

# Más allá del poder de fuego: aplicaciones de la IA en el conflicto ruso-ucraniano y su impacto en la defensa nacional

Denisse Olguín Arias<sup>1</sup>

## Resumen:

*El conflicto entre Rusia y Ucrania ha representado un punto de inflexión en el uso contemporáneo de tecnologías de inteligencia artificial (IA) aplicadas a operaciones militares. Esta confrontación ha demostrado cómo la IA puede transformar las tácticas y estrategias en el campo de batalla, desde el uso de drones autónomos para reconocimiento y ataques hasta la implementación de sistemas de guerra electrónica basados en IA para interferir en las comunicaciones enemigas. Asimismo, ha cobrado relevancia el uso del deep learning en el análisis de inteligencia, especialmente en áreas como el procesamiento de imágenes satelitales, la automatización logística y la ciberdefensa. Este artículo examina el impacto de estas tecnologías en el desarrollo de la guerra, contrastando su aplicación en este conflicto y extrayendo aprendizajes clave para fortalecer la defensa en países como Chile.*

## Abstract:

*The conflict between Russia and Ukraine has marked a turning point in the modern use of artificial intelligence (AI) technologies in military operations. This confrontation has demonstrated how AI can transform battlefield tactics and strategies from the deployment of autonomous drones for reconnaissance and strikes to the implementation of AI-driven electronic warfare systems designed to disrupt enemy communications. The use of deep learning in intelligence analysis has also gained prominence, particularly in areas such as satellite image processing, logistical automation,*

1 Ingeniera en Automatización y Robótica de la Universidad Andrés Bello, Máster en Ingeniería Aeronáutica de la Universidad Técnica Federico Santa María. Investigadora de Electrónica y TIC's en el Centro de Estudios en Ciencia y Tecnología de la Academia Politécnica Militar (CECTAP) del Ejército de Chile y docente de la misma Unidad.



### Palabras clave

Inteligencia artificial  
Guerra ruso-ucraniana  
Drones autónomos  
Guerra electrónica  
Deep Learning

### Keywords

Artificial intelligence  
Russia-Ukraine war  
Autonomous Drones  
Electronic Warfare  
Deep Learning



and cyber defense. This article examines the impact of these technologies on the development of the conflict, contrasting their application in this context and drawing key lessons to strengthen national defense in countries such as Chile.

## Introducción

La guerra entre Rusia y Ucrania, que comenzó en febrero de 2022 con la invasión a gran escala por parte de Rusia, constituye un hito en el desarrollo de conflictos bélicos contemporáneos. Este enfrentamiento no solo es el resultado de años de tensiones políticas y militares, incluidos eventos clave como la anexión de Crimea por parte de Rusia en 2014 y la guerra en el este de Ucrania en las regiones de Donetsk y Luhansk, sino que también ha sido un escenario crucial para la implementación de tecnologías avanzadas en el campo de batalla.<sup>2</sup> En particular, la inteligencia artificial (IA) ha desempeñado un papel fundamental, transformando las tácticas y estrategias militares.

A lo largo de este conflicto, se ha evidenciado cómo la IA puede ser aplicada de manera significativa en diversas áreas, desde la automatización de drones hasta el análisis de inteligencia utilizando técnicas de *deep learning*.<sup>3</sup> Del mismo modo la guerra ha subrayado la creciente importancia de la defensa cibernética y la logística automatizada en un contexto de combate de alta intensidad, lo que demuestra la evolución del conflicto armado hacia un dominio tecnológico cada vez más sofisticado.

Este artículo tiene como objetivo analizar cómo la IA ha sido aplicada en la guerra ruso-ucraniana y extraer lecciones relevantes para la defensa de países como Chile. En esta ocasión se abordarán temas como el uso de drones autónomos, sistemas de guerra electrónica basados en IA, análisis de inteligencia mediante *deep learning* y la automatización en la logística y la defensa cibernética.

## Drones autónomos para reconocimiento y ataques

Uno de los aspectos más innovadores y decisivos del conflicto ruso-ucraniano ha sido la incorporación de drones autónomos equipados con IA para tareas tanto de reconocimiento como de ataque. Estos sistemas no tripulados pueden operar de manera semi o completamente autónoma, procesando datos en tiempo real, identificando objetivos y tomando decisiones operativas sin necesidad de intervención humana directa.<sup>4</sup> Esto ha redefinido el paradigma del combate moderno al reducir la necesidad de presencia humana en zonas de alto riesgo.

Un ejemplo destacado ha sido el uso, por parte de Ucrania, del Bayraktar TB2,<sup>5</sup> un dron táctico turco de mediano alcance que ha demostrado

2 KRAMPE, Oliver. The Ukraine war and the international order. *International Politics*, 61(1), 2024, pp. 120.

3 *Deep learning* es un subcampo del aprendizaje automático que utiliza redes neuronales artificiales con múltiples capas para modelar representaciones complejas de datos, aprendiendo a partir de grandes volúmenes de información y se utilizan ampliamente en tareas como el reconocimiento de voz, visión por computadora y el procesamiento del lenguaje natural.

