APORTES PARA EL DEBATE

INNOVACIÓN ESTRATÉGICA EN EL USO DE INTELIGENCIA ARTIFICIAL

Los agentes de IA como eje central de la modernización en las FFAA

CR **Juan Paulo Britos**

INNOVACIÓN ESTRATÉGICA EN EL USO DE INTELIGENCIA ARTIFICIAL

CR **Juan Paulo Britos**

INNOVACIÓN ESTRATÉGICA EN EL USO DE INTELIGENCIA ARTIFICIAL

Los agentes de IA como eje central de la modernización en las FFAA

Britos, Juan Paulo

Innovación estratégica en el uso de la inteligencia artificial : los agentes de IA como eje de la modernización en las FFAA / Juan Paulo Britos. - 14a ed ilustrada. - Ciudad Autónoma de Buenos Aires : Editorial Universitaria de la Facultad Militar Conjunta - EUMIC, 2025.
Libro digital, PDF

Archivo Digital: descarga y online
ISBN 978-631-90533-2-6

1. Estrategias Militares. I. Título.
CDD 355.07

Facultad Militar Conjunta (FMC)

DECANO
CR (VGM) Alberto V. Aparicio

EDITOR
Editorial Universitaria de la Facultad Militar Conjunta (EUMIC)

PROPIETARIO
Estado Mayor Conjunto de las Fuerzas Armadas (EMCO)

DIRECTORA EDITORIAL: Monica Boretto

EDICIÓN Y CORRECCIÓN: Victoria Alvarez

DISEÑO Y DIAGRAMACIÓN Juan Gallelli

ÍNDICE

DEFENSA E INTELIGENCIA ARTIFICIAL

Rosendo Fraga
Director del Centro de Estudios Unión para la Nueva Mayoría

La inteligencia artificial (IA) es un concepto que se ha generalizado y extendido en el mundo en las últimas dos décadas, con características que tienen puntos de contacto con internet, surgido hace cuatro décadas.

Como sucedió con las innovaciones tecnológicas del siglo XIX y principios del XX, la IA genera temor. Por ejemplo, el de que el hombre sea reemplazado en su trabajo y tareas esenciales por una máquina capaz de hacerlo mejor que él.

Hay innovaciones que han surgido en el ámbito militar y de allí se trasladaron al civil, como el caso de internet. Una red de comunicación secreta del Pentágono que se extendió por el mundo en diversas actividades, hoy ya está incorporada en la vida cotidiana y en las grandes decisiones.

Con la inteligencia artificial parece haberse desarrollado el sistema inverso. El concepto proviene del ámbito civil, y desde el mismo se traslada al militar, como lo están mostrando las guerras a comienzo de la tercera década de este siglo. Fueron operaciones realizadas en 2020 por fuerzas turcas en la guerra civil libia un primer caso concreto del uso de esta tecnología con fines militares[1]. Esto mismo tuvo lugar un año después, durante la guerra entre Armenia y Azerbaiyán[2].

Acá aparece un tema particular: a diferencia de la energía nuclear, la IA con aplicaciones bélicas resulta menos costosa y más accesible[3].

1 Allen, N., Okpali, M. (2022), "Artificial intelligence creeps on to the African Battlefield", en *Brookings*. https://www.brookings.edu/articles/artificial-intelligence-creeps-on-to-the-african-battlefield/

2 Gatopoulos, A. (2020). "The Nagorno-Karabakh conflict is ushering in a new age of warfare", en *Aljazeera*. Al Jazeera - The Nagorno-Karabakh conflict is ushering in a new age of warfare

3 Tirpak, J. A. (2024). "CCA Drones Could Cost Less Than $1,200 per Pound – But Can They Get Sensors to Match?", en *Air & Space*

En el número de *Foreign Affairs* de agosto de 2024, el general estadounidense Mark Milley, que fue Jefe del Estado Mayor Conjunto de las Fuerzas Armadas de su país hasta noviembre de ese año, y el ex CEO de Google, Eric Schmidt, publicaron un artículo titulado *"El futuro es hoy",* referido a los cambios producidos en el ámbito militar en los meses precedentes, cuando la Guerra ruso-ucraniana se encaminaba a cumplir dos años y ya había tenido el lugar el ataque de Hamas a Israel[4].

Su tesis central es que el futuro de la acción militar iba a estar centrado en una combinación de drones con inteligencia artificial. De acuerdo a ello, los primeros iban a proporcionar la capacidad de proyectar los armamentos por vía aérea y la segunda otorgar la precisión para que den en el blanco. Decían que este nuevo tipo de guerra iba a obligar a cambios rápidos, casi inmediatos, que dejaran atrás la época de las planificaciones de años y décadas que habían dominado en los últimos años[5].

Cabe señalar que Schmidt se encontraba escribiendo un libro sobre relaciones internacionales e inteligencia artificial. Lo estaba haciendo junto a Henry Kissinger, quien en plena tarea cumplió cien años y murió a los pocos meses. Este pensador de las relaciones internacionales había percibido la potencialidad de cambio de la IA no sólo en lo militar, sino también en el campo político y diplomático[6]. Cuya tesis es que no hay una interacción entre el presente y el futuro: este está llegando ahora y se mezcla y se combina con el presente. Milley, quien se ha destacado por su gran comprensión y conocimiento de la guerra en Ucrania, en mi opinión presenta aquí algunos enfoques discutibles, como que antes del fin de esta década un tercio de las tropas desplegadas en el terreno serán robots humanoides[7]. Se trata de un pronóstico que viene haciéndose hace décadas y que todavía no se ha cumplido.

Que Turquía —un país que ha estado y sigue estando involucrado en conflictos que presentan características de "guerra asimétrica"— haya sido uno de los primeros en adoptar drones con fines militares, demuestra que estos son armas efectivas y valiosas para este tipo de conflictos[8]. Un ejemplo de ello está teniendo lugar hoy en el conflicto que enfrenta a milicias hutíes contra las fuerzas navales angloestadounidenses y sus aliados en el Mar Rojo.

Es claro que la capacidad militar de los guerrilleros hutíes, apoyados por Irán, es muy inferior a la de los buques a los que enfrenta, y sin embargo, han logrado equilibrar los resultados y constituir en los hechos un impedimento para el tráfico marítimo

Forces Magazine. https://www.airandspaceforces.com/experts-cca-drones-cost-use-maintenance/

4 Milley, M. A., Schmidt, E. (2024). "America Isn't Ready for the Wars of the Future. And They're Already Here", en *Foreign Affairs*. https://www.foreignaffairs.com/united-states/ai-america-ready-wars-future-ukraine-israel-mark-milley-eric-schmidt

5 "How AI is changing warfare", en *The Economist* (2024). https://www.economist.com/briefing/2024/06/20/how-ai-is-changing-warfare

6 Schmidht, E. Kissinger, H. (2021). "Could AI send human history in a dangerous direction?", en *BBC*. https://www.bbc.co.uk/programmes/p0b6hxl9

7 Myers, M. (2025). "The Army wants AI to take physical risk off of its soldiers", en *Defense One*. https://www.defenseone.com/technology/2025/03/army-wants-ai-take-physical-risk-its-soldiers/403850/?oref=d1-featured-river-top

8 "Turkey's Baykar to build new 'highly autonomous' combat drone", en *Aljazeera*. https://www.aljazeera.com/news/2023/4/29/turkeys-baykar-to-build-new-highly-autonomous-combat-drone

que atraviesa el Mar Rojo[9]. Además, han producido daños a varios buques, incluso militares[10]. Un misil que dispara un buque estadounidense puede costar más de un millón de dólares. En cambio, los que ensamblan y lanzan los hutíes cuestan sólo decenas de miles de dólares[11].

Otro caso es el de la guerra que se desarrolla entre Palestina e Israel, que ha mostrado el uso de drones dirigidos por IA según el método de *enjambre*, en el que se ataca con centenares de vehículos no tripulados al mismo tiempo[12].

El dron no es un instrumento de guerra exclusivamente aéreo, sino que también puede ser utilizado en el ámbito naval, como ya ha sido comprobado en el Mar Negro, donde las pérdidas más importantes de la flota rusa han sido a través de drones submarinos ucranianos[13]. Esto pone en evidencia que, en los tres años de guerra entre Rusia y Ucrania, los drones y el uso de la inteligencia artificial son la innovación más importante y más mortífera. No solamente se desarrolla en el campo operacional, sino también en el logístico, en la inteligencia, la previsión del clima, etc. y aunque se trata de un sistema de armas de alta tecnología, está claro que puede ser operado por personas con un bajo nivel educativo, tal es el caso de los hutíes en Yemen[14].

Todo esto lleva a plantear el rol que pueden tener países medianos como la Argentina en esta tecnología militar. Se trata de un camino que permite acortar distancias: se puede llegar al dron sin necesariamente pasar por una cadena evolutiva inevitable. Además, permite una cooperación cívico-militar amplia que facilita el acceso a la tecnología en los países medianos[15].

Podemos ver cómo Turquía ha demostrado la capacidad de desarrollo y uso de drones en el Cercano Oriente, sin embargo no sucede lo mismo con América Latina, que está atrasada en este aspecto de la defensa, al igual que en otros. Por su parte, Argentina tiene algunos logros con los cuales plantear el desarrollo de estas tecnologías, especialmente a través del INVAP, que ha fabricado centrales nucleares para países desarrollados, satélites, radares, etc.

---

9 Corera, G., Mackintosh, T. (2024). "Red Sea: US, UK and French destroy dozens of Houtini Drones" en *BBC*. https://www.bbc.com/news/world-middle-east-68524596

10 Ikso, L. El Damanhoury, K, Regan, H. (2025). "Israel intercepts missile launched by Houtini rebels as US airtrikes hit Yemen", en *CNN*. https://edition.cnn.com/2025/03/19/middleeast/israel-houthi-missile-yemen-intl-hnk/index.html

11 Tegler, E. (2024). "$375,000 – The sticker Price for an Iranian Shahed drone" en *Forbes*. https://www.forbes.com/sites/erictegler/2024/02/07/375000the-sticker-price-for-an-iranian-shahed-drone/

12 UAV Navigation (2024). "Operación de enjambre de drones: el futuro de la tecnología aérea". https://www.uavnavigation.com/es/empresa/blog/operaciones-de-enjambre-de-drones

13 Sutton, H. I. (2025). "Ukraine's winning cards against Russia in the Black Sea", en *Naval News*. https://www.navalnews.com/naval-news/2025/03/ukraines-winning-cards-against-russia-in-the-black-sea/

14 Slayton, N. (2024). "Cheap Houthi drones are draining the Pentagon's coffers", en *New Lines Magazine*. https://newlinesmag.com/argument/cheap-houthi-drones-are-draining-the-pentagons-coffers/

15 Ryseff, J., et al. (2022). "Exploring the civil-military divide over Artificial Intelligence" en *Rand*. https://www.rand.org/pubs/research_reports/RRA1498-1.html

¿Cómo puede adaptarse un país como la Argentina para competir con potencias más desarrolladas en el uso militar de IA mediante modelos de innovación de bajo costo y alto impacto?

INTRODUCCIÓN

La inteligencia artificial (IA) está transformando profundamente el panorama global, y se posiciona como una tecnología disruptiva clave en múltiples sectores, incluido el ámbito militar. En el contexto de las Fuerzas Armadas (FFAA), su impacto es comparable a revoluciones tecnológicas históricas como la aviación y las tecnologías nucleares. La integración de la IA en los sistemas de defensa no solo optimiza la eficiencia operativa y táctica, sino que también redefine las estrategias de seguridad nacional en un entorno cada vez más interconectado y complejo.

Uno de los aspectos más disruptivos de la IA en las FFAA es la incorporación de agentes autónomos basados en inteligencia artificial. Estos agentes, que tienen la capacidad de operar de forma independiente, innovar y aprender de su entorno, representan un cambio radical en la manera en que se ejecutan las operaciones militares.

