



IA en las operaciones militares del Ejército de Colombia. Estudio de caso del Ejército de Ucrania 2022 – 2024.

Mayor (EJC) Javier Rene Martínez Maldonado

Artículo para optar al título profesional:

Magister en Estrategia y Geopolítica

Escuela Superior de Guerra “General Rafael Reyes Prieto”
Bogotá D.C., Colombia
2025

DATOS GENERALES	
Nombre del estudiante	: Mayor (EJC) Javier Rene Martínez Maldonado
Identificación	: 88131714
Programa académico	: Maestría en Estrategia y Geopolítica
Tutor metodológico	: Gineth Esmeralda Narváz
Tutor temático	: Teniente coronel Jorge Mauricio Cardona Angarita
Fecha de entrega	: 27 de agosto de 2025
Extensión	: 7.700 palabras

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

El autor declara que este artículo fue escrito de acuerdo con la normatividad de la Escuela Superior de Guerra “General Rafael Reyes Prieto” (ESDEG) y no existe ningún potencial conflicto de interés relacionado con este. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representan la posición oficial ni institucional de la ESDEG, las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.

Este artículo es enteramente mi propio trabajo y no ha sido presentado para la obtención de un título en esta u otra Institución de Educación Superior. Se han referenciado todos los trabajos y puntos de vista de otros autores, así como los datos de otras fuentes utilizadas. No se emplearon herramientas de generación de contenido por Inteligencia Artificial para su elaboración.

El autor acepta ceder los derechos de publicación en favor de la ESDEG y su Sello Editorial de acuerdo con los términos de la licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.

AUTORIZACIÓN DE PUBLICACIÓN

El autor autoriza / no autoriza que este artículo sea publicado por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto.

IA en las operaciones militares del Ejército de Colombia. Estudio de caso del Ejército de Ucrania 2022 – 2024.

AI in the military operations of the Colombian Army. Case study of the Ukrainian Army 2022 - 2024.

Javier Rene Martínez Maldonado¹

Escuela Superior de Guerra “General Rafael Reyes Prieto”

Resumen: El desarrollo de las operaciones militares en el espectro mundial ha permitido observar las guerras de quinta generación en casos como el de Ucrania quien libra una contra Rusia desde el 2022 y es en ese sentido que, las lecciones de los casos ocurridos en Ucrania podrían aplicar en Colombia para mejorar la efectividad operacional en seguridad y la defensa de la Nación, en cuanto al manejo de la inteligencia artificial IA. Con esto en mente, esta investigación busca entender cómo el Ejército de Colombia podría aprovechar la inteligencia artificial en sus operaciones, tomando como referencia lo aprendido del caso ucraniano. La idea es reflexionar sobre qué se está haciendo bien, qué se podría mejorar y, sobre todo, cómo prepararnos mejor para los nuevos retos que trae consigo el mundo actual.

Palabras clave: IA, G5G, G6G, Colombia, Estrategia.

Abstract: The development of military operations on a global scale has revealed the dynamics of fifth-generation warfare, as seen in the case of Ukraine, which has been engaged in conflict with Russia since 2022. In this context, the lessons learned from Ukraine could be applicable to Colombia, particularly in enhancing operational effectiveness in national security and defense through the use of artificial intelligence (AI). This research aims to explore how the Colombian Army could leverage AI in its operations, drawing insights from the Ukrainian experience. The goal is to reflect on current strengths, areas for improvement, and, most importantly, how to better prepare for the emerging challenges of the modern world

Keywords: IA, G5W, G6W, Colombia, Strategy.

¹ Mayor del Ejército Nacional de Colombia. Candidato a magíster en estrategia y geopolítica, Escuela Superior de Guerra “General Rafael Reyes Prieto”, Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes “General José María Córdova”, Colombia. <https://orcid.org/0009-0005-3885-9309> - Contacto: javier.martinezm@esdeg.edu.co.

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

Introducción

En las últimas décadas, la forma en que se desarrollan los conflictos armados ha cambiado radicalmente. Ya no se trata solo de enfrentamientos con soldados y armas convencionales; Hoy, la guerra también se libra en espacios digitales, informativos y hasta psicológicos. Este cambio ha sido impulsado por la cuarta revolución industrial, que trajo consigo avances tecnológicos como la inteligencia artificial, el uso de drones, la robótica y el ciberespacio como nuevos escenarios de combate. En este nuevo panorama, surgen las llamadas guerras de quinta y sexta generación, donde la tecnología, más que la cantidad de tropas o armamento pesado, puede marcar la diferencia.

Un ejemplo claro de esta transformación es lo que ha ocurrido en la guerra entre Ucrania y Rusia desde 2022. A pesar de las limitaciones, el Ejército ucraniano ha logrado adaptarse rápidamente, utilizando la inteligencia artificial de formas innovadoras para planear y ejecutar operaciones militares. Su experiencia ha demostrado que, incluso frente a un adversario más grande, es posible hacerle frente con creatividad, tecnología y estrategia. Esto ofrece valiosas lecciones que podrían ser útiles para otros países, como Colombia, que también enfrenta amenazas complejas y diversas en su territorio.

En este ambiente, actualmente observamos en Colombia el inicio de empleo de vehículos aéreos no tripulados denominados drones, como también el empleo del ciberespacio y el dominio cognitivo por parte de organizaciones al margen de la ley para afectar la seguridad del estado. Por otro lado, por experiencia, se tiene una percepción de que el Ejército de Colombia se ha quedado rezagado en el tema de la guerra de quinta

generación, teniendo en cuenta el planeamiento y el resultado de las operaciones militares realizadas en el 2024.

El desarrollo de las operaciones militares en el espectro mundial ha permitido observar las guerras de quinta generación en casos como el de Ucrania quien libra una contra Rusia desde el 2022 y es en ese sentido que, las lecciones de los casos ocurridos en Ucrania podrían aplicar en Colombia para mejorar la efectividad operacional en seguridad y la defensa de la Nación, en cuanto al manejo de la inteligencia artificial IA.

Con esto en mente, esta investigación busca entender cómo el Ejército de Colombia podría aprovechar la inteligencia artificial en sus operaciones, tomando como referencia lo aprendido del caso ucraniano. La idea es reflexionar sobre qué se está haciendo bien, qué se podría mejorar y, sobre todo, cómo prepararnos mejor para los nuevos retos que trae consigo el mundo actual.