4 SCHARRE, Paul. "Four Battlegrounds: Power in the Age of Artificial Intelligence". W.W. Norton & Company. Capítulo 22: "Robotics Row". 2023. Véase también en HERN, Alex. "AI's 'Oppenheimer Moment': Autonomous Weapons Enter the Battlefield". *The Guardian*. 2024, [en línea]. Disponible en: <https://www.theguardian.com/technology/article/2024/jul/14/ais-oppenheimer-moment-autonomous-weapons-enter-the-battlefield>

5 El Bayraktar TB2 es un dron táctico turco fabricado por Baykar con 6,5 m de largo, 12 m de envergadura y 700 kg de peso máximo. Tiene una autonomía de hasta 72 horas, un enlace operativo de 150 km y puede cargar hasta 150 kg en sensores y armamento.

una eficacia significativa en la destrucción de vehículos blindados, baterías antiaéreas y centros de comando rusos<sup>6</sup> (véase figura N°1). Estos sistemas no solo han sido valiosos por su precisión, sino también por su bajo costo relativo frente a las plataformas tradicionales tripuladas.<sup>7</sup>



Figura N°1. Bayraktar TB2, el dron táctico turco de mediano alcance.

**Fuente:** [https://militaryuv.com/equipment/ucav/bayraktar\\_tb2](https://militaryuv.com/equipment/ucav/bayraktar_tb2)

La incorporación de IA permite a los drones analizar imágenes satelitales, patrones térmicos, señales electromagnéticas y otras fuentes de datos para mejorar la detección y clasificación de blancos. Por otra parte, los algoritmos de aprendizaje automático permiten que los drones aprendan de sus misiones anteriores, incrementando progresivamente su eficiencia operativa.<sup>8</sup> Esta capacidad ha sido particularmente útil para evitar sistemas rusos de interferencia y defensa electrónica.

Otro desarrollo crucial ha sido el uso de enjambres de drones autónomos, donde múltiples unidades cooperan como un sistema distribuido para realizar misiones coordinadas, tales como ataques simultáneos a varios blancos, reconocimiento en profundidad o saturación de defensas enemigas (véase figura N°2). Esta táctica ha ofrecido a Ucrania una ventaja táctica frente a un adversario con superioridad numérica y tecnológica en varios frentes.<sup>9</sup>



Figura N°2: Operador militar pasa junto a los drones de reconocimiento DJI Matrice 300, establecido para vuelos de prueba en la región de Kiev el 2 de agosto de 2022, antes de ser enviados al frente.

**Fuente:** <https://www.theatlantic.com/photo/2023/05/photos-ukraine-war-drones/674160/>

La efectividad de estos sistemas ha resaltado la importancia de la IA en la guerra moderna. Los drones autónomos han permitido ejecutar operaciones de precisión con menor riesgo para las tropas, al tiempo que han dificultado la defensa para fuerzas convencionales, acostumbradas

- 6 DEVORE, Mark. "Winning by Outlasting The United States and Ukrainian Resistance to Russia". Military Review, Army University Press. 2022, [en línea]. Disponible en: <https://www.armyupress.army.mil/journals/military-review/online-exclusive/2022-ole/devore/>
- 7 MACCABELLIO, Pietro. Are drones a war game changer? The Ukrainian case. Defence Industry Europe. 2023, [en línea]. Disponible en: <https://defence-industry.eu/are-drones-a-war-game-changer-the-ukrainian-case/>
- 8 FREEDBERG, Sydney. The revolution that wasn't: How AI drones have fizzled in Ukraine (so far). Breaking Defense. 20 de febrero de 2024, [en línea]. Disponible en: <https://breakingdefense.com/2024/02/the-revolution-that-wasnt-how-ai-drones-have-fizzled-in-ukraine-so-far/>
- 9 KALLENBORN, Zachary. "InfoSwarms: Drone Swarms and Information Warfare". Parameters 52, núm. 2. 2022, pp. 87–102, [en línea]. Disponible en: <https://press.armywarcollege.edu/parameters/vol52/iss2/13/>

a amenazas tradicionales.<sup>10</sup> Esto representa un cambio estructural en la doctrina militar, en donde la superioridad tecnológica puede compensar asimetrías en recursos humanos y materiales.

