de operaciones de información, ciberataques y desestabilización económica, lo que hace que el concepto de "guerra" sea menos útil que el de "competencia estratégica" (Münkler, 2016). Esta ambigüedad en la atribución de responsabilidades obliga a las entidades de seguridad a depender cada vez más de capacidades analíticas avanzadas para identificar la fuente y la naturaleza de los ataques, es por esto que, la gestión de este riesgo híbrido requiere un enfoque integral y multidisciplinar de seguridad (Sipahi, 2020).

El crecimiento exponencial de la producción científica entre 2000 y 2025 puede interpretarse bajo la teoría de la difusión de innovaciones de Rogers (2003), quien afirma que el proceso de adopción tecnológica depende de la percepción de ventaja relativa y compatibilidad con las

necesidades del sistema. En este sentido, la convergencia entre la inteligencia artificial (IA) y la defensa ha transitado de una fase inicial de innovadores hacia una etapa de mayoría temprana en el último lustro. Este fenómeno sugiere que la IA ha superado las barreras de incertidumbre en materia tecnológica, siendo percibida por la comunidad estratégica como una innovación con alta capacidad de respuesta ante las amenazas híbridas.

Desde la perspectiva de los paradigmas científicos de Kuhn (1970), los hallazgos sugieren que el sector de la seguridad atraviesa una fase de ciencia extraordinaria. El surgimiento de clústeres temáticos centrados en ciberdefensa y aprendizaje profundo indica el desplazamiento de los paradigmas tradicionales de defensa lineal hacia un nuevo paradigma de seguridad cognitiva.

Como señala Kuhn (1970), un cambio de paradigma ocurre cuando los modelos existentes no pueden resolver anomalías críticas; en este caso, la sofisticación de las amenazas híbridas ha forzado la adopción de la IA como el nuevo marco de resolución de problemas en la literatura científica global.

Según Rogers (2003), este desplazamiento ocurre cuando una innovación demuestra una ventaja relativa crítica; en este caso, la capacidad de la IA para procesar volúmenes masivos de datos frente a amenazas híbridas ha acelerado su adopción y difusión en la literatura académica. A su vez, Hoffman (2022), plantea desafíos multidimensionales que desdibujan las fronteras entre el conflicto convencional y el irregular, exigiendo una respuesta tecnológica superior. Boulanin y Giammatteo (2023), sostienen que la IA ha dejado de ser una tecnología emergente para consolidarse como un pilar de la seguridad nacional, con implicaciones estratégicas y políticas que redefinen el equilibrio de poder. No obstante, esta rápida integración conlleva riesgos éticos significativos. Al respecto, la UNESCO (2023) enfatiza que el desarrollo de sistemas inteligentes en ámbitos de gobernanza y seguridad debe estar sujeto a marcos éticos globales que garanticen la transparencia y el control humano, evitando que la autonomía algorítmica vulnere principios fundamentales de derechos y estabilidad internacional.

En el contexto colombiano, la convergencia tecnológica en el sector de la seguridad no es solo un fenómeno académico, sino que responde a directrices de política pública; por ejemplo, el Ministerio de Hacienda y Crédito Público de Colombia (2023) subraya la importancia de una planeación estratégica del gasto para asegurar que las inversiones en ciencia y tecnología contribuyan efectivamente a la seguridad nacional. Asimismo, el Departamento Nacional de Planeación (2024) subraya que el fortalecimiento de capacidades en IA se alinea con los objetivos de soberanía y protección ciudadana.

Finalmente, la dimensión de la desinformación dentro de las amenazas híbridas constituye un riesgo particularmente crítico, dado que las narrativas falsas pueden sembrar la desconfianza y polarizar a las sociedades de manera sistemática (Gottfried & Mutz, 2021).

3. Metodología

La presente investigación adoptó un enfoque mixto. Inicialmente se desarrolló una revisión teórica de carácter cualitativo que permitió contextualizar el fenómeno de estudio; posteriormente, se implementó un enfoque cuantitativo basado en técnicas bibliométricas y análisis de clústeres, para examinar la producción científica sobre la Inteligencia Artificial (IA) y las amenazas híbridas en los ámbitos de defensa y seguridad durante el periodo 2000–202. La base de datos seleccionada fue Scopus, debido a su cobertura global y a su sólida indexación en áreas como ciencias de la computación, ingeniería y ciencias sociales (Mongeon & Paul-Hus, 2016).

La ecuación de búsqueda aplicada en los campos de título, resumen y palabras clave (TITLE-ABS-KEY) fue:

"artificial+intelligence" AND "hybrid+-threats" OR "defense" OR "security"

El proceso metodológico se estructuró en tres fases principales: (i) diseño de la estrategia de búsqueda, (ii) recolección y depuración de Datos, y (iii) análisis bibliométrico y de clústeres (Donthu et al., 2021).

La búsqueda inicial en Scopus permitió la extracción de 19.999 documentos relacionados con la temática. Los metadatos asociados —incluyendo año de publicación (*Year*), número de citas (*Cited_by*), tipo de documento (*Document_Type*), etapa de publicación (*Publication_Stage*) y acceso abierto (*Open_Access*)—fueron exportados para el análisis. Posteriormente, los datos fueron estandarizados y codificados para el posterior análisis estadístico, asegurando la calidad y la uniformidad de las variables utilizadas en el proceso de clustering (Aria & Cuccurullo, 2017).

La fase bibliométrica se centró en la descripción de la producción por año de publicación (mostrando el crecimiento exponencial y punto máximo en 2023), país de origen (evidenciando la hegemonía de India, China y EE. UU.), y área de conocimiento (identificando la primacía de Ciencias de la Computación).

Adicionalmente, se empleó el software VOSviewer (Van Eck & Waltman, 2010) para la construcción de mapas de coocurrencia de palabras clave (*network visualization*) y el mapa temporal (*overlay visualization*). Estas herramientas permitieron identificar la estructura temática dominante, sus cuatro núcleos principales y la evolución de los temas hacia la ética y la privacidad.

Para el análisis de agrupamiento, se aplicó el método de análisis jerárquico de clústeres utilizando la distancia euclidiana, con el objetivo de identificar conjuntos de publicaciones con características bibliométricas similares. El modelo fue optimizado mediante el criterio de información bayesiano (BIC), lo que permitió la identificación de diez clústeres diferenciados. En este contexto, el aprendizaje automático se entiende como un conjunto de técnicas orientadas a la identificación de patrones en datos y a la generación de predicciones a partir de estos (Johnson, 2019).

