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

Definición conceptual sobre la transición del factor humano hacia el uso de la IA en operaciones de información en el caso colombiano

Autor

Luis Carlos González-Carrillo
https://orcid.org/0009-0009-6574-4258
✉luiscarlosgonzalez2021@gmail.com
Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano", Colombia

Citación APA: González-Carrillo, L. C. (2025). Definición conceptual sobre la transición del factor humano hacia el uso de la IA en operaciones de información en el caso colombiano. *Perspectivas en Inteligencia, 17*(26), 185-199. http://doi.org/10.47961/2145194X.835

Publicado en línea: 2025

Para enviar un artículo:
https://revistascedoc.com/index.php/pei/about/submissions
.

Esta página queda intencionalmente en blanco

PERSPECTIVAS EN INTELIGENCIA 2025

Revista Científica en Ciencias Sociales e Interdisciplinaria
Bogotá D.C., Colombia
Volumen 17, N° 26, enero - diciembre 2025, pp. 185-199
http://doi.org/10.47961/2145194X.835

Definición conceptual sobre la transición del factor humano hacia el uso de la IA en operaciones de información en el caso colombiano[1]

A conceptual framework for the transition of the human factor toward Artificial Intelligence in information operations: the Colombian context

Luis Carlos González-Carrillo[1]

(1) Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano", Bogotá, D. C., Colombia,
✉luiscarlosgonzalez2021@gmail.com

Resumen

La inteligencia estratégica en Colombia se encuentra en un proceso de transformación marcado por la incorporación progresiva de tecnologías de inteligencia artificial (IA) en las operaciones de información. Este artículo analiza los impactos estratégicos, riesgos y oportunidades que genera esta transición, con base en un enfoque cualitativo-documental sustentado en literatura académica, doctrina internacional y estudios de caso, en particular las operaciones *Jaque* y *Fénix*. Los resultados evidencian que la IA fortalece la capacidad estatal para procesar información masiva, detectar patrones ocultos y anticipar amenazas emergentes en escenarios híbridos en los que confluyen el ciberespacio, la guerra informacional y la influencia de actores no estatales. No obstante, también plantea riesgos significativos: dependencia tecnológica de proveedores extranjeros, manipulación algorítmica, desplazamiento del criterio humano y desafíos éticos vinculados a la responsabilidad en decisiones críticas.

Asimismo, el estudio subraya que, en el plano regional, la integración de políticas públicas orientadas por transparencia, responsabilidad y confianza social resulta indispensable para garantizar que la IA contribuya al fortalecimiento de la seguridad nacional y no se convierta en una fuente de vulnerabilidad. En conclusión, la investigación muestra que la IA debe entenderse como un complemento y no como un reemplazo del factor humano, ya que su verdadero valor radica en multiplicar la efectividad del juicio experto bajo marcos normativos claros y principios éticos que respalden la legitimidad de la defensa en Colombia.

Clasificación JEL: D81, F52.

Palabras clave: inteligencia estratégica; inteligencia artificial; operaciones de información; guerra híbrida; seguridad nacional.

Abstract

Strategic intelligence in Colombia is in a process of transformation marked by the progressive incorporation of artificial intelligence (AI) technologies in information operations. This article analyzes the strategic impacts, risks, and opportunities generated by this transition, based on a qualitative-docu-

[1] Artículo de investigación elaborado como opción de grado para obtener el título de Magíster en Inteligencia Estratégica en la Institución Universitaria Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano".

mentary approach supported by academic literature, international doctrine, and case studies, particularly the *Jaque* and *Fénix* operations. The results show that AI strengthens the state's capacity to process massive information, detect hidden patterns, and anticipate emerging threats in hybrid scenarios where cyberspace, informational warfare, and the influence of non-state actors converge. However, it also presents significant risks: technological dependence on foreign providers, algorithmic manipulation, the displacement of human judgment, and ethical challenges related to responsibility in critical decisions.

Likewise, the study emphasizes that, at the regional level, the integration of public policies guided by transparency, accountability, and social trust is essential to ensure that AI contributes to strengthening national security and does not become a source of vulnerability. In conclusion, the research shows that AI should be understood as a complement and not as a replacement for the human factor, since its true value lies in multiplying the effectiveness of expert judgment under clear regulatory frameworks and ethical principles that support the legitimacy of defense in Colombia.

Keywords: strategic intelligence; artificial intelligence; information operations; hybrid warfare; national security.

Introducción

La inteligencia estratégica en Colombia vive un momento de inflexión, marcado por la incorporación de tecnologías de inteligencia artificial (IA) en el ciclo de la información: Recolección, procesamiento, análisis y diseminación. Esta transformación no es meramente técnica, sino que responde a un contexto en el que la seguridad nacional ya no se limita al control del territorio físico, sino que se extiende al ciberespacio y al ámbito informacional, escenarios donde se libra hoy gran parte de la competencia estratégica (Singer y Brooking, 2018).

La literatura especializada advierte que la IA está modificando no solo las tácticas operacionales, sino también los marcos conceptuales de la seguridad nacional. Khan y Khan (2025) sostienen que la tecnología se ubica en el centro de un nuevo paradigma de poder, pues redefine tanto las capacidades militares como los equilibrios geopolíticos. Para Colombia, este debate tiene especial relevancia: su adopción en los sistemas de defensa no puede concebirse únicamente como innovación tecnológica, sino como un proceso que impacta la soberanía, la gobernanza de la información y la proyección estratégica del Estado en un mundo digitalizado.

El avance de la autonomía algorítmica plantea, además, interrogantes éticos y psicológicos de fondo. A medida que las máquinas asumen funciones decisionales, aparece el riesgo de desplazar la autoridad humana hacia lo que algunos autores han denominado un *"comandante artificial"*. Johnson (2022) advierte que esta delegación no solo genera dilemas sobre responsabilidad en la conducción de la guerra, sino que puede inducir sesgos cognitivos que reduzcan la capacidad crítica de los mandos. En el caso colombiano, donde las decisiones militares han estado históricamente ligadas a contextos de alta complejidad social y política, confiar ciegamente en sistemas automatizados puede erosionar la legitimidad y la prudencia en el uso de la fuerza.

El país enfrenta así un doble desafío: aprovechar la velocidad de procesamiento y las capacidades predictivas que ofrece la IA, al tiempo que preserva la flexibilidad y creatividad propias del factor humano. Como advierte Crawford (2021), los sistemas algorítmicos dependen de los datos que los alimentan, y en sociedades polarizadas esos datos pueden amplificar narrativas sesgadas, reproduciendo visiones parciales en lugar de ofrecer información neutral. Este riesgo es especialmente delicado en operaciones de información en las que la manipulación de percepciones constituye una herramienta de poder estratégico.