La experiencia de Ucrania proporciona lecciones en todos los niveles de la conducción (estratégica, operacional y táctica) relevantes para países como Chile, que están evaluando la modernización de sus fuerzas armadas. Invertir en sistemas autónomos con soporte de inteligencia artificial no solo representa una mejora en la capacidad de reconocimiento y ataque, sino que también puede aumentar la capacidad de respuesta rápida y la resiliencia operacional en escenarios complejos. Además, esto posiciona a los países en desarrollo dentro de las tendencias tecnológicas que están marcando la evolución del poder militar global.<sup>11</sup>

## Sistemas de guerra electrónica basados en IA

Uno de los elementos más destacados del conflicto ruso-ucraniano ha sido el uso intensivo de sistemas de guerra electrónica (EW, por sus siglas en inglés) integrados con capacidades de inteligencia artificial. Estos sistemas no solo son capaces de interferir en las comunicaciones enemigas, sino también de inutilizar drones, alterar la navegación satelital (GPS) y detectar señales

electromagnéticas en tiempo real para su bloqueo automático. Rusia ha empleado plataformas como el Krasukha-4, el Leer-3 y el Zhitel, que han demostrado efectividad tanto en el frente táctico como estratégico al neutralizar redes de comando, control y comunicaciones ucranianas.<sup>12</sup>



Figura N°3. Sistema de guerra electrónica rusa, el Krasukha-4.

**Fuente:** [https://www.elespanol.com/omicron/tecnologia/20220324/krasukha-sistema-aviones-satelites-ucrania-quitado-rusia/659434092\\_0.html](https://www.elespanol.com/omicron/tecnologia/20220324/krasukha-sistema-aviones-satelites-ucrania-quitado-rusia/659434092_0.html).

La inteligencia artificial desempeña un papel central en estos sistemas, ya que permite el análisis autónomo de señales electromagnéticas, la clasificación automática de amenazas y la adaptación dinámica a nuevos patrones de emisión del enemigo. Esta capacidad de aprendizaje continuo (*machine learning*) optimiza la respuesta frente a entornos altamente cambiantes, como los que se presentan en escenarios de guerra híbrida. Según

- 10 SCHARRE, Paul. *Army of None: Autonomous Weapons and the Future of War*. New York: W. W. Norton & Company. Part II: "Autonomous missiles, drones and robot swarms". 2018. Véase también EDMONDS, Jeffrey. A. & BENDETT, Samuel. *Russia's Use of Uncrewed Systems in Ukraine*. CNA Research Memorandum. Marzo de 2023, [en línea]. Disponible en: <https://www.cna.org/reports/2023/05/Russias-Use-of-Uncrewed-Systems-in-Ukraine.pdf>
- 11 KONAIEV, Margarita. "Tomorrow's Technology in Today's War: The Use of AI and Autonomous Technologies in the War in Ukraine and Implications for Strategic Stability". CNA Corporation, September 2023, [en línea]. Disponible en: <https://www.cna.org/reports/2023/10/Use-of-AI-and-Autonomous-Technologies-in-the-War-in-Ukraine.pdf>
- 12 CLARK, Brayan. "The fall and rise of Russian electronic warfare". *IEEE Spectrum*. 12 de octubre de 2023, [en línea]. Disponible en: <https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare> Véase también en LING, Justin. *The invisible RussiaUkraine battlefield*. *Wired*. 23 de diciembre de 2024. [en línea]. Disponible en: <https://www.wired.com/story/electronic-warfare-russia-ukraine>



Pujol,<sup>13</sup> este tipo de tecnologías representa una transición hacia una guerra más cognitiva, en la que la capacidad de aprender más rápido que el adversario se convierte en un factor decisivo.

Un ejemplo significativo ha sido la capacidad de Rusia para degradar de forma continua la conectividad de drones ucranianos como los Bayraktar TB2, interferir con los sistemas Starlink de SpaceX y manipular el espectro radioeléctrico para bloquear el GPS, limitando la eficacia de misiles guiados y unidades de artillería inteligente.<sup>14</sup>

Estos avances ofrecen lecciones para países como Chile que buscan modernizar sus capacidades militares. La incorporación de sistemas de guerra electrónica potenciados por IA permitiría una mayor autonomía en la defensa de infraestructura crítica, así como capacidades de disuasión electrónica en conflictos asimétricos o cibernéticos.

El uso de IA en guerra electrónica puede actuar como un multiplicador de fuerza, permitiendo a ejércitos medianos alcanzar niveles de eficacia tecnológica comparables a los de grandes potencias, especialmente en operaciones conjuntas o de defensa territorial.<sup>15</sup>

La experiencia rusa en este conflicto ha demostrado que los sistemas de guerra electrónica basados en IA no solo aumentan la eficacia táctica, sino que también generan ventajas operacionales sostenidas mediante la superioridad en el dominio electromagnético. Esta evolución resalta la necesidad urgente de integrar capacidades similares en las doctrinas y adquisiciones militares modernas.