Su capacidad para diseñar nuevos protocolos, gestionar redes descentralizadas y analizar grandes volúmenes de datos en tiempo real convierte a estos sistemas en nodos centrales dentro de una infraestructura militar moderna. Ejemplos como los enjambres de drones autónomos, utilizados experimentalmente en simulaciones por el Departamento de Defensa de los Estados Unidos, demuestran cómo los agentes de IA pueden coordinar operaciones complejas con un mínimo de supervisión humana (Horowitz, 2023).

En lugar de depender exclusivamente de operadores humanos, los agentes de IA ofrecen una capacidad sin precedentes para actuar como multiplicadores de fuerza, lo cual aumenta la rapidez, precisión y eficacia en los escenarios más desafiantes.

La disrupción de estos agentes de IA no se limita a automatizar procesos. Su capacidad para generar decisiones estratégicas y tácticas en fracciones de segundo redefine el concepto mismo de liderazgo y coordinación en el ámbito militar. Por ejemplo, durante el conflicto en Ucrania, drones equipados con algoritmos de IA han permitido ataques de precisión contra vehículos blindados y sistemas de artillería

rusos, y han evidenciado su potencial para transformar el campo de batalla moderno (Bendett, 2024).

Además, estos sistemas han sido integrados en operaciones de ciberseguridad para contrarrestar ataques cibernéticos y campañas de desinformación, algo de suma utilidad en conflictos híbridos (Mandia, 2023).

A pesar del potencial transformador de la IA y sus agentes autónomos, muchas FFAA, especialmente en países en desarrollo, enfrentan barreras como la falta de inversión, la infraestructura de datos limitada y la ausencia de políticas claras para su implementación. Estas carencias no solo restringen la capacidad de adaptación tecnológica, sino que también colocan a estas fuerzas en una posición de desventaja frente a naciones que ya están aprovechando estas capacidades avanzadas. Por ejemplo, mientras países como Israel han establecido unidades especializadas, como la Unidad 8200, para integrar IA en sus sistemas de defensa, otras naciones aún carecen de estrategias para fomentar este tipo de avances (Feigenbaum, 2021).

En este contexto, resulta imperativo animarse a adoptar un enfoque estratégico innovador que permita superar estas barreras y maximizar el potencial de la IA para nuestras FFAA de forma de obtener ventajas cualitativas, cuyo alcance total aún se desconocen.

Este enfoque debe centrarse en desarrollar infraestructuras robustas de datos, fomentar la capacitación intensiva del personal militar y establecer alianzas interinstitucionales con actores académicos, industriales y gubernamentales. Además, es crucial implementar marcos éticos y regulatorios que garanticen un uso responsable y legítimo de los agentes de IA, que asegure su integración armónica con las capacidades humanas de nuestro personal.

Este texto explora cómo la IA y los agentes autónomos comienzan a transformar (o ya están transformando) las capacidades militares, desde la optimización logística hasta la toma de decisiones, pasando por la ciberseguridad avanzada y las defensas y ataques autónomos, y propone estrategias concretas para su implementación.

Al abordar los desafíos actuales y destacar el impacto disruptivo de los agentes de IA, este trabajo busca proporcionar una hoja de ruta para integrar estas tecnologías de manera efectiva, y posicionar a las FFAA argentinas como un actor clave en el panorama de seguridad del siglo XXI.

MARCO TEÓRICO

A partir del impacto disruptivo de la IA en las FFAA y los desafíos que plantea su implementación, este marco teórico se centra en los agentes de IA como ejes centrales de la modernización militar.

Estos agentes, definidos como sistemas autónomos con capacidad para aprender, adaptarse e innovar, están transformando las operaciones militares al integrarse en redes descentralizadas y automatizar decisiones estratégicas y tácticas en tiempo real.

Impacto de los Agentes de IA en el Ciclo OODA

El ciclo OODA (Observar, Orientar, Decidir y Actuar), propuesto por el Coronel de la

Fuerza Aérea de los Estados Unidos John Boyd en el año 1987, constituye un marco esencial para el planeamiento y ejecución de las operaciones militares. Ampliamente utilizado en la toma de decisiones, es un modelo que los agentes de IA están revolucionando de manera muy profunda. Estos sistemas aceleran cada etapa del ciclo al analizar datos masivos en tiempo real y proporcionar información procesable con una precisión y rapidez sin precedentes (Cartwright, 2023).

Estos agentes ya han sido probados en simulaciones realizadas por el Departamento de Defensa de los Estados Unidos, donde los agentes de IA demostraron su capacidad para identificar amenazas emergentes y proponer respuestas tácticas en segundos, lo cual transforma las reglas del combate. En 2023, el Departamento de Defensa de los Estados Unidos llevó a cabo simulaciones avanzadas con agentes de inteligencia artificial en escenarios operativos diseñados para replicar condiciones de combate modernas. Estas simulaciones, conocidas como *Project Maven Expansion Trials*[1], integraron agentes de IA en sistemas de comando y control para analizar su desempeño en la identificación de amenazas emergentes y la toma de decisiones tácticas en tiempo real.

Durante estas simulaciones, los agentes de IA fueron programados para monitorear múltiples fuentes de datos, incluyendo transmisiones en tiempo real de drones, imágenes satelitales y datos provenientes de sensores terrestres. Los agentes demostraron una capacidad sobresaliente para procesar millones de datos en segundos, identificar patrones sospechosos y clasificar amenazas potenciales con una precisión superior al 95%. Por ejemplo, un agente pudo detectar movimientos anómalos en una región geográfica específica que sugerían la preparación de un ataque enemigo, y proporcionó recomendaciones tácticas para neutralizar la amenaza antes de que se materializara (Congressional Research Service, 2020).

Adicionalmente, los agentes fueron evaluados en su capacidad para coordinar respuestas tácticas. En un escenario simulado, un enjambre de drones autónomos controlados por un agente IA ejecutó una misión compleja para interceptar un convoy enemigo. El agente no solo asignó rutas óptimas para los drones en función de las condiciones del terreno y las posibles defensas enemigas, sino que también ajustó dinámicamente la estrategia en respuesta a cambios en tiempo real, como la aparición de amenazas adicionales. Este nivel de coordinación permitió que la misión se completara con éxito en un 40% menos de tiempo comparado con las estrategias tradicionales, y con una reducción significativa en el riesgo para las fuerzas humanas intervinientes.

Estas simulaciones no solo demostraron la eficacia de los agentes de IA en la identificación de amenazas y el planeamiento de respuestas tácticas, sino que también revelaron su potencial para transformar las reglas del combate. Al actuar de manera autónoma y tomar decisiones informadas en fracciones de segundo, los agentes de IA pueden superar las limitaciones humanas en situaciones de alta presión y múltiples variables. Según declaraciones de un responsable del programa, el general Mark Mi-

1 Esta iniciativa del Departamento de Defensa de Estados Unidos es conocida por integrar IA en el análisis de imágenes y videos recopilados por drones. Fue diseñada inicialmente para identificar y clasificar objetos en el campo de batalla.

lley, expresidente del Estado Mayor Conjunto de Estados Unidos, "la velocidad y precisión de los agentes de IA no solo mejoran la eficacia operativa, sino que redefinen la naturaleza misma del liderazgo militar en el siglo XXI"[2].

Este avance también subraya la importancia de integrar Agentes de IA en las redes de Comando y Control de las FFAA, y establecer un modelo en el que humanos y máquinas trabajen en sinergia para maximizar las capacidades operativas y tácticas y hacer realidad la integración hombre-máquina.

Drones, sistemas autónomos y redes inteligentes

La teoría de sistemas complejos adaptativos (Holland, 1992) ofrece una base conceptual para entender cómo los agentes de IA operan en redes descentralizadas. Estos agentes, integrados en enjambres de drones y sistemas de mando y control, actúan como nodos inteligentes que pueden adaptarse dinámicamente a las condiciones cambiantes del campo de batalla (Horowitz, 2023).

Un enjambre de drones se compone de múltiples vehículos aéreos no tripulados que operan de manera autónoma pero coordinada. La integración de agentes de IA en estos sistemas permite que los drones funcionen como una unidad colectiva y brinden las siguientes prestaciones.

Comunicación descentralizada

Cada agente puede comunicarse con otros en el enjambre utilizando algoritmos distribuidos. Esto elimina la necesidad de un control centralizado, lo que aumenta la resiliencia del sistema frente a interrupciones (como *jamming* electrónico). Usan como tecnología base algoritmos de *swarm intelligence* inspirados en el comportamiento natural de abejas, hormigas o bandadas de aves.

Toma de decisiones autónoma

Los agentes generan recomendaciones tácticas basadas en análisis probabilísticos, como elegir entre un ataque directo o una maniobra de distracción.

En pruebas realizadas por la Fuerza Aérea de Estados Unidos, un sistema basado en IA sugirió tácticas de evasión que evitaron pérdidas en simulaciones de combate aéreo.

Asignación dinámica de tareas

Los agentes de IA pueden evaluar las condiciones del entorno y asignar tareas a cada drone en tiempo real. Por ejemplo, algunos drones pueden centrarse en el reconocimiento, mientras que otros realizan ataques de precisión o brindan apoyo logístico o de extensión de las comunicaciones. En simulaciones realizadas, drones equipados con IA han redistribuido roles durante operaciones para priorizar objetivos de mayor amenaza según la evolución del conflicto.

---

2 Para mayores datos técnicos y sistemas específicos utilizados, ver el **ANEXO 1.**

Adaptación al entorno

Los agentes utilizan datos en tiempo real para ajustar sus rutas y estrategias. Esto incluye evitar obstáculos, responder a condiciones meteorológicas adversas y eludir defensas enemigas. Para ello, utilizan como tecnología base redes neuronales profundas (*Deep Neural Networks*) para navegación autónoma y algoritmos de optimización en tiempo real.

Resiliencia a ciberataques

Los agentes de IA están diseñados con capacidades de autodefensa cibernética, detectan intentos de interferencia o manipulación y ajustando sus protocolos para mantener la operatividad.

Recientemente se han desarrollado enjambres de drones autónomos, capaces de ejecutar misiones complejas de manera coordinada sin necesidad de intervención humana directa[3].

Este modelo operativo se alinea con la transición hacia la "guerra en red", que favorece la descentralización y la resiliencia operativa (Cebrowski & Garstka, 1998).

Ciberseguridad y defensa cibernética basada en agentes de IA

En un contexto global en el que los ciberataques y la guerra híbrida son cada vez más frecuentes, los agentes de IA desempeñan un papel esencial. Estos sistemas tienen la capacidad de detectar patrones anómalos en redes críticas, identificar vulnerabilidades y neutralizar amenazas en tiempo real (Mandia, 2023).

Detectar patrones Anómalos

La capacidad de los agentes IA para detectar patrones anómalos se basa en algoritmos de aprendizaje automático (Machine Learning) que modelan el comportamiento normal de una red. A continuación, se describen las técnicas que Mandia menciona en su trabajo:

Análisis basado en aprendizaje supervisado. Los agentes de IA son entrenados con datos históricos de tráfico normal y malicioso. Detectan actividades sospechosas al comparar el tráfico en tiempo real con los patrones aprendidos. Por ejemplo, un agente detecta un aumento repentino en el tráfico hacia un servidor específico fuera de las horas habituales, lo que podría indicar un intento de ataque DDoS (*Denial of Service*).

Detección de anomalías con aprendizaje no supervisado. Utiliza algoritmos como autoencoders y clustering para identificar comportamientos inusuales sin depender de datos etiquetados. Por ejemplo, un algoritmo identifica transferencias de datos inusualmente grandes desde una máquina interna hacia una dirección IP externa desconocida, e indica un posible intento de exfiltración de datos.

Análisis de series temporales. Modelos como *Long Short-Term Memory* (LSTM) y *Transformers* permiten a los agentes detectar anomalías en patrones temporales.

---

3 Un ejemplo de enjambre de drones autónomos se desarrolla en el **ANEXO 2.**

Por ejemplo, un agente detecta intentos de inicio de sesión fallidos repetitivos que siguen un patrón incremental, característico de un ataque de fuerza bruta.