La experiencia nacional ofrece ejemplos ilustrativos. La Operación Jaque[2] evidenció cómo la compartimentación de la información, la disciplina estratégica y la resiliencia cognitiva permitieron alcanzar un éxito sin precedentes: rescatar a quince secuestrados sin disparar un solo tiro. Este episodio demostró que, incluso en un entorno de presión, la creatividad y la moral de mando fueron decisivas. En contraste, la Operación Fénix[3] mostró otra cara de la superioridad informacional: el uso combinado de inteligencia técnica "Signals Intelligence" (SIGINT) y cooperación interinstitucional permitieron neutralizar a un alto mando de las FARC, aunque generó tensiones diplomáticas y cuestionamientos jurídicos sobre la soberanía. Ambos casos revelan que la tecnología es un recurso esencial, pero nunca suficiente por sí sola; requiere siempre de un juicio humano que evalúe las consecuencias políticas, jurídicas y estratégicas.

La trayectoria de las Fuerzas Militares desde la crisis de El Billar[4] hasta las operaciones conjuntas[5] de 2008 refuerza esta idea. Como señala Ramsey III (2009), el aprendizaje institucional y la adaptabilidad fueron claves para revertir una situación cercana al colapso. En este sentido, la integración de la IA en la inteligencia estratégica debe asumirse como un complemento al criterio humano y no como su sustituto. La clave está en construir un modelo híbrido que preserve la experiencia acumulada, incorpore innovaciones tecnológicas y mantenga la legitimidad como eje de toda acción.

De esta reflexión surge la pregunta que orienta esta investigación, ¿cuáles son los impactos estratégicos, riesgos y oportunidades que implica la transición del factor humano hacia la inteligencia artificial en las operaciones de información en Colombia? Para responderla, se adoptó un enfoque cualitativo-documental apoyado en literatura académica, doctrina internacional y estudios de caso. El propósito es identificar lecciones que fortalezcan un modelo híbrido humano-IA, en el que la tecnología actúe como multiplicador del poder informacional, pero siempre bajo la supervisión crítica del ser humano.

Metodología

En coherencia con los objetivos de esta investigación, se adoptó un enfoque cualitativo-documental idóneo para examinar fenómenos estratégicos en inteligencia y seguridad, en el que los procesos no pueden reducirse a métricas cuantitativas. Este método permite interpretar la interacción entre tecnología, doctrina y contexto político, integrando fuentes diversas bajo un análisis crítico.

El enfoque cualitativo-documental fue seleccionado por su pertinencia para analizar fenómenos complejos de carácter estratégico y doctrinal, en los cuales el contexto, el discurso y la interpretación de la información resultan más relevantes que la medición numérica. Este diseño permitió comprender la relación entre el factor humano y la tecnología a través del estudio de documentos oficiales, doctrina militar, literatura académica y fuentes normativas.

Los criterios de inclusión consideraron materiales publicados entre 2008 y 2025 relacionados con inteligencia, tecnología y seguridad nacional; mientras que los criterios de exclusión descartaron artículos sin rigor metodológico o fuentes de carácter meramente divulgativo.

[2] El 2 de julio de 2008, tras un arduo planeamiento de inteligencia militar, el Ejército Nacional desplegó una acción de infiltración en el departamento del Guaviare con la misión de rescatar a quince secuestrados de las FARC, entre los que se encontraba la excandidata presidencial Ingrid Betancourt. El éxito de la Operación Militar Jaque se basó en un rescate en el que no se registraron pérdidas humanas y en el que tampoco se hizo uso de armas de fuego; asimismo, se logró arrestar a alias "Gafas", importante comandante del extinto grupo armado (Ejército Nacional de Colombia, 2023b).

[3] La Operación Fénix consistió en el bombardeo al territorio ecuatoriano y la incursión con helicópteros y personal militar dentro de una zona selvática a 1.800 metros de la frontera de Ecuador con Colombia, denominada "Angostura", en las cercanías de la población Yamarú, en la provincia ecuatoriana de Sucumbíos, el 1º de marzo de 2008; así como el bombardeo del campamento guerrillero donde se presumía la presencia de alias "Raúl Reyes", con el resultado de la muerte del señalado miembro del secretariado de las FARC y 17 guerrilleros más (Pastrana-Buelvas y Trujillo-Méndez, 2011).

[4] *"... ataque indiscriminado contra el Batallón de Contraguerrillas N° 52, de la Brigada Móvil N° 3, en la quebrada El Billar, jurisdicción del municipio de Cartagena del Chairá, Caquetá. Allí, el 1 de marzo de 1998 perdieron la vida 64 soldados, 19 resultaron heridos y 43 más fueron secuestrados"* (Ejército Nacional de Colombia, 2023a, párr. 1).

[5] Término general para describir las acciones militares llevadas a cabo por las fuerzas conjuntas y aquellas unidades de las fuerzas bajo relaciones de mando específicas entre sí (Fuerzas Militares de Colombia, 2018).

El análisis de la información se realizó mediante un proceso de triangulación teórica y **categorización temática,** aplicando análisis de discurso de manera manual, con fichas de codificación estructuradas, lo cual permitió contrastar la literatura, la doctrina y los casos de estudio sin recurrir a software especializado.

El procedimiento se sustentó en la revisión sistemática de literatura académica, normativa y doctrinal, articulando tres niveles de análisis: el conceptual, centrado en los desarrollos teóricos sobre inteligencia artificial y operaciones de información; el doctrinal, basado en documentos oficiales y manuales estratégicos; y el normativo, referido al marco jurídico que regula las actividades de inteligencia en Colombia. Esta triple perspectiva aseguró una triangulación efectiva entre conocimiento teórico, orientaciones institucionales y criterios legales.

Se priorizaron obras publicadas entre 2008 y 2025, periodo que coincide con la transformación de la seguridad colombiana tras las operaciones *Jaque* y *Fénix* y con la adopción global de sistemas de inteligencia artificial en defensa. La búsqueda se realizó en bases de datos como Scopus, JSTOR y Google Scholar, utilizando palabras clave relacionadas con inteligencia artificial, operaciones de información, guerra híbrida, ciberseguridad y soberanía tecnológica.

Entre los autores más destacados de referencia se destacan Marr y Ward, Crawford, Singer y Brooking y el análisis doctrinal de la Joint Chiefs of Staff of the United States Government. Estos textos proporcionaron un marco conceptual para evaluar cómo la IA incide en la recolección, procesamiento y análisis de información, así como en la conducción de operaciones estratégicas.