## Análisis de inteligencia con *deep learning*

El análisis de inteligencia mediante técnicas de *deep learning* ha sido un componente crucial en el conflicto ruso-ucraniano, evidenciando una transformación en la forma en que se recopila, procesa y utiliza la información táctica y estratégica. Las tecnologías de *deep learning* permiten el procesamiento masivo de datos no estructurados, como imágenes satelitales, señales de radar, audio interceptado y publicaciones en redes sociales. En el caso de Ucrania, estas capacidades han sido clave para detectar movimientos de tropas, anticipar ataques y planificar contraofensivas con mayor precisión y rapidez que con los métodos convencionales.<sup>16</sup>

13 PUJOL, Irene. La guerra cognitiva convierte la mente en campo de batalla. El Financiero. 16 de octubre de 2024, [en línea]. Disponible en: <https://www.elfinanciero.com.mx/opinion/colaborador-invitado/2024/10/16/la-guerra-cognitiva-convierte-la-mente-en-campo-de-batalla/>

14 SEGURA, Cristian. Rusia consigue cortar la comunicación de los satélites Starlink del ejército de Ucrania. El País. 24 de mayo de 2024, [en línea]. Disponible en: <https://elpais.com/internacional/2024-05-24/rusia-consigue-cortar-la-comunicacion-de-los-satelites-starlink-del-ejercito-de-ucrania.html> Véase también en MANLEY, Cameron. USsupplied HIMARS 'completely ineffective' against superior Russian jamming technology. Business Insider. 25 de mayo 2024. [en línea]. Disponible en: <https://www.businessinsider.com/us-himars-completely-ineffective-against-russian-jamming-report-2024-5>

15 MONZÓN Baeza, Víctor; PARADA, Raúl; CONCHA Salor, Laura & MONZÓ, Carlos. AI-Driven Tactical Communications and Networking for Defense: A Survey and Emerging Trends. 2025, [en línea]. Disponible en: <https://arxiv.org/abs/2404.05071> Véase también ARMY UNIVERSITY PRESS. AI as a Combat Multiplier. Military Review – Online Exclusive. 2024, [en línea]. Disponible en: <https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2024-OLE/AI-Combat-Multiplier/>

16 MINISTERIO DE DEFENSA (CESEDEN). "La inteligencia artificial y la guerra de Ucrania". José Pardo de Santayana. 17 de diciembre 2024, [en línea]. Disponible en: [https://www.defensa.gob.es/ceseden/-/la\\_inteligencia\\_artificial\\_y\\_la\\_guerra\\_de\\_ucrania](https://www.defensa.gob.es/ceseden/-/la_inteligencia_artificial_y_la_guerra_de_ucrania). Véase también EUROPEAN Council on Foreign Relations (ECFR). "Star Tech Enterprise: Tecnologías emergentes en la guerra rusa contra Ucrania". 2023, [en línea]. Disponible en: <https://ecfr.eu/madrid/publication/star-tech-enterprise-tecnologias-emergentes-en-la-guerra-rusa-contra-ucrania/>



Un ejemplo concreto es el uso de sistemas de aprendizaje profundo para analizar imágenes satelitales captadas por constelaciones de satélites comerciales como los de Maxar Technologies o Planet Labs. Mediante redes neuronales convolucionales (CNN),<sup>17</sup> Ucrania ha logrado detectar patrones de actividad militar, camuflaje y construcción de infraestructura bélica en tiempo real.<sup>18</sup> Estos análisis han sido combinados con algoritmos de fusión de datos (*data fusion*) que integran señales de inteligencia humana (HUMINT), de señales (SIGINT) y de fuentes abiertas (OSINT), optimizando la toma de decisiones militares.<sup>19</sup>

El *deep learning* también ha sido fundamental en el monitoreo de redes sociales, donde se han utilizado modelos como BERT y GPT para identificar publicaciones que podrían revelar ubicaciones geográficas, movimientos de tropas o campañas de desinformación rusas. De hecho, un informe del Atlantic Council destaca cómo Ucrania ha empleado IA para rastrear nodos de desinformación y automatizar respuestas en campañas de contranarrativa digital, lo que ha sido clave para mantener la cohesión nacional y el apoyo internacional.<sup>20</sup>

Adicionalmente, los sistemas de *deep learning* han sido aplicados en tareas de ciberinteligencia para identificar patrones de ataques de *malware*,

*phishing* o intrusiones en redes de mando y control. Estas herramientas, entrenadas con grandes conjuntos de datos, permiten detectar amenazas cibernéticas antes de que generen daños críticos, lo que representa un nuevo frente de guerra híbrida.<sup>21</sup>

La experiencia ucraniana proporciona lecciones valiosas para otras naciones que buscan modernizar sus capacidades de inteligencia. La inversión en IA aplicada a la defensa puede traducirse en ventajas tácticas significativas, como mayor capacidad de reacción, reducción de la incertidumbre en escenarios bélicos y optimización de recursos mediante una inteligencia más ágil y precisa. Así, el *deep learning* no solo se convierte en una herramienta operativa, sino en un factor decisivo dentro del campo de batalla moderno.