De acuerdo a lo anterior, en esta investigación se trazó como pregunta de investigación ¿Cómo el Ejército de Colombia puede emplear la inteligencia artificial en el desarrollo de las operaciones militares teniendo como modelo las experiencias del Ejército ucraniano durante el periodo 2022 al 2024? Para responder a ello, se propuso como objetivo principal analizar el uso de la inteligencia artificial del Ejército Ucraniano en el periodo 2022 al 2024 con el fin de servir como modelo para el desarrollo de las operaciones militares en el Ejército de Colombia dentro del concepto de guerra de quinta generación y como objetivos secundarios Identificar el empleo de la inteligencia artificial IA en las operaciones militares con el fin de observar las ventajas y desventajas en la efectividad operacional; Analizar las operaciones militares del Ejército ucraniano en el ámbito de la inteligencia artificial con el fin de observar las acciones positivas y negativas de su empleo;

y, Analizar el empleo de la inteligencia artificial en el Ejército de Colombia a la luz del modelo del ejército ucraniano con el fin de proponer estrategias para la efectividad operacional en el ámbito de la guerra de quinta generación .

Esta investigación empleara la teoría realista de Morgenthau, el cual plantea que el poder nacional es la sumatoria del poder tangible entendido como las armas con las que cuenta un Estado, su extensión territorial y la cantidad de acuerdos militares, unido con el poder intangible que en este caso se entiende como la influencia que puede generar su cultura, así mismo en el liderazgo que puede tener en la región y su capacidad en la intervención para cambiar la toma de decisiones en otros Estados (Morgenthau, 1985). Por otro lado, el principio de acción de los Estados está determinado por el uso o la amenaza del uso de la fuerza y en este sentido, la agenda de la política del Estado está marcada por temas militares y de seguridad colocando los demás temas de esa agenda en un segundo plano.

Metodología

Esta investigación se desarrolló bajo el método cualitativo e inductivo (Hernández Sampieri et al., 2014) partiendo de lo particular, donde se analizaron casos positivos y negativos que conllevaron a una generalidad que podría servir como modelo de aplicación para otros estudios. El diseño metodológico con sus técnicas e instrumentos estuvo compuesto inicialmente por una revisión documental detallada con análisis crítico de documentos (fuentes primarias y/o secundarias basadas en artículos científicos) a través de una hoja de Excel en donde se plasmó la información por las diferentes categorías que se

propusieron para realizar la investigación (IA, G5G y Seguridad). Así mismo, empleando la técnica de la bola de nieve, se hizo revisión a documentales y noticias audiovisuales, como también a las redes sociales donde se encuentra evidencia de actividades de IA durante el desarrollo de operaciones militares en Ucrania y en Colombia.

IA en las operaciones militares

La inteligencia artificial se entiende como cualquier sistema creado por el ser humano que pueda llevar a cabo tareas en entornos variables o impredecibles sin necesidad de supervisión constante, además de mejorar su desempeño con base en la experiencia adquirida (Álvarez & Ramírez, 2020; Freedman, 2019). Su implementación en el ámbito de la seguridad nacional puede generar desafíos, ya que estos algoritmos tienen la capacidad de identificar patrones en el campo táctico, otorgando ventajas estratégicas a ciertos actores mediante el uso de plataformas automatizadas interconectadas.

A partir de 1950, después de la segunda guerra mundial, la guerra ha evolucionado y con la cuarta revolución industrial el concepto de conflicto y de guerra se desarrolla en el dominio de la información y el crecimiento de la inteligencia artificial, lo cual ha cambiado el espectro y la velocidad de la guerra. Actualmente las operaciones militares a nivel mundial se desarrollan bajo los conceptos de guerras de cuarta, quinta y sexta generación (Álvarez et al., 2022). De acuerdo a lo anterior, una guerra de quinta generación trata de reducir el costo del armamento y piensa en sistemas no manejados directamente por personas con el fin de evitar el envío de soldados al teatro de operaciones, como también evolucionó hacia el uso de los sistemas digitales de apoyo a las decisiones humanas a través del manejo de grandes cantidades de datos y se evolucionó también hacia la nanotecnología

con su nanoarmamento, la cual pondría en riesgo posiblemente la existencia humana (Freedman, 2019).

La cuarta revolución tiene que ver con los avances en inteligencia artificial y las nuevas computadoras que están restando importancia al trabajo de las personas y reemplazándolo por máquinas (Álvarez & Ramírez, 2020). De manera similar, la guerra Gen 6 o Sexta Generación involucra inteligencia artificial, cambiando constantemente la naturaleza del enemigo y agregando reinos físicos como tierra, mar, espacio y ciberespacio. Más Cognitivo/Humano, Más Información (Álvarez et al., 2022). Además de la 4ª revolución industrial, se puede decir que es difícil enfrentarse a otro enemigo cuando se tiene ventaja en combinar elementos como las redes sociales y los robots (o vehículos terrestres, aéreos y marítimos no tripulados) en la guerra de la 6ª generación. Por ejemplo, la guerra entre Ucrania y Rusia, donde los drones israelíes son utilizados por Rusia, Ucrania utiliza la guerra de información para enfrentarse a este formidable adversario (Freedman, 2019).

Las guerras de sexta generación integran los escenarios propios de la quinta generación con la incorporación de nuevos actores, entre ellos el acceso cibernético potenciado por la cuántica, la robótica y la inteligencia artificial. En este marco tecnológico destacan avances como desarrollos en el ciberespacio, misiles hipersónicos, interferencia en procesos electorales de otros países y misiles terrestres capaces de destruir satélites en el espacio (Barrero & Álvarez, 2022).

A medida que los proyectos de investigación comenzaron a introducirse en el terreno de la ciberguerra, la inteligencia artificial y la robótica, la ciencia ficción se convirtió en el ámbito más lógico al que recurrir para hallar inspiración. En 2015, el

periodista August Cole y el politólogo Peter Singer redactaron *Ghost Fleet*, una novela en la que las preocupaciones sobre el poderío chino se entremezclan con la escasez de fuentes de energía y el desarrollo de las tecnologías bélicas, inspirándose en la obra de Tom Clancy *Tormenta roja* (Freedman, 2019). En este sentido, se puede decir que la ciencia ficción ha sido auténticamente un referente para realizar investigaciones en busca de nuevas tecnologías en cuanto a la ciberguerra, la inteligencia artificial y la robótica, indagando nuevos límites en la automatización y la guerra digital, en resumen, este género funciona como un puente entre la ilusión y la realidad, promoviendo ideas que antes solo existían en la mente de los escritores.

Por otro lado, las redes sociales desempeñan un rol fundamental en este tipo de conflictos, dado que herramientas como blogs, wikis, podcasts, etiquetas y motores de búsqueda permiten la recopilación y divulgación de información sensible sin autorización. Esto supone un riesgo considerable, ya que las organizaciones no solo enfrentan la posibilidad de filtraciones de datos, sino también amenazas a la seguridad de sus transacciones comerciales (Álvarez & Ramírez, 2020).