La calidad del modelo se evaluó mediante diversas métricas: el Coeficiente de Correlación de Pearson para la coherencia estructural, Índice de Silueta (Silhouette) para la cohesión interna (Rousseeuw, 1987), Índice de Calinski–Harabasz para la diferenciación global entre grupos, e Índice de Dunn y Entropía para evaluar la compactación y la estabilidad de la clasificación.

En cuanto a las limitaciones del estudio, si bien el análisis bibliométrico ofrece una visión robusta del campo, presenta restricciones inherentes, partiendo por la recolección de datos que se limitó a la base de datos Scopus; que pese a ser una de las más completas, el uso de otras fuentes como Web of Science o Google Scholar podría ofrecer matices adicionales. Adicionalmente, existe un sesgo idiomático hacia publicaciones en inglés, lo que podría subrepresentar desarrollos tecnológicos documentados exclusivamente en otros idiomas locales.

Criterios de inclusión: artículos de investigación y revisión, publicados entre 2000 y 2025, indexados en Scopus, que contienen los términos clave en título, resumen o palabras clave.

Procedimiento de depuración: Se realizó una limpieza manual de los metadatos para eliminar entradas duplicadas y asegurar la normalización de términos técnicos, garantizando que el tamaño muestral final de 19.999 documentos fuera consistente para el análisis de clústeres en JASP y VOSviewer.

4. Resultados

La Figura 1 muestra la evolución de la producción documental en la temática analizada. Se observa una dinámica incipiente entre 1962 y 2010; no obstante, a partir de 2015 se evidencia un crecimiento sostenido que alcanza su punto máximo en 2023, con cerca de 9.000 documentos publicados. Este comportamiento refleja la consolidación del tema como un eje central de la investigación tecnológica contemporánea.

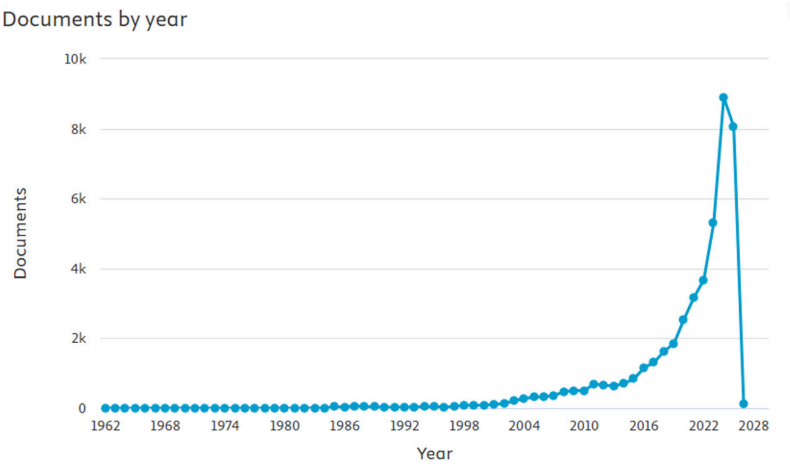

Figura 1. Documentos de Seguridad, Defensa y Medio Ambiente por Año en Scopus.
Fuente: Elaboración propia a partir de datos de búsqueda de Scopus (2025).

En términos geográficos, los principales contribuyentes son India, China y Estados Unidos, países que lideran la producción con volúmenes cercanos a los 9.000 documentos cada uno, seguidos por Reino Unido, Italia y Arabia Saudita en un escenario de distribución que evidencia la hegemonía de las potencias asiáticas y norteamericanas en el desarrollo de la IA, al tiempo que refleja la inserción gradual de Europa y Oceanía (ver Figura 2).

Como se observa en la Figura 3, la productividad por sub-área del conocimiento permite identificar patrones relevantes que anticipan el análisis de clústeres en términos de interdisciplinariedad. En este sentido, se evidencia una expansión pro gresiva hacia diversas áreas, entre las que se destacan ciencias de la computación, ingeniería, matemáticas, ciencias de la decisión, ciencias sociales, medicina, física y astronomía, energía, administración y negocios, así como ciencia de materiales.

Adicionalmente, la categoría "otros", con una participación del 10.1%, refleja un aumento significativo en la diversificación de la investigación, lo que sugiere la incorporación de nuevas líneas temáticas y enfoques emergentes en el estudio de la IA y las amenazas híbridas.

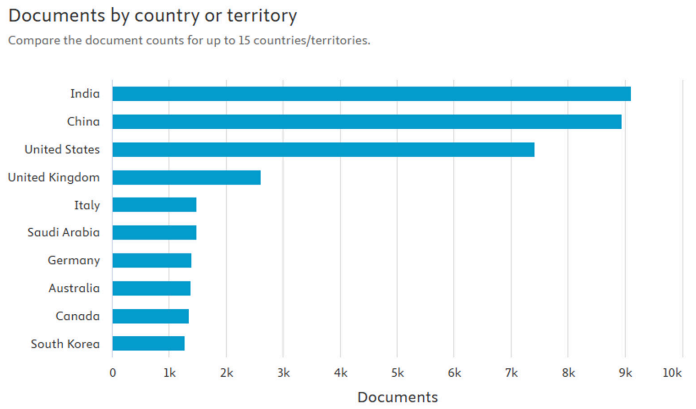

Figura 2. Documentos de la productividad científica de Seguridad, Defensa y Medio. Ambiente por países en Scopus. **Fuente:** Elaboración propia a partir de datos de búsqueda de Scopus (2024).

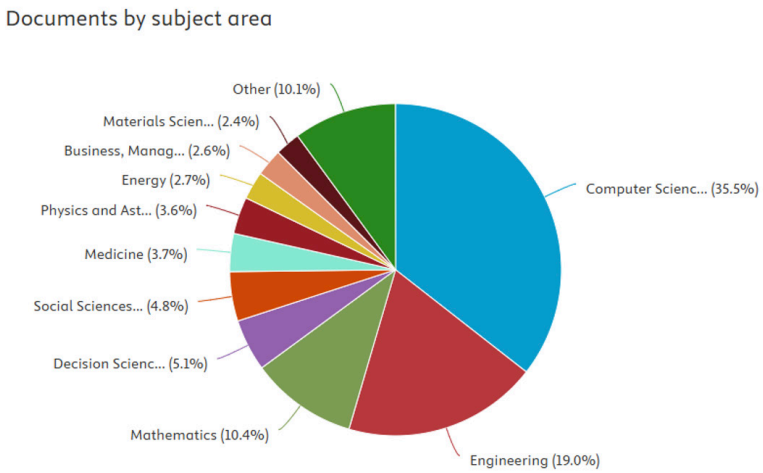

Figura 3. La productividad por sub-área del conocimiento por documento. **Fuente:** Elaboración propia a partir de datos de búsqueda de Scopus (2024).