El corpus documental incluyó también normas nacionales como la Ley Estatutaria 1621 de 2013 que, aunque no menciona la IA de manera explícita, fija principios jurídicos -necesidad, idoneidad, proporcionalidad y reserva- aplicables a cualquier sistema de información. Este contraste permitió examinar la tensión entre la innovación tecnológica y las limitaciones normativas aún vigentes en Colombia.

Asimismo, se incorporaron estudios regionales y comparativos, como los de Ceballos et al. (2020), sobre soberanía tecnológica en América Latina y sobre implicaciones de la dependencia tecnológica. Estos aportes situaron el análisis colombiano dentro de un marco latinoamericano, mostrando cómo la integración humano-IA en defensa se enmarca en una disputa global por el control de infraestructuras críticas y datos estratégicos.

Un componente esencial del método fue el análisis de casos. La Operación Jaque se examinó a partir de fuentes primarias, como el relato de Torres-Cuéllar (2009) y el estudio de Ramsey III (2009), que documentan la planeación y ejecución de la misión. La Operación Fénix, en cambio, se examinó desde los debates de derecho internacional, resaltando las tensiones jurídicas y diplomáticas derivadas de la acción militar en territorio extranjero. Estos casos sirvieron para evaluar en qué medida la incorporación de inteligencia artificial podría potenciar o limitar la toma de decisiones en entornos de alta incertidumbre.

Finalmente, la triangulación de fuentes permitió derivar tres categorías analíticas que articularon el desarrollo del estudio: (i) evolución doctrinal de la inteligencia estratégica, (ii) integración tecnológica humano-IA y (iii) tensiones ético-jurídicas en las operaciones de información. Estas categorías se aplicaron transversalmente a los casos seleccionados, garantizando la coherencia entre teoría, método y resultados, y fortaleciendo la validez interpretativa del análisis.

Marco teórico

La inteligencia estratégica se define como el proceso que permite anticipar riesgos y orientar decisiones de alto nivel en seguridad nacional. En Colombia, este campo ha evolucionado en paralelo a un escenario de conflicto interno prolongado, en el que la guerra irregular, la desinformación y las amenazas híbridas han configurado un entorno particularmente complejo (Hernández-Estupiñán, 2020; Singer y Brooking, 2018). En este marco, la inteligencia artificial (IA) surge como un factor disruptivo, al introducir capacidades de automatización en la recolección, procesamiento y análisis de datos que modifican la naturaleza misma de la inteligencia (Marr y Ward, 2019; Russell, 2022).

Para comprender la transición del factor humano hacia la inteligencia artificial en operaciones de información, resulta necesario apoyarse en un marco teórico que permita explicar cómo se articulan los elementos tecnológicos, organizacionales y cognitivos dentro de sistemas complejos. Desde esta perspectiva, tres enfoques ofrecen bases analíticas sólidas para interpretar el fenómeno: la teoría del factor humano en sistemas complejos (Reason, 1990), la paradoja de la automatización (Bainbridge, 1983) y el constructivismo tecnológico (Pinch y Bijker, 1984).

En el contexto contemporáneo, la inteligencia artificial representa uno de los mayores desafíos para la seguridad y la defensa, no solo por su capacidad tecnológica, sino por las implicaciones éticas y estratégicas que genera en la toma de decisiones. Cummings (2017) sostiene que el verdadero poder de la IA no radica en la velocidad de procesamiento, sino en cómo los Estados logran mantener el control humano sobre los sistemas automatizados, garantizando legitimidad y responsabilidad. De forma complementaria, Scharre (2016) advierte que la incorporación de sistemas autónomos y semiautónomos introduce nuevos riesgos operacionales y morales, derivados de la delegación parcial de decisiones críticas a algoritmos que pueden carecer de juicio contextual. Estas reflexiones resultan fundamentales para el caso colombiano, donde la integración de la IA en las operaciones de información debe realizarse bajo un marco de control ético, proporcionalidad doctrinal y soberanía institucional, evitando que la tecnología desplace el papel decisivo del factor humano en la inteligencia estratégica.

Reason (1990) plantea que en los sistemas de alta fiabilidad -como la aviación o la defensa- los errores humanos no son simples fallas individuales, sino consecuencia de interacciones entre personas, procedimientos y tecnología. Este enfoque es aplicable a la inteligencia estratégica, donde la incorporación de la IA no elimina el error, sino que lo redistribuye entre el operador humano y el sistema algorítmico. La comprensión de esta dinámica permite analizar cómo las fallas en la programación, el entrenamiento o la supervisión pueden generar vulnerabilidades críticas, incluso cuando los dispositivos actúan conforme a su diseño.

Por su parte, Bainbridge (1983) advierte que la automatización introduce una paradoja estructural: a medida que los sistemas se vuelven más autónomos, el papel del operador humano se vuelve más complejo y exigente. Cuando la máquina falla, el ser humano debe intervenir en condiciones de alta presión y con información incompleta. En el contexto militar, esta paradoja cobra relevancia porque el comandante no solo depende de algoritmos para el procesamiento de datos, sino que debe mantener la capacidad de juicio y decisión aun cuando el sistema presente sesgos o errores. De esta tensión entre autonomía tecnológica y control humano surge la necesidad de una supervisión significativa que preserve la responsabilidad moral y jurídica del mando.

Finalmente, el constructivismo tecnológico de Pinch y Bijker (1984) sostiene que toda innovación técnica refleja decisiones sociales y valores institucionales. La inteligencia artificial no es una entidad neutral, sino el resultado de procesos de negociación entre actores que definen qué problemas deben resolverse y bajo qué criterios. En el ámbito de la seguridad y defensa, esto implica reconocer

que los sistemas de IA incorporan visiones doctrinales sobre la amenaza, la legitimidad del uso de la fuerza y la prioridad de los objetivos estratégicos. Por tanto, su análisis debe incluir tanto el componente técnico como las estructuras de poder que lo moldean.

Integrar estas tres perspectivas permite abordar la relación humano-IA en la inteligencia estratégica desde un enfoque más profundo. La teoría del factor humano explica la gestión del error y la fiabilidad; la paradoja de la automatización revela los límites del control; y el constructivismo tecnológico introduce una dimensión sociopolítica que vincula la tecnología con la cultura institucional. En conjunto, estos marcos teóricos fortalecen la comprensión del modelo híbrido que Colombia requiere para equilibrar la eficacia tecnológica con la responsabilidad ética y la legitimidad institucional en sus operaciones de información.

En este sentido, la inteligencia artificial aplicada a operaciones de información estratégicas puede entenderse como la incorporación de sistemas algorítmicos para apoyar la recolección, el análisis y la interpretación de datos en escenarios de seguridad y defensa, con el propósito de anticipar riesgos y reforzar la toma de decisiones, bajo un esquema que preserva el criterio humano como garante de legitimidad, flexibilidad y responsabilidad.