En el contexto de la cuarta revolución industrial, es posible llevar a cabo espionaje, interferir en actividades cotidianas o causar daños a través del uso de ordenadores, internet y conocimientos avanzados en informática. Ejemplos de ello incluyen la acusación de Estados Unidos contra China en 2003 por ciberataques, la explosión del oleoducto BTC en Refahiye, Turquía, en 2008 debido a un ataque cibernético, y el daño provocado en plantas de uranio iraníes en 2010 por el gusano informático Stuxnet, el cual sabotó proyectos estratégicos. Asimismo, la divulgación de información clasificada a través de WikiLeaks expuso datos sensibles sobre conflictos, espionaje y corrupción (Ospina & Sanabria, 2020).

Por otro lado, las interrelaciones sociales trascienden al individuo y a lo humano, y el entorno globalizado exige la creación de nuevas alianzas alejándose de la visión del humano para hacer frente a los no humanos, como la inteligencia artificial y los robots de cuarta generación. Estos últimos plantean debates sobre conceptos como la personalidad electrónica o "e-personality" (García, 2020), donde los algoritmos abiertos del software se convierten en sistemas complejos y no lineales, alineados con el concepto de homo digitalis y la robótica con capacidades de autopoiesis (Hernández, 2005). Aquí es donde está el dilema ético si hay q dejar d q la IA avance.

Como puede observarse, no se trata únicamente de un problema vinculado a la seguridad y defensa en el marco de las guerras de sexta generación, sino de un desafío mucho más amplio y complejo que abarca múltiples perspectivas, tanto humanas como no humanas.

Operaciones militares del Ejército ucraniano en el ámbito de la inteligencia artificial

La guerra de Ucrania está acelerando el proceso de desarrollo de esta tecnología para fines bélicos y, aunque el carácter de esta contienda aún no esté determinado por la IA, dicho conflicto armado se asemeja a un laboratorio en el que las grandes potencias y las empresas del sector pueden entrenar y probar constantemente sistemas de IA para una amplia gama de capacidades, funcionalidades y aplicaciones. (Santayana, 2024).

El conflicto en Ucrania está impulsando el avance de esta tecnología con fines militares y, aunque la inteligencia artificial aún no define la naturaleza de la guerra, el enfrentamiento actúa como un campo de prueba en el que las grandes potencias y las compañías del sector pueden desarrollar, evaluar y perfeccionar continuamente sistemas de IA con diversas capacidades, funciones y aplicaciones.

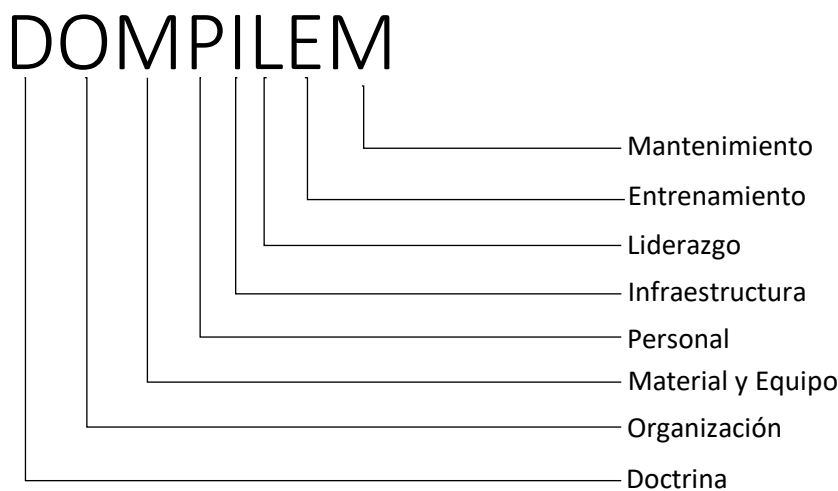
Los algoritmos en el Ejército Ucraniano trabajaron con una gran cantidad de información, como lo que pasa en redes sociales, eventos políticos internacionales y datos en tiempo real del campo de batalla, con esto, los comandantes militares pudieron adelantarse a las acciones de los rusos, usaron mejor sus recursos e hicieron que las operaciones fueran más efectivas (Tsozniashvili, 2024)

Durante la guerra en Ucrania, el Ejército Ucraniano usó algoritmos para analizar mucha información al mismo tiempo. Esta información venía de redes sociales, noticias políticas del mundo y datos en tiempo real del campo de batalla. Gracias a eso, los comandantes pudieron tomar decisiones más rápidas y anticiparse a los movimientos de los soldados rusos. También les ayudó a usar mejor sus recursos y a que las operaciones militares fueran más efectivas (Tsozniashvili, 2024). Esto muestra cómo la tecnología y la inteligencia artificial están cambiando la forma en que se hacen las guerras hoy en día.

Existe una tecnología llamada deepfake que está cambiando la manera en que se crean y manipulan videos o audios. Esta herramienta permite hacer grabaciones falsas que parecen reales, como si alguien dijera o hiciera cosas que nunca ocurrieron. Esto se logra gracias a programas de inteligencia artificial que aprenden a imitar voces, caras y

movimientos de personas, incluso de personajes famosos. Aunque puede parecer algo curioso, esta tecnología también se ha usado para confundir a la gente y difundir noticias falsas, lo que la hace bastante peligrosa en temas de política o redes sociales. (Tsozniashvili, 2024)

En la actualidad, la Inteligencia Artificial se aplica en prácticamente todos los ámbitos, y su funcionamiento depende del uso de software especializado. En el caso de una unidad militar, su capacidad para ejecutar operaciones debería evaluarse a partir del modelo **DOMPILEM**, lo que permitiría identificar qué tipo de IA puede ser más útil en cada componente de combate. Los algoritmos juegan un papel central en este proceso, especialmente aquellos orientados al **análisis cognitivo** y al **procesamiento de grandes volúmenes de datos (Big Data)**. Gracias a ellos, es posible transformar información dispersa en decisiones estratégicas más precisas, considerando los cinco dominios operacionales: terrestre, aéreo, marítimo, espacial y ciberespacial. A partir de este enfoque, se pueden llevar a cabo acciones como:



El modelo DOMPILEM ofrece una visión estructurada para identificar necesidades y resolver brechas en las capacidades militares. Este enfoque abarca ocho componentes clave: doctrina, organización, material, personal, infraestructura, liderazgo, entrenamiento y mantenimiento. Cada uno de estos elementos permite analizar cómo se articulan los recursos, la preparación y la disposición de una fuerza para cumplir sus objetivos operacionales. Además, esta herramienta facilita la identificación de problemas comunes como la improvisación, la falta de disciplina o la temporalidad en la ejecución de tareas, proporcionando así una base concreta para mejorar el desempeño institucional en escenarios reales (Whinsec, 2017).

