ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

35/2026 29 de abril de 2026

Teniente general Miguel Ballenilla y García de Gamarra

El mando ante el algoritmo: Inteligencia artificial, doctrina, inteligencia y disuasión

El mando ante el algoritmo: Inteligencia artificial, doctrina, inteligencia y disuasión

Resumen:

La aparición de modelos avanzados de inteligencia artificial con capacidades aplicadas a la ciberseguridad, como Claude Mythos Preview de Anthropic, ha provocado una alarma internacional que trasciende el ámbito tecnológico. La cuestión no reside únicamente en la eventual capacidad de estos sistemas para descubrir vulnerabilidades, desarrollar exploits o acelerar operaciones defensivas y ofensivas en el ciberespacio, sino en el efecto estratégico que produce su mera existencia, comunicación y restricción de acceso.

Este documento analiza el tránsito de la inteligencia artificial desde herramienta auxiliar hacia infraestructura estratégica con efectos cuasi-actoriales. Para ello, sitúa el caso Anthropic/Mythos en una secuencia más amplia de irrupciones tecnológicas —telefonía móvil, Internet, robots y sistemas autónomos e IA generativa— que han modificado progresivamente la relación entre información, conectividad, autonomía y decisión. A partir de ese marco, examina sus implicaciones para la doctrina militar, la inteligencia y la disuasión, incorporando referencias a la OTAN, la Unión Europea, las prioridades tecnológicas españolas, la producción reciente del Instituto Español de Estudios Estratégicos (IEEE) y el debate ético-jurídico sobre autonomía y control humano.

Finalmente, subraya la necesidad de que la enseñanza militar superior, en particular desde el Centro Superior de Estudios de la Defensa Nacional (CESEDEN) y la Escuela Superior de las Fuerzas Armadas (ESFAS), actúe como motor de adaptación doctrinal, ética y profesional de las Fuerzas Armadas españolas, formando mandos capaces de comprender la tecnología sin abdicar del juicio, la responsabilidad y las virtudes superiores de la profesión militar.

Palabras clave: Ciberseguridad, autonomía cognitiva, juicio militar, control humano.

Command before the Algorithm: Artificial Intelligence, Doctrine, Intelligence and Deterrence

Abstract:

The emergence of advanced artificial intelligence models with cybersecurity capabilities, such as Anthropic's Claude Mythos Preview, has generated international concern that goes beyond the technological sphere. The issue lies not only in the potential ability of these systems to discover vulnerabilities, develop exploits or accelerate defensive and offensive operations in cyberspace, but also in the strategic effect produced by their mere existence, public communication and restricted access. This paper analyses the transition of artificial intelligence from an auxiliary tool to a strategic infrastructure with quasi-actorial effects. It places the Anthropic/Mythos case within a broader sequence of technological disruptions —mobile telephony, the Internet, robots and autonomous systems, and generative AI— that have progressively transformed the relationship between information, connectivity, autonomy and decision-making. It then examines the implications for military doctrine, intelligence and deterrence, and underlines the need for higher military education to prepare commanders capable of understanding technology without renouncing judgment, responsibility and the higher virtues of the military profession.

Keywords:

Cybersecurity; cognitive autonomy; military judgment; human control; higher military education.

Cómo citar este documento:

BALLENILLA Y GARCÍA DE GAMARRA, Miguel. *El mando ante el algoritmo. Inteligencia artificial, doctrina, inteligencia y disuasión*. Documento de Análisis IEEE 35/2026. enlace web IEEE y/o enlace bie[3] (consultado día/mes/año).

Introducción: el caso Anthropic y la nueva alarma estratégica

La información publicada recientemente sobre Claude Mythos Preview, el nuevo modelo de inteligencia artificial de Anthropic orientado a tareas avanzadas de ciberseguridad, ha actuado como detonante de una alarma de alcance internacional. Según la información disponible, Anthropic habría optado por no liberar públicamente el modelo y ponerlo inicialmente a disposición de un grupo restringido de socios tecnológicos a través de Project Glasswing, con el propósito declarado de identificar y corregir vulnerabilidades en sistemas digitales críticos. La propia compañía afirma que los socios del proyecto recibirán acceso a Mythos Preview para encontrar y reparar vulnerabilidades o debilidades en sistemas fundacionales que representan una parte muy significativa de la superficie global de ciberataque compartida. Entre las tareas previstas figuran la detección local de vulnerabilidades, el análisis de binarios, la seguridad de *endpoints* y las pruebas de penetración[1].

Lo relevante del episodio no es solo la potencia técnica atribuida al sistema, sino el umbral conceptual que revela. Anthropic ha sostenido que usuarios no expertos podrían aprovechar Mythos Preview para encontrar y explotar vulnerabilidades sofisticadas; incluso ha señalado que ingenieros sin formación reglada en seguridad han podido solicitar al modelo la búsqueda de vulnerabilidades de ejecución remota y obtener *exploits* funcionales[2]. Esta afirmación, tomada con la prudencia debida ante cualquier comunicación empresarial, desplaza el problema desde el terreno puramente técnico al estratégico: no se trata únicamente de una herramienta para especialistas, sino de una capacidad potencialmente democratizadora del ataque y de la defensa en el ciberespacio.