## Automatización en la logística y la defensa cibernética

La guerra ruso-ucraniana ha puesto en evidencia cómo la inteligencia artificial (IA) puede redefinir el ámbito militar, particularmente en dos dimensiones críticas: la logística y la defensa cibernética. En el campo logístico, la automatización mediante algoritmos de IA ha permitido a las Fuerzas Armadas ucranianas gestionar eficientemente el transporte y distribución de suministros, municiones y personal hacia las líneas

17 Las redes neuronales convolucionales son un tipo de red neuronal artificial diseñado para procesar datos de forma jerárquica, particularmente útiles para el reconocimiento de patrones en imágenes. Se utilizan ampliamente para la clasificación de imágenes, el reconocimiento de objetos y la detección de patrones.

18 VAN DER BURG, Erik; TOET Alexander, *et al.* A Convolutional Neural Network as a Potential Tool for Camouflage Assessment. Applied Sciences. 2025, [en línea]. Disponible en: <https://www.mdpi.com/2076-3417/15/9/5066>

19 ABEDIN, Afia; BAIS, Abdul; BUNTAIN, Cody; COURCHESNE, Laura, *et al.* (2024, 13 de diciembre). A Call to Arms: AI Should be Critical for Social Media Analysis of Conflict Zones, [en línea]. Disponible en: <https://arxiv.org/html/2311.00810v2>

20 SOLOPOVA, Veronika. From Trust to Truth: Actionable policies for the use of AI in fact-checking in Germany and Ukraine. 2025, [en línea]. Disponible en: <https://arxiv.org/abs/2503.18724>

21 CHUAN-LONG, Yin; YUE-FEI, Zhu; JIN-LONG, Fei y XIN-ZHENG, He. "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks". IEEE. 2027. vol. 5, pp. 21954-21961, [en línea]. Disponible en: <https://ieeexplore.ieee.org/document/8066291>



del frente. Esto ha sido posible mediante sistemas que integran sensores, aprendizaje automático y análisis predictivo para anticipar necesidades y reducir tiempos de respuesta, incluso en entornos hostiles y cambiantes.<sup>22</sup>

Por ejemplo, plataformas como DELTA, desarrolladas por el Ministerio de Transformación Digital de Ucrania, han sido clave para coordinar la logística de donaciones, transferencias de recursos y movimientos estratégicos durante la guerra, apoyadas por tecnologías de IA para la toma de decisiones basada en datos en tiempo real.<sup>23</sup>

En paralelo, la defensa cibernética ha requerido un uso intensivo de herramientas automatizadas de detección y respuesta ante amenazas. Ucrania ha estado bajo constante ataque de ciberarmas rusas, incluyendo campañas de *malware* como NotPetya y múltiples intentos de sabotaje a su red eléctrica. Frente a ello, los sistemas basados en IA han desempeñado un papel crucial al permitir la detección en tiempo real de patrones anómalos, la contención automática de intrusiones y la orquestación de contramedidas digitales.<sup>24</sup>

Asimismo, el uso de algoritmos de análisis de tráfico en red y aprendizaje profundo ha posibilitado la defensa de infraestructuras críticas como las redes de comunicación, energía y transporte. Una de las iniciativas más destacadas ha sido la colaboración con empresas tecnológicas occidentales para refor-

zar el “*cyber shield*” ucraniano, permitiendo actuar de manera proactiva frente a amenazas cibernéticas con alta sofisticación.<sup>25</sup>

El caso ucraniano ofrece lecciones fundamentales que es necesario observar y analizar con profundidad, siendo especialmente útil para naciones como Chile, que se encuentran en procesos de modernización de sus capacidades militares. Sin duda un desafío importante para el Ministerio de Defensa y nuestras Fuerzas Armadas.

La adopción de soluciones basadas en IA en logística militar no solo aumenta la eficiencia operativa, sino que puede ser determinante para mantener el ritmo táctico frente a escenarios impredecibles. Del mismo modo, la ciberdefensa automatizada es esencial en un entorno digital donde las infraestructuras críticas pueden ser blanco de ataques cibernéticos de Estado, incluso fuera del contexto bélico declarado.<sup>26</sup>

Por tanto, la experiencia de Ucrania representa un precedente útil para diseñar doctrinas nacionales de defensa apoyadas en IA, tanto para responder a amenazas tradicionales como para anticiparse a conflictos híbridos del siglo XXI.