Las amenazas híbridas, entendidas como la combinación deliberada de medios militares, políticos, tecnológicos y comunicativos (Peña-Suarez, 2023), representan lo que Nilsson et al. (2025) denominan "problemas perversos". Estos fenómenos no pueden ser resueltos mediante respuestas unidimensionales, ya que se apoyan en vulnerabilidades sociales y digitales que trascienden la capacidad del poder militar tradicional. Frente a este panorama, la inteligencia no solo debe producir información útil para las operaciones, sino también fortalecer la resiliencia social y cognitiva como componente de defensa estratégica.

En el plano doctrinal, Joint Chiefs of Staff of the United States Government (2014) define el ambiente informacional como un entramado de individuos, organizaciones y sistemas interconectados, donde se cruzan tres dimensiones: la física, la informacional y la cognitiva. Esta última resulta crucial, pues involucra percepciones, juicios y procesos de decisión de actores estatales y no estatales. En este escenario, las operaciones de información se conciben como acciones destinadas a influir, interrumpir o degradar la toma de decisiones adversarias, al tiempo que se protege la propia capacidad decisional. La incorporación de IA en este marco amplía la velocidad y precisión del análisis, pero también introduce nuevos dilemas éticos y operativos.

El valor estratégico de la IA radica en su capacidad para convertir grandes volúmenes de datos en conocimiento accionable en tiempo real (Marr y Ward, 2019). Sin embargo, su implementación en contextos de defensa no está exenta de riesgos. Crawford (2021) advierte sobre la opacidad de los modelos algorítmicos y los sesgos de entrenamiento, problemas que podrían comprometer la legitimidad institucional. Otros autores resaltan la dependencia de plataformas externas, que genera vulnerabilidades en términos de soberanía tecnológica (Ceballos et al., 2020). Estas advertencias muestran que la IA no es solo un recurso técnico, sino un factor geopolítico que reconfigura relaciones de poder.

En Colombia, los casos de la Operación Jaque y la Operación Fénix constituyen ejemplos concretos del rol de la inteligencia en operaciones estratégicas. *Jaque*, mediante el secreto, la compartimentación y la disciplina en la ejecución, demostró que la creatividad humana y la resiliencia cognitiva son capacidades imposibles de replicar algorítmicamente (Ramsey III, 2009; Torres-Cuéllar, 2009). *Fénix*, en cambio, evidenció la eficacia de la superioridad informacional a través del uso de SIGINT y cooperación interagencial, pero también desató controversias diplomáticas y jurídicas so-

bre la soberanía territorial. Estos casos muestran que la IA puede complementar el criterio humano, pero no sustituirlo, especialmente cuando las decisiones involucran dilemas legales y éticos.

En el plano normativo, la Ley Estatutaria 1621 de 2013 establece principios, como necesidad, idoneidad, proporcionalidad y reserva en las actividades de inteligencia. Aunque no menciona explícitamente la IA, constituye el marco jurídico que delimita su aplicación en Colombia. A nivel internacional, organismos como el Stockholm International Peace Research Institute (SIPRI) han resaltado los dilemas asociados a los sistemas autónomos en armamento, subrayando la importancia de mantener un control humano significativo sobre las decisiones críticas (Boulanin y Verbruggen, 2017).

La literatura también destaca el avance hacia modelos híbridos, donde la IA actúa como multiplicador estratégico sin desplazar la capacidad interpretativa del ser humano. McAfee y Brynjolfsson (2017) sostienen que la sinergia entre personas y algoritmos genera un valor superior al que ambos podrían alcanzar de forma aislada. En la misma línea, investigaciones recientes (Van-Diggelen et al., 2025) señalan que la interacción humano-IA resulta clave para fortalecer la resiliencia cognitiva en escenarios de guerra informacional.

En síntesis, el marco teórico evidencia que la IA redefine la naturaleza de la inteligencia estratégica al ampliar capacidades técnicas y acelerar procesos decisionales. Sin embargo, también introduce riesgos éticos, jurídicos y políticos que obligan a repensar la relación entre tecnología, soberanía y legitimidad democrática. En este contexto, Colombia debe avanzar hacia un modelo híbrido humano-IA que preserve la creatividad, el juicio experto y la adaptabilidad del factor humano, al tiempo que aprovecha el potencial algorítmico como herramienta multiplicadora del poder informacional.

Este debate global sobre el papel de la inteligencia artificial en la transformación del poder estratégico se amplía con el aporte de Horowitz (2018), quien advierte que la IA no es, por sí misma, un arma, sino una tecnología que puede alterar el equilibrio de poder entre las naciones según la rapidez con que cada Estado logre integrarla en su doctrina, estructura y toma de decisiones. Como advierte Scharre (2016), el desarrollo de sistemas autónomos en contextos militares no solo transforma la dinámica operativa, sino que introduce nuevos riesgos estratégicos derivados de la delegación parcial de decisiones críticas a algoritmos.

En este sentido, la ventaja estratégica no proviene del algoritmo, sino de la capacidad institucional para adaptarlo sin perder el control humano ni la legitimidad política. Aplicado al caso colombiano, este planteamiento refuerza la necesidad de que la transición tecnológica en las operaciones de información se acompañe de un marco doctrinal y ético sólido, que preserve el juicio humano como eje rector de toda decisión de inteligencia.

Resultados y Reflexiones

Impactos estratégicos de la transición hacia la IA (en clave Operación Jaque)

La incorporación de la inteligencia artificial (IA) en las operaciones de información estratégica en Colombia marca un punto de inflexión en la doctrina de seguridad nacional. Más que una herramienta técnica, constituye un cambio cultural en la forma de entender la recopilación, procesamiento y utilización de datos. Marr y Ward (2019) resaltan que la verdadera fortaleza de la IA radica en transformar grandes volúmenes de información en conocimiento accionable en tiempo real, lo que otorga ventajas decisivas frente a la velocidad con que circula la desinformación en redes sociales.

En el caso colombiano, esta capacidad adquiere relevancia frente a amenazas híbridas, como el

narcotráfico, los grupos armados organizados y las campañas de manipulación digital. Los algoritmos de aprendizaje automático permiten detectar patrones de comunicación, anomalías digitales y campañas coordinadas de desinformación, configurando así sistemas de alerta temprana frente a riesgos emergentes. Nilsson et al. (2025) destacan que la preparación de las comunidades de inteligencia para escenarios de alta volatilidad exige esta integración entre tecnología y juicio humano, pues solo el análisis contextual puede dar sentido a los datos procesados por la máquina.