La reacción internacional confirma ese desplazamiento. Informaciones posteriores han descrito alarma en la comunidad global de ciberseguridad y en ámbitos gubernamentales por la capacidad atribuida al modelo para analizar código y descubrir vulnerabilidades. Según *The Washington Post*, investigadores de Mozilla habrían empleado Mythos para identificar 271 fallos graves en Firefox, lo que provocó una respuesta de emergencia; el mismo medio señalaba que el Gobierno estadounidense habría revisado su

[1] ANTHROPIC. *Project Glasswing: Securing critical software for the AI era* [en línea]. Anthropic, 7 de abril de 2026. [Consulta: 25 abril 2026]. Disponible en: https://www.anthropic.com/glasswing
[2] ANTHROPIC RED TEAM. *Claude Mythos Preview* [en línea]. Anthropic Red Team, 7 de abril de 2026. [Consulta: 25 abril 2026]. Disponible en: https://red.anthropic.com/2026/mythos-preview/

aproximación a la seguridad y regulación de la IA a raíz de estas capacidades[3]. Reuters informó también de que usuarios no autorizados accedieron al modelo Mythos a través de un entorno de terceros, lo que añade una dimensión adicional: incluso los modelos restringidos pueden verse expuestos a filtraciones, usos no previstos o accesos indebidos[4].

Conviene, sin embargo, evitar tanto el alarmismo acrítico como la complacencia. Es posible que la comunicación de Anthropic contenga un componente de posicionamiento competitivo, reputacional o incluso publicitario. En un mercado de inteligencia artificial sometido a una intensa rivalidad tecnológica, la alarma también puede convertirse en un activo comunicativo. Pero ese posible sesgo no anula el hecho estratégico; al contrario, forma parte de él. La capacidad real, la capacidad atribuida y la capacidad comunicada producen efectos en gobiernos, empresas, aliados, competidores y adversarios. La IA avanzada empieza a generar consecuencias estratégicas no solo cuando se despliega, sino cuando se anuncia, se restringe, se evalúa o se percibe como amenaza.

La hipótesis de este trabajo nace de ese punto: la inteligencia artificial está dejando de ser entendida como una herramienta auxiliar para convertirse en una infraestructura estratégica con capacidad de producir efectos propios en los procesos de percepción, decisión y acción. No es un actor estratégico en sentido clásico, porque carece de voluntad política, soberanía e intencionalidad propia. Pero sí puede comportarse funcionalmente como un actor indirecto cuando condiciona agendas gubernamentales, decisiones empresariales, prioridades de seguridad nacional, doctrinas militares y percepciones de riesgo.

Desde esa premisa, este documento analiza el tránsito de la IA desde tecnología habilitadora hacia infraestructura estratégica con efectos cuasi-actoriales. Para ello, sitúa el caso Anthropic/Mythos en una secuencia más amplia de irrupciones tecnológicas que han alterado progresivamente la relación entre información, conectividad, autonomía y decisión. A continuación, examina su impacto en tres ámbitos especialmente sensibles

[3] *The Washington Post*. «A secretive AI hacking system has sparked a global scramble» [en línea]. *The Washington Post*, 24 de abril de 2026. [Consulta: 25 abril 2026]. Disponible en: https://www.washingtonpost.com/technology/2026/04/24/anthropic-mythos-ai-washington-cybersecurity-hacking-risk/

[4] REUTERS. *Anthropic's Mythos model accessed by unauthorized users, Bloomberg News reports* [en línea]. *Reuters*, 21 de abril de 2026. [Consulta: 25 abril 2026]. Disponible en: https://www.reuters.com/technology/anthropics-mythos-model-accessed-by-unauthorized-users-bloomberg-news-reports-2026-04-21/

para la defensa: la doctrina militar, la inteligencia y la disuasión. Finalmente, plantea la necesidad de que la enseñanza militar superior, y en particular el CESEDEN y la ESFAS, conviertan la reflexión sobre la IA en adaptación doctrinal, formativa y cultural para preparar mandos capaces de decidir en un entorno crecientemente asistido, condicionado y acelerado por sistemas inteligentes.

De la conectividad a la autonomía cognitiva: una secuencia de irrupciones tecnológicas

La alarma provocada por Mythos no surge en el vacío. Forma parte de una secuencia más amplia de irrupciones tecnológicas que, durante las últimas décadas, han ido modificando la relación entre Fuerzas Armadas, sociedad, información, conectividad, autonomía y decisión. Cada una de ellas fue inicialmente percibida como una herramienta auxiliar; sin embargo, con el paso del tiempo terminó alterando prácticas profesionales, vulnerabilidades, procedimientos, estructuras y formas de pensar.