DOCTRINA: Hace poco, el Ejército español lanzó una iniciativa llamada *Zeus*, con la que busca transformar su forma de operar usando inteligencia artificial como eje central. Lo más llamativo de este proyecto es que no se trata solo de adquirir tecnología, sino de repensar toda su doctrina de combate. Están integrando elementos como redes 5G, sensores, realidad aumentada y análisis de datos en una nube táctica que permite coordinar unidades y decisiones en tiempo real. Esta transformación, que se está probando en el centro de entrenamiento de San Gregorio en Zaragoza, cuenta con una inversión inicial de 15 millones de euros (HuffPost, 2024). Más allá del aspecto técnico, lo valioso es que plantea una nueva forma de entender la guerra moderna, algo que podría inspirar a Colombia a desarrollar sus propios espacios de experimentación doctrinal, adaptados a sus capacidades y amenazas.

ORGANIZACIÓN: La forma en que las fuerzas militares se organizan para operar está cambiando rápidamente, y la inteligencia artificial se está convirtiendo en parte fundamental de esa transformación. Un buen ejemplo de ello es el nuevo documento

doctrinal publicado por la Fuerza Aérea de los Estados Unidos en abril de 2025, donde se establecen las bases para integrar la IA en sus operaciones sin perder el control humano sobre las decisiones clave. El enfoque es claro: aprovechar las capacidades de la tecnología para apoyar, no reemplazar, al comandante en el campo de batalla. Esto incluye desde el análisis de información hasta la coordinación entre unidades y el manejo logístico. Esta propuesta no solo es técnica, también es organizativa, ya que implica repensar cómo se estructuran los equipos, cómo se distribuye la información y cómo se responde a escenarios cambiantes (U.S. Air Force, 2025). Para Colombia, esta iniciativa puede servir de guía para fortalecer su estructura militar, adaptándola a los desafíos actuales sin necesidad de grandes inversiones iniciales, pero con una visión clara de futuro.

MATERIAL Y EQUIPO: Uno de los cambios más notorios en el campo de batalla moderno tiene que ver con cómo la tecnología ha empezado a modificar directamente el material y el equipo disponible para las tropas. Un buen ejemplo de esto es lo que está ocurriendo en Ucrania, donde se están usando kits de inteligencia artificial desarrollados por la empresa Auterion para convertir drones convencionales en sistemas de ataque autónomos. Se trata de más de 33 000 módulos que permiten a estos drones identificar y seguir objetivos en movimiento, incluso si hay interferencias electrónicas o el operador pierde contacto visual. Lo interesante no es solo la tecnología en sí, sino la forma en que ha sido integrada rápidamente al equipo ya existente, multiplicando su efectividad sin requerir grandes cambios logísticos (Reuters, 2025). Este tipo de innovación demuestra que la IA no solo mejora la toma de decisiones o la organización, sino que también transforma el mismo material con el que se libra la guerra. Para Colombia, pensar en soluciones similares podría

representar una vía práctica y escalable para fortalecer su capacidad operativa sin depender exclusivamente de grandes plataformas bélicas.

PERSONAL: El gobierno de Estados Unidos ha impulsado millonarias inversiones en inteligencia artificial para modernizar sus fuerzas armadas, lo que ha llevado a empresas como Google, Microsoft, OpenAI, Meta y xAI a integrarse en proyectos militares. Aunque estas alianzas fortalecen la innovación, también generan debates éticos y preocupaciones sobre la concentración de poder y la vulnerabilidad de los sistemas digitales (Pascual, 2025).

INFRAESTRUCTURA: Los ciberataques basados en inteligencia artificial representan una amenaza creciente para la infraestructura de defensa, ya que permiten ataques baratos, difíciles de detectar y capaces de afectar cadenas de suministro críticas. La propuesta central es adoptar defensas proactivas también apoyadas en IA para anticipar y contener estas vulnerabilidades (Antani, 2025).

LIDERAZGO: Ucrania ha reunido una impresionante base de datos de 2 millones de horas de video de drones desde 2022, gracias a su plataforma OCHI que centraliza imágenes de más de 15 000 tripulaciones. Esta enorme fuente de información se utiliza para entrenar modelos de IA capaces de mejorar la identificación de blancos, tácticas de combate y efectividad de sistemas armamentísticos, para la toma de decisiones en el campo de batalla (News Desk, 2024).

ENTRENAMIENTO: Desde hace un par de años, Ucrania viene utilizando las grabaciones de sus drones millones de horas acumuladas no solo para vigilar, sino para enseñar a sistemas inteligentes cómo actuar en plena guerra. Estos videos ayudan a que la inteligencia artificial aprenda a reconocer lo que sucede en el terreno, a distinguir equipos

enemigos y a apoyar decisiones urgentes, casi como si pensara por sí sola. Con este enfoque, los datos dejan de ser simples registros y se convierten en una herramienta clave para ganar ventaja sin necesidad de intervención directa (Sattar, 2024).

MANTENIMIENTO: Utilizando grabaciones reales de zonas de conflicto en Ucrania, una herramienta de inteligencia artificial alcanza un notable 92 % de precisión al predecir el desgaste de las orugas de excavadoras. Esta tecnología permite anticipar el deterioro, ahorrar costes en mantenimiento e incluso adaptar las predicciones a las condiciones más exigentes, asegurando que el equipo siga operativo aun en entornos difíciles (GatorTrack, 2025)

Hoy la guerra no solo se libra con armas, sino también con ideas. El dominio cognitivo busca influir en cómo piensa y siente una población. A través del análisis de grandes volúmenes de datos, como redes sociales o noticias, se diseñan mensajes que moldean percepciones y decisiones. Esta estrategia silenciosa permite ganar sin disparar, afectando directamente la voluntad del adversario.

La noopolítica, concepto desarrollado por Arquilla y Ronfeldt en los años noventa, plantea que el poder contemporáneo se desplaza del dominio físico hacia la gestión de narrativas, percepciones y conciencias colectivas (Arquilla & Ronfeldt, 1999). Esta estrategia se articula con la Big Data, que permite anticipar emociones y comportamientos sociales, y con la Noosfera, concebida como el espacio de batalla cognitiva donde proliferan *fake news*, *deepfakes* y guerras narrativas (Lévy, 1997; Morin, 1999).