La experiencia de la Operación Jaque ofrece un referente ineludible. El éxito de esta operación se debió a la creatividad estratégica, la disciplina del secreto y la capacidad de interpretar al adversario en un entorno de incertidumbre (Ramsey III, 2009; Torres-Cuéllar, 2009). Ningún algoritmo puede replicar esos factores humanos, pero sí puede complementarlos. La IA puede acelerar simulaciones, anticipar escenarios y filtrar señales débiles, pero la decisión final continúa dependiendo del criterio humano que reconoce matices sociales, emocionales y culturales imposibles de modelar.

En contraste, la Operación Fénix demuestra el poder de la superioridad informacional mediante el uso de inteligencia técnica y cooperación interagencial. Sin embargo, también expuso dilemas jurídicos y diplomáticos al realizarse en territorio extranjero. Este antecedente revela que la transición hacia la IA no se limita a aspectos técnicos, sino que implica riesgos normativos y políticos que deben ser regulados para evitar que la innovación tecnológica erosione la legitimidad estatal.

En términos de gobernanza, Crawford (2021) advierte que la adopción indiscriminada de sistemas algorítmicos puede amplificar sesgos presentes en los datos, lo cual, en contextos polarizados como el colombiano, representa un riesgo de estigmatización y de profundización de narrativas parciales. Por eso, la integración de la IA en operaciones estratégicas debe regirse por criterios éticos y marcos normativos sólidos que garanticen la supervisión humana.

Riesgos identificados en el caso colombiano (versión fortalecida)

El uso creciente de inteligencia artificial en la seguridad nacional de Colombia trae riesgos importantes que no se pueden ignorar. Uno de los más urgentes es la dependencia de tecnología proveniente de proveedores extranjeros. Muchas de las plataformas que el Estado utiliza para ciberseguridad y análisis de datos vienen de empresas fuera del país, lo cual limita su autonomía. Esa situación abre portones para varias vulnerabilidades estratégicas: desde condiciones impuestas para acceder a las actualizaciones hasta el riesgo de que existan puertas traseras que pongan en peligro la seguridad nacional.

Otro riesgo corresponde a la manipulación algorítmica. Linares-Torres (2024) señala que los sistemas de IA pueden ser objeto de desinformación inversa, es decir, la introducción deliberada de datos falsos para inducir errores de clasificación. En esa misma línea, Gaeta et al. (2025) demuestran que la guerra cognitiva no requiere complejidad técnica, sino la explotación de la vulnerabilidad psicológica de las audiencias a través de mensajes diseñados con simplicidad textual y alta capacidad persuasiva. Para el caso colombiano, donde la polarización política amplifica la circulación de narrativas falsas, este riesgo es especialmente crítico.

A nivel ético y operativo, también emerge el peligro del desplazamiento del criterio humano. La Operación Jaque demostró que la improvisación táctica, la coordinación interinstitucional y la creatividad estratégica fueron decisivas para alcanzar el éxito (Torres-Cuéllar, 2009). Cualidades de este tipo difícilmente pueden ser replicadas por algoritmos. Una excesiva confianza en sistemas automatizados podría restringir la flexibilidad necesaria en escenarios dinámicos, lo que coincide con Boulanin y Verbruggen (2017), quienes subrayan la necesidad de mantener siempre un control huma-

no significativo en operaciones militares.

Asimismo, la literatura reciente advierte sobre los riesgos de la responsabilidad desplazada. Erskine (2024) plantea que, cuando los algoritmos asumen un rol decisorio, los comandantes pueden delegar indebidamente juicios esencialmente humanos, mientras que Downey (2025) alerta sobre el *"alibi tecnológico"*, en el que las fallas se atribuyen al sistema y no a la cadena de mando. En un país como Colombia, esta dinámica podría erosionar la legitimidad institucional en operaciones críticas.

Finalmente, la soberanía digital constituye un reto estructural. La dependencia de infraestructuras y servicios digitales gestionados por corporaciones extranjeras refuerza la vulnerabilidad estratégica de la región (Ceballos et al., 2020). Para Colombia, esto implica la necesidad de avanzar hacia desarrollos propios y esquemas de cooperación regional que reduzcan la dependencia tecnológica y fortalezcan la autonomía decisoria.

En conjunto, estos riesgos evidencian que la incorporación de la inteligencia artificial en la seguridad nacional no puede limitarse a un enfoque técnico. Se requiere un marco integral que combine supervisión humana, gobernanza tecnológica y autonomía estratégica, garantizando que la IA funcione como complemento y no como sustituto del juicio humano.

Oportunidades estratégicas para Colombia

Si bien la transición hacia sistemas de inteligencia artificial (IA) implica riesgos, también abre un espectro amplio de oportunidades que Colombia puede aprovechar en su estrategia de seguridad y defensa. La primera de ellas es la velocidad de procesamiento y análisis de datos, que constituye un activo frente a campañas de desinformación y amenazas híbridas. La capacidad de responder de manera inmediata a narrativas maliciosas fortalece la legitimidad institucional y reduce el impacto de operaciones psicológicas adversarias.

Una segunda oportunidad radica en la detección predictiva de amenazas. Los algoritmos de aprendizaje automático aplicados a redes sociales y fuentes abiertas pueden identificar patrones y tendencias antes de que escalen en crisis de seguridad. Bono et al. (2024) demuestran que el uso de IA generativa en centros de operaciones de seguridad reduce significativamente los tiempos de respuesta, mientras que Khayat et al. (2025) destacan su utilidad para anticipar comportamientos hostiles y apoyar la toma de decisiones bajo presión. Estos avances resultan especialmente valiosos en el contexto colombiano, donde la dinámica de la violencia requiere respuestas rápidas y precisas.

Un tercer ámbito de oportunidad se vincula a la optimización de recursos humanos. La automatización de tareas rutinarias -como la clasificación preliminar de información o la traducción automática de fuentes- libera a los analistas para que se concentren en la interpretación y la planificación estratégica. McAfee y Brynjolfsson (2017) sostienen que este modelo de colaboración potencia al ser humano en lugar de reemplazarlo, generando sinergias que incrementan la eficacia institucional.

La transformación de los Security Operations Centers (SOC) ilustra este proceso. Chamkar et al. (2024) resaltan que la integración de marcos como MITRE ATT&CK[6] permite mapear técnicas adversarias y cerrar brechas de detección, mientras que Islam (2023) evidencia cómo la IA contribuye a reducir la sobrecarga cognitiva de los analistas. Estos hallazgos sugieren que los SOC de próxima generación no solo funcionan como nodos tecnológicos, sino como espacios donde se articula la resiliencia operativa entre capacidades algorítmicas y supervisión humana.