En 1996, la expansión de la telefonía móvil planteaba ya un problema profesional novedoso para las Fuerzas Armadas. Una tecnología civil, aparentemente asociada a la comodidad de la comunicación personal, comenzaba a penetrar en unidades y ejercicios militares. Aquello abría posibilidades evidentes de enlace, pero también vulnerabilidades de seguridad, indiscreción, interceptación y pérdida de control de la información. El análisis de entonces señalaba que la popularización de la telefonía móvil hacía inevitable su extensión entre los militares, obligando a diferenciar entre uso oficial y uso privado, y a regular su empleo en recintos y actividades militares[5]. En el fondo, el problema era ya reconocible: una tecnología de uso social masivo alteraba prácticas militares sin haber sido previamente absorbida por la doctrina, la normativa ni la cultura de seguridad.

En 1997, Internet aparecía como un nuevo espacio para la defensa. No solo como medio de comunicación, sino como fuente de información, ámbito de presencia institucional, instrumento de influencia y vector de riesgo. Aquel análisis advertía que la red podía servir a las Fuerzas Armadas para divulgar información, pero también para obtenerla, y que los órganos de inteligencia debían aprender a explotar esa nueva fuente. Se

[5] BALLENILLA Y GARCÍA DE GAMARRA, Miguel. «Telefonía móvil y Fuerzas Armadas». *Revista Ejército*, núm. 676, octubre de 1996, pp. 91-94.

señalaba, además, que en la Guerra del Golfo los servicios aliados habían utilizado Internet para difundir inteligencia y contrainteligencia, y que su empleo militar crecería como medio de obtención de información y alerta temprana. Al mismo tiempo, se advertía que Internet era una puerta de entrada para intrusiones y ataques a redes de ordenadores, en una pugna comparada con la vieja dialéctica entre coraza y proyectil perforante[6].

Dos décadas después, el debate se desplazó desde la conectividad a la autonomía. En 2018, al abordar el impacto de robots y sistemas autónomos, el centro de gravedad ya no era únicamente la transmisión de información, sino la progresiva delegación de funciones físicas y operativas en máquinas. Aquel trabajo señalaba que la combinación entre robótica e inteligencia artificial tendría implicaciones operacionales, doctrinales y éticas, especialmente ante la posibilidad de que un sistema autónomo militar, apoyado en sensores y algoritmos, llegara a tomar la decisión de emplear fuerza letal. También advertía que el impacto más relevante se produciría en las estructuras de mando y control, dada la necesidad de integrar la actuación de hombres y máquinas y gestionar grandes volúmenes de información mediante sistemas de inteligencia artificial como auxilio al planeamiento y a la toma de decisiones[7].

Esta continuidad no se limitó a publicaciones escritas. En julio de 2019, el CESEDEN y la Universidad Politécnica de Madrid organizaron, en el marco de la Cátedra Ingeniero General D. Antonio Remón y Zarco del Valle, el curso de verano *Impacto de la inteligencia artificial en Defensa y seguridad*. El programa abordó la IA desde una perspectiva notablemente amplia para la fecha: I+D en defensa, estrategias españolas de inteligencia artificial, programas europeos, visión industrial, ciberseguridad, sistemas autónomos, fricción de la guerra y desafíos éticos. Aquella iniciativa anticipaba ya que la IA, combinada con sensores de bajo coste, análisis de grandes volúmenes de datos y robótica inteligente, abría un campo de aplicaciones del que la defensa no podía permanecer alejada[8].

[6] BALLENILLA Y GARCÍA DE GAMARRA, Miguel. «Internet ¿un nuevo espacio para la defensa?». *Revista Ejército*, núm. 679, enero-febrero de 1997, pp. 70-75.
[7] BALLENILLA Y GARCÍA DE GAMARRA, Miguel. «Robots y sistemas autónomos: el futuro que se avecina». *Revista Ejército*, núm. 924, abril de 2018, pp. 24-29.
[8] CESEDEN y UNIVERSIDAD POLITÉCNICA DE MADRID. *Impacto de la inteligencia artificial en Defensa y seguridad*. Programa del curso de verano de la Cátedra Ingeniero General D. Antonio Remón y Zarco del Valle, 2-4 de julio de 2019.

Finalmente, en 2023, la inteligencia artificial generativa empezó a mostrar que su ámbito de influencia no se limitaba al cálculo, la búsqueda o la automatización de plataformas. En una «última lección» dirigida a oficiales con potencial de acceso al generalato, se empleó ChatGPT como interlocutor para reflexionar sobre los valores morales del general en un entorno de guerra 4.0[9]. La respuesta del sistema —centrada en integridad, responsabilidad, liderazgo, empatía, innovación, respeto y compromiso— permitió extraer una conclusión de gran valor doctrinal: la tecnología no cambia los valores militares, aunque sí modifica las competencias profesionales necesarias para ejercerlos.

La secuencia resulta clara: primero la red, después la conectividad ubicua, más tarde la autonomía física y finalmente la autonomía cognitiva. En cada fase, una tecnología inicialmente percibida como herramienta terminó modificando prácticas, riesgos, estructuras y formas de pensar. Mythos representa un nuevo umbral porque ya no se limita a comunicar, conectar o automatizar: interviene en la identificación de vulnerabilidades, en la generación de cursos de acción técnicos y en la configuración misma de la percepción estratégica.