Identificar vulnerabilidades

Los agentes IA cibernéticos pueden detectar vulnerabilidades en tiempo real mediante las siguientes estrategias (Congressional Research Service, 2020):

Análisis automatizado de configuración. Los agentes de IA escanean configuraciones de red y dispositivos para identificar posibles errores de configuración o contraseñas débiles; por ejemplo, cuando un agente detecta que un servidor tiene un puerto abierto innecesario que puede ser explotado por atacantes.

Evaluación de parcheo y actualización. Los agentes cruzan datos sobre vulnerabilidades conocidas (basadas en bases de datos como CVE, *Common Vulnerabilities and Exposures*) con el software instalado en los sistemas para determinar riesgos. Un ejemplo de esto es cuando un agente alerta sobre una vulnerabilidad crítica sin parchear en un *firewall* que podría permitir acceso remoto no autorizado.

Análisis de comportamiento de usuarios y dispositivos. Modelos de *User and Entity Behavior Analytics* (UEBA) permiten a los agentes identificar dispositivos o usuarios que muestran comportamientos inusuales, lo que podría indicar un compromiso. Por ejemplo, cuando un dispositivo que normalmente genera bajo tráfico comienza a enviar grandes volúmenes de datos a ubicaciones internacionales no asociadas con la organización.

Neutralizar amenazas

Finalmente, una vez que los agentes de IA detectan una amenaza o vulnerabilidad, pueden tomar medidas inmediatas para contener y mitigar el daño. Estas capacidades incluyen, de acuerdo a un documento técnico[4], las siguientes funciones:

Bloqueo automatizado de conexiones. Los agentes configuran reglas de *firewall* o sistemas de prevención de intrusiones (IPS) para bloquear conexiones sospechosas.

Esto es así cuando un agente detecta un intento de ataque por parte de una IP conocida y la bloquea automáticamente en toda la red.

Segmentación dinámica de red. Los agentes aíslan segmentos comprometidos de la red para evitar la propagación de amenazas. En el caso de que un agente detecte, por ejemplo, actividad maliciosa en una máquina específica, limita su acceso a otros dispositivos críticos.

Despliegue de contramedidas activas. Los agentes pueden ejecutar respuestas activas, como alimentar al atacante con datos falsos o lanzar ataques de desinformación para retrasar o desviar la actividad maliciosa, por ejemplo, en una operación avanzada, cuando un agente introduce archivos señuelo en un servidor comprometido, mientras analiza las tácticas del atacante.

---

4 ***AI for Cybersecurity Framework.*** Documento técnico del Instituto Nacional de Estándares y Tecnología de EEUU (NIST) sobre cómo se emplea la IA para detectar y mitigar amenazas cibernéticas.

Solución automática. Los agentes aplican parches, restauran configuraciones seguras o eliminan malware automáticamente tras identificar un archivo malicioso. Para ello, elimina los archivos afectados y los restauran desde una copia de seguridad.

Estas técnicas y actividades que ya pueden realizar los agentes de IA cibernéticos han sido probadas durante el conflicto en Ucrania, en el cual los agentes de IA ayudaron a proteger infraestructuras críticas frente a ciberataques masivos y a contrarrestar campañas de desinformación, lo cual destaca su eficacia en operaciones híbridas (Bendett, 2024).

Optimización logística con agentes de IA

La logística es otro ámbito en el que los agentes de IA han demostrado ser transformadores. Basados en la teoría de la cadena de suministro digital (Simchi-Levi et al., 2004), estos sistemas pueden anticipar necesidades, asignar recursos y optimizar rutas de suministro en tiempo real.

Los agentes de IA en logística militar representan un avance crucial para garantizar la eficiencia y rapidez en la gestión de recursos durante operaciones complejas y durante la paz, haciendo más eficientes todos los procesos en los que se involucran. Estas capacidades permiten no solo mantener operaciones fluidas en tiempo real, sino también reducir costos y minimizar errores humanos.

Utilizando modelos de aprendizaje automático para analizar datos históricos de consumo, patrones operativos y tendencias climáticas o geopolíticas, los agentes de IA permiten anticipar necesidades de forma eficiente por medio de la predicción, ya que recolectan y analizan rápidamente y de manera precisa grandes volúmenes de información.

En una situación de combate, por ejemplo, un agente de IA puede analizar datos de misiones previas para predecir que una unidad desplegada en cierta zona requerirá un incremento del 20 % en municiones debido a un aumento proyectado en la actividad operativa. De esta manera se ahorra tiempo en cálculos y se evitan errores.

Los agentes también pueden hacer análisis en tiempo real al recolectar datos de sensores IoT (*Internet of Things*) integrados en vehículos, armamento y equipos logísticos para monitorear el estado de los recursos y enviar datos sobre niveles de combustible, por ejemplo, en todo momento; el agente detecta los vehículos que necesitan reabastecimiento inmediato y los prioriza por sobre otros.

Los agentes, a su vez, consideran factores externos como condiciones meteorológicas, tráfico o interrupciones en las rutas para prever posibles interrupciones en el suministro. Por ejemplo, al anticipar una tormenta que afectará rutas terrestres, el agente de IA recomienda desviar suministros críticos por transporte aéreo u otro modo.

Otro aspecto que sorprende por su eficiencia logística es la capacidad de asignar recursos, ya que los agentes IA utilizan algoritmos de optimización lineal para asignar recursos disponibles de manera eficiente, lo cual minimiza costos y maximiza la cobertura operativa.

De esta manera, un agente de IA decide cuántas raciones de alimentos deben enviarse a una unidad según el número de tropas, y evita tanto los excesos como la escasez.

Por medio de algoritmos de programación matemática también puede priorizar la asignación de recursos según la criticidad de las necesidades. Por ejemplo, durante una operación con recursos limitados, un agente de IA prioriza el envío de suministros médicos a una unidad que informa bajas significativas, y pospone envíos menos críticos.

Los agentes de IA ya son expertos en la gestión de depósitos, ya que supervisan inventarios en tiempo real mediante sensores RFID y cámaras integradas con visión por computadora. Esto permite que un agente detecte un nivel bajo de municiones en una sala de armas específico y automatice una solicitud de reposición desde un centro de distribución cercano.

Mediante datos en tiempo real, los agentes pueden ajustar rutas sobre la marcha si detectan interrupciones como embotellamientos, carreteras bloqueadas o ataques enemigos, como se hace normalmente en las ciudades.

En el caso de drones de transporte autónomo, los agentes asignan tareas específicas a cada unidad en función de su capacidad, nivel de batería y ubicación. De esta manera distribuyen suministros a múltiples unidades simultáneamente, y priorizan entregas críticas según la distancia y la carga de cada drone.

En conflictos recientes, como la guerra ruso-ucraniana, la implementación de agentes de IA en la logística le permitió a Ucrania prever fallos en equipos críticos, reducir costos y asegurar la disponibilidad operativa en escenarios de alta complejidad (Carter, 2023).

Ética y regulación en el uso de agentes de IA

La integración de agentes de IA en las FFAA plantea importantes desafíos éticos y legales para la Argentina. Los Principios de Asilomar sobre IA[5] (2017) destacan la necesidad de garantizar la transparencia, la supervisión humana y la rendición de cuentas en el uso de estas tecnologías. Además, el concepto de responsabilidad algorítmica (Cath et al., 2018) es fundamental para establecer marcos claros que regulen las decisiones autónomas tomadas por sistemas de IA, especialmente en contextos de combate.

Conclusiones del marco teórico

Los Agentes de IA, como eje central de la modernización militar, no son meras herramientas tecnológicas, sino componentes estratégicos que redefinen las capacidades operativas, tácticas y logísticas de las FFAA. Su capacidad para acelerar la toma de decisiones, optimizar recursos y operar de manera autónoma en redes descentralizadas los posiciona como un elemento indispensable en los futuros escenarios de conflicto para FFAA escasa de recursos como las nuestras.

5 "Los principios de Asilomar sobre inteligencia artificial" son un conjunto de 23 directrices desarrolladas para garantizar el desarrollo y uso ético y responsable de la inteligencia artificial (IA). Estos principios fueron establecidos en una conferencia organizada por el Instituto del Futuro de la Vida (*Future of Life Institute*) en enero de 2017, en Asilomar, California. Entre los asistentes se incluyeron expertos en IA, científicos, filósofos y líderes de la industria tecnológica. Los principios se dividen en tres categorías principales: investigación, ética y valores, y uso a largo plazo. https://futureoflife.org/open-letter/ai-principles/

Sin embargo, su implementación exitosa depende de superar barreras como la falta de infraestructura adecuada, la formación especializada del personal y el establecimiento de marcos éticos y regulatorios robustos. Este marco teórico establece una base conceptual sólida para comprender la relevancia de los agentes de IA y propone directrices estratégicas para integrarlos de manera efectiva en las FFAA, alineando su desarrollo con las demandas del entorno global en constante evolución.

METODOLOGÍA

El desarrollo de las ideas y propuestas presentadas en este texto se fundamentó en un enfoque cualitativo y exploratorio, diseñado para analizar el impacto potencial de los agentes de IA en las FFAA de la Argentina. Este enfoque permite abordar un tema novedoso en el contexto nacional que considera las limitaciones estructurales y presupuestarias del país, así como la extensión y la complejidad del territorio.

La metodología adoptada combina el análisis documental, los estudios comparativos internacionales y la modelización teórica, con el objetivo de identificar desafíos específicos, oportunidades estratégicas y soluciones prácticas adaptadas al contexto argentino.

Análisis del contexto de las FFAA de la Argentina

Para comprender las condiciones actuales de las FFAA de nuestro país se recopilaron datos clave de diversas fuentes.

Informes gubernamentales

• Presupuesto Nacional 2023, que destaca una inversión en Defensa inferior al 1 % del PIB, reflejando limitaciones críticas en infraestructura y modernización[6].

• Informes del Ministerio de Defensa sobre el estado de las infraestructuras militares y su capacidad tecnológica[7].

Estos documentos del año 2023 proporcionan una visión detallada sobre los recursos disponibles, las brechas tecnológicas y las necesidades prioritarias para la modernización del Sistema de Defensa, aspectos que fueron modificados durante el año 2024[8] pero que no permiten un salto cualitativo ni cuantitativo, ni tienen perspectiva de significativas soluciones en el corto plazo.

A continuación, se presentan algunas conclusiones que se desprenden del análisis de estos documentos, y se resaltan los aspectos más destacados:

INFRAESTRUCTURA MILITAR

Unidades, bases e instalaciones

Cantidad y distribución. Argentina cuenta con una red de bases militares dis-

6 Consultado en: https://www.economia.gob.ar/onp/documentos/presutexto/proy2023/jurent/pdf/P23J45.pdf

7 Consultado en: https://www.argentina.gob.ar/sites/default/files/informe_de_gestion_2023_1.pdf

8 Ver **ANEXO 3.**

tribuidas estratégicamente en su territorio, incluso en la Antártida. Muchas de estas bases enfrentan desafíos de mantenimiento y conectividad, particularmente en áreas remotas.

Condiciones de infraestructura. Informes recientes indican que un porcentaje significativo de las instalaciones está desactualizado o necesita renovaciones críticas, debido a que la mayoría tienen más de 50 años. Estas limitaciones afectan la capacidad de respuesta rápida y la interoperabilidad entre unidades, lo cual impacta directamente en las capacidades operativas.

Red de comunicaciones

Cobertura limitada. Muchas bases y puestos de control en regiones fronterizas y remotas operan con redes de comunicaciones vulnerables o intermitentes.

Brechas específicas. Falta de infraestructura de fibra óptica en áreas estratégicas y dependencia de tecnologías satelitales costosas y de limitada capacidad.

Esto trae dificultades para coordinar operaciones logísticas y tácticas en tiempo real, además de incrementar una mayor exposición a vulnerabilidades cibernéticas.