[6] MITRE ATT&CK (Tácticas, Técnicas y Conocimiento Común de Adversarios) es un marco abierto para establecer programas de detección y respuesta en ciberseguridad, desarrollado por la Corporación MITRE, que ha facilitado la codificación y estandarización del conocimiento para los defensores.

En el ámbito regional, Moussaoui et al. (2025) destacan que los modelos híbridos de aprendizaje automático y federado permiten equilibrar precisión, privacidad y escalabilidad. Para Colombia, esta innovación es especialmente relevante, pues reduce los riesgos derivados de la centralización de información sensible en infraestructuras vulnerables a ciberataques.

Finalmente, la literatura internacional advierte que limitar el debate sobre IA militar a los sistemas de armas autónomas es un error estratégico. Meerveld et al. (2023) señalan que la IA puede fortalecer cada fase del ciclo de decisión militar, desde la planeación hasta el análisis posterior, ofreciendo ventajas en velocidad y reducción de sesgos. Para Colombia, esta perspectiva abre la posibilidad de integrar la IA en la logística, la simulación de escenarios y la ciberdefensa, consolidando un modelo híbrido humano-máquina orientado a la protección del Estado.

En conjunto, estas oportunidades muestran que la IA no debe concebirse como sustituto del ser humano, sino como un multiplicador de poder informacional. El reto consiste en aprovechar sus capacidades sin comprometer la ética, la legitimidad y la autonomía estratégica, asegurando que la tecnología se mantenga al servicio de la seguridad nacional y no a la inversa.

Reflexión crítica: modelo híbrido humano-IA (lecciones Jaque/Fénix)

El debate sobre la incorporación de la inteligencia artificial (IA) en la seguridad nacional colombiana conduce inevitablemente a un punto de equilibrio: la tecnología no debe desplazar las cualidades humanas, sino potenciarlas. La experiencia de la Operación Jaque simboliza esta afirmación. Su éxito descansó en la creatividad de los mandos, la disciplina del secreto y la coordinación interinstitucional, atributos imposibles de replicar por un algoritmo (Ramsey III, 2009; Torres-Cuéllar, 2009). La IA, en este sentido, no reemplaza esas virtudes, pero puede amplificarlas al ofrecer mayor rapidez en el análisis de datos, detección de patrones y simulación de escenarios complejos.

La literatura reciente refuerza esta visión. Mohsin et al. (2025) proponen marcos de colaboración humano-IA en los Security Operations Centers, orientados a fortalecer la supervisión de los analistas y evitar la delegación irresponsable de decisiones críticas en algoritmos. De forma complementaria, Van-Diggelen et al. (2025) destacan que los modelos híbridos permiten mejorar la resiliencia cognitiva en escenarios de guerra informacional, aunque advierten que sus limitaciones en explicabilidad y dependencia tecnológica exigen mecanismos de control y transparencia.

La reflexión también conecta con la dimensión ética. Downey (2025) alerta sobre el *"alibi tecnológico"*, es decir, la posibilidad de que los sistemas algorítmicos funcionen como coartada para diluir responsabilidades en la cadena de mando. Este riesgo, lejos de disminuir la incertidumbre, podría prolongar los conflictos y erosionar la legitimidad de las operaciones. En paralelo, Kanellopoulos (2024) resalta que la IA constituye un multiplicador estratégico de la contrainteligencia, capaz de reforzar la protección de infraestructuras críticas y la detección de infiltraciones, pero su aplicación debe regirse por principios democráticos que eviten abusos en la vigilancia.

La Operación Fénix también ofrece lecciones para esta reflexión. Aunque su éxito se sustentó en la integración de inteligencia técnica (SIGINT) y cooperación interagencial, la operación generó tensiones diplomáticas y cuestionamientos jurídicos sobre la soberanía. Este antecedente advierte que, aun cuando la IA mejore la superioridad informacional, no elimina los dilemas éticos ni políticos, por lo que siempre se requerirá un mando humano que asuma la responsabilidad estratégica.

En suma, el modelo híbrido humano-IA emerge como la opción más viable para Colombia. La

IA puede reducir tiempos de reacción, optimizar procesos y detectar amenazas con precisión, pero la interpretación contextual, el juicio ético y la adaptabilidad seguirán siendo funciones insustituibles del factor humano. La clave no está en delegar, sino en integrar para aprovechar la capacidad algorítmica como un multiplicador que refuerce, y nunca sustituya, las cualidades que hicieron posible el éxito de operaciones como *Jaque* y *Fénix*. Estudios recientes muestran que los modelos de aprendizaje automático empleados en entornos de seguridad alcanzan niveles de precisión cercanos al 90 % en la detección de anomalías informacionales (Khayat et al., 2025), lo que evidencia su potencial para reforzar el análisis sin sustituir la supervisión humana.

Las operaciones *Jaque* y *Fénix* constituyen referentes estratégicos fundamentales para comprender la evolución del factor humano en la toma de decisiones antes de la incorporación formal de tecnologías basadas en inteligencia artificial. Ambas demostraron que el éxito operativo dependió del liderazgo, la planeación y la capacidad de anticipación humana frente a contextos de alta incertidumbre. Analizar estos casos desde la perspectiva de transición hacia la IA permite proyectar cómo dichas competencias podrían potenciarse mediante la integración gradual de sistemas inteligentes en el ciclo de inteligencia, manteniendo el principio de control humano significativo (Allen y Chan, 2017; Horowitz, 2018).

Los riesgos del uso de la inteligencia artificial en la inteligencia estratégica se concentran en la posible pérdida del criterio humano, la dependencia tecnológica y los sesgos algorítmicos que pueden comprometer la legitimidad institucional. Sin embargo, sus fortalezas -como la capacidad de procesar grandes volúmenes de información, identificar patrones ocultos y anticipar escenarios operativos- representan oportunidades reales de fortalecimiento del sistema de inteligencia nacional. La clave está en equilibrar eficiencia tecnológica con responsabilidad ética, garantizando que la IA actúe como soporte y no como sustituto del juicio humano (Brundage et al., 2018).

Conclusiones

La investigación permitió confirmar que la inteligencia estratégica en Colombia atraviesa un momento de transición crucial frente a la incorporación de la inteligencia artificial (IA). Si bien la tecnología ofrece ventajas innegables -mayor velocidad de procesamiento, capacidad de correlacionar datos masivos y de anticipar amenazas emergentes-, estos beneficios no sustituyen el ingenio, la adaptabilidad y la intuición que caracterizan al factor humano en escenarios de seguridad y defensa.