La inteligencia artificial como infraestructura estratégica

El concepto de “actor estratégico” debe manejarse con precisión. En sentido estricto, un actor estratégico posee voluntad, intencionalidad, capacidad de decisión política y medios para producir efectos orientados a fines propios. Los Estados, las organizaciones internacionales, las empresas tecnológicas globales, los grupos armados o determinados actores no estatales pueden cumplir esas condiciones en grados distintos. La inteligencia artificial, en cambio, carece de voluntad soberana y de propósito autónomo en sentido político.

Sin embargo, limitarse a afirmar que la IA es “solo una herramienta” resulta ya insuficiente. Los sistemas avanzados de IA perciben —a través de datos—, orientan —mediante modelos de inferencia—, recomiendan —mediante generación de opciones—

[9] BALLENILLA Y GARCÍA DE GAMARRA, Miguel. «Última lección». Intervención en la clausura del XXIV Curso de Capacitación para el Desempeño de los Cometidos de Oficial General, ESFAS, Madrid, 9 de marzo de 2023. Transcripción custodiada en el Centro de Documentación del CESEDEN. La intervención, pronunciada con presencia de la ministra de Defensa, jefes de Estado Mayor y primeras autoridades civiles y militares, incorporó una reflexión sobre los valores morales del general en un entorno de guerra 4.0 elaborada con ChatGPT, circunstancia que fue expresamente indicada al auditorio. ChatGPT había sido presentado públicamente por OpenAI el 30 de noviembre de 2022.

y, en determinados entornos, ejecutan acciones o activan procesos delegados. No poseen intención política propia, pero pueden producir efectos estratégicos cuando sus resultados condicionan decisiones humanas, alteran percepciones de amenaza, redistribuyen ventajas competitivas o modifican el equilibrio entre defensa y ataque.

Por ello, tal vez resulte más riguroso definir la IA avanzada como una infraestructura estratégica con efectos cuasi-actoriales. Es infraestructura porque se integra en procesos críticos: comunicaciones, inteligencia, ciberseguridad, mando y control, logística, industria, finanzas y administración. Es estratégica porque afecta a la distribución del poder, a la seguridad nacional, a la autonomía tecnológica y a la capacidad de anticipación. Y posee efectos cuasi-actoriales porque, aun careciendo de voluntad propia, puede intervenir en la generación de consecuencias que antes dependían exclusivamente de sujetos humanos organizados.

Esta definición permite evitar dos errores simétricos. El primero sería reducir la IA a una aplicación técnica más, intercambiable con cualquier otra herramienta digital. El segundo consistiría en atribuirle una agencia plena, casi antropomórfica, como si poseyera voluntad estratégica propia. Entre ambos extremos se sitúa su verdadera relevancia: la IA no sustituye al actor humano o político, pero se inserta en la arquitectura que permite a ese actor percibir, interpretar, decidir y actuar. Su poder deriva menos de una supuesta autonomía absoluta que de su capacidad para modificar las condiciones en las que se ejerce la autonomía humana.

En el ámbito español, esta lectura se ve reforzada por la *Visión de la Inteligencia Artificial en las FAS*, que concibe la IA como un marco de implantación en las capacidades militares y en el planeamiento y conducción de las operaciones, especialmente en operaciones multidominio. El documento define la IA aplicada a las capacidades militares como la combinación de elementos y técnicas que permiten aprender, prever, modificar y adaptar automáticamente el comportamiento de sistemas conforme evoluciona el entorno operativo. Esta formulación confirma que la IA no opera como una aplicación aislada, sino como una capacidad transversal que afecta al modo en que las Fuerzas Armadas perciben, procesan, deciden y actúan[10].

[10] ESTADO MAYOR DE LA DEFENSA. *Visión de la inteligencia artificial en las FAS*. Madrid, Estado Mayor Conjunto de la Defensa, División de Planes, marzo de 2024. Documento de uso oficial.

La misma interpretación encuentra respaldo en la reciente *Estrategia de Tecnología e Innovación para la Defensa 2026* (ETID), que sitúa la tecnología y la innovación como elementos estratégicos de primer orden para la seguridad nacional, vinculándolos con la superioridad tecnológica, la integración multidominio, la resiliencia operativa y la libertad de acción. La ETID no contempla la inteligencia artificial como una herramienta sectorial, sino como una capacidad habilitadora transversal para mejorar la conciencia situacional, automatizar funciones críticas, apoyar la toma de decisiones y operar en entornos multidominio en todos los niveles de conducción militar, desde el estratégico hasta el táctico[11].

Esta interpretación se refuerza si se atiende a los trabajos prospectivos desarrollados en el marco de la Fundación Círculo de Tecnologías de la Defensa y la Seguridad, que distinguen entre tecnologías habilitadoras horizontales, tecnologías clave y sistemas multitecnológicos. Desde esta perspectiva, la IA no opera como una capacidad aislada, sino como una tecnología transversal que adquiere verdadero valor estratégico al integrarse con sistemas de mando y control, ciberseguridad, comunicaciones, nube de combate, simulación, sistemas autónomos, tecnologías cuánticas y capacidades ISR. La transformación no se produce, por tanto, por la IA considerada en abstracto, sino por su incorporación a arquitecturas complejas de defensa capaces de procesar datos, generar conocimiento, apoyar decisiones y producir efectos en distintos dominios[12].