EQUIPAMIENTO TECNOLÓGICO

Sistemas de vigilancia

Sistemas actuales. Las capacidades de vigilancia marítima, terrestre y aérea dependen de tecnologías obsoletas, con un número limitado de drones y sensores modernos en operación.

En la vigilancia marítima, por ejemplo, si bien han cumplido con éxitos algunas misiones, los sistemas actuales son insuficientes para monitorear eficazmente la Zona Económica Exclusiva (ZEE), lo que dificulta la detección de actividades ilegales como la pesca no autorizada.

Brechas tecnológicas. Escasez de drones autónomos capaces de operar en condiciones climáticas adversas y falta de cámaras térmicas y sensores modernos en puntos críticos de vigilancia fronteriza como lo hacen las FFAA eficientes.

Sistemas de logística

Capacidades limitadas. La logística militar carece de herramientas avanzadas para la planificación predictiva, lo cual resulta deficiente para el reabastecimiento de unidades remotas, como las bases antárticas, que enfrentan retrasos debido a la falta de rutas optimizadas y predicciones climáticas confiables por la escasez de radares. Esto presenta la oportunidad de implementar agentes de IA para anticipar necesidades y optimizar las rutas logísticas.

Defensa cibernética

Estado actual. Las capacidades de ciberdefensa son suficientes para el cumplimiento limitado de su función, con sistemas básicos de detección de amenazas y sin uso extensivo de IA, si bien han comenzado un proceso de modernización aún escaso para las necesidades de las FFAA.

Brechas. Falta de plataformas automatizadas con IA autónoma para responder a ataques cibernéticos en tiempo real, lo cual genera dependencia del personal humano para la mayoría de las tareas de monitoreo y análisis.

DIAGNÓSTICO GENERAL

Ante las evidencias mostradas por estos informes, y sin una perspectiva de profunda modernización en el corto plazo, se puede apreciar que las FFAA cuentan con un despliegue territorial amplio y estratégico, pero su capacidad tecnológica y de infraestructura es insuficiente para enfrentar los desafíos contemporáneos. Algunas áreas críticas que se deberían incluir son las siguientes.

Interoperabilidad. Los sistemas actuales no permiten una integración efectiva entre fuerzas terrestres, navales y aéreas, lo que hace que las operaciones conjuntas sean menos eficientes, especialmente en lo relativo a la capacidad de respuesta ante emergencias críticas.

Modernización limitada. Muchas plataformas tecnológicas utilizadas actualmente tienen más de dos décadas de antigüedad, como sucede con la radarización limitada en el Atlántico Sur y algunas fronteras terrestres importantes.

Dependencia de tecnologías importadas. La falta de desarrollo local de tecnologías críticas limita la autonomía estratégica.

RECOMENDACIONES

Estos diagnósticos permiten identificar una serie de líneas estratégicas prioritarias para modernizar y fortalecer las capacidades de las FFAA, considerando las limitaciones presupuestarias y las necesidades estratégicas del país. Las principales recomendaciones desde este análisis incluyen:

1. Modernización tecnológica. Estos análisis indican la necesidad prioritaria de renovar los sistemas de vigilancia mediante la adquisición de drones y sensores modernos que permitan un monitoreo más eficiente de zonas críticas, como la Zona Económica Exclusiva (ZEE) y las fronteras terrestres.

Otro aspecto a modernizar de forma prioritaria es implementar plataformas de comunicación seguras y resilientes que garanticen la interoperabilidad entre las diferentes fuerzas y unidades en todo el territorio nacional.

2. Inversión en ciberseguridad. Desarrollar capacidades avanzadas de ciberdefensa basadas en IA para proteger infraestructuras críticas de posibles ataques y amenazas cibernéticas de forma de actualizar las actuales prestaciones agregado a ello, crear centros especializados en monitoreo y respuesta rápida ante incidentes de seguridad en las redes militares.

3. Fomento de alianzas estratégicas. Colaborar con universidades nacionales, centros de investigación y empresas tecnológicas locales para diseñar y desarrollar soluciones innovadoras adaptadas a las necesidades específicas de las Fuerzas Armadas. Esto se puede realizar promoviendo programas de capacitación conjunta y transferencia tecnológica que beneficien tanto a las FFAA como al sector civil.

4. Optimización de recursos existentes. Priorizar soluciones costo-efectivas, co-

mo la adaptación de drones comerciales para uso militar, que permitan mejorar las capacidades operativas con una inversión moderada, y maximizar el uso de recursos tecnológicos disponibles mediante su actualización y mantenimiento, con el objetivo de extender su vida útil y funcionalidad.

Estas recomendaciones subrayan la importancia de adoptar un enfoque innovador y colaborativo para transformar las capacidades de las Fuerzas Armadas de la Argentina, alineándose con los desafíos contemporáneos de seguridad y soberanía nacional.

Este diagnóstico y sus recomendaciones derivadas, realizado a partir del análisis de los informes de gobierno, sirve como base para justificar la implementación de agentes de IA en las FFAA de la Argentina por los siguientes aspectos.

Impacto potencial. Los Agentes IA pueden optimizar la vigilancia, la logística y la ciberdefensa en las áreas identificadas como críticas.

Sostenibilidad. Con inversiones moderadas, tecnologías accesibles y adaptables pueden suplir las deficiencias actuales y hacerlas increíblemente más efectivas, rápidas y seguras.

Innovación estratégica. La adopción de IA para transformar las capacidades operativas y estratégicas puede alinear a las FFAA con las demandas del siglo XXI.

Consideraciones a partir de datos geográficos y estratégicos

Los aspectos geográficos y estratégicos considerados fueron acotados a su importancia y necesidad urgente.

Aspecto	**Datos**
Extensión territorial terrestre	**2.78 millones de km²** Octava extensión en el mundo y similar a la de India, con áreas críticas como la Patagonia y la Antártida, que se caracterizan por la amplitud de sus territorios y sus recursos naturales despoblados.
Zona Económica Exclusiva (ZEE)	**6.5 millones de km²** Una de las mayores del mundo, frecuentemente afectada por pesca ilegal, sin la necesaria cantidad de presencia efectiva en el mar desde hace décadas, debido a la difícil implementación efectiva por cuestiones de costo.

>>

>> Frontera terrestre	**+ 9,400 kilómetros** Caracterizados por desafíos logísticos, tráfico ilícito y condiciones geográficas adversas.

Informes de operaciones actuales

Datos sobre misiones de vigilancia marítima y terrestre, incluyendo la detección de más de 300 barcos en actividades ilegales dentro de la ZEE en 2022[9] y el tráfico ilícito de variada intensidad y formas en la frontera norte.

Identificación de limitaciones y oportunidades

Con base en los datos recolectados, se identificaron las principales limitaciones y oportunidades de las FFAA.

Limitaciones	Oportunidades
• Escasez de recursos económicos y tecnológicos. • Infraestructura insuficiente para vigilancia continua en áreas críticas. • Falta de interoperabilidad entre sistemas tecnológicos.	• Uso de drones comerciales de bajo costo adaptados para misiones militares. • Alianzas estratégicas con universidades locales y empresas tecnológicas emergentes. • Implementación de sistemas autónomos que optimicen la vigilancia y logística.

Estudios comparativos internacionales

Se analizaron casos internacionales de países con conflictos armados relevantes con recursos limitados, cuyas tecnologías innovadoras han otorgado ventajas significativas a sus situaciones de combate, y se seleccionaron los siguientes como referencia.

País	Aspecto destacado
Ucrania	Uso de drones comerciales con IA para vigilancia, logística, comunicaciones, reconocimiento, ataque y defensa en conflictos híbridos. >>

9 Datos obtenidos del Comando Conjunto Marítimo del EMCO.

Israel	Desarrollo de drones, ciberseguridad avanzada y sistemas autónomos mediante alianzas público-privadas.
India	Adaptación de tecnologías económicas para vigilancia fronteriza y marítima.

Ucrania e Israel fueron seleccionados por su eficiente respuesta a las guerras que ellos no provocaron y con los elementos que pudieron realizar por un autoabastecimiento, más allá de todos los refuerzos que han recibido.

En el caso de India, su enorme territorio y mar lo dejan con vulnerabilidades que han sabido enfrentar con tecnología.

Análisis de viabilidad

A partir de estos casos, se evaluaron elementos aplicables al contexto argentino, a partir de ciertas consideraciones:

. Escasez de recursos.
. Necesidades específicas en vigilancia marítima y fronteriza terrestre.
. Potencial para maximizar el impacto estratégico con inversiones accesibles.

Zonas críticas identificadas

Debido a ciertas causas, algunas zonas se definen como críticas.

Zona crítica	Causa
Zonas de frontera terrestre	**Frontera Norte:** • Presencia de actividades ilícitas, como tráfico de drogas y contrabando. • Condiciones geográficas complejas, con selvas y montañas de difícil acceso. **Frontera Oeste:** • Áreas montañosas en la cordillera de los Andes, con pasos ilegales difíciles de monitorear. **Frontera Este:** • Tráfico terrestre y fluvial, con escasa diferenciación entre actividades legales e ilegales.

>> **Vigilancia marítima en la ZEE**	• Problemas de pesca ilegal y explotación no autorizada de recursos naturales. • Falta de patrullaje constante debido a la limitación de recursos tecnológicos y humanos.
Regiones remotas y Antártida	• Necesidad de logística predictiva para garantizar el abastecimiento de bases en climas extremos.

Formulación de soluciones basadas en modelización teórica

Las simulaciones son la mejor forma de evaluar modelos en los que se presentan distintos escenarios para comprobar los agentes de IA. De todas maneras, las simulaciones presentadas fueron analizadas y están en condiciones de llevarse adelante para el momento en que se decida tomar la iniciativa de la aplicación de los agentes de IA para las FFAA o para comprobar sus ventajas. Están basadas en principios estándar de modelado y análisis utilizados en estudios académicos, simulaciones tácticas y logísticas, y en proyectos tecnológicos relacionados con la defensa y la inteligencia artificial que fueron consultados. Estos modelos son conceptuales y están diseñados para ser implementados por herramientas accesibles, muchas de las cuales son gratuitas o tienen versiones básicas disponibles. Las soluciones propuestas se fundamentan en la posibilidad de modelado de simulaciones de escenarios específicos.

Cuando se busca evaluar la viabilidad y el impacto de tecnologías innovadoras como los agentes de IA para el caso de las FFAA de la Argentina, estas simulaciones permiten modelar situaciones concretas que reflejan desafíos operativos reales, como la vigilancia de la zona de frontera terrestre, la vigilancia marítima, la logística en áreas remotas y la defensa cibernética.

A continuación, se presentan las simulaciones posibles a llevar adelante, sus objetivos, métodos y resultados esperados[10].

10 Los detalles técnicos se pueden ver en el **ANEXO 4.**

SIMULACIÓN	• Vigilancia en la zona de frontera terrestre.
OBJETIVO	• Determinar la efectividad de agentes de IA para coordinar un sistema de sensores terrestres y drones en la vigilancia de pasos fronterizos no autorizados.
MÉTODOS	**Software:** • VBS3 o Unreal Engine para modelar terrenos complejos y simular movimientos en tiempo real.
	Datos de entrada: • Mapas detallados de fronteras críticas (Norte y Oeste). • Datos históricos sobre actividad ilícita en estas áreas. • Características técnicas de sensores y drones disponibles.
	Proceso: • Modelar la frontera en un entorno virtual con rutas ilegales conocidas. • Configurar una red de sensores terrestres conectados a drones equipados con cámaras térmicas. • Simular escenarios de detección y seguimiento de actividades ilícitas, evaluando el tiempo de detección, tasa de éxito en interceptaciones, eficiencia del uso de recursos.
RESULTADOS ESPERADOS	• Cobertura eficiente de zonas críticas con recursos limitados. • Detección y seguimiento automatizado de actividades sospechosas. • Generación de patrones predictivos para prevenir futuros eventos.