## Conclusiones

La guerra entre Rusia y Ucrania ha marcado un antes y un después en la forma en que se conciben

- 22 KOTT, Alexander; DUBYNSKYI, George; PAZIUK, Andrii; GALAITSI, Stephanie *et al.* Russian cyber onslaught was blunted by Ukrainian cyber resilience, not merely security. 2024, [en línea]. Disponible en: <https://arxiv.org/abs/2408.14667>
- 23 MANTELLASSI, Federico; RICKLI, Jean- Marc. (2024, abril). “The War in Ukraine: Reality Check for Emerging Technologies and the Future of Warfare. Geneva Centre for Security Policy. (Geneva Paper, pp. 34/24), [en línea]. Disponible en: [https://www.researchgate.net/publication/379744204\\_The\\_War\\_in\\_Ukraine\\_Reality\\_Check\\_for\\_Emerging\\_Technologies\\_and\\_the\\_Future\\_of\\_Warfare](https://www.researchgate.net/publication/379744204_The_War_in_Ukraine_Reality_Check_for_Emerging_Technologies_and_the_Future_of_Warfare)
- 24 Microsoft. Defending Ukraine: Early lessons from the cyber war. Microsoft Security Insider. 2022, [en línea]. Disponible en: <https://www.microsoft.com/es-cl/security/security-insider/intelligence-reports/defending-ukraine-early-lessons-from-the-cyber-war>
- 25 RED TEAM ANALYSIS SOCIETY. AI at War (1) – Ukraine. Red Team Analysis Society. 8 de abril 2024, [en línea]. Disponible en: <https://redanalysis.org/2024/04/08/ai-at-war-1-ukraine/>
- 26 KOTT, Alexander; THÉRON, Paul; DRAŠAR, Martin; DUSHKU, Edlira *et al.* (2018). Autonomous Intelligent Cyberdefense Agent (AICA) Reference Architecture. Release 2.0. NATO Research Task Group IST152, [en línea]. Disponible en: <https://arxiv.org/abs/1803.10664>



los conflictos armados modernos, evidenciando el rol protagónico que la inteligencia artificial (IA) puede desempeñar en el campo de batalla. Tecnologías como drones autónomos, sistemas de guerra electrónica basados en IA, herramientas de análisis de inteligencia mediante técnicas de *deep learning*, automatización logística y capacidades de defensa cibernética han sido utilizadas de forma intensiva durante este conflicto, redefiniendo las tácticas y estrategias militares tradicionales.

Este escenario ha demostrado que el poder de fuego ya no es el único determinante del dominio en combate. Hoy, la capacidad de recolectar, procesar y actuar sobre información en tiempo real, así como la habilidad para adaptarse a entornos operacionales cambiantes, son elementos estratégicos esenciales. La guerra entre Rusia y Ucrania ha convertido a la IA en un componente indispensable de la superioridad táctica y operativa.

Para países como Chile, este conflicto representa una fuente valiosa de aprendizajes sobre el papel que las tecnologías emergentes pueden desempeñar en la defensa nacional. En un país con una geografía extensa, zonas de difícil acceso y diversos desafíos fronterizos, el uso de sistemas autónomos basados en IA puede mejorar significativamente la vigilancia territorial, la capacidad de respuesta rápida y el control de espacios críticos, tanto aéreos como marítimos.

La experiencia de Ucrania también pone de manifiesto que, frente a una desventaja en cuanto a número de tropas o equipamiento convencional, las tecnologías inteligentes pueden nivelar el campo de batalla. La automatización de la logística, el mantenimiento predictivo de equipos militares y el uso de sensores inteligentes permiten optimizar recursos, reducir los tiempos de reacción

y aumentar la eficiencia operativa de las Fuerzas Armadas.

En este sentido, para Chile, la adopción de IA en defensa no debe concebirse únicamente como una medida de modernización tecnológica, sino como una necesidad estratégica para asegurar la soberanía nacional en un contexto geopolítico cada vez más competitivo y tecnológicamente sofisticado.

No obstante, esta transformación requiere más que la adquisición de tecnología: demanda el desarrollo de capacidades nacionales mediante inversión en investigación aplicada, cooperación entre las Fuerzas Armadas y la industria tecnológica y la formación de talento humano especializado en áreas como ciberseguridad, robótica e inteligencia artificial.

Sobre lo señalado, el Ministerio de Defensa Nacional, como órgano superior, juega un rol fundamental en incentivar, apoyar, coordinar, articular la modernización de las Fuerzas Armadas en lo específico de cada rama como también bajo una mirada conjunta.

Sin embargo, el uso militar de la IA también plantea desafíos éticos y de seguridad. La posibilidad de que sistemas autónomos tomen decisiones letales sin intervención humana ha encendido debates sobre el control, la moralidad y la responsabilidad en el uso de estas tecnologías. Asimismo, una mayor dependencia de sistemas basados en IA incrementa la vulnerabilidad frente a ciberataques y la manipulación de algoritmos por parte de adversarios. Por ello, cualquier implementación debe estar acompañada de marcos normativos robustos, mecanismos de supervisión y estrategias de ciberdefensa avanzadas.