El mapa de coocurrencia de palabras clave (*network visualization*) generado en VOSviewer (Figura 4) revela una estructura temática dominada por cuatro núcleos interrelacionados: el primero (en rojo) se concentra en *machine learning*, *convolutional neural networks* y *cybersecurity*; el segundo (en azul) aborda *internet of things* y *blockchain*; el tercero (en verde) se enfoca en *healthcare*, *data privacy* y *clinical applications*; y el cuarto (en amarillo) vincula temas emergentes como 5G, *data analytics* y *digital transformation*, evidenciando la transversalidad de la inteligencia artificial y su articulación con sectores estratégicos como la salud, la seguridad y la conectividad digital.

El mapa temporal (Figura 5 y 6) sugiere una transición temática desde enfoques tradicionales de *cybersecurity* y *machine learning* hacia aplicaciones recientes centradas en *healthcare, data privacy* y *responsible AI*, con un predominio de publicaciones entre 2022 y 2023. Esto indica una madurez del campo y una reorientación hacia la ética, la sostenibilidad y la confianza tecnológica, consolidando a la inteligencia artificial como un motor interdisciplinario de innovación global.

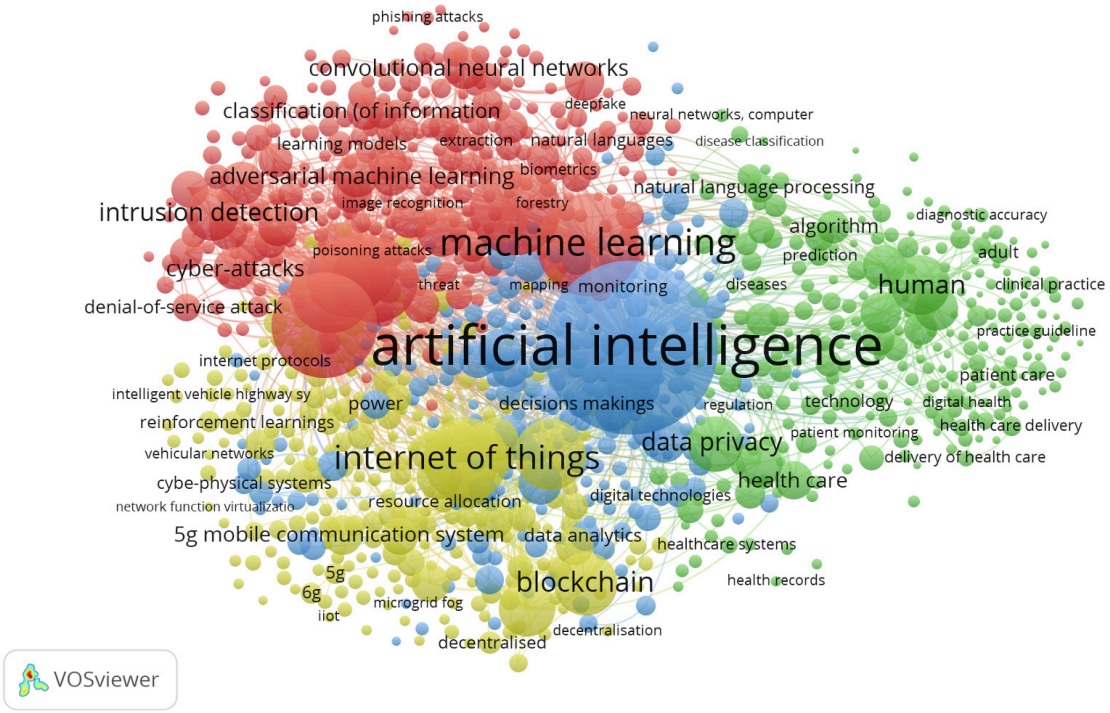

Figura 4. Mapa visualización de red basado en datos de red del término Seguridad, Defensa y Medio Ambiente.

Fuente: Elaboración propia a partir de datos de búsqueda de Scopus (2024).

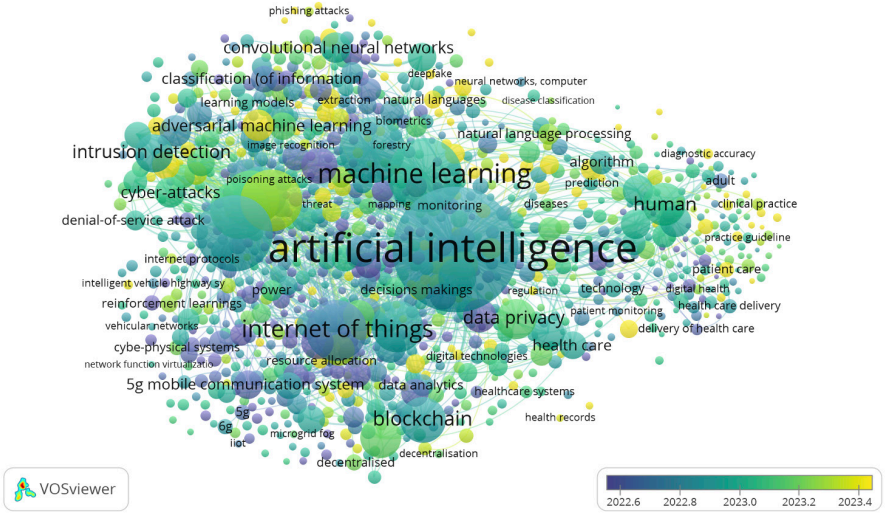

Figura 5. Overlay Visualization.
Fuente: Elaboración propia a partir de datos de búsqueda de Scopus (2024).