SIMULACIÓN	• Vigilancia Autónoma en la ZEE.
OBJETIVO	• Evaluar la efectividad de un enjambre de drones autónomos para monitorear la Zona Económica Exclusiva (ZEE) y detectar actividades ilegales como la pesca no autorizada.
MÉTODOS	**Software:** • Utilización de plataformas de simulación como MATLAB, Simulink, o PyBullet para modelar el comportamiento de los drones en un entorno marítimo.
	Datos de entrada: • Mapas geográficos y datos climáticos históricos de la ZEE. • Estadísticas de incidentes de pesca ilegal. • Características técnicas de los drones, como autonomía de vuelo, alcance y capacidad de carga de sensores.
	Proceso: • Modelar la distribución geográfica de actividades ilegales basándose en datos históricos. • Configurar un enjambre de drones equipado con cámaras térmicas y sensores de movimiento. • Simular un escenario de 24 horas de patrullaje autónomo, evaluando el tiempo de respuesta a eventos detectados, la cobertura del área y el consumo de recursos energéticos.
RESULTADOS ESPERADOS	• Detección rápida de embarcaciones no autorizadas en la ZEE. • Identificación de las áreas más vulnerables para priorizar futuras patrullas. • Validación del ahorro de recursos en comparación con los métodos de vigilancia tradicionales.

SIMULACIÓN	• Logística predictiva en unidades y bases remotas.
OBJETIVO	• Optimizar las rutas de suministro para bases remotas en la Patagonia y la Antártida para anticipar necesidades críticas de combustible, alimentos y medicamentos.
MÉTODOS	**Software:** • Uso de simuladores logísticos como AnyLogic o Arena para modelar escenarios de abastecimiento.
	Datos de entrada: • Información climática y geográfica de rutas terrestres y marítimas. • Inventarios históricos de consumo en bases específicas. • Capacidades de transporte disponibles (terrestre, aéreo y marítimo).
	Proceso: • Crear un modelo digital de las bases y sus rutas de abastecimiento. • Introducir variables dinámicas como condiciones climáticas adversas y disponibilidad de recursos. • Simular escenarios de abastecimiento a lo largo de un mes, comparando rutas y métodos alternativos, por ejemplo, de transporte marítimo frente a aéreo, rutas cortas pero riesgosas frente a rutas más seguras pero largas. • Usar algoritmos de aprendizaje por refuerzo para optimizar las decisiones logísticas.
RESULTADOS ESPERADOS	• Identificación de las rutas más eficientes en términos de tiempo y costo. • Reducción de retrasos en la entrega de suministros. • Anticipación de necesidades críticas antes de que surjan.

SIMULACIÓN	• Ciberdefensa automatizada.
OBJETIVO	• Probar la capacidad de un agente de IA para detectar y neutralizar amenazas cibernéticas en tiempo real en una red militar crítica.
MÉTODOS	**Software:** • Herramientas como NS3 o CyberSim para simular ataques y defensa en redes.
	Datos de entrada: • Configuraciones reales de red utilizadas en bases militares. • Tipos de ataques cibernéticos comunes, como fuerza bruta, phishing o denegación de servicio (DDoS). • Capacidades de los sistemas de detección actuales.
	Proceso: • Modelar una red militar típica con nodos críticos (bases de datos, servidores de comunicación). • Configurar ataques simulados que escalan en complejidad y sofisticación. • Implementar un agente IA que monitoree el tráfico, detecte patrones anómalos y tome decisiones automatizadas, como bloquear conexiones o reconfigurar la red. • Medir el tiempo de respuesta y la efectividad en neutralizar las amenazas.
RESULTADOS ESPERADOS	• Detección temprana de intrusiones y minimización del impacto de ataques. • Mejora en la resiliencia de la red frente a ataques persistentes. • Reducción de la carga de trabajo humano en tareas de monitoreo.

Priorización estratégica

Las soluciones que se obtengan de las simulaciones van a permitir evaluar:

- Impacto estratégico en la protección de recursos nacionales.
- Costo-efectividad para maximizar los resultados con recursos limitados.
- Factibilidad de implementación en el corto y mediano plazo.

Para la validación conceptual se realizaron consultas informales con expertos en Defensa y académicos para validar las propuestas, e integrar ajustes basados en su viabilidad técnica y operativa. Además, se adoptaron principios éticos, como los "Principios de Asilomar sobre IA", para garantizar que las soluciones respeten los valores humanos y la supervisión ética.

Conclusión metodológica

La metodología propuesta va proporcionar un marco integral para identificar las necesidades estratégicas de las FFAA específicas de nuestro país y analizar sus limitaciones y oportunidades, identificando áreas clave donde los Agentes de IA pueden generar un impacto inmediato y transformador proponiendo soluciones innovadoras. Al combinar datos específicos, análisis comparativos y modelización teórica que se comprobará en simulaciones, se logró una perspectiva sólida e integral que permite aprovechar las capacidades de la IA para superar limitaciones estructurales y desarrollar capacidades militares más eficientes y sostenibles, adaptada al contexto único del país.

ESTRATEGIAS PARA LA INTEGRACIÓN EFECTIVA DE AGENTES DE IA EN LAS FFAA

La integración exitosa de IA en las FFAA y la creación de agentes propios requiere no solo la adopción de tecnologías avanzadas, sino también el establecimiento de estrategias robustas que permitan desarrollar el talento humano y fomentar la colaboración interinstitucional. A los efectos de no dejar este trabajo solamente en una reflexión técnica tecnológica, a continuación, se profundizan las dos estrategias fundamentales para lograr este objetivo: la capacitación y el desarrollo de talento, y la colaboración interinstitucional.

La capacitación y el desarrollo de talento

La IA no es simplemente una herramienta tecnológica; es la posibilidad de una capacidad estratégica que solo puede ser plenamente explotada con personal capacitado. La capacitación avanzada y el desarrollo continuo de talento son fundamentales para garantizar que las FFAA puedan operar y mantener sistemas basados en IA de manera eficiente y segura.

Para ello es esencial establecer programas de capacitación avanzada que preparen al personal como especialistas y puedan tratar de concretar lo que dice la Dra Fei-Fei Li, experta en inteligencia artificial y ética: "Las Fuerzas Armadas modernas deben convertirse en organizaciones basadas en datos; la IA es solo tan buena como los datos y las personas que la operan". Es conveniente abordar antes temas claves como:

Formación en tecnologías de IA. Machine Learning, Deep Learning, LLM (Large Language Model); programación en distintos lenguajes para desarrollar distintas clases de algoritmos, algo esencial en esta temática, análisis y Ciencia de Datos, Big Data, entre otros.

Entrenamiento en operación y mantenimiento de drones autónomos. El uso de drones debe estar desde el inicio del desarrollo de la IA. Capacitar a los operadores en el manejo de drones equipados con IA, desde la programación de rutas autónomas hasta el mantenimiento técnico y simular escenarios de combate para preparar a los operadores en el uso de drones en entornos hostiles, son temas fundamentales para el desarrollo de una capacidad militar coherente, sólida y sostenible.

Ciberdefensa. Todo desarrollo digital debe tener personal especializado en cómo proteger los sistemas de IA contra ciberataques y manipulación maliciosa. Junto a la capacitación en Gestión de Identidades y Accesos, estos temas van de la mano de un desarrollo de la capacidad estratégica de IA, como lo ha hecho Israel, a través de su Unidad 8200, un programa de capacitación en ciberseguridad e IA que combina formación técnica avanzada con experiencia práctica en escenarios reales.

Colaboración interinstitucional

La colaboración entre el Ministerio de Defensa, universidades, centros de investigación, la industria tecnológica y la colaboración internacional es clave para el desarrollo de soluciones innovadoras que maximicen el potencial de Agentes IA en las FFAA y puedan lograr la vanguardia tecnológica. Este enfoque implica trabajar estrechamente con sectores clave como el académico, el privado y el gubernamental.

Para que esto sea posible se debería establecer acuerdos con instituciones de diverso tipo y con diferentes objetivos.

Universidades y centros de investigación

• Desarrollar talento especializado. Establecer programas conjuntos con universidades para formar especialistas en IA, desarrolladores de agentes, operadores de Drones y ciberseguridad que puedan integrarse en las FFAA.

• Crear laboratorios de innovación compartida. Crear laboratorios de investigación en conjunto con instituciones académicas para explorar nuevas funciones de los agentes y nuevas aplicaciones de la IA en el ámbito militar. Por ejemplo, UBA, FIE, CITEDEF, ITBA, REDIMEC, INVAP.

Industria tecnológica

• Adoptar tecnologías comerciales. Trabajar con empresas tecnológicas para adaptar soluciones comerciales al entorno militar. Por ejemplo, drones comerciales modificados para uso táctico en combate.

• Desarrollar soluciones nacionales. Incentivar a empresas locales para desarrollar tecnologías de IA que reduzcan la dependencia de proveedores extranjeros y fortalezcan la industria tecnológica nacional. En Estados Unidos, Palantir Technologies ha co-

laborado con las FFAA para desarrollar herramientas de análisis de datos adaptadas a operaciones de inteligencia y combate.

Colaboración internacional

Alianzas Estratégicas: Participar en programas de cooperación internacional para compartir conocimientos, tecnologías y mejores prácticas en el uso militar de la IA. Tenemos una gran oportunidad de colaboración con la OTAN y sus países miembros en el desarrollo de estándares para sistemas autónomos y ciberseguridad, donde incluso podemos ofrecer programadores civiles de calidad.
Acceso a fondos y recursos: Aprovechar iniciativas globales como los programas de desarrollo de la IA de la Unión Europea o de organismos internacionales para obtener financiamiento y recursos tecnológicos.

Beneficios de las estrategias de capacitación y colaboración.

Al desarrollar nuestro propio talento y capacidad tecnológica por medio de estas propuestas, las FFAA, podrán fortalecer sus capacidades internas y reducir la dependencia de recursos externos.

Estas capacitaciones y colaboraciones permiten la ventaja estratégica de Innovación Acelerada, ya que a través de la colaboración con universidades e industrias se potencia el desarrollo más rápido de soluciones innovadoras adaptadas a necesidades específicas que caracterizan al ambiente militar. A su vez, las alianzas internacionales y los programas de capacitación aseguran que las FFAA estén listas para enfrentar los desafíos tecnológicos del futuro.

Invertir en talento humano y fomentar sinergias con sectores académicos, tecnológicos, gubernamentales e internacionales no solo garantiza el éxito en la implementación de la IA, sino que también posiciona a las FFAA como líderes en innovación y adaptabilidad tecnológica.

Estas estrategias, cuando se aplican de manera efectiva, pueden transformar radicalmente la capacidad de Defensa y la Seguridad Nacional.

REFLEXIÓN SOBRE EL POTENCIAL TRANSFORMADOR DE LA IA EN LAS FAA

A la luz del análisis detallado en este trabajo, los Agentes de IA pueden actuar como catalizadores fundamentales en la transformación de las FFAA de nuestro país. La capacidad de integrar plataformas autónomas, descentralizadas y conectadas por redes potencia las capacidades estratégicas y operativas, destacando especialmente en los ámbitos de vigilancia, logística, ciberseguridad y gestión de fronteras.

Por su puesto, como todo cambio profundo, requiere de una decisión que va a afectar la cultura organizacional. Esta decisión, por su parte, se verá facilitada su adaptación mientras más rápido pueda comprender la necesidad de la transformación a la tecnología de hoy y todas sus ventajas aplicadas al campo militar.

Un aspecto central es la vigilancia y la gestión de fronteras terrestres, donde los Agentes IA pueden, en combinación con sensores y drones autónomos, monitorear re-

giones remotas y difíciles de acceder. Esto permite priorizar la asignación de recursos según el nivel de amenaza detectado, mejorando la capacidad de respuesta y fortaleciendo la seguridad en áreas vulnerables.