La combinación entre IA y Big Data potencia estas dinámicas, posibilitando la creación de mensajes personalizados con alto impacto político y social, como evidenció el

caso de Cambridge Analytica (Zuboff, 2019). Sin regulación ética, este tipo de prácticas puede derivar en formas de control social cercanas al totalitarismo digital.

Un ejemplo actual se observa en la guerra en Ucrania, donde tanto Rusia como Ucrania emplean campañas digitales, bots y narrativas emocionales para moldear la opinión global y legitimar sus posiciones en el escenario internacional (Pomerantsev, 2019; Törnberg, 2022).

Inteligencia artificial en el Ejército de Colombia a la luz del modelo del ejército ucraniano

Enfrentar una guerra de sexta generación representa un gran reto para las Fuerzas Militares de Colombia, ya que, para adaptarse al actual entorno multidominio, Carlos Álvarez, en el seminario "*Fuerzas Armadas ante las amenazas en un entorno operativo complejo*", sugiere la necesidad de combatir en múltiples frentes simultáneamente. Esto se lograría mediante el uso de la supervelocidad y la superinteligencia para desbordar al adversario como estrategia de derrota. Su propuesta se basa en el empleo de recursos económicos y versátiles que permitan la integración de pequeños sistemas no tripulados, conformando un binomio entre máquina y equipo con intuición estratégica. Este enfoque facilitaría la realización de ataques simultáneos con el objetivo de provocar el colapso del sistema enemigo. Además, al entorno caracterizado por Volatilidad, Incertidumbre, Complejidad y Ambigüedad (VICA), se le añade el concepto de hiperconectividad (VICAH). En este contexto, Álvarez concluye que las Fuerzas Militares no solo requieren

una transformación tecnológica, sino también una revolución en su forma de pensar (Álvarez, 2023).

En el caso de Colombia, la filtración de estos archivos tuvo repercusiones significativas, ya que la Comisión de la Historia del Conflicto y sus Víctimas utilizó esta información en el informe de Renán Vega Cantor. En dicho documento, se afirmaba que la Agencia Central de Inteligencia (CIA) habría instruido a militares colombianos en técnicas de tortura y desaparición forzada (Vega, 2015). Estas declaraciones pusieron en entredicho la legalidad de las acciones de la fuerza pública y, en consecuencia, afectaron su credibilidad y efectividad.

Aunque Colombia ha trabajado en fortalecer la ciberseguridad y la ciberdefensa desde la década de 2010, solo recientemente ha logrado delimitar los roles y conceptos necesarios para enfrentar la ciberguerra y los ciberdelitos de manera efectiva (Ospina & Sanabria, 2020).

En lo que respecta a la ciberguerra, los ataques cibernéticos representan una amenaza crítica para la seguridad nacional. Por esta razón, el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional, la Policía y el Grupo de Emergencias Cibernéticas de Colombia (ColCERT) han unido esfuerzos para prevenir incidentes que puedan poner en riesgo la soberanía del país (Ospina & Sanabria, 2020).

Por otro lado, en el ámbito de los ciberdelitos y el cibercrimen, la Policía Nacional ha liderado la lucha contra estas amenazas, las cuales se han manifestado en diversas formas, como la clonación de tarjetas SIM, el vishing (robo de información financiera), el carding (compraventa ilegal de datos bancarios), las transacciones ilícitas en internet, la

Escuela Superior de Guerra “General Rafael Reyes Prieto”

Bogotá D.C., Colombia

distribución de pornografía infantil, el skimming (fraude en cajeros automáticos) y la suplantación de identidad de ejecutivos, clientes y proveedores mediante el uso de inteligencia artificial para realizar transferencias de dinero de manera fraudulenta (Ospina & Sanabria, 2020).

Observando lo anterior, la guerra de 6ª generación abarca todos los escenarios posibles de daño mutuo, desde transmisiones de noticias o robo de información en Twitter o X, hasta ataques físicos con misiles hipersónicos o enjambres de drones kamikaze por aire, por tierra o por mar. Ante estos avances tecnológicos, el ejército colombiano no está preparado ya que necesita el apoyo del gobierno y obviamente la falta de apoyo del gobierno creo que representa un gran desafío para las fuerzas armadas. Otra cosa es que Colombia pueda prepararse para esta guerra con la ayuda de otros países como Corea del Sur al frente de sus tropas y podemos ver ejemplos que se pueden ver en guerras como la del Mar de China Meridional o Rusia y Ucrania (Barrero-Barrero & Alvarez-Calderon, 2022).

La oportunidad para que las fuerzas armadas colombianas participen en una guerra de sexta generación existe porque las fuerzas armadas como Corea del Sur son socios globales de la OTAN y pueden aprender de las guerras que libran. Para enfrentar los nuevos desafíos de seguridad y conflicto, es indispensable que se evolucione hacia los principios de la **sexta generación de guerra**, donde el dominio cognitivo, la tecnología y la adaptación estratégica son esenciales.

El Ejército de Colombia enfrenta el desafío de adaptarse a una guerra moderna donde la tecnología y la información juegan un papel decisivo. La experiencia del Ejército ucraniano y el enfoque estadounidense del “empleo de combate ágil” muestran cómo la

inteligencia artificial puede ser clave para anticiparse al enemigo, mover recursos con rapidez y tomar mejores decisiones. Colombia, aunque limitada por recursos y políticas, tiene la oportunidad de iniciar este camino aprovechando herramientas de IA accesibles, como PROMPTs bien diseñados. Esto permitiría fortalecer la toma de decisiones, mejorar las operaciones y enfrentar amenazas en un entorno cada vez más cambiante y conectado (coronel Benjamin Buzz Hagardt & Aérea de EUA, 2025).

A partir del modelo ucraniano analizado en esta investigación, una de las propuestas aplicables a las operaciones militares en Colombia consiste en incorporar herramientas de análisis predictivo mediante algoritmos de aprendizaje automático. Esta tecnología permitiría anticipar escenarios operacionales y realizar simulaciones de conflictos con mayor precisión y agilidad en la toma de decisiones. Sin embargo, para su implementación sería necesario adquirir software especializado, ofrecido por empresas del sector tecnológico. Estos sistemas suelen tener costos elevados, lo que limitaría su disponibilidad para todos los comandantes de unidad, representando un desafío logístico y presupuestal para su adopción generalizada en las Fuerzas Militares. Por ejemplo, al integrar datos históricos con información de inteligencia actual, sería posible anticipar los resultados de los distintos cursos de acción durante el proceso de planeamiento operacional, lo que fortalecería significativamente la toma de decisiones. Por otra parte, el uso de **inteligencia artificial mediante software de acceso libre** podría, al menos en una fase inicial, satisfacer algunas de las necesidades del Ejército Nacional de Colombia, permitiendo conceptualizar y explorar el potencial de esta tecnología. En este contexto, la capacidad de procesar millones de datos para apoyar decisiones estratégicas podría ser alcanzada a través de herramientas impulsadas por IA. Como propuesta, se sugiere el uso de un *prompt*