El caso Mythos ilustra esta mutación. Un modelo orientado a ciberseguridad puede acelerar la detección de vulnerabilidades, pero también aumentar la incertidumbre sobre el equilibrio ataque-defensa. Puede fortalecer la protección de sistemas críticos, pero también elevar el listón de capacidades disponibles para actores hostiles si se filtra, se replica o se desarrolla de forma equivalente por competidores menos restrictivos. Puede ser una herramienta defensiva para grandes empresas tecnológicas, pero también un factor de presión sobre gobiernos que deben decidir si regulan, restringen, colaboran o compiten.

[11] MINISTERIO DE DEFENSA. *Estrategia de Tecnología e Innovación para la Defensa: ETID 2026*. Madrid, Secretaría de Estado de Defensa, Dirección General de Estrategia e Innovación de la Industria de Defensa, marzo de 2026.
[12] FUNDACIÓN CÍRCULO DE TECNOLOGÍAS DE LA DEFENSA Y LA SEGURIDAD. *Áreas tecnológicas y científicas de especial relevancia para la defensa: resumen de los informes finales de los grupos de trabajo del año 2024*. Madrid, Fundación Círculo de Tecnologías de la Defensa y la Seguridad, noviembre de 2025.

La tensión entre capacidad tecnológica privada y empleo militar de la IA no es ya hipotética. La controversia entre Anthropic y el Departamento de Defensa estadounidense, recogida por BBC Mundo, muestra hasta qué punto las empresas desarrolladoras de modelos avanzados pueden condicionar el acceso militar a sus sistemas mediante cláusulas de uso, límites éticos o restricciones contractuales. Anthropic habría defendido que Claude no se utilizara para vigilancia masiva doméstica ni para armas completamente autónomas, mientras que el Pentágono reclamaba acceso para todos los usos considerados legales. El episodio confirma que la IA avanzada se sitúa en una zona de fricción entre innovación privada, seguridad nacional, ética empresarial y poder estatal: no solo importa qué puede hacer técnicamente un sistema, sino quién autoriza su empleo, bajo qué límites y con qué capacidad de supervisión pública[13].

La propia OTAN ha reconocido la necesidad de protegerse frente al uso adversario de la IA, incluyendo desinformación, operaciones de información y otros usos que afectan a sociedades y democracias aliadas. Su estrategia revisada de inteligencia artificial identifica principios de uso responsable como legalidad, responsabilidad y rendición de cuentas, explicabilidad y trazabilidad, fiabilidad, gobernabilidad y mitigación de sesgos[14]. La Unión Europea, por su parte, ha desarrollado un marco regulatorio que introduce obligaciones para sistemas de alto riesgo y requisitos de transparencia, aunque su aplicación plena se despliega gradualmente[15]. La cuestión de fondo es que la IA ha dejado de ser un asunto sectorial de innovación tecnológica para convertirse en problema de gobernanza estratégica.

Esta dimensión de gobernanza estratégica se ha hecho visible también en el debate europeo reciente. En los *Military Talks of the AI Action Summit*, celebrados en París en febrero de 2025, se abordó específicamente el uso de la IA en el teatro de operaciones, la evaluación de modelos, sus implicaciones militares, la sostenibilidad, la responsabilidad y los riesgos de la IA avanzada en defensa. La intervención francesa

[13] BBC MUNDO. «Anthropic, la empresa de IA que se enfrentó al Pentágono en EE. UU. y por qué esto nos concierne a todos» [en línea]. *BBC Mundo*. [Consulta: 25 abril 2026]. Disponible en: https://www.bbc.com/mundo/articles/cddnjd34p7no

[14] NATO. *Summary of NATO's revised artificial intelligence strategy* [en línea]. Bruselas, NATO, 10 de julio de 2024. [Consulta: 25 abril 2026]. Disponible en: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy

[15] UNIÓN EUROPEA. *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial*. *Diario Oficial de la Unión Europea*, L 2024/1689.

insistió en la necesidad de principios éticos, doctrina, regulación, estándares comunes y cooperación entre aliados, confirmando que el problema de la IA militar ya no se limita al desarrollo tecnológico, sino que alcanza de lleno a la articulación política, normativa y doctrinal de su empleo[16].

En esa misma línea, las *Directrices éticas para una IA fiable* elaboradas en el ámbito europeo ofrecen un marco general especialmente útil al exigir que los sistemas de IA sean lícitos, éticos y robustos. Sus requisitos —supervisión humana, solidez técnica y seguridad, gobernanza de datos, transparencia, equidad y rendición de cuentas— adquieren una especial intensidad cuando se trasladan al ámbito de la defensa, donde los errores de diseño, interpretación, supervisión o empleo pueden producir consecuencias operativas, jurídicas y políticas de primer orden[17].