A nivel global, esta guerra ha consolidado la idea de que el liderazgo militar del futuro estará determinado por la capacidad de innovación tecnológica. Potencias como Estados Unidos y China encabezan la carrera por la supremacía en IA, mientras que regiones como América Latina corren el riesgo de quedar rezagadas. Para Chile, esto implica asumir un compromiso firme con el desarrollo tecnológico en defensa, promoviendo una estrategia nacional integral que vincule al sector público y el ámbito privado.

En definitiva, la guerra ruso-ucraniana nos entrega una advertencia y una oportunidad: la defensa del siglo XXI no solo dependerá del armamento más sofisticado, sino de la capacidad de integrar la tecnología de forma inteligente, ética y estratégica. La IA representa un factor transformador, cuyo verdadero potencial radica en cómo se aplica para proteger los intereses nacionales y fortalecer la seguridad del país, sin perder de vista los principios fundamentales de la humanidad.

## Bibliografía

- ABEDIN, Afia; BAIS, Abdul; BUNTAIN, Cody; COURCHESNE, Laura *et al.* A Call to Arms: AI Should be Critical for Social Media Analysis of Conflict Zones. 13 de diciembre de 2024, [en línea]. Disponible en: <https://arxiv.org/html/2311.00810v2>
- ARMY UNIVERSITY PRESS. "AI as a Combat Multiplier". Military Review – Online Exclusive. 2024, [en línea]. Disponible en: <https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2024-OLE/AI-Combat-Multiplier/>
- CHUAN-LONG, Yin; YUE-FEI, Zhu; JIN-LONG, Fei y XIN-ZHENG, He. "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks". IEEE Access, vol. 5, pp. 21954-21961. 2017, [en línea]. Disponible en: <https://ieeexplore.ieee.org/document/8066291>
- CLARK, Brayan. 12 de octubre 2023. "The fall and rise of Russian electronic warfare". IEEE Spectrum, [en línea]. Disponible en: <https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare>
- DEVORE, Mark. R. Winning by Outlasting The United States and Ukrainian Resistance to Russia. Military Review, Army University Press. 2022, [en línea]. Disponible en: <https://www.armyupress.army.mil/journals/military-review/online-exclusive/2022-ole/devore/>
- EDMONDS, Jeffrey A. & BENDETT, Samuel. Russia's Use of Uncrewed Systems in Ukraine. CNA Research Memorandum. Marzo 2023. Disponible en: <https://www.cna.org/reports/2023/05/Russias-Use-of-Uncrewed-Systems-in-Ukraine.pdf>
- EUROPEAN COUNCIL ON FOREIGN RELATIONS (ECFR). Star'Tech'Enterprise: Tecnologías emergentes en la guerra rusa contra Ucrania. 2023, [en línea]. Disponible en: <https://ecfr.eu/madrid/publication/star-tech-enterprise-tecnologias-emergentes-en-la-guerra-rusa-contra-ucrania/>
- FREEDBERG, Sydney. The revolution that wasn't: How AI drones have fizzled in Ukraine (so far). Breaking Defense. 20 de febrero de 2024, [en línea]. Disponible en: <https://breakingdefense.com/2024/02/the-revolution-that-wasnt-how-ai-drones-have-fizzled-in-ukraine-so-far/>
- HERN, Alex. AI's 'Oppenheimer Moment': Autonomous Weapons Enter the Battlefield. The Guardian. 2024, [en línea]. Disponible en: <https://www.theguardian.com/technology/2024/apr/11/ai-weapons-ukraine>



theguardian.com/technology/article/2024/jul/14/ais-oppenheimer-moment-autonomous-weapons-enter-the-battlefield

Europe. 2023, [en línea]. Disponible en: <https://defence-industry.eu/are-drones-a-war-game-changer-the-ukrainian-case/>

KALLENBORN, Zachary. "InfoSwarms: Drone Swarms and Information Warfare." *Parameters* 52, núm. 2. 2022, pp. 87–102. [en línea]. Disponible en: <https://press.armywarcollege.edu/parameters/vol52/iss2/13/>

MANLEY, Cameron. USsupplied HIMARS'completely ineffective' against superior Russian jamming technology. *Business Insider*. 25 de mayo de 2024, [en línea]. Disponible en: <https://www.businessinsider.com/us-himars-completely-ineffective-against-russian-jamming-report-2024-5>

KONAEV, Margarita. *Tomorrow's Technology in Today's War: The Use of AI and Autonomous Technologies in the War in Ukraine and Implications for Strategic Stability*. CNA Corporation, September 2023, [en línea]. Disponible en: <https://www.cna.org/reports/2023/10/Use-of-AI-and-Autonomous-Technologies-in-the-War-in-Ukraine.pdf>