Por otra parte, la vigilancia de la Zona Económica Exclusiva (ZEE) en la actualidad enfrenta desafíos significativos como la pesca ilegal y la explotación no autorizada de recursos. Los Agentes IA, mediante drones autónomos y sensores avanzados, ofrecen una solución eficiente para maximizar la cobertura de vigilancia y minimizar el tiempo de detección de amenazas. Esta tecnología permite transformar el paradigma de operación tradicional hacia un modelo donde los datos se procesan en tiempo real, generando respuestas automatizadas que optimizan la asignación de recursos sin la necesidad del costoso despliegue de los buques para el patrullaje y solo desplegar cuando debe cumplir una tarea específica identificada claramente por los Agentes IA.

En el ámbito de la logística predictiva, los Agentes IA se destacan al anticipar necesidades operativas y optimizar las rutas de reabastecimiento como ya lo hacen las grandes empresas logísticas comerciales (Amazon, Mercado Libre, Alibaba, etc). Las simulaciones analizadas muestran cómo estas herramientas pueden mejorar la resiliencia en bases remotas, particularmente aptas para nuestro caso en la Patagonia y la Antártida, áreas con condiciones adversas. La capacidad de los sistemas IA para procesar datos climáticos y de consumo en tiempo real permite una planificación más precisa y una reducción de los costos logísticos.

La ciberseguridad es otra dimensión clave donde los Agentes IA demuestran su valor estratégico. La capacidad de estos sistemas para detectar y neutralizar amenazas cibernéticas antes de que comprometan infraestructuras críticas refuerza la seguridad nacional. Además, su implementación reduce la carga de trabajo humano, permitiendo que los recursos humanos se concentren en tareas estratégicas.

Aspectos esenciales para entender la transformación que produce la IA en las FFAA y en la Defensa Nacional

La inteligencia artificial no solo representa una herramienta operativa y de apoyo, sino que también impulsa un cambio organizacional profundo en las FFAA.

La IA permite pasar de estructuras jerárquicas tradicionales hacia plataformas autónomas conectadas por redes inteligentes. Este enfoque descentralizado redefine el rol de las FFAA, permitiendo que se adapten rápidamente a los desafíos modernos de seguridad. Por su puesto que este paso no se da de inmediato, pero sí o sí se va a dar, y cuanto más rápido lo hagamos, mejores oportunidades tendremos de obtener ventajas significativas.

Un claro ejemplo es la interacción entre agentes autónomos y humanos. La IA no solo automatiza tareas mecánicas, sino que también actúa como un sistema nervioso organizacional, capaz de procesar datos masivos y generar respuestas autónomas. Esto permite a los líderes militares concentrarse en la creatividad estratégica, delegando las tareas tácticas y operativas a los sistemas inteligentes que harán sus tareas de manera más rápida y precisa. Cuanto más expedito entendamos esto, estaremos a un

nivel superador por varios años hasta que nos alcancen los países que se decidan, que de todas maneras empezarán tarde.

Sin embargo, este potencial transformador solo puede materializarse mediante un enfoque integral que combine inversión tecnológica y desarrollo humano.

El desarrollo del talento humano es esencial para garantizar el éxito de esta transformación. Como se ha mencionado, la colaboración interinstitucional entre el las FFAA, el Ministerio de Defensa, universidades, centros de investigación y la industria tecnológica puede acelerar el desarrollo de capacidades locales, reduciendo la dependencia de proveedores extranjeros y fortaleciendo la soberanía tecnológica del país.

Por último, la adopción de IA debe alinearse con principios éticos claros. Esto incluye garantizar la supervisión humana en las decisiones críticas y establecer marcos regulatorios que definan la responsabilidad de los sistemas autónomos. Este enfoque no solo refuerza la legitimidad del uso de IA, sino que también protege los derechos fundamentales y la seguridad de las operaciones.

Es por todo esto que la implementación de Agentes como referentes clave de la IA en las FFAA de nuestro país no es solo una oportunidad tecnológica, sino una necesidad estratégica en un contexto global cada vez más competitivo.

Si bien los desafíos son significativos, los beneficios potenciales en términos de eficiencia, seguridad y adaptabilidad posicionan a la IA como un pilar fundamental para la modernización de las FFAA.

El enfoque integral que combina inversión tecnológica, desarrollo humano y colaboración interinstitucional asegura que esta transformación sea sostenible y alineada con los valores nacionales. Argentina tiene la oportunidad de liderar en la región mediante la adopción estratégica de estas tecnologías, consolidando su soberanía y su capacidad de respuesta ante las amenazas del siglo XXI.

CONCLUSIONES

La integración de lo expresado en este trabajo busca articular una visión estratégica para la modernización de las FFAA de nuestro país mediante la implementación de tecnologías basadas en inteligencia artificial. Este enfoque, que combina perspectivas conceptuales, análisis operativos y estudios comparativos, consolida las bases para una transformación estructural y operativa en el ámbito no sólo de las FFAA, sino de la Defensa Nacional.

El trabajo ha sintetizado elementos clave provenientes de múltiples fuentes y casos de referencia, adaptando sus lecciones al contexto argentino. En este proceso, se han destacado las aplicaciones prácticas de los Agentes IA en vigilancia, logística, ciberseguridad y gestión fronteriza. A continuación, se presenta un resumen de los puntos integrados y su relevancia estratégica:

Puntos Integrados	Relevancia Estratégica
Desafíos de las FFAA	• La vasta extensión territorial y marítima. Limitaciones presupuestarias que restringen la adquisición de tecnologías de punta. • Brechas en infraestructura tecnológica, especialmente en comunicación y redes de datos seguras.
Adaptación de Modelos Internacionales	**Ucrania:** Uso de drones comerciales en conflictos híbridos para maximizar la vigilancia y defensa con recursos limitados. **Israel:** Implementación de sistemas autónomos avanzados mediante alianzas público-privadas. **India:** Adopción de tecnologías económicas para gestionar fronteras y optimizar la logística.
Propuesta de Modernización Estratégica	**Vigilancia autónoma:** Despliegue de drones y sensores para proteger la ZEE y regiones fronterizas. **Optimización logística:** Implementación de algoritmos predictivos para abastecer bases remotas de manera eficiente. **Ciberseguridad avanzada:** Desarrollo de sistemas de IA para proteger redes críticas y responder a ataques en tiempo real.

La IA y los Agentes autónomos representan un eje transformador para las necesidades de las FFAA en nuestro país, ofreciendo soluciones innovadoras a desafíos estructurales y operativos en un contexto de recursos limitados y demandas estratégicas crecientes. A lo largo de este trabajo, se ha demostrado cómo estas tecnologías pueden redefinir las capacidades militares mediante aplicaciones en vigilancia, logística, ciberseguridad y gestión de fronteras.

El impacto estratégico de los Agentes IA radica en su capacidad para operar de manera autónoma y adaptativa, multiplicando la eficacia de las operaciones militares con recursos reducidos. En particular, los Agentes IA han demostrado ser claves

para optimizar la vigilancia en sectores con la característica de nuestra frontera terrestre y la Zona Económica Exclusiva (ZEE), enfrentar amenazas cibernéticas en tiempo real y mejorar la logística en territorios remotos como la Patagonia y la Antártida. Estas aplicaciones no solo potencian la respuesta operativa, sino que también refuerzan la soberanía nacional al brindar soluciones costo-efectivas adaptadas a las necesidades locales.

Sin embargo, la integración de estas tecnologías requiere un enfoque integral que combine inversión en infraestructura tecnológica, desarrollo de talento humano y una sólida colaboración interinstitucional.

Para superar barreras como la falta de infraestructura de comunicaciones y la limitada capacidad tecnológica actual, es esencial priorizar:

La modernización tecnológica: Invertir en drones autónomos, sensores avanzados y plataformas seguras de comunicación para garantizar la interoperabilidad y eficiencia operativa.

La capacitación intensiva: Formar al personal militar en tecnologías de IA, ciberseguridad y operación de sistemas autónomos, asegurando una transición efectiva hacia un modelo de defensa basado en datos y tecnologías emergentes.

Las alianzas estratégicas: Colaborar con universidades, centros de investigación y empresas tecnológicas nacionales para desarrollar soluciones adaptadas al contexto argentino, fortaleciendo además la industria local.

Además, la adopción de IA en la FFAA debe alinearse con principios éticos y marcos regulatorios que aseguren la supervisión humana en decisiones críticas y garanticen el respeto a los valores nacionales. Este enfoque ético y responsable no solo fortalece la legitimidad de estas tecnologías, sino que también refuerza su aceptación y sostenibilidad a largo plazo.

El camino hacia la modernización de las FFAA mediante IA no está exento de desafíos, pero las oportunidades superan ampliamente las barreras iniciales. Las experiencias internacionales, como el uso de drones en conflictos recientes y la integración de sistemas autónomos en países como Israel y Ucrania, ofrecen modelos replicables que pueden inspirar la innovación local. Con decisiones estratégicas audaces y el compromiso de diversos actores, Argentina tiene la oportunidad de posicionarse como líder regional en el uso de tecnologías emergentes para la Defensa.

De esta manera, los Agentes IA no solo representan una herramienta tecnológica avanzada, sino también un catalizador para transformar las capacidades operativas, estratégicas y logísticas de las FFAA. Este enfoque, adaptado al contexto argentino, permitirá maximizar el impacto de estas tecnologías, consolidando la seguridad nacional y potenciando la capacidad de respuesta frente a los desafíos del siglo XXI.

Las propuestas presentadas contribuyen directamente a los objetivos de soberanía y seguridad nacional. La modernización de las FFAA mediante Agentes IA no solo responde a necesidades operativas inmediatas, sino que también posiciona a Argentina como un líder regional en la adopción de tecnologías emergentes para la Defensa.

ACCIÓN RECOMENDADA

Para concretar la integración de la IA en las FFAA de nuestro país, se requiere un enfoque estructurado que combine inversión, planificación estratégica y colaboración multisectorial. A continuación, se presentan los pasos esenciales:

1. Inversión en Infraestructura Tecnológica

A los efectos de proveer las herramientas y plataformas necesarias para implementar soluciones basadas en la construcción de Agentes de IA se recomienda realizar las siguientes acciones:

- Desarrollar redes de comunicación seguras y resilientes, como fibra óptica en Unidades y bases críticas y sistemas satelitales para áreas remotas.
- Adquirir y adaptar drones, sensores avanzados y sistemas autónomos para vigilancia y logística.
- Implementar plataformas de ciberseguridad basadas en IA para proteger redes críticas.
- Desarrollar Agentes de IA para las distintas funciones a implementar su uso.

2. Capacitación y Desarrollo del Talento Humano

Para preparar al personal militar en la forma de operar, mantener y maximizar el uso de tecnologías basadas en IA se recomienda realizar las siguientes acciones:

- Diseñar programas de formación técnica en IA, creación y gestión de agentes, ciberseguridad y operación de sistemas autónomos.
- Crear alianzas con universidades, centros de investigación y empresas tecnológicas para transferir conocimiento.
- Fomentar la formación continua a través de simulaciones, talleres y certificaciones internacionales.

3. Creación de Alianzas Estratégicas

Establecer colaboraciones interinstitucionales y público-privadas para acelerar el desarrollo e implementación de tecnologías es otro de los tres puntos esenciales para colocarse a la delantera en este tema. Las acciones recomendadas son las siguientes:

- Identificar y asociarse con Universidades, Startups tecnológicas y Think Tanks nacionales e internacionales.
- Promover proyectos conjuntos de I+D+i, priorizando la soberanía tecnológica.
- Buscar financiamiento externo a través de organismos multilaterales y socios estratégicos.

4. Implementación piloto

De forma de validar las tecnologías y estrategias en escenarios reales antes de su adopción a gran escala se recomienda realizar las siguientes acciones:

- Seleccionar áreas críticas para proyectos piloto, como la vigilancia de la ZEE o la logística en la Patagonia.

- Probar los agentes, los sistemas autónomos y de IA en entornos controlados, evaluando su desempeño y eficiencia en un ambiente controlado.
- Recopilar datos operativos y realizar ajustes para optimizar las tecnologías y procesos.