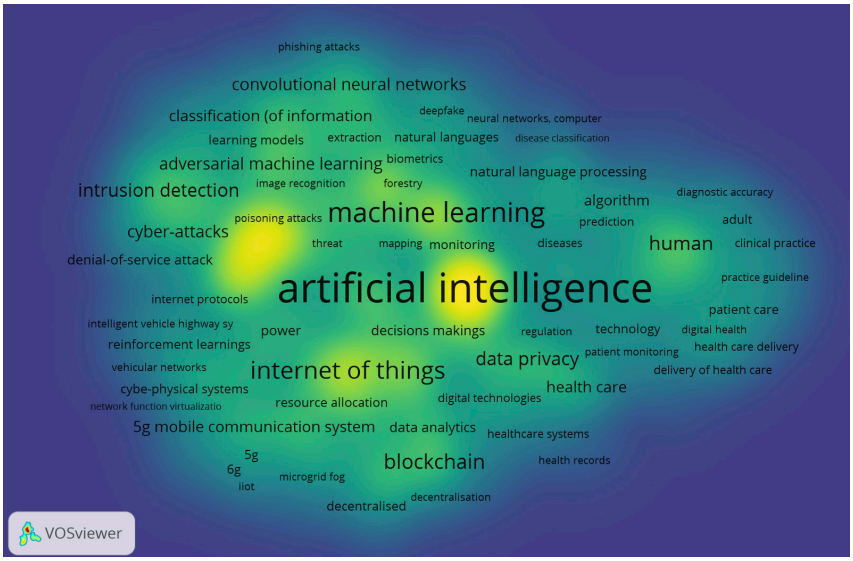

Figura 6. Density Visualization
Fuente: Elaboración propia a partir de datos de búsqueda de Scopus (2024).

A partir del análisis de clústeres, se evidencia que el modelo generó diez clústeres bien definidos, en el marco de 19.999 documentos extraídos de Scopus, relacionados con inteligencia artificial, amenazas híbridas, defensa y seguridad, presentando un nivel de ajuste adecuado (R^2 = 0.429; BIC = 80559.220) y un alto grado de cohesión interna (Silhouette = 0.770), lo cual evidencia la existencia de núcleos temáticos sólidos y diferenciados.

Estos clústeres reflejan la diversidad epistemológica y tecnológica del campo, abarcando desde la automatización y la ciberdefensa hasta los enfoques éticos y estratégicos de la IA en la seguridad global.

Tabla 1. Hierarchical Clustering

Clusters	N	R^2	AIC	BIC	Silhouette
10	19999	0.429	80005.980	80559.220	0.770

Note. The model is optimized with respect to the BIC value. The optimum number of clusters is the maximum number of clusters. You might want to adjust the range of optimization.
Fuente: Elaboración propia a partir de JASP (2025).

El modelo jerárquico sugiere que el campo de estudio "AI – Hybrid Threats – Defense – Security" presenta una estructura concentrada y madura, en la que la mayor parte de la literatura se articula en torno a un eje temático dominante (clúster 1), mientras que emergen grupos más pequeños y especializados. Este comportamiento es característico de áreas en las que existe una corriente científica dominante, acompañada de subáreas emergentes que se desarrollan alrededor de nuevas aplicaciones tecnológicas, contextos regionales o enfoques interdisciplinarios.

Tabla 2. Cluster Information

Cluster	1	2	3	4	5	6	7	8	9	10
Size	19676	55	106	123	1	31	1	4	1	1
Explained proportion within-cluster heterogeneity	0.981	0.002	0.009	0.004	0.000	0.003	0.000	4.954×10^{-4}	0.000	0.000
Within sum of squares	78372.067	191.149	756.731	285.237	0.000	221.232	0.000	39.566	0.000	0.000
Silhouette score	0.765	0.787	0.703	0.870	0.000	0.621	0.000	0.545	0.000	0.000

Note. The Between Sum of Squares of the 10 cluster model is 60120.02. The Total Sum of Squares of the 10 cluster model is 139986.
Fuente: Elaboración propia a partir de JASP (2025).

El clúster 1 que resulta ser el núcleo dominante, representa la corriente principal de investigación sobre Inteligencia Artificial aplicada a defensa y seguridad, este grupo probablemente concentra artículos científicos en inglés, de tipo *article* o *conference paper*, publicados en etapa final y con acceso abierto, su Silhouette (0.765) confirma alta homogeneidad temática. Por su parte, el clúster 2 (Silhouette 0.787) y clúster 4 (0.870) representan subcomunidades científicas más específicas, posiblemente: ciberseguridad y sistemas autónomos de defensa (Clúster 4), análisis estratégico de amenazas híbridas o defensa

Los clústeres 3 y 6 de Producción técnica o regional agrupan trabajos con estructuras diferentes: *conference papers*, publicaciones técnicas o documentos en otros idiomas, reflejando diversidad regional o metodológica. Finalmente, los clústeres 5, 7, 8, 9 y 10 actuan como *Outliers* con tamaño de 1 a 4 documentos que son probablemente artículos aislados, erratas, o trabajos con metadatos atípicos.

Tabla 3. Cluster Means

	Year	Page_count	Cited_by	Language_of_Original_Document	Document_Type	Publication_Stage	Open_Access
Cluster 1	3.019×10^{-4}	-0.035	-0.025	-0.059	-0.005	-0.079	0.001
Cluster 2	-0.296	10.641	-0.292	-0.153	2.026	-0.079	0.653
Cluster 3	-0.196	-0.097	-0.249	11.219	-0.133	-0.079	-0.294
Cluster 4	0.576	-0.097	-0.094	-0.153	0.086	12.712	0.050
Cluster 5	0.957	86.752	-0.292	-0.153	2.026	-0.079	0.653
Cluster 6	-1.058	-0.097	11.229	-0.153	-0.357	-0.079	-0.826
Cluster 7	0.038	-0.097	61.465	-0.153	0.064	-0.079	-1.531
Cluster 8	-1.340	-0.097	22.317	-0.153	-0.589	-0.079	-0.985
Cluster 9	-0.880	33.838	-0.292	-0.153	2.026	-0.079	0.653
Cluster 10	-1.799	-0.097	40.927	-0.153	-1.243	-0.079	-1.531

Fuente: Elaboración propia a partir de JASP (2025).