Esta visión conecta con la producción reciente del IEEE, que ya había tratado la IA no solo como una tecnología emergente, sino como factor geopolítico, operativo e industrial. El *Cuaderno de Estrategia 226* aborda expresamente la inteligencia artificial en la geopolítica y los conflictos, mientras que los documentos de trabajo de 2018 y 2019 analizaron su aplicación a la defensa y sus usos militares junto con la automatización y la robótica[18]. La novedad del presente análisis no consiste, por tanto, en señalar la importancia de la IA, sino en proponer una lectura funcional: su tránsito desde tecnología habilitadora a infraestructura estratégica con efectos cuasi-actoriales.

De ahí que el problema central no sea únicamente tecnológico, sino político-estratégico y doctrinal. La cuestión no es solo qué puede hacer la IA, sino qué efectos produce su integración en sistemas de poder, qué dependencias genera, qué vulnerabilidades introduce, qué márgenes de autonomía preserva y qué responsabilidades desplaza o redefine. En ese sentido, la IA se aproxima a otras infraestructuras críticas del poder contemporáneo —la energía, las comunicaciones, el espacio, el ciberespacio o las

[16] MINISTÈRE DES ARMÉES. *AI Action Summit – Military Talks* [en línea]. París, Ministère des Armées, 2025. [Consulta: 25 abril 2026]. Disponible en: https://www.defense.gouv.fr/en/ai-action-summit-military-talks

[17] COMISIÓN EUROPEA. Grupo Independiente de Expertos de Alto Nivel sobre Inteligencia Artificial. *Directrices éticas para una IA fiable* [en línea]. Bruselas, Comisión Europea, 2019. [Consulta: 25 abril 2026]. Disponible en: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[18] Véanse IEEE. *Cuaderno de Estrategia 226: La inteligencia artificial en la geopolítica y los conflictos*. Madrid, Ministerio de Defensa, junio de 2024; ROLDÁN TUDELA, José María. *La inteligencia artificial aplicada a la defensa*. Documento de Trabajo 06/2018. Madrid, IEEE-CESEDEN, diciembre de 2018; y CCDC. *Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R)*. Documento de Trabajo 04/2019. Madrid, IEEE-CESEDEN, octubre de 2019.

cadenas de suministro tecnológicas—, pero con una diferencia sustancial: actúa directamente sobre el proceso cognitivo que precede a la decisión.

Impacto en la doctrina militar

Tecnología, historia militar y doctrina

La doctrina militar no cambia por la mera aparición de una tecnología. Cambia cuando esa tecnología modifica de forma significativa la manera de concebir, organizar y ejecutar las operaciones. La pólvora, el ferrocarril, la aviación, la radio, el carro de combate, la energía nuclear o la digitalización no transformaron la guerra por su existencia aislada, sino por su integración doctrinal, organizativa e industrial.

Esta conclusión remite a una lección constante de la historia militar: ninguna innovación tecnológica produce por sí sola superioridad duradera si no se integra en doctrina, organización, formación y cultura de mando. La historia de la guerra muestra que cada ventaja técnica genera también incentivos para su neutralización, adaptación adversaria y aparición de vulnerabilidades nuevas. Por ello, la superioridad tecnológica solo se convierte en superioridad militar cuando se acompaña de aprendizaje institucional, versatilidad, entrenamiento y capacidad de adaptación al entorno operativo[19]. En la era de la IA, como en las revoluciones militares anteriores, la tecnología podrá acelerar la decisión, pero no sustituirá la comprensión de la guerra ni el juicio del mando.

La inteligencia artificial plantea un desafío semejante, aunque con una singularidad: no actúa solo sobre la fuerza física, la movilidad o el alcance, sino sobre el proceso cognitivo de la guerra. Incide en cómo se observa, cómo se orienta, cómo se decide y cómo se actúa. En términos del ciclo OODA de John Boyd, la IA puede acelerar la observación mediante sensores y explotación masiva de datos; puede transformar la orientación mediante correlación automatizada y generación de hipótesis; puede influir en la decisión mediante recomendaciones y simulaciones; y puede activar la acción mediante sistemas autónomos, ciberoperaciones o automatización de procesos.

[19] GAJATE BAJO, María y GONZÁLEZ PIOTE, Laura, eds. *Guerra y tecnología: interacción desde la Antigüedad al Presente*. Madrid, Editorial Centro de Estudios Ramón Areces / Fundación Ramón Areces, 2017. ISBN 978-84-9961-258-4.

Decisión, C2 y operaciones multidominio

Esta orientación coincide con la *Visión de la Inteligencia Artificial en las FAS*, que vincula su empleo a la mejora de la toma de decisiones mediante el procesamiento de grandes cantidades de datos, la generación de análisis rápidos y precisos, el perfeccionamiento de la conciencia situacional y el acortamiento del proceso decisorio. El mismo documento advierte, sin embargo, que la IA presenta limitaciones en la comprensión del contexto, la intuición y el razonamiento flexible, por lo que debe ser entrenada, utilizada y supervisada por personas, especialmente cuando las decisiones en el teatro de operaciones exijan juicio humano.

En el caso español, la ETID 2026 formula esta transformación en términos de integración multidominio: operar de forma coordinada en los dominios terrestre, marítimo, aéreo, ciberespacial, espacial y cognitivo exige una arquitectura de mando, control y decisión más ágil, distribuida y digitalizada, capaz de integrar en tiempo real sensores, datos, decisiones y efectos. El desafío, subraya la propia Estrategia, no es solo técnico, sino también doctrinal, organizativo y formativo.