El contraste entre la Operación Jaque y la Operación Fénix ilustra este punto con claridad. Jaque demostró que el secreto, la creatividad y la disciplina estratégica fueron determinantes en el éxito de la misión, mientras que Fénix expuso los dilemas diplomáticos y jurídicos que acompañan el uso de la superioridad informacional en operaciones militares. Ambas experiencias confirman que la IA puede fortalecer las capacidades operativas, pero no desplazar la centralidad del juicio humano en la conducción estratégica.

En relación con la hipótesis planteada, los hallazgos la validan de forma parcial. La IA amplifica la eficiencia de los sistemas de inteligencia al procesar información con rapidez y detectar patrones ocultos, pero al mismo tiempo introduce riesgos críticos: la dependencia de proveedores extranjeros, la manipulación algorítmica mediante datos alterados y la posibilidad de que se desplace la responsabilidad de mando hacia sistemas incapaces de asumir consecuencias éticas. Estos factores muestran que el uso de la IA debe estar siempre bajo supervisión humana y regido por marcos normativos claros.

El estudio también permite extraer una lección de fondo: el futuro de la inteligencia estratégica en Colombia dependerá de la capacidad de integrar equilibradamente lo humano y lo tecnológico. La

IA puede acelerar procesos y reducir márgenes de error, pero la interpretación contextual, la prudencia ética y la legitimidad institucional siguen siendo atributos exclusivamente humanos. Más que un sustituto, la IA debe concebirse como un multiplicador de poder informacional, cuyo verdadero valor surge cuando se combina con la experiencia y la creatividad de los analistas.

En el plano regional se recomienda orientar el uso de la IA en el sector público bajo principios de transparencia, responsabilidad y confianza social. Para Colombia, este marco es esencial: asegura que la innovación tecnológica se desarrolle en armonía con los valores democráticos y que la seguridad nacional no dependa únicamente de la eficiencia algorítmica, sino también de la legitimidad política y social que garantizan su sostenibilidad a largo plazo.

En síntesis, los impactos estratégicos de la transición hacia la IA en Colombia refuerzan la idea de un modelo híbrido: la tecnología amplifica las capacidades humanas, pero no sustituye la creatividad, la intuición ni el criterio estratégico. El desafío consiste en mantener el equilibrio entre eficiencia algorítmica y prudencia humana, garantizando que la IA sea un multiplicador del poder informacional sin desplazar los valores que han guiado históricamente la conducción militar en el país.

En conclusión, el desafío no es tecnológico sino estratégico: construir un modelo híbrido humano-IA que aproveche las ventajas de los algoritmos sin sacrificar la esencia humana de la inteligencia. Solo así la transición hacia la IA en operaciones de información podrá convertirse en una oportunidad y no en una amenaza para la seguridad y defensa nacional.

La aplicación del enfoque cualitativo-documental, sustentado en teorías del factor humano, automatización y constructivismo tecnológico, permitió comprender cómo la inteligencia artificial redefine la práctica de la inteligencia estratégica sin sustituir el juicio humano.

De esta manera, el estudio consolida un marco teórico y metodológico que puede servir de base para futuras investigaciones sobre la relación entre el factor humano, la inteligencia artificial y los desafíos ético-jurídicos de la seguridad nacional en Colombia.

Referencias

Allen, G. y Chan, T. (2017). *Artificial Intelligence and National Security.* Belfer Center for Science and International Affairs, Harvard Kennedy School. https://www.belfercenter.org/publication/artificial-intelligence-and-national-security

Bainbridge, L. (1983). Ironies of automation. *Automatica, 19*(6), 775-779. https://doi.org/10.1016/0005-1098(83)90046-8

Bono, J., Grana, J. y Xu, A. (2024). Generative AI and security operations center productivity: evidence from live operations. *Arxiv – Microsoft Corporation.* https://doi.org/10.48550/arXiv.2411.03116

Boulanin, V. y Verbruggen, M. (2017). *Mapping the development of autonomy in weapon systems.* Stockholm International Peace Research Institute (SIPRI). https://www.jstor.org/stable/resrep24528

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Ó hÉigeartaigh, S., Beard, S. J., Belfield, H., Farquhar, S., Lyle, C., Crootof, R., Evans, O., Page, M.,

Bryson, J., Yampolskiy, R. y Amodei, D. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. *Arxiv – Cryptography and Security.* https://doi.org/10.48550/arXiv.1802.07228

Ceballos, L. D., Maisonnave, M. A. y Britto-Londoño, C. R. (2020). Soberanía tecnológica digital en Latinoamérica. *Propuestas para el Desarrollo,* (4), 151-167. https://www.propuestasparaeldesarrollo.com/index.php/ppd/article/view/108

Chamkar, S. A., Maleh, Y. y Gherabi, N. (2024). Security operations centers: use case best practices, coverage, and gap analysis based on MITRE adversarial tactics, techniques, and common knowledge. *Journal of Cybersecurity and Privacy, 4*(4), 777-793. https://doi.org/10.3390/jcp4040036

Crawford, K. (2021). *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence.* Yale University Press. https://doi.org/10.12987/9780300252392 https://doi.org/10.2307/j.ctv1ghv45t

Cummings, M. L. (2017). *Artificial intelligence and the future of warfare.* International Security Department and US and the Americas Programme – Chatham House. https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf

Downey, A. (2025). The alibi of AI: algorithmic models of automated killing. *Digital War, 6*(1). https://doi.org/10.1057/s42984-025-00105-7

Ejército Nacional de Colombia. (3 de marzo de 2023a). *El Billar*. https://www.ejercito.mil.co/el-billar/

Ejército Nacional de Colombia. (4 de julio de 2023b). *Operación Militar JAQUE*. https://www.ejercito.mil.co/operacion-militar-jaque/

Erskine, T. (2024). Before algorithmic Armageddon: Anticipating immediate risks to restraint when AI infiltrates decisions to wage war. *Australian Journal of International Affairs, 78*(2), 175-190. https://doi.org/10.1080/10357718.2024.2345636

Fuerzas Militares de Colombia. (2018). *Manual Fundamental Conjunto MFC 1.0: Doctrina Conjunta.* Centro de Doctrina Conjunta de las Fuerzas Militares de Colombia - CEDCO. https://doi.org/10.25062/MFC10

Gaeta, A., Loia, V., Lorusso, A., Orciuoli, F. y Pascuzzo, A. (2025). Computational analysis of information disorder in cognitive warfare. *Online Social Networks and Media, 48*, 100322. https://doi.org/10.1016/j.osnem.2025.100322