El análisis jerárquico de clústeres (*Cluster Means*) sobre la producción en Scopus refleja una estructura bibliométrica estratificada en la que los clústeres de años antiguos concentran los artículos de mayor impacto, no abiertos y de tipo científico formal, mientras que los clústeres recientes se caracterizan por publicaciones extensas, en acceso abierto. Este patrón sugiere un proceso de maduración y democratización del conocimiento en inteligencia artificial aplicada a defensa y seguridad, con una expansión hacia enfoques multidisciplinares e idiomas no anglófonos.

En las métricas de evaluación, se destaca el coeficiente de correlación de Pearson (γ = 0.731), el cual evidencia una relación positiva entre las distancias de los puntos y sus asignaciones de clúster, indicando que el modelo de agrupamiento mantiene una coherencia estructural aceptable: los objetos cercanos tienden a pertenecer al mismo grupo. Sin embargo, el *Dunn index* (0.059), que evalúa la compacidad interna y la separación entre grupos, es bajo; esto sugiere que los clústeres no están claramente delimitados y que podría existir cierta superposición entre ellos.

Asimismo, el valor de la entropía (0.105), al ser bajo, refleja una clasificación relativamente estable, con un nivel reducida de aleatoriedad en la asignación de los elementos. Finalmente, el Calinski–Harabasz index (1671.883) presenta un valor elevado, lo cual es un signo positivo indicando una buena relación entre la dispersión inter-clúster y la intra-clúster, es decir, los grupos están bien diferenciados entre sí en términos globales.

Tabla 4. Evaluation Metrics

Evaluation Metrics	
	Value
Maximum diameter	12.650
Minimum separation	0.745
Pearson's γ	0.731
Dunn index	0.059
Entropy	0.105
Calinski-Harabasz index	1.671.883

Fuente: Elaboración propia a partir de JASP (2025).

El gráfico del método del codo (*Elbow Method Plot*) muestra la relación entre el número de clústeres y la suma de los errores cuadráticos dentro de los grupos (*Within-Cluster Sum of Squares, WSS*), que representa la compacidad interna de los clústeres.

A medida que se incrementa el número de grupos, el WSS disminuye, reflejando una mejor homogeneidad interna. Sin embargo y lo que es destacable es que este descenso no es lineal: se observan puntos de inflexión que ayudan a determinar el número óptimo de clústeres.

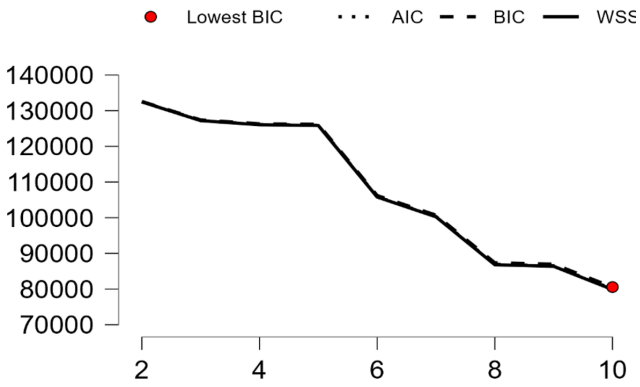

Figura 7. Dendrograma.
Fuente: Elaboración propia a partir de datos de búsqueda de Scopus (2024).

El dendrograma revela que las uniones iniciales (en la parte inferior) son de corta longitud, lo que sugiere una alta similitud entre la mayoría de los documentos. A medida que se asciende, las uniones se hacen más largas, reflejando la mayor distancia entre grupos de publicaciones que difieren en características como idioma, tipo de documento o número de citas.

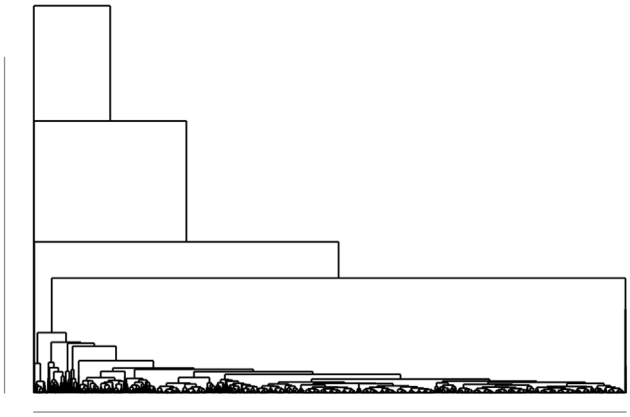

Figura 8. Cluster Mean Plots All Features.
Fuente: Elaboración propia a partir de JASP (2025).

El gráfico de medias por clúster para todas las variables (Cluster Mean Plots – All Features) permite interpretar cómo se comportan las variables promedio en cada grupo identificado durante el análisis de clústeres jerárquico. Esta visualización resulta clave para comprender las diferencias estructurales entre los clústeres y la contribución de variables como *Year, Page_count, Cited_by, Language_of_Original_Document, Document_Type, Publication_Stage y Open_Access* a su formación.

Las variables más determinantes en la diferenciación de los grupos son *Cited_by* (número de citas), *Page_count* (extensión del documento) y *Publication_Stage* (etapa de publicación). En particular, el clúster 8 (color violeta) resalta de manera marcada en la variable Cited_by, lo que indica que agrupa los artículos más influyentes y altamente citados dentro del cuerpo analizado; estos corresponden, a trabajos que pueden representar estudios pioneros o de referencia en el campo de la inteligencia artificial aplicada a la defensa o la seguridad.

Por su parte, el clúster 3 de color verde presenta los valores más altos en *Publication_Stage*, lo que sugiere que agrupa documentos en etapas finales o publicados formalmente, posiblemente en revistas académicas consolidadas. El Clúster 2 de color amarillo destaca por su elevado promedio en *Page_count*, reflejando documentos extensos, probablemente revisiones o capítulos de libros con desarrollo conceptual amplio.

La variable *Language_of_Original_Document* muestra escasa variabilidad, lo que confirma que el idioma predominante en todas las agrupaciones es el inglés, coherente con la tendencia internacional en las publicaciones científicas de alta visibilidad.

En resumen, este gráfico evidencia la existencia de tres grandes núcleos de publicaciones que inician con clústeres consolidados y de alta citación, como el 8, que concentra los aportes más influyentes, seguido de clústeres de producción académica madura como es el caso del 3 y el 2, caracterizados por publicaciones completas y revisadas y clústeres incipientes o periféricos (como el 1, 4 y 6), que reflejan la base de literatura reciente y menos citada.