Escuela Superior de Guerra “General Rafael Reyes Prieto”

Bogotá D.C., Colombia

diseñado para orientar ese análisis: (Es el texto inicial que guía o condiciona la salida de un modelo de lenguaje. Puede incluir preguntas, instrucciones, ejemplos o estructuras para obtener resultados específicos) (OpenAI, 2024) para poder analizar millones de datos en el planeamiento para la conducción de operaciones militares o también para análisis de los mismos datos que generen cursos de acción en las operaciones de información. Un Prompt de calidad incluye:

- Contexto u objetivo claro, dar fondo y propósito (qué quieres lograr, y para quién) ayuda al modelo a entender el marco de la tarea una tarea u objetivo claro.
- Precisión y estructura, usa lenguaje directo, define formato, longitud, tono y estilo deseados.
- Ejemplos o “few-shot prompting”, incluir uno o varios ejemplos guía al modelo en el estilo y contenido esperado.
- Chain-of-thought (razonamiento paso a paso) indica que el modelo desarrolle su razonamiento en pasos para respuestas más profundas y acertadas.
- Asignar roles específicos, pide al modelo que actúe como un experto, profesor, traductor, etc., para dar el tono y enfoque adecuados.
- Interacción y refinamiento, reescribe, prueba y ajusta continuamente hasta optimizar la respuesta.

Teniendo en cuenta las cualidades previamente mencionadas del uso de *prompts*, y empleando el software ChatGPT 4.0, se formuló la siguiente consulta:

Pregunta a GPT: redacte un párrafo de manera formal o científica de cómo se usa la IA en las operaciones militares del Ejército Ucraniano en la guerra contra Rusia en el 2025,

desde la perspectiva de un comandante de operaciones de información del Ejército ucraniano, empleando formato APA. En menos de un segundo se obtuvo la siguiente respuesta:

Desde la perspectiva de las operaciones de información del Ejército de Ucrania, la inteligencia artificial (IA) ha transformado radicalmente el entorno operacional en el conflicto contra la Federación Rusa en el año 2025. La IA se ha integrado en sistemas de comando y control, análisis de inteligencia en tiempo real y procesos automatizados de toma de decisiones, permitiendo una respuesta más ágil, precisa y adaptativa frente a las amenazas híbridas y cinéticas del adversario. Herramientas de IA aplicadas al análisis de grandes volúmenes de datos —incluyendo imágenes satelitales, comunicaciones interceptadas y patrones de comportamiento en redes sociales— han optimizado la identificación de objetivos prioritarios, la evaluación del terreno y la anticipación de movimientos enemigos. Además, los sistemas de aprendizaje automático contribuyen a la defensa cibernética y a la gestión de operaciones psicológicas orientadas a influir en la percepción del enemigo y de la población civil en zonas de combate. Estas capacidades son fundamentales para sostener la superioridad informativa y garantizar la interoperabilidad entre unidades de combate y estructuras de mando (Ministry of Digital Transformation of Ukraine, 2023; NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE], 2024).

Referencias (formato APA 7):

Ministry of Digital Transformation of Ukraine. (2023). Strategy for Artificial Intelligence Development in Ukraine. <https://digitalstrategyua.gov.ua>

NATO CCDCOE. (2024). AI and Cyber Capabilities in Modern Warfare: A Case Study on Ukraine. <https://ccdcoe.org/research> (Chatgpt, 2025).

Las respuestas podrían ser más efectivas, objetivas y funcionales cuando se emplean bien el PROMPT o la calidad del PROMPT.

Otro ejemplo empleando el software gratuito para analizar millones de datos puede ser:

Pregunta a GPT: Teniendo en cuenta las noticias que existen en la red sobre Ucrania, redacte un párrafo donde se presente una propuesta sobre cómo se puede emplear la IA en las operaciones de información en Colombia, desde la perspectiva táctica de un comandante de batallón, empleando formato Apa. La respuesta del GPT en menos de un segundo fue:

Como comandante de batallón, propongo implementar un sistema de inteligencia artificial aplicado a las operaciones de información en el Ejército Nacional de Colombia, inspirado en la experiencia ucraniana en 2025. Este sistema integraría herramientas de detección y respuesta automáticas de desinformación, similares a Ucrania con plataformas como Osavul y Mantis Analytics, que identifican patrones de propaganda y activan contramensajes en tiempo real (Global Governance, 2024). Asimismo, se podría desarrollar un centro de inteligencia geoespacial acelerada, usando algoritmos de reconocimiento de objetivos a partir de imágenes satelitales y fuentes abiertas, replicando modelos como Delta o la integración con Palantir’s MetaConstellation (CSIS, 2024). Adicionalmente, se recomienda la capacitación de personal operativo en el uso táctico de IA para fortalecer nuestras unidades de comunicaciones e inteligencia electrónica, adoptando marcos regulatorios de uso responsable como la Declaración Política sobre IA militar (CSIS, 2024; State

Department, 2023). Esta estrategia fortalecería la capacidad del batallón para anticiparse a narrativas adversas, mejorar la coordinación con los escalones superiores y contribuir a la protección de la soberanía informativa del país. (Chatgpt, 2025).

En este sentido y observando cómo una IA de acceso gratuito hace un análisis de BIG DATA para facilitar el planeamiento de las operaciones militares, se propone en este artículo, el diseño y aplicación de *prompts* en aplicaciones de IA de uso exclusivo del Ejército de Colombia, como herramienta para el análisis eficiente de grandes volúmenes de datos a partir del modelo **DOMPILEM**, lo que permitiría identificar que podría ser más útil en cada componente de combate y como podría transformarse la información dispersa en decisiones estratégicas más precisas considerando los diferentes dominios de la guerra.

Recomendaciones

Desarrollar una doctrina nacional de inteligencia artificial aplicada a la defensa.

Es necesario que el Ejército de Colombia, en conjunto con el Ministerio de Defensa, formule un documento doctrinal que establezca lineamientos claros sobre el uso de IA en operaciones militares. Esta doctrina debe inspirarse en modelos como el caso ucraniano, pero adaptada a las condiciones del entorno colombiano y a las amenazas específicas que enfrenta el país.

Fortalecer la formación y capacitación del personal militar.

La IA requiere operadores y comandantes capacitados en su uso. Se recomienda implementar programas de entrenamiento que incluyan el diseño de prompts, el análisis de Big Data y la operación de sistemas de apoyo a la decisión. Estos programas deben integrarse en la formación básica, avanzada y de Estado Mayor.