Hernández-Estupiñán, P. A. (2020). Aportes al concepto de inteligencia estratégica. *Perspectivas en Inteligencia, 12*(21), 81–94. https://doi.org/10.47961/2145194X.233

Horowitz, M. C. (2018). Artificial intelligence, international competition, and the balance of power. T*exas National Security Review, 1*(3), 36-57. https://doi.org/10.15781/T2639KP49

Islam, M. A. (2023). Application of artificial intelligence and machine learning in a security operations center. *Issues in Information Systems, 24*(4), 311-327. https://doi.org/10.48009/4_iis_2023_124

Johnson, J. (2022). The AI commander problem: Ethical, political, and psychological dilemmas of human–machine interactions in AI-enabled warfare. *Journal of Military Ethics, 21*(3–4), 246-271. https://doi.org/10.1080/15027570.2023.2175887

Joint Chiefs of Staff of the United States Government. (2014). *Joint publication 3-13: Information operations (27 November 2012, Incorporating Change 1, 20 November 2014)*. U.S. Department of Defense - jcs.mil. https://irp.fas.org/doddir/dod/jp3_13.pdf

Kanellopoulos, A. N. (2024). Counterintelligence, artificial intelligence and national security: Synergy and challenges. *Journal of Politics and Ethics in New Technologies and AI, 3*(1). https://doi.org/10.12681/jpentai.35617

Khan, R. N. A. y Khan, A. U. (2025). Artificial intelligence and the national security matrix. *Research Journal for Social Affairs, 3*(4), 139-145. https://doi.org/10.71317/RJSA.003.04.0268

Khayat, M., Barka, E., Serhani, M. A., Sallabi, F., Shuaib, K. y Khater, H. M. (2025). Empowering security operation center with artificial intelligence and machine learning—A systematic literature review. *IEEE Access, 13*, 19162–19188. https://doi.org/10.1109/ACCESS.2025.3532951

Ley Estatutaria 1621 de 2013. Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones. 17 de abril de 2013. D. O. No. 48764. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=52706

Linares-Torres, F. (2024). Inteligencia artificial y ciberdefensa. *Revista Seguridad y Poder Terrestre, 3*(4), 139-150. https://revistas.ceeep.mil.pe/index.php/seguridad-y-poder-terrestre/article/view/72 https://doi.org/10.56221/spt.v3i4.72

Marr, B. y Ward, M. (2019). A*rtificial intelligence in practice: How 50 successful companies used AI and machine learning to solve problems*. Wiley.

McAfee, A. y Brynjolfsson, E. (2017). *Machine, platform, crowd: harnessing our digital future.* W.W. Norton & Company.

Meerveld, H. W., Lindelauf, R. H. A., Postma, E. O. y Postma, M. (2023). The irresponsibility of not using AI in the military. *Ethics and Information Technology, 25.* https://doi.org/10.1007/s10676-023-09683-0

Mohsin, A., Janicke, H., Ibrahim, A., Sarker, I. H. y Camtepe, S. (2025). A unified framework for human–AI collaboration in security operations centers with trusted autonomy. *Arxiv*. https://doi.org/10.48550/arXiv.2505.23397

Moussaoui, J. E., Kmiti, M., El Gholami, K. y Maleh, Y. (2025). A systematic review on hybrid AI models integrating machine learning and federated learning. *Journal of Cybersecurity and*

Privacy, 5(3). https://doi.org/10.3390/jcp5030041

Nilsson, N., Weissmann, M. y Palmertz, B. (2025). Hybrid threats and the intelligence community: priming for a volatile age. *International Journal of Intelligence and CounterIntelligence.* https://doi.org/10.1080/08850607.2024.2435265

Pastrana-Buelvas, E. y Trujillo-Méndez, L. (2011). La Operación Fénix de las Fuerzas Armadas colombianas a luz del Derecho Internacional. *Diálogos de saberes: investigaciones y ciencias sociales,* (34), 197-226. https://revistas.unilibre.edu.co/index.php/dialogos/article/view/1887

Peña-Suarez, 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

Pinch, T. J. y Bijker, W. E. (1984). The social construction of facts and artefacts: or how the sociology of science and the sociology of technology might benefit each other. *Social Studies of Science, 14*(3), 399-441. https://doi.org/10.1177/030631284014003004

Ramsey III., R. D. (2009). F*rom El Billar to Operations Fénix and Jaque: The Colombian security force experience,* 1998–2008 (Occasional Paper No. 34). Combat Studies Institute Press. https://doi.org/10.21236/ADA514131

Reason, J. (1990). The contribution of latent human failures to the breakdown of complex systems. *Philosophical Transactions of the Royal Society of London B: Biological Sciences, 327*(1241), 475-484. https://doi.org/10.1098/rstb.1990.0090 PMid:1970893

Russell, S. (2022). Artificial intelligence and the problem of control. En H. Werthner, E. Prem, E. A. Lee, y C. Ghezzi (Eds.), *Perspectives on digital humanism* (pp. 19-28). Springer. https://doi.org/10.1007/978-3-030-86144-5_3

Scharre, P. (2016). *Autonomous weapons and operational risk*. Center for a New American Security. https://www.cnas.org/publications/reports/autonomous-weapons-and-operational-risk

Singer, P. W. y Brooking, E. T. (2018). *Like war: the weaponization of social media.* Eamon Dolan/ Houghton Mifflin Harcourt.

Torres-Cuéllar, J. C. (2009). *Operación Jaque: la verdadera historia.* Editorial Planeta.

Van-Diggelen, J., Aidman, E., Rowa, J. y Vince, J. (2025). Designing AI-Enabled Countermeasures to Cognitive Warfare. *Arxiv – NATO Science and Technology Organization*. https://doi.org/10.48550/arXiv.2504.11486

Esta página queda intencionalmente en blanco

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

Definición conceptual sobre la transición del factor humano hacia el uso de la IA en operaciones de información en el caso colombiano

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)
Luis Carlos González-Carrillo es estudiante de Maestría en Inteligencia Estratégica de la Institución Universitaria Escuela de Inteligencia y Contrainteligencia "BG. Ricardo Charry Solano" (Colombia), es Especialista en Derecho Penal y Ciencias Forenses de la Universidad Católica de Colombia, es Especialista en Derecho Administrativo de la Universidad Libre de Colombia, es Especialista en Derechos Humanos y Sistemas de Protección de la Universidad Militar Nueva Granada (Colombia), es Especialista en Derecho Internacional de los Conflictos Armados (DICA) de la Escuela Militar de Cadetes "General José María Córdova" (Colombia), es Abogado de la Universidad Cooperativa de Colombia.

https://orcid.org/0009-0009-6574-4258 - Contacto: luiscarlosgonzalez2021@gmail.com