El gráfico de densidad por clúster para todas las variables (*Cluster Density Plots – All Features*) evidencia una alta concentración de valores cercanos a cero, lo que sugiere una distribución homogénea en la mayoría de los casos. No obstante, se observan desviaciones puntuales que reflejan diferencias significativas entre los grupos, lo cual contribuye a la identificación de patrones distintivos en la estructura de los clústeres.

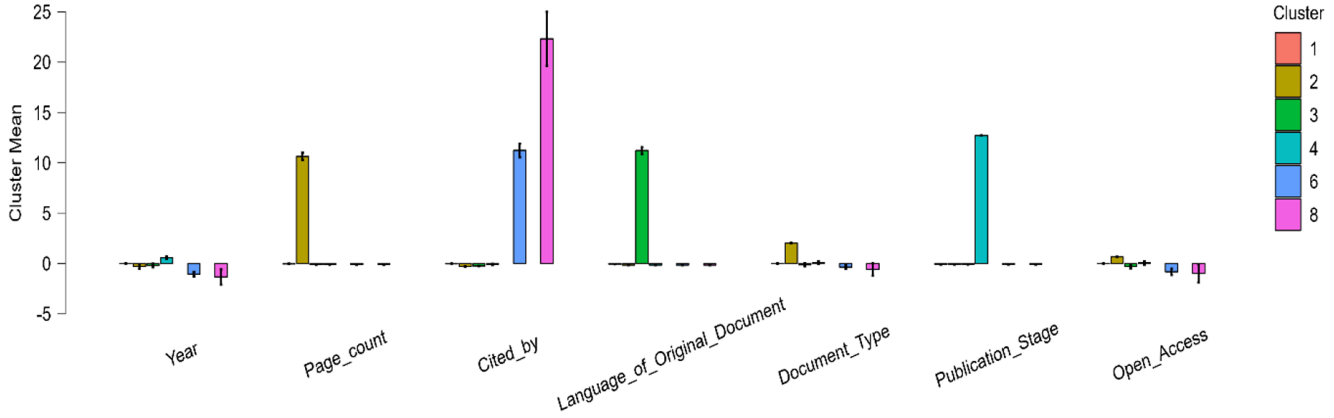

Figura 9. Cluster Mean Plots All Features.

Fuente: Elaboración propia a partir de JASP (2025).

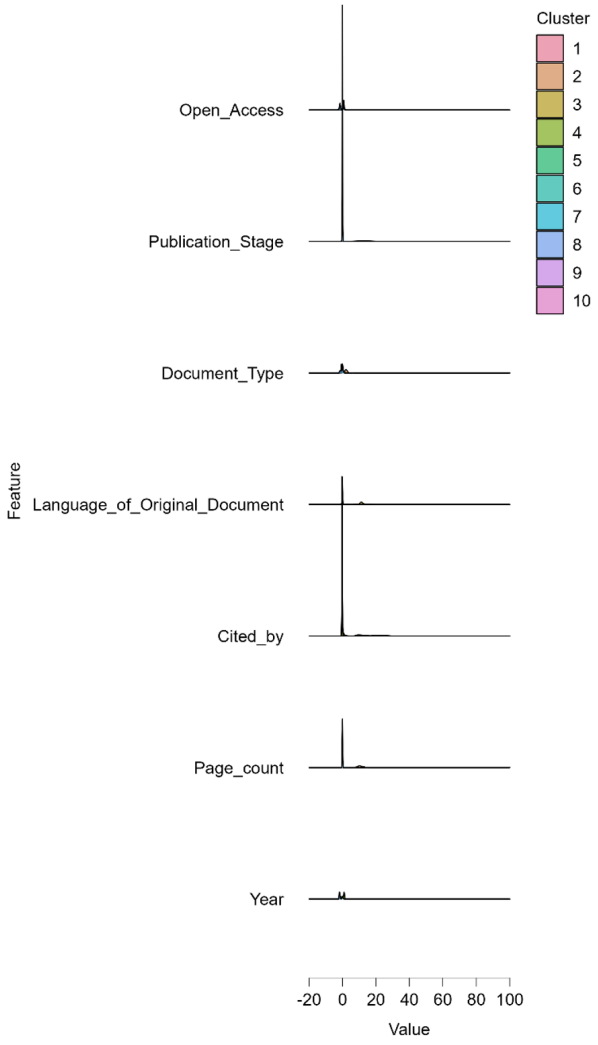

Figura 10. Cluster Density Plots All Features.

Fuente: Elaboración propia a partir de JASP (2025).

Los clústeres permiten identificar cómo ciertas características se asocian con mayor intensidad entre sí. En este caso, las variables *Open Access* y *Publication Stage* presentan agrupamientos definidos, lo que sugiere una relación entre el acceso abierto y las etapas de publicación de los documentos científicos.

De igual manera, la variable *Cited_by* muestra concentraciones específicas que evidencian distintos niveles de impacto académico entre los grupos, posiblemente vinculados con el tipo de documento y el año de publicación.

Las variables *Page count* y *Year* presentan comportamientos más dispersos, lo que puede interpretarse como evidencia de una diversidad temporal y estructural en las publicaciones analizadas.

Finalmente, la técnica *t-distributed Stochastic Neighbor Embedding* (t-SNE) representa cada publicación en un espacio bidimensional, agrupando según similitud multivariable (año, citas, idioma, tipo de documento, etc.) en el que cada color corresponde a uno de los 10 clústeres obtenidos en el análisis.

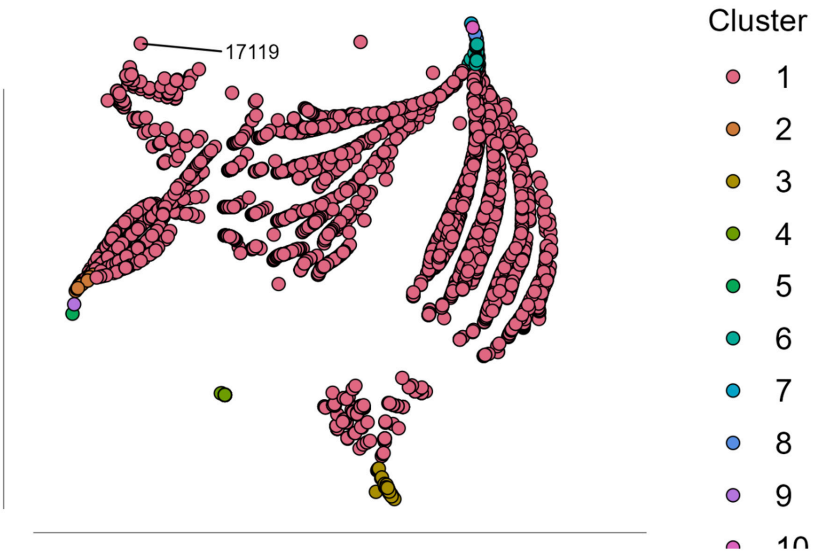

Figura 11. t-SNE Cluster Plot.
Fuente: Elaboración propia a partir de JASP (2025).