En el ámbito del mando y control, esa transformación aparece ya claramente identificada en los estudios prospectivos nacionales, que describen tendencias hacia la toma de decisión inteligente en C2 multidominio, la automatización de determinadas decisiones tácticas, la gestión integrada de activos autónomos y la explotación de analítica avanzada para mejorar la conciencia situacional. Esta evolución confirma que el impacto doctrinal de la IA se proyectará sobre el núcleo mismo del mando: obtención de información, análisis, planeamiento, decisión, transmisión de órdenes y evaluación continua de la situación.

La primera consecuencia doctrinal es la compresión del tiempo de decisión. La superioridad ya no dependerá solo de disponer de mejores medios, sino de interpretar antes, decidir mejor y actuar con mayor rapidez sin perder control humano significativo. Esto introduce una tensión creciente entre velocidad y deliberación. El mando militar siempre ha exigido juicio, pero en entornos saturados de datos, amenazas híbridas y ciclos acelerados, el juicio deberá ejercerse con apoyo de sistemas que procesan más información de la que cualquier estado mayor puede absorber por medios tradicionales.

Esta compresión del tiempo no debe interpretarse únicamente como aceleración mecánica del ciclo de decisión. Implica también una presión creciente sobre la calidad del juicio. Decidir antes no equivale necesariamente a decidir mejor. La ventaja doctrinal dependerá de la capacidad para combinar rapidez, comprensión contextual, control humano y evaluación crítica de las recomendaciones generadas por sistemas algorítmicos. La IA puede reducir incertidumbre, pero también puede producir una falsa sensación de certeza si sus resultados se reciben como conclusiones objetivas y no como inferencias probabilísticas condicionadas por datos, modelos y supuestos previos.

Esta tendencia no es únicamente conceptual. La reciente *Army Transformation Initiative* del Ejército de Estados Unidos parte de la constatación de que los campos de batalla están cambiando rápidamente, que los sistemas autónomos son cada vez más letales y asequibles, y que las tecnologías de uso dual evolucionan con mayor rapidez que los procesos tradicionales. En ese marco, prevé integrar inteligencia artificial en los nodos de mando y control para acelerar la toma de decisiones y preservar la iniciativa. La IA aparece así no como un complemento periférico, sino como un elemento de transformación orgánica de la fuerza: afecta a cómo se combate, cómo se estructura, cómo se adquiere material, cómo se entrena y cómo se eliminan programas considerados obsoletos[20].

En el nivel operacional, esta transformación ya ha sido abordada en publicaciones del IEEE que analizan la contribución de la IA al planeamiento de operaciones militares, especialmente en las fases de generación de conocimiento y toma de decisiones[21]. Del mismo modo, la evolución hacia operaciones multidominio exige adaptar procesos como el *targeting* conjunto a un entorno tecnológico en el que la IA contribuye a crear efectos convergentes, simultáneos y sincronizados entre dominios[22].

[20] U.S. ARMY. *Letter to the force: Army Transformation Initiative* [en línea]. Washington, D. C., U.S. Army, 2025. [Consulta: 25 abril 2026]. Disponible en: https://www.army.mil/article/285100/letter_to_the_force_army_transformation_initiative

[21] GARAT GONZÁLEZ, José María. «La inteligencia artificial como factor de transformación de las operaciones militares en el nivel operacional». Documento de Opinión IEEE 12/2024, 1 de febrero.

[22] LORENTE CRESPO, Manuel. «La evolución del entorno operativo: implicaciones de las operaciones multidominio en el proceso de *targeting* conjunto» [en línea]. CESEDEN, 12 de septiembre de 2025. [Consulta: 25 abril 2026]. Disponible en: https://www.defensa.gob.es/ceseden/-/esfas/la_evolucion_del_entorno_operativo_implicaciones_de_las_operaciones_multidominio_en_el_proceso_de_targeting_conjunto

Integración hombre-máquina y responsabilidad

La segunda consecuencia es la integración hombre-máquina. La IA no sustituirá de forma generalizada al jefe militar, pero alterará el ecosistema en el que ejerce el mando. El problema no será elegir entre humano o máquina, sino diseñar adecuadamente la relación entre ambos. En unos casos, el humano estará "en el bucle"; en otros, "sobre el bucle"; y en otros deberá decidir qué procesos no deben automatizarse. Esta gradación, ya presente en el debate sobre sistemas autónomos, adquiere una dimensión nueva con la IA generativa y la IA aplicada a ciberseguridad, inteligencia y planeamiento.

El elemento decisivo será la confianza calibrada. Una desconfianza absoluta impedirá aprovechar las ventajas de la IA; una confianza acrítica convertiría al mando en mero validador formal de decisiones preconfiguradas por el sistema. La doctrina deberá precisar qué funciones pueden delegarse, cuáles deben permanecer sometidas a supervisión humana significativa y en qué circunstancias resulta obligado ralentizar el ciclo para preservar la responsabilidad de la decisión. Esta cuestión será especialmente sensible en procesos de *targeting*, ciberoperaciones, defensa aérea y antimisil, guerra electrónica, empleo de enjambres o protección de infraestructuras críticas.