Impulsar proyectos piloto de IA en operaciones reales.

Antes de su adopción masiva, se sugiere implementar pruebas controladas en brigadas o batallones específicos, utilizando software de acceso libre o convenios con universidades y empresas tecnológicas. Estos pilotos permitirían evaluar ventajas y limitaciones, generando lecciones aprendidas aplicables a una expansión progresiva.

Establecer alianzas estratégicas internacionales.

Siguiendo el modelo de Ucrania, Colombia debe buscar cooperación tecnológica con países y organizaciones aliados. Estas alianzas pueden facilitar la transferencia de conocimiento, el acceso a plataformas digitales y la capacitación de personal. Al mismo tiempo, se recomienda fomentar la innovación nacional mediante convenios con centros de investigación y universidades.

Priorizar la ciberdefensa y el dominio cognitivo.

Se recomienda crear unidades especializadas en operaciones de información apoyadas por IA, capaces de anticipar, detectar y neutralizar campañas de desinformación que afectan la confianza ciudadana en las instituciones. En paralelo, se debe fortalecer la infraestructura de ciberseguridad para proteger datos estratégicos y sistemas críticos.

Invertir en innovación y desarrollo local.

Para reducir la dependencia de proveedores externos, Colombia debe incentivar el

desarrollo de software y soluciones de IA propias. Esto no solo permitirá adaptarse mejor a las condiciones del país, sino también generar un ecosistema tecnológico nacional con aplicaciones duales, tanto militares como civiles.

Incorporar la IA en el modelo DOMPILEM.

Se sugiere integrar proyectos de IA en cada componente del modelo: doctrinal (manuales de empleo), organizacional (reestructuración de unidades), material (drones autónomos), personal (capacitación), infraestructura (centros de datos), liderazgo (cultura de innovación), entrenamiento (simuladores) y mantenimiento (logística predictiva).

Emitir una directiva del Comando Superior.

Finalmente, es imprescindible que el Comando del Ejército emita una directiva institucional que oficialice la adopción progresiva de la IA como política de Estado Mayor. Este documento garantizaría continuidad en el tiempo, más allá de cambios de gobierno o coyunturas presupuestales.

Conclusiones

El análisis realizado sobre el empleo de la inteligencia artificial en las operaciones militares, tomando como referencia el caso del Ejército de Ucrania entre 2022 y 2024, permite extraer lecciones significativas para el Ejército de Colombia. En primer lugar, se confirma que la guerra contemporánea, enmarcada en los conceptos de quinta y sexta generación, desborda los esquemas tradicionales centrados en el uso exclusivo de medios convencionales. Hoy, los dominios cognitivo, informacional y cibernético se han convertido en escenarios tan determinantes como el terrestre, marítimo y aéreo. El conflicto en Ucrania evidencia que la incorporación de algoritmos, sistemas de análisis predictivo y

plataformas de información en tiempo real puede equilibrar la balanza incluso frente a adversarios con mayores capacidades bélicas.

En el caso ucraniano, la capacidad de procesar millones de datos provenientes de sensores, satélites, redes sociales y fuentes abiertas permitió anticipar movimientos del enemigo y maximizar la eficiencia de recursos limitados. Esto demuestra que la inteligencia artificial, más allá de ser un recurso tecnológico, se constituye en un multiplicador de fuerza que permite optimizar la toma de decisiones en ambientes de alta incertidumbre. La experiencia ucraniana también revela que la IA no actúa de forma aislada: requiere de una doctrina que la respalde, de una organización que la incorpore en todos sus niveles, de un personal capacitado y de un liderazgo que asuma la innovación como prioridad estratégica.

Colombia enfrenta un escenario particular. El Ejército Nacional, tras décadas de guerra irregular contra actores armados no estatales, posee experiencia en operaciones de contrainsurgencia, control territorial y lucha contra amenazas híbridas. Sin embargo, estas fortalezas deben complementarse con una visión de futuro que incorpore la inteligencia artificial como herramienta transversal en todas las funciones de combate. La realidad nacional muestra rezagos en materia de modernización tecnológica, dependencia de presupuestos limitados y una cultura organizacional aún apegada a modelos del pasado. Esta situación demanda una transformación cultural y doctrinal que vaya más allá de la simple adquisición de equipos: se trata de adoptar un nuevo modo de concebir la guerra.

Las guerras de sexta generación plantean desafíos que Colombia no puede ignorar. El dominio cognitivo, entendido como la capacidad de influir en percepciones y narrativas, está siendo empleado por actores al margen de la ley mediante campañas de desinformación en redes sociales. El ciberespacio, por su parte, ya constituye un campo de

batalla donde se disputan no solo datos estratégicos, sino también la confianza institucional de la ciudadanía. La integración de la inteligencia artificial en estos escenarios permitiría al Ejército colombiano anticipar amenazas, neutralizar operaciones de influencia adversaria y proteger la soberanía informativa del país.

Un hallazgo central de esta investigación es que la IA no reemplaza al ser humano, sino que potencia sus capacidades. El modelo ucraniano muestra que los algoritmos funcionan como apoyo al comandante, facilitando decisiones rápidas y fundamentadas en datos. En Colombia, donde la efectividad militar está en debate, la IA puede convertirse en un aliado para garantizar disciplina, rigor y precisión en la planificación y ejecución de operaciones. Esto es particularmente relevante en el marco del modelo DOMPILEM, que permite identificar vacíos en doctrina, organización, material, personal, infraestructura, liderazgo, entrenamiento y mantenimiento.

Asimismo, la comparación entre Ucrania y Colombia evidencia la importancia de la interoperabilidad. El Ejército ucraniano logró integrar herramientas tecnológicas con el respaldo de sus aliados internacionales, consolidando un ecosistema de cooperación. Para Colombia, fortalecer las alianzas estratégicas con socios como la OTAN, Corea del Sur o Estados Unidos puede ser decisivo para acceder a tecnologías de vanguardia y procesos de capacitación especializados. No obstante, esta cooperación debe adaptarse a la realidad nacional, evitando la dependencia excesiva y promoviendo el desarrollo de capacidades locales.

Finalmente, se concluye que el Ejército de Colombia está en una encrucijada histórica. Mantenerse en modelos del pasado implica el riesgo de quedar rezagado en un escenario regional y global donde la guerra se transforma de manera acelerada. En

contraste, adoptar la inteligencia artificial de forma progresiva y estructurada representa la posibilidad de fortalecer la seguridad nacional, proteger la soberanía y garantizar la adaptabilidad frente a las amenazas del futuro. La clave estará en asumir la IA no solo como tecnología, sino como un cambio cultural, doctrinal y estratégico que redefina la forma en que Colombia concibe la guerra y la defensa de su Nación.