Se evidencia una estructura del conocimiento dominada por un núcleo central de publicaciones consolidadas en inglés, acompañado de subgrupos periféricos especializados. En este punto los clústeres periféricos se dividen entre aquellos históricos y altamente citados (base teórica del campo), los técnicos y recientes (innovación aplicada) y los idiomáticamente diversos (expansión internacional).

En conjunto, la distribución refleja un campo bibliométrico maduro, con una base consolidada y líneas emergentes que se articulan en torno a la aplicación de la inteligencia artificial en contextos de defensa, seguridad y amenazas híbridas.

Tabla 5. Análisis de Clústeres t-SNE Cluster Plot

Color / Clúster	***Zona del gráfico (aprox.)***	***Descripción bibliométrica***	***Representa / Significado conceptual***
Clúster 1 (Rosado)	Núcleo central, con ramas extensas hacia diferentes direcciones.	Mayor densidad de documentos; valores medios en todas las variables. Publicaciones típicas en inglés, artículos científicos estándar, moderadas en citas y extensión.	Eje central del conocimiento en IA aplicada a defensa y seguridad; producción consolidada y representativa del campo.
Clúster 2 (Amarillo mostaza)	Parte inferior y ligeramente separada del núcleo.	Documentos extensos (*page count* alto), predominantemente *conference papers y review papers*, con alto acceso abierto y baja citación.	Producción técnica reciente, enfocada en innovación, experimentación y aplicaciones tecnológicas.
Clúster 3 (Verde)	Aislado en el sector inferior izquierdo.	Publicaciones en otros idiomas (español, portugués, alemán). Pocas citas, documentos más cortos y regionales.	Diversificación lingüística y geográfica, aporte de comunidades no anglófonas al debate sobre IA y seguridad.
Clúster 4 (Verde oliva claro)	Periferia media del mapa, pocos puntos.	Años recientes, alta etapa de publicación (final), bajo número de citas.	Investigaciones emergentes y actuales, aún en proceso de consolidación y reconocimiento.
Clúster 5 (Marrón claro)	Inferior derecha, próximo a C2.	Publicaciones recientes, extensas y en acceso abierto.	Líneas contemporáneas y maduras en desarrollo, revisiones amplias o informes integradores.
Clúster 6 (Azul oscuro)	Extremo superior derecho del mapa.	Artículos antiguos, muy citados, sin acceso abierto.	Canon académico o corpus fundacional, base teórica del campo IA-defensa.
Clúster 7 (Morado)	Extremo derecho, aislado.	Muy alto número de citas, acceso cerrado, publicaciones en revistas de élite.	Núcleo de alto impacto académico, influencia científica concentrada en pocas publicaciones.
Clúster 8 (Celeste)	Extremo inferior medio.	Trabajos antiguos, de alta citación y sin acceso abierto.	Producción clásica con vigencia conceptual y metodológica.
Clúster 9 (Naranja)	Inferior derecho, próximo a C5.	Publicaciones intermedias (2018–2021), extensas y de acceso abierto.	Etapa de consolidación del campo, transición entre lo clásico y lo emergente.
Clúster 10 (Gris oscuro)	Extremo inferior izquierdo.	Publicaciones muy antiguas, alto impacto, no open access.	Semilla histórica del conocimiento sobre IA y seguridad; punto de partida del desarrollo bibliométrico.

Fuente: Elaboración propia a partir de JASP (2025).

Se configura, por tanto, una estructura núcleo–periferia en la producción científica sobre inteligencia artificial, amenazas híbridas y seguridad, en el que el núcleo (Cluster 1) concentra la mayor parte de los artículos consolidados, mientras que las periferias revelan tanto los polos fundacionales del conocimiento como los brotes emergentes de innovación, internacionalización y acceso abierto.

En este contexto, se puede afirmar que el núcleo (C1) representa el cuerpo principal y homogéneo del conocimiento, la periferia inferior de los clústeres 2, 5 y 9 apuntan hacia la innovación técnica reciente y producción open access. Adicionalmente, la periferia superior clústeres de C6 a C10 concentran artículos fundacionales, de alto impacto histórico, finalmente, en la periferia lateral los clústeres 3 y 4 abarcan diversificación idiomática y líneas emergentes.

5. Conclusiones

El presente artículo evidencia, desde la teoría de las relaciones internacionales, que la incorporación de la inteligencia artificial en el ámbito de las amenazas híbridas redefine la naturaleza misma del poder y la seguridad en el siglo XXI. En este contexto, las fronteras entre lo militar, lo informacional y lo cognitivo tienden a difuminarse, generando un entorno estratégico donde la superioridad no depende solo de la fuerza, sino de la capacidad para anticipar, interpretar y responder a flujos dinámicos y cambiantes de información. Así, la articulación entre teoría, tecnología y política se convierte en un elemento clave para comprender y contener las nuevas formas de coerción y disuasión propias de la guerra híbrida contemporánea.

En cuanto a la producción científica sobre la Inteligencia Artificial (IA), las amenazas híbridas y la seguridad, se identificó una consolidación temática notable, con un crecimiento exponencial desde 2015 y un punto máximo en 2023. Este desarrollo se estructura en torno a cuatro núcleos temáticos interconectados que configuran el campo de estudio.

La tendencia evolutiva reveló una migración del foco tradicional en *machine learning* y ciberseguridad hacia áreas de aplicación más recientes. Estas áreas emergentes se centran en la ética, la privacidad de datos, y las aplicaciones clínicas y de infraestructura crítica.