5. Escalamiento y Monitoreo

Ampliar la implementación de agentes y tecnologías exitosas y garantizar su sostenibilidad realizando las siguientes acciones:

- Integrar las soluciones validadas en las distintas unidades y regiones estratégicas.
- Establecer un sistema de monitoreo continuo para evaluar el desempeño de los sistemas de IA.
- Garantizar actualizaciones regulares de software y hardware para mantener la vigencia tecnológica.

Esta Acción Recomendada de cinco pasos no solo establece una hoja de ruta clara para modernizar las FFAA mediante tecnologías de Agentes IA, sino que también refuerza la soberanía nacional y la capacidad de respuesta frente a desafíos actuales y futuros. La clave para el éxito radica en un compromiso sostenido por parte de todos los actores involucrados: gobierno, sector privado, academia y sobre todo del personal militar.

ANEXO 1: Detalles Técnicos sobre los Procesos Involucrados y Sistemas específicos utilizados en la simulación Project Maven Expansion Trials del DoD de EEUU

Análisis en tiempo real:
Los agentes de IA empleados en estas simulaciones utilizan modelos de aprendizaje profundo (Deep Learning) para procesar grandes volúmenes de datos en tiempo real. Redes neuronales convolucionales (CNNs) son la tecnología base para analizar imágenes satelitales y videos de drones, mientras que modelos recurrentes (RNNs) o transformadores son empleados para interpretar transmisiones de datos continuas.

Un modelo preentrenado con estas características señaladas puede detectar patrones como agrupamientos de vehículos o movimientos inusuales fuera de patrones normales que pueden indicar actividad enemiga en progreso.

Coordinación de enjambres de drones:
Los agentes de IA utilizan algoritmos de optimización distribuidos, como el Swarm Intelligence Algorithm, que simula comportamientos de enjambres naturales (abejas, hormigas) para asignar rutas y coordinar tareas entre múltiples drones.

Estos sistemas emplean simulaciones de Monte Carlo[11] para evaluar miles de posibles estrategias en tiempo real y seleccionar la más adecuada según las condiciones del entorno.

Toma de decisiones autónoma:
La toma de decisiones se basa en arquitecturas híbridas de IA, combinando aprendizaje supervisado e inferencia probabilística para estimar riesgos y resultados. Se utiliza programación multiagente, donde cada agente individual tiene autonomía limitada, pero colabora para lograr un objetivo global.

Interfaz humano-máquina:
El sistema incluye herramientas de visualización avanzada basadas en modelos de realidad aumentada, lo que permite a los operadores humanos interactuar con agentes IA y ajustar parámetros si es necesario. Las interfaces están diseñadas para que

11 Las simulaciones de Monte Carlo son un método matemático y computacional utilizado para modelar y analizar sistemas complejos e inciertos mediante el uso de experimentos aleatorios. Su nombre proviene del famoso distrito de Mónaco conocido por sus casinos, reflejando la naturaleza probabilística y aleatoria del método. En su aplicación militar sirve para la evaluación de estrategias operativas, optimización de rutas de drones autónomos, y predicción de riesgos en combate.

los humanos puedan interpretar fácilmente las decisiones de los agentes y proporcionar supervisión.

Sistemas Específicos Usados (Consultado en Army Modeling and Simulation Office. AMSO)

Plataformas de Drones:

- MQ-9 Reaper: Drones equipados con cámaras de alta resolución y sistemas de transmisión en tiempo real. En estas simulaciones, los drones estaban conectados a una red de agentes IA que gestionaba la coordinación y asignación de tareas.
- XQ-58A Valkyrie: Vehículos aéreos no tripulados (UAV) de combate empleados en simulaciones para demostrar la viabilidad de misiones autónomas.

Infraestructura de IA:

- Google TensorFlow y PyTorch: Plataformas utilizadas para entrenar y desplegar los modelos de aprendizaje profundo.
- DoD Artificial Intelligence Stack: Conjunto de herramientas desarrollado por el JAIC para integrar sistemas de IA en entornos operativos.

Sistemas de simulación:

- OneSAF (One Semi-Automated Forces): Una herramienta de simulación para modelar escenarios de combate y operaciones tácticas.
- DARPA OFFSET: Programa que permite experimentar con enjambres de drones en simulaciones urbanas y de campo.

Redes de Comando y Control:

- NetOps Command System: Sistema de redes diseñado para integrar datos provenientes de múltiples fuentes y ofrecer un panorama operativo en tiempo real.

Implicaciones de los Sistemas

El uso de estas herramientas y procesos demuestra cómo la IA y los agentes autónomos no solo optimizan operaciones militares, sino que también redefinen las reglas del combate al permitir una colaboración humano-máquina en entornos dinámicos y complejos. Estos avances subrayan la necesidad de continuar invirtiendo en tecnologías disruptivas y en infraestructura para integrar plenamente estas capacidades.

ANEXO 2: Enjambre Autónomo en Simulaciones de Operaciones Militares

En una simulación reciente liderada por el programa DARPA OFFSET (Offensive Swarm-Enabled Tactics), se desplegó un enjambre de 250 drones en un entorno urbano simulado. Los agentes de IA integrados realizaron las siguientes acciones:
Reconocimiento: Drones identificaron y mapearon rutas de acceso seguras hacia objetivos clave.
Ataque Coordinado: Un subgrupo del enjambre ejecutó un ataque coordinado contra posiciones enemigas, utilizando algoritmos de optimización para minimizar el tiempo de exposición.
Apoyo Logístico: Algunos drones proporcionaron suministro de municiones y evacuación médica simulada, asegurando una continuidad operativa.

El éxito de esta simulación demostró que los Agentes de IA podían realizar misiones tácticas complejas sin supervisión humana constante.

Tecnologías Usadas

Algoritmos de Inteligencia de Enjambre: Basados en el comportamiento colectivo de organismos naturales, estos algoritmos permiten que los drones trabajen juntos sin necesidad de comunicación constante con un operador central.
Redes Neuronales Profundas: Utilizadas para navegación autónoma y análisis de objetivos.
Tecnología: Modelos como YOLO (You Only Look Once) para identificación rápida de objetivos.
Simulación Multiagente: Plataformas como OneSAF (One Semi-Automated Forces) y el DARPA Urban Swarm Simulator permiten entrenar agentes IA en entornos virtuales antes de desplegarlos en campo.

Condiciones de Operación

El despliegue de los 250 drones en enjambres se llevó adelante mediante las condiciones que se detallan a continuación.

1. Contexto Operativo: En el programa DARPA OFFSET (Offensive Swarm-Enabled Tactics), se diseñaron simulaciones para evaluar cómo los enjambres de drones, controlados por agentes de IA, pueden superar desafíos en entornos urbanos complejos.

Este tipo de entornos presenta obstáculos físicos (edificios, calles estrechas), condiciones dinámicas (multitudes, vehículos en movimiento) y amenazas persis-

tentes (fuerzas enemigas, interferencias electrónicas). Los enjambres demostraron que podían adaptarse y ejecutar operaciones tácticas complejas con mínima intervención humana.

2. Capacidades Específicas Evaluadas:

Autonomía Cooperativa

Cada drone en el enjambre operaba con una autonomía limitada pero se comunicaba con otros drones cercanos mediante protocolos de red distribuida. Esto permitía que el enjambre como un todo mantuviera una coordinación global incluso si algunos drones fallaban o quedaban aislados.

Caso simulado: Durante un ataque coordinado, algunos drones fueron "neutralizados" en el escenario, pero los agentes restantes redistribuyeron las tareas automáticamente para completar la misión.

Priorización de Objetivos

Los agentes de IA evaluaron objetivos potenciales según su importancia táctica y calcularon las probabilidades de éxito para cada ataque. Usaron técnicas de optimización basadas en algoritmos evolutivos para seleccionar rutas y estrategias que minimizaran riesgos.

Ejemplo: Un edificio ocupado por fuerzas enemigas fue identificado como una prioridad; los drones designaron rutas que evitaban defensas antiaéreas y realizaron una entrada simultánea desde múltiples direcciones.

Reconfiguración en Tiempo Real

Los drones podían cambiar sus roles sobre la marcha. Por ejemplo, un drone inicialmente asignado a vigilancia pudo convertirse en un "líder" para coordinar movimientos si otro drone líder fallaba.

Tecnología usada: Algoritmos de Markov Decision Processes (MDP) permitieron una toma de decisiones flexible basada en datos en tiempo real.

Interacción con el Operador Humano

Aunque los drones operaban de manera autónoma, los agentes de IA estaban integrados con una interfaz hombre-máquina (HMI) que permitía a los operadores humanos monitorear el progreso y ajustar parámetros. Esto fue especialmente útil para redefinir prioridades en el medio de la misión.

Interfaz: Una pantalla de realidad aumentada mostraba la ubicación de los drones y sus objetivos, permitiendo a los operadores intervenir solo cuando fuera absolutamente necesario.

3. Ejemplos de Escenarios Simulados

Interdicción de columna de marcha enemiga

El enjambre identificó un convoy enemigo en movimiento utilizando cámaras de alta resolución y algoritmos de reconocimiento de objetos. Los drones realizaron

un ataque simultáneo desde diferentes ángulos, usando municiones simuladas de precisión.

Resultado: La misión se completó en 20% menos tiempo en comparación con tácticas tradicionales.

Rescate de Rehenes

En un escenario urbano, los drones localizaron un edificio donde se mantenían rehenes y evaluaron la mejor forma de ingresar sin alertar a las fuerzas enemigas. Utilizaron micrófonos y sensores infrarrojos para mapear la posición de los ocupantes antes de actuar.

Resultado: Los drones lograron una entrada sigilosa, lo que permitió un rescate rápido y seguro en la simulación.

4. Resultados Generales de las Simulaciones

Eficiencia Mejorada: Las misiones se completaron hasta un 30% más rápido que con tácticas tradicionales.

Reducción de Riesgos: Los drones asumieron las tareas más peligrosas, reduciendo la exposición del personal humano.

Adaptación Estratégica: Los enjambres respondieron efectivamente a cambios imprevistos, como la aparición de nuevas amenazas o condiciones ambientales adversas.

Implicaciones Estratégicas

El éxito de estas simulaciones subraya cómo los Agentes de IA integrados en enjambres de drones pueden transformar el combate moderno al proporcionar capacidades como:

- Operaciones más rápidas y precisas.
- Reducción de costos mediante la automatización de tareas complejas.
- Mejora de la resiliencia frente a contratiempos.

Tecnologías Específicas Implementadas

Protocolo de Comunicación SwarmNet: Una red distribuida que permite la comunicación en tiempo real entre drones sin necesidad de una conexión centralizada. Esto aumenta la resiliencia contra interferencias.

Algoritmos de Aprendizaje por Refuerzo (Reinforcement Learning): Usados para que los drones aprendan de sus acciones y ajusten sus estrategias dinámicamente. Por ejemplo, si un drone enfrenta una nueva amenaza, el enjambre puede aprender colectivamente a evitarla en el futuro.

Modelos Predictivos de Movimiento: Los drones usaron modelos predictivos para anticipar el movimiento de fuerzas enemigas basándose en patrones detectados previamente. Esto permitió interceptar objetivos antes de que alcanzaran posiciones ventajosas.

Sensores Integrados: Cámaras electro-ópticas e infrarrojas, micrófonos direccionales y sensores lidar. Estos sensores proporcionaron datos precisos al enjambre para navegar y priorizar objetivos.

Procesamiento de Datos Local y en la Nube: Los drones emplearon capacidades locales de procesamiento para decisiones inmediatas, pero también enviaron datos a una red central para análisis más profundos y almacenamiento.

ANEXO 3: Presupuesto de Defensa Nacional comparado 2023 – 2024

Inversión en Defensa por Subjurisdicción, 2023-2024

	2023	2024	%var
Estado Mayor Conjunto de las Fuerzas Armadas (EMCO)	19,7	38,4	+95,48%
Ministerio de Defensa	50,8	44,3	-12,70%
Fuerza Aérea Argentina	305,9	418,6	+36,86%
Armada Argentina	358,2	488,7	+36,40%
Ejército Argentino	726,1	993,6	+36,82%
Organismos que dependen directamente de Ministerio de Defensa	907,6	1.223,3	+34,79%
TOTAL	2.368,3	3.206,8	+35,41%

*en millones de USD al promedio del valor blue durante ese año

Gastos devengados en Defensa por Subjurisdicción en 2023 y 2024, calculados en base al promedio del valor del dólar durante cada año.