MANTELLASSI, Federico; RICKLI, Jean-Marc. "The War in Ukraine: Reality Check for Emerging Technologies and the Future of Warfare". Geneva Centre for Security Policy. (Geneva Paper 34/24). Abril de 2024, [en línea]. Disponible en: [https://www.researchgate.net/publication/379744204\\_The\\_War\\_in\\_Ukraine\\_Reality\\_Check\\_for\\_Emerging\\_Technologies\\_and\\_the\\_Future\\_of\\_Warfare](https://www.researchgate.net/publication/379744204_The_War_in_Ukraine_Reality_Check_for_Emerging_Technologies_and_the_Future_of_Warfare)

KOTT, Alexander; DUBYNSKYI, George; PAZIUK, Andrii; GALAITSI, Stephanie *et al.* Russian cyber onslaught was blunted by Ukrainian cyber resilience, not merely security. 2024, [en línea]. Disponible en: <https://arxiv.org/abs/2408.14667>

MICROSOFT. Defending Ukraine: Early lessons from the cyber war. *Microsoft Security Insider*. 2022, [en línea]. Disponible en: <https://www.microsoft.com/es-cl/security/security-insider/intelligence-reports/defending-ukraine-early-lessons-from-the-cyber-war>

KOTT, Alexander; THÉRON, Paul; DRAŠAR, Martín; DUSHKU, Edlira *et al.* Autonomous Intelligent Cyberdefense Agent (AICA) Reference Architecture. Release 2.0. NATO Research Task Group IST152. 2028, [en línea]. Disponible en: <https://arxiv.org/abs/1803.10664>

MINISTERIO DE DEFENSA (CESEDEN). "La inteligencia artificial y la guerra de Ucrania". José Pardo de Santayana. 17 de diciembre 2024, [en línea]. Disponible en: [https://www.defensa.gob.es/ceseden/-/la\\_inteligencia\\_artificial\\_y\\_la\\_guerra\\_de\\_ucrania](https://www.defensa.gob.es/ceseden/-/la_inteligencia_artificial_y_la_guerra_de_ucrania)

KRAMPE, Oliver. The Ukraine war and the international order, *International Politics*, 61(1), 2024, pp. 120.

LING, Justin. The invisible RussiaUkraine battlefield. *Wired*. 23 de diciembre de 2024, [en línea]. Disponible en: <https://www.wired.com/story/electronic-warfare-russia-ukraine>

MONZÓN Baeza, Víctor; PARADA, Raúl; CONCHA Salor, Laura & MONZÓ, Carlos. AI-Driven Tactical Communications and Networking for Defense: A Survey and Emerging Trends. *arXiv*. 2025, [en línea]. Disponible en: <https://arxiv.org/abs/2404.05071>

MACCABELLIO, Pietro. Are drones a war game changer? The Ukrainian case. *Defence Industry*



- PUJOL, Irene. La guerra cognitiva convierte la mente en campo de batalla. *El Financiero*. 16 de octubre de 2024, [en línea]. Disponible en: <https://www.elfinanciero.com.mx/opinion/colaborador-invitado/2024/10/16/la-guerra-cognitiva-convierte-la-mente-en-campo-de-batalla/>
- RED TEAM ANALYSIS SOCIETY. AI at War (1) – Ukraine. Red Team Analysis Society. 8 de abril 2024. [en línea]. Disponible en: <https://redanalysis.org/2024/04/08/ai-at-war-1-ukraine/>
- SCHARRE, Paul. *Army of None: Autonomous Weapons and the Future of War*. New York: W. W. Norton & Company. Part II: "Autonomous missiles, drones, and robot swarms". 2028.
- SCHARRE, Paul. *Four Battlegrounds: Power in the Age of Artificial Intelligence*. W.W. Norton & Company. Capítulo 22: "Robotics Row". 2023.
- SEGURA, Cristian. Rusia consigue cortar la comunicación de los satélites Starlink del ejército de Ucrania. *El País*. 24 de mayo de 2024, [en línea]. Disponible en: <https://elpais.com/internacional/2024-05-24/rusia-consigue-cortar-la-comunicacion-de-los-satelites-starlink-del-ejercito-de-ucrania.html>
- SOLOPOVA, Veronika. From Trust to Truth: Actionable policies for the use of AI in fact-checking in Germany and Ukraine. 2025, [en línea]. Disponible en: <https://arxiv.org/abs/2503.18724>
- VAN DER BURG, Erik; TOET, Alexander *et al.*. A Convolutional Neural Network as a Potential Tool for Camouflage Assessment. *Applied Sciences*. 2025, [en línea]. Disponible en: <https://www.mdpi.com/2076-3417/15/9/5066>