Desde el punto de vista metodológico, la distribución de la literatura confirma una estructura bien definida de núcleo-periferia en el que resalta el núcleo clúster 1 que concentra el cuerpo principal del conocimiento homogéneo y altamente citado del campo; mientras que la periferia evidencia focos de innovación técnica, la aparición de literatura *open access*, y una clara diversificación idiomática que en resumen, apunta a que el campo está madurando hacia un enfoque multidisciplinar y urgente para la política de defensa y la seguridad global.

El diagnóstico cuantitativo revela una sólida madurez del campo, marcada por un ritmo de producción que alcanzó su máximo en 2023 con cerca de 9.000 documentos, tras un crecimiento sostenido desde 2015, una dinámica productiva que a nivel geográfico se concentra en India, China y Estados Unidos, cifras que se solidifican al dar paso a la fase del análisis de clústeres que se sustenta en

en métricas objetivas, como el alto índice Calinski–Harabasz (1671.883), asegurando la diferenciación óptima entre los 10 grupos temáticos identificados.

De igual forma, el coeficiente de correlación de Pearson (γ=0.731) valida la coherencia estructural del modelo de agrupación en el que el núcleo central del conocimiento (Clúster 1) es innegablemente la corriente dominante al consolidar 19.676 documentos del cuerpo confirmando un crecimiento exponencial, una clara concentración temática y una hegemonía geográfica bien definida en la investigación.

En términos prospectivos, es probable que la evolución de las amenazas híbridas se direccione hacia la automatización de la influencia cognitiva, utilizando la IA generativa para producir desinformación a escala masiva y propaganda dirigida a socavar la cohesión social y la confianza institucional del adversario. Este escenario implicará que las naciones prioricen la resiliencia integral —social, económica y cibernética— por encima de enfoques exclusivamente militares, impulsando inversiones en sistemas de defensa autónomos capaces de responder en tiempo real.

En conclusión, la medición del poder nacional no radicará solo en la posesión de capacidades militares tradicionales, sino en la supremacía tecnológica en inteligencia artificial y en la capacidad de establecer marcos de gobernanza, política y ética a nivel internacional que permita gestionar los riesgos inherentes a los sistemas autónomos en conflicto.

Referencias Bibliográficas

Aria, M., & 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

Boulanin, V., & Giammatteo, M. (2023). *Artificial intelligence and national security: A literature review of the strategic and political implications*. Stockholm International Peace Research Institute (SIPRI). https://www.sipri.org/publications/2023/other-publications/artificial-intelligence-and-national-security-literature-review-strategic-and-political

Danyk, Y., & Briggs, C. M. (2023). Modern cognitive operations and hybrid warfare. *Journal of Strategic Security*, 16(1), 35–50. https://doi.org/10.5038/1944-0472.16.1.2032

Departamento Nacional de Planeación. (2024). *ABC del Plan Nacional de Desarrollo y las Inversiones Públicas*. https://www.dnp.gov.co

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, 133, 285–296. https://doi.org/10.1016/j.jbusres.2021.04.070

Galeotti, M. (2018). *Hybrid war or Gerasimov doctrine?* Strategic Studies Institute, U.S. Army War College Press. https://press.armywarcollege.edu/monographs/651

Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, 35(2), 137–144. https://doi.org/10.1016/j.ijinfomgt.2014.10.007

Gottfried, J., & Mutz, D. (2021). The effects of partisan polarization and trust in news on misperceptions about the COVID-19 pandemic. *Journal of Communication*, 71(5), 629–652. https://doi.org/10.1093/joc/jqab026

Hoffman, F. G. (2022). Hybrid warfare and challenges. *Small Wars Journal*. https://smallwarsjournal.com/jrnl/art/hybrid-warfare-and-challenges

Johnson, J. (2019). Artificial intelligence & future warfare: implications for international security. *Defense & Security Analysis*, 35(2), 147–169. https://doi.org/10.1080/14751798.2019.1600800

Kuhn, T. S. (1970). *The structure of scientific revolutions* (2nd ed.). University of Chicago Press.

Ministerio de Hacienda y Crédito Público. (2023). *Presupuesto Ciudadano: Guía didáctica sobre el gasto público*. https://www.minhacienda.gov.co

Mongeon, P., & Paul-Hus, A. (2016). The journal coverage of Web of Science and Scopus: A comparative analysis. *Scientometrics*, 106(1), 213–228. https://doi.org/10.1007/s11192-015-1765-5

Münkler, H. (2016). Warfare in the twenty-first century: An essay on hybrid wars. *Global Policy*, 7(3), 329–336. https://doi.org/10.1111/1758-5899.12328

Renz, B. (2016). Russia's "Hybrid Warfare" and its Implications for European Security. *Contemporary Security Policy*, 37(3), 331-356. https://nottingham-repository.worktribe.com/OutputFile/793615

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.

Romero, J. R., Barbosa, L. M., & Palacios, J. J. (2025a). Estudio bibliométrico de Fintech. En *La bibliometría como herramienta para la producción científica* (pp. 51–58). Universidad Colegio Mayor de Cundinamarca, Sello Editorial. https://www.universidadmayor.edu.co/vicerectoria-investigacion-innovacion/subdireccion-investigacion-innovacion-1/area-sello-editorial/libros/novedades/bibliometria-herramienta-para-produccion

Rousseeuw, P. J. (1987). Silhouettes: A graphical aid to the interpretation and validation of cluster analysis. *Journal of Computational and Applied Mathematics*, 20, 53–65. https://doi.org/10.1016/0377-0427(87)90125-7

Scharre, P. (2019). *Artificial intelligence and the future of warfare*. Center for a New American Security (CNAS). https://www.cnas.org/publications/podcast/artificial-intelligence-and-the-future-of-warfighting

Sipahi, B. (2020). From hybrid threats to hybrid security: An integrated approach for future threats. *Journal of Strategic Security*, 13(1), 1-18. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC129019/JRC129019_01.pdf

UNESCO. (2023). Recomendación sobre la Ética de la Inteligencia Artificial. https://unesdoc.unesco.org/ark:/48223/pf0000381115_spa

Van Eck, N. J., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics*, 84(2), 523–538. https://doi.org/10.1007/s11192-009-0095-y

Zupic, I., & Čater, T. (2015). Bibliometric methods in management and organization. *Organizational Research Methods*, 18(3), 429-472. https://doi.org/10.1177/1094428114562629