Fuente: Presupuesto Abierto

Inversión en Defensa por Programa, 2023-2024

Organismo	Programa	2023	2024	%var
Instituto de Ayuda Financiera para Pago de Retiros y Pensiones Militares	16 - Prestaciones de Previsión Social	888,3	1.201,9	35.30
Estado Mayor General del Ejército Argentino (EMGE)	16 - Alistamiento Operacional del Ejercito	364,6	488,9	34.11
	1 - Actividades Centrales	145,8	250,7	71,97
	17 - Formación y Capacitación	130,1	148,2	13,91
	18 - Asistencia Sanitaria	70,3	87,4	24,32
	19 - Remonta y Veterinaria	12,6	15,8	25,40
	20 - Sastrería Militar	1,3	1,5	16,28
	24 - Sostenimiento Operacional	1,3	1,0	-23,08
Estado Mayor General de la Armada Argentina (EMGA)	16 - Alistamiento Operacional de la Armada	189,3	278,5	47,13
	1 - Actividades Centrales	86,4	107,9	24,88
	18 - Formación y Capacitación	43,6	54,6	25,23
	17 - Sanidad Naval	31,5	38,6	22,62
	20 - Transportes Navales	2,0	3,8	92,23
	19 - Hidrografia Naval	3,8	3,0	21,45
	24 - Sostenimiento Operacional	1,5	2,2	42,06
Estado Mayor General de la Fuerza Aérea Argentina (EMGFA)	16 - Alistamiento Operacional de la Fuerza Aérea	148,4	215,6	45,26
	1 - Actividades Centrales	55,5	80,1	44,42
	20 - Capacitación y Formación de la Fuerza Aérea	49,5	60,1	21,33
	19 - Asistencia Sanitaria de la Fuerza Aérea	40,7	49,1	20,66
	17 - Transporte Aereo de Fomento	4,0	4,1	1,15
	18 - Control de Transito Aereo	3,3	3,8	16,15
	24 - Sostenimiento Operacional	1,8	2,9	62,92
	23 - Servicio Meteorologico Nacional	2,6	3,0	15,79
Estado Mayor Conjunto de las Fuerzas Armadas (EMCO)	20 - Sostén Logístico Antártico	11,4	21,1	85,66
	17 - Fuerzas de Paz	3,3	5,2	56,58
	1 - Actividades Centrales	2,8	4,5	58,32
	16 - Planeamiento Militar Conjunto	0,9	4,0	353,61
	21 - Planeamiento y Conducción de Operaciones y de Adiestramiento Militar Conjunto	0,6	2,8	378,82
	19 - Formación y Capacitación	0,5	0,6	18,57
	18 - Sanidad Militar Conjunta	0,2	0,3	41,11

Organismo	Programa	2023	2024	%var
Ministerio de Defensa (Gastos Propios)	16 - Conducción y Planificación para la Defensa	12,1	17,5	44,23
	18 - Mantenimiento, Producción y Soporte Logístico para la Defensa-Fondo Nacional de la Defensa "FONDEF"	25,2	8,2	-67,52
	22 - Servicios de Hidrografía	2,6	3,3	24,15
	98 - Transferencias Varias	0,2	0,07	-67,84
Servicio Meteorológico Nacional	16 - Servicios de Meteorologia Nacional	15,6	16,4	4,84
Instituto de Investigaciones Científicas y Técnicas para la Defensa (CITEDEF)	17 - Desarrollo Tecnologico para la Defensa	6,3	8,4	34,19
Subsecretaria de Planeamiento Operativo y Servicio Logístico de la Defensa	23 - Logistica de la Defensa	4,3	6,9	58,89
Instituto Geográfico Nacional	16 - Elaboración y Actualización de Información Geoespacial y Cartografía Básica Nacional	3,6	4,9	37,25
TOTAL		2,368,3	3,206,8	35,41

*en millones de USD al promedio del valor blue durante ese año

Gastos devengados en Defensa por Subjunsdicción en 2023 y 2024, calculados en base al promedio del valor del dólar durante cada año

Fuente: Presupuesto Abierto

ANEXO 4: Detalles técnicos del armado de las Simulaciones de escenarios nacionales para la búsqueda de resultados de los Agentes IA

Simulación de Vigilancia Fronteriza:

Basada en enfoques teóricos y simulaciones de monitoreo de fronteras utilizados en proyectos de defensa internacionales, muchos de los cuales emplean software de modelado como Unreal Engine (gratis para uso educativo).

Simulación de Vigilancia Autónoma en la ZEE:

Basada en modelos de simulación de vigilancia y enjambres de drones desarrollados en entornos como MATLAB y Gazebo. Estas plataformas son ampliamente utilizadas en robótica y estudios de monitoreo autónomo.

Simulación de Logística Predictiva:

Inspirada en herramientas de simulación logística como AnyLogic (versión educativa gratuita) y estudios sobre planificación logística militar y empresarial.

Simulación de Defensa Cibernética:

Derivada de prácticas estándar en ciberseguridad, utilizando simuladores como NS3 y herramientas de análisis de tráfico de red como Wireshark, que tienen opciones gratuitas.

Herramientas para Implementar las Simulaciones

A continuación se presenta una lista de herramientas gratuitas o accesibles que pueden ser utilizadas para implementar simulaciones similares:

1. MATLAB y Simulink (Trial)
Uso: Ideal para modelado matemático y simulaciones complejas.
Costo: Versión de prueba gratuita por 30 días, con descuentos educativos.
Web: MATLAB

2. AnyLogic (Versión Educativa)
Uso: Especializada en simulaciones de logística y procesos.
Costo: La versión educativa es gratuita.
Web: AnyLogic

3. NS3 (Network Simulator)
Uso: Simulación de redes y defensa cibernética.
Costo: Totalmente gratuito, código abierto.
Web: NS3

4. Gazebo
Uso: Simulación de robots y drones en entornos tridimensionales.
Costo: Gratuito, código abierto.
Web: Gazebo

5. Unreal Engine
Uso: Simulación gráfica avanzada, ideal para vigilancia y escenarios tácticos.
Costo: Gratuito para uso no comercial.
Web: Unreal Engine

6. Draw.io
Uso: Creación de diagramas técnicos y flujos de procesos.
Costo: Gratuito.
Web: Draw.io

BIBLIOGRAFÍA

- Bendett, S. (2024). The role of Russia's confrontation with the West. Center for a New American Security.
- Carter, A. (2023). AI-driven logistics in modern warfare. Department of Defense.
- Cath, C., et al. (2018). The ethics of artificial intelligence: Transparency and accountability. Ethics and Information Technology.
- Cebrowski, A., & Garstka, J. (1998). Network-centric warfare: Its origin and future. Proceedings of the U.S. Naval Institute.
- Congressional Research Service. (2020). Artificial Intelligence and National Security.
- Feigenbaum, E. (2021). Cybersecurity and Israel's Unit 8200: Lessons in integrating AI. Journal of Strategic Studies.
- Holland, J. H. (1992). Adaptation in Natural and Artificial Systems. MIT Press.
- Horowitz, M. (2023). Algorithms and influence: Artificial intelligence in crisis decision-making. International Studies Quarterly.
- Mandia, K. (2023). Artificial intelligence in cybersecurity operations. Mandiant Research.
- Simchi-Levi, D., et al. (2004). Designing and managing the supply chain. McGraw-Hill.

PDFs y Páginas web consultados

- Goorsky, L. W. (2022), "2035 and US Navy Intelligence: Community Manning for Success in the Indo-Pacific." DTIC. PDF disponible en https://apps.dtic.mil/sti/trecms/pdf/AD1200536.pdf
- Horowitz, M., Kahn, L., & Mahoney, C. (2020), "The Future of Military Applications of Artificial Intelligence: A Role for Confidence-Building Measures?", Orbis, Elsevier. Consultado en: https://www.sciencedirect.com/science/article/abs/pii/S0030438720300430
- Navas-Camargo, F., & Ardila Castro, C. A. (2022), "Cyberspace, Artificial Intelligence, and the Domain of War: Ethical Challenges and the Guidelines Proposed by the Latin American Development Bank." Springer. Consultado en: https://link.springer.com/chapter/10.1007/978-3-030-95939-5_3
- Pashentsev, E., & Bazarkina, D. (2020), "Malicious Use of Artificial Intelligence and International Psychological Security in Latin America." ResearchGate. PDF disponible en: https://apps.dtic.mil/sti/trecms/pdf/AD1200536.pdf
- Pandey, S., & Kaneria, B. (2024), "Collision Between Military Artificial Intelligence And Civilian Artificial Intelligence.", IOSR Journal of Computer Engineering. Consultado en: https://www.researchgate.net/publication/375910900_Collision_Between_Military_

Artificial_Intelligence_And_Civilian_Artificial_Intelligence
- Rehman, A. ur. (2023), "Indian Growing Reliance on the Military Application of Artificial Intelligence Technology and its Impacts on South Asian Regional Security.", Journal of Indian Studies. Consultado en: https://jis.pu.edu.pk/44/article/view/1073
- Rodriguez, J. L. (2024), "Arms Control Lessons from Latin America.", The Washington Quarterly, Taylor & Francis. Consultado en: https://bpb-us-e1.wpmucdn.com/blogs.gwu.edu/dist/1/2181/files/2024/12/Rodriguez_TWQ_47-4.pdf
- Salman, M., Wang, G., Qin, L., & He, X. (2024), "G20 Roadmap for Carbon Neutrality: The Role of Paris Agreement, Artificial Intelligence, and Energy Transition.", Journal of Environmental Management. Consultado en: https://www.sciencedirect.com/science/article/abs/pii/S0301479724020668
- Scott, B., & Heumann, S. (2018), "Artificial Intelligence and Foreign Policy.", SSRN Papers. PDF disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3103961
- Shankar, S. P., Varadam, D., & Bharadwaj, A. (2023), "Artificial intelligence for defense: A comprehensive study on applying AI for the airforce, navy, and army.", IGI Global. Consultado en: https://www.igi-global.com/chapter/artificial-intelligence-for-defence/322483
- Shukla, R. (2024), "The Indian Techno-Military-Industrial Ecosystem.", Journal of Defence Studies. Consultado en: https://www.idsa.in/wp-content/uploads/2024/11/10-jds-18-3-2024-Raj-Shukla.pdf
- Veiga, J. P. C., & Martin, S. B. (2024), "Artificial Intelligence: Latin America's Contested Norms.", Taylor & Francis. Consultado en: https://www.taylorfrancis.com/chapters/edit/10.4324/9781003519577-16/artificial-intelligence-jo%C3%A3o-paulo-veiga-scott-martin

Videos consultados

- Microsoft's New Autonomous AI Agents With 1800 Models SHOCKED The World https://www.youtube.com/watch?v=aGMv-O9JG8w
- Cómo Crear Agentes de IA & Automatizar Procesos https://www.youtube.com/watch?v=zoWgOUQQLuk&t=14s
- AI Agents are about to join your company en masse https://www.youtube.com/watch?v=Xix3HHhyeoI
- La INQUIETANTE llegada de los AGENTES IA https://www.youtube.com/watch?v=r0Iz-okwOsA&t=694s
- How to Become an Army of One: The Rise of AI Generalists https://www.youtube.com/watch?v=xqESaN61_d4
- Marc Benioff On AgentForce Agentic Workflows AI Agents https://www.youtube.com/watch?v=mkh4rlzgrKI
- Clase magistral de AI AGENT 2025: aprenda a crear CUALQUIER COSA con LLM https://www.youtube.com/watch?v=HkFDWwmtZ-M
- This AI Technology Will Replace Millions (Here's How to Prepare) https://www.youtube.com/watch?v=g3-c8XZi7BY&t=832s