Referencias

Álvarez, C., Santafé, J., & Urbano, O. (2022). *Methamorphosis Bellum*.

¿Mutando a guerras de Quinta Generación? (Desafíos y Nuevos

Escenarios de La Seguridad Multidimensional En El Contexto Nacional,

Regional y Hemisférico En El Decenio 2015 - 2025).

<https://esdeglibros.edu.co/index.php/editorial/catalog/download/27/23/1627?inline=1>

Álvarez, C., & Ramírez, Y. (2020). La cuarta revolución y la era de la

inteligencia artificial: implicaciones en la seguridad y el trabajo. In Y.

Rico, D. López, & A. Cerón (Eds.), *Enfoques y gestión en seguridad*

integral. Escuela de Posgrados Fuerza Aérea Colombiana.

<https://doi.org/https://doi.org/10.8667/9789585996199.08>

Álvarez, C. (2023, fecha). *Fuerzas Armadas ante las amenazas en un entorno operativo complejo* [Ponencia]. Seminario interno, Escuela Superior de

Guerra, Bogotá, Colombia. Comunicación personal.

Antani, S. (2025, 15 de agosto). *How AI-powered cyberattacks are challenging national defense infrastructure*. TechRadar Pro.

https://www.techradar.com/pro/how-ai-powered-cyberattacks-are-challenging-national-defense-infrastructure?utm_source=chatgpt.com

Arquilla, J., & Ronfeldt, D. (1999). *The emergence of noopolitik: Toward an American information strategy*. RAND Corporation.

Barrero-Barrero, D., & Alvarez-Calderon, C. E. (2022). Mutación de la guerra y amenazas contemporáneas en el multidominio criminal y terrorista.

Revista Científica General José María Córdova, 20(39), 549–570.

<https://doi.org/10.21830/19006586.1024>

Coronel Benjamin Buzz Hagar dt, T., & Aérea de EUA, F. (2025). *La inteligencia artificial y el empleo de combate ágil Teniente coronel Benjamin «Buzz» Hagar dt, Fuerza Aérea de EUA*. 31–43.

De Santayana, J. P. (2024). *La inteligencia artificial y la guerra de Ucrania*. *Cuadernos de Estrategia* (Núm. 226), 87–104. Instituto Español de Estudios Estratégicos (IEEE).

Freedman, L. (2019). *La guerra futura. Un estudio sobre el pasado y el presente*. Crítica.

García Sánchez, M. D. (2020). *Inteligencia artificial y oportunidad de creación de una personalidad electrónica*. *Ius et Scientia*, 6(2), 83-95.

<https://doi.org/10.12795/IETSCIENTIA.2020.i02.07>

GatorTrack. (2025, febrero). *Predicción del desgaste de las orugas de excavadoras basada en IA: 92 % de precisión con datos de campo de la zona de conflicto de Ucrania*. GatorTrack Noticias.

https://www.gatortrack.com/es/news/ai-driven-excavator-track-wear-prediction-92-accuracy-with-ukraine-conflict-zone-field-data/?utm_source=chatgpt.com

Hernández, I. (2005). *Estética, ciencia y tecnología: creaciones electrónicas y numéricas*. Javegraf Pontificia Universidad Javeriana.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. del P. (2014). *Metodología de la Investigación* (M. G. Hill (ed.); Sexta edición).

HuffPost. (2024, 4 de junio). *Zeus provoca una transformación única en el ejército español*. <https://www.huffingtonpost.es/sociedad/zeus-transformacion-digital-ejercito-espanol.html>

Lévy, P. (1997). *Collective intelligence: Mankind's emerging world in cyberspace*. Perseus Books.

Morin, E. (1999). *La cabeza bien puesta: Repensar la reforma, reformar el*

pensamiento. Seuil.

News Desk. (2024, 20 de diciembre). *Ukraine collects 2 million hours of drone footage to train AI for battlefield decisions*. Tribune (Reuters).

Recuperado de https://tribune.com.pk/story/2517256/ukraine-collects-2-million-hours-of-drone-footage-to-train-ai-for-battlefield-decisions?utm_source=chatgpt.com

OpenAI. (2024). *ChatGPT* (versión GPT-4) [Modelo de lenguaje de gran escala]. <https://chat.openai.com/>

OpenAI. (2025). *ChatGPT* (versión GPT-4) [Modelo de lenguaje de gran escala]. <https://chat.openai.com/>

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

Pascual, M. G. (2025, 21 de julio). *Las grandes tecnológicas se lanzan al negocio de la guerra: así se militariza Silicon Valley*. El País.

Pomerantsev, P. (2019). *This is not propaganda: Adventures in the war against reality*. PublicAffairs.

Reuters. (2025, July 28). *Auterion says it will provide Ukraine with 33,000 AI drone guidance kits*. <https://www.reuters.com/business/aerospace->

[defense/auterion-says-it-will-provide-ukraine-with-33000-ai-drone-guidance-kits-2025-07-28/](#)

Sattar, M. (2024, julio 18). *Ukraine collects 2 million hours of drone footage to train AI for battlefield decisions*. The Express Tribune.

<https://tribune.com.pk/story/2517256/ukraine-collects-2-million-hours-of-drone-footage-to-train-ai-for-battlefield-decisions>

Törnberg, P. (2022). Echo chambers and viral misinformation: Modeling fake news as complex contagion. *PLOS ONE*.

Tsotniashvili, Z. (2024). Silicon Tactics: Unravelling the Role of Artificial Intelligence in the Information Battlefield of the Ukraine Conflict. *Asian Journal of Research*, 1–3, 54–65. <https://doi.org/10.37057/2433-202x>

U.S. Air Force. (2025, April 12). *Air Force releases new doctrine note on artificial intelligence to guide future operations*.
<https://www.aetc.af.mil/News/Article-Display/Article/4153064/air-force-releases-new-doctrine-note-on-artificial-intelligence-to-guide-future/>

Vega Cantor, R. (2015). *La dimensión internacional del conflicto social y armado en Colombia: injerencia de los Estados Unidos, contrainsurgencia y terrorismo de Estado*. En Comisión Histórica del Conflicto y sus Víctimas, *Informe final*. Bogotá: Comisión Histórica del

Conflicto y sus Víctimas.

WHINSEC. (2017, septiembre). F102: Joint and Army Capability

Development – Lectura F102RA. Curso de Comando y Estado Mayor
para Oficiales. Fort Benning, GA: Western Hemisphere Institute for
Security Cooperation.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human
future at the new frontier of power*. PublicAffairs.