El principio de responsabilidad humana debe permanecer en el centro de esta transformación. La *Visión de la Inteligencia Artificial en las FAS* establece que, para autorizar el empleo de un sistema de IA en operaciones, este debe ser confiable y previsible, de modo que siempre se mantenga el control sobre su resultado. También subraya que los miembros de las FAS deben conocer su responsabilidad respecto de los sistemas de IA, el nivel de autonomía que puede cederse y quién está autorizado a hacerlo, con mecanismos de trazabilidad de todo el proceso de decisión y delegación de responsabilidad. En todo caso, la responsabilidad siempre recae en un ser humano[23].

Vulnerabilidad doctrinal y resiliencia algorítmica

La tercera consecuencia es la vulnerabilidad doctrinal. Una fuerza armada dependiente de sistemas de IA deberá proteger no solo sus redes, sino también sus datos, modelos, procesos de entrenamiento, interfaces y cadenas de confianza. El adversario no buscará

[23] ESTADO MAYOR DE LA DEFENSA. *Visión de la inteligencia artificial en las FAS*, op. cit.

únicamente destruir capacidades, sino contaminar datos, inducir errores, manipular recomendaciones, provocar alucinaciones operativas o degradar la confianza del mando en sus propios sistemas. La doctrina deberá incorporar, por tanto, una cultura de resiliencia algorítmica: saber operar con IA, contra IA y sin IA.

La vulnerabilidad doctrinal se ve agravada por la propia naturaleza de los sistemas de IA. La *Visión de la Inteligencia Artificial en las FAS* advierte que estos sistemas pueden ser objeto de ciberataques dirigidos a inhabilitarlos, replicarlos o manipular su comportamiento, incluyendo ataques de envenenamiento de datos, extracción o inversión del modelo. Además, la IA puede ser utilizada de forma maliciosa para suplantación de identidad, obtención de datos personales o corporativos, difusión de desinformación, descubrimiento automático de vulnerabilidades y creación de malware[24].

Esta vulnerabilidad resulta especialmente relevante en el ciberespacio. En una conferencia impartida en la ESFAS, el comandante del Mando Conjunto del Ciberespacio[25] subrayaba que el peligro no reside únicamente en la destrucción de sistemas, sino en su manipulación inadvertida, capaz de comprometer operaciones sin necesidad de un ataque visible. Esta idea adquiere nueva profundidad cuando se proyecta sobre sistemas apoyados en IA: un dato alterado, una recomendación inducida o una confianza degradada pueden producir efectos operativos sin que el mando perciba inmediatamente la agresión.

Esta resiliencia algorítmica exigirá procedimientos de verificación, redundancia y degradación controlada. Las unidades y estados mayores deberán estar preparados para detectar incoherencias, contrastar recomendaciones, operar con datos incompletos o degradados, y recuperar procedimientos analógicos o semiautomatizados cuando el entorno técnico lo exija. La dependencia de sistemas inteligentes no puede conducir a la pérdida de competencias militares básicas, del mismo modo que la navegación por satélite no debería eliminar la capacidad de orientarse sin ella.

[24] ESTADO MAYOR DE LA DEFENSA. *Visión de la inteligencia artificial en las FAS*, op. cit.
[25] ROCA RIVERO, Javier. Comandante del Mando Conjunto del Ciberespacio Conferencia sobre ciberdefensa impartida en la Escuela Superior de las Fuerzas Armadas, 18 de febrero de 2025. Transcripción custodiada en el Centro de Documentación del CESEDEN.

Interoperabilidad aliada

La cuarta consecuencia es la interoperabilidad. En alianzas como la OTAN, la ventaja tecnológica debe ser compatible con la acción combinada. Si los aliados adoptan sistemas de IA con distintos grados de explicabilidad, seguridad, certificación y control humano, la interoperabilidad no será solo técnica, sino jurídica, ética y doctrinal. La IA obligará a revisar conceptos tradicionales de compatibilidad, enlace y mando conjunto.

Esta preocupación no es menor en el ámbito aliado. Un estudio del NATO Cooperative Cyber Defence Centre of Excellence advertía ya en 2021 que la IA militar se encontraba todavía en una fase temprana, con enfoques nacionales desiguales, brechas de capacidad entre aliados e innovación fragmentada. Esa innovación en silos puede traducirse en futuros problemas de interoperabilidad, especialmente en el intercambio de datos y aplicaciones de IA en operaciones multinacionales[26].

En el ámbito aliado, la estrategia revisada de IA de la OTAN confirma que la interoperabilidad será una condición esencial de la adopción militar de la IA. Entre sus resultados deseados incluye una mayor interoperabilidad entre los sistemas de IA de la Alianza, pasos medibles para integrar IA habilitada por datos de calidad en las capacidades aliadas, estándares y procesos de revisión, así como un entorno común de pruebas, evaluación, verificación y validación. La interoperabilidad en la era de la IA no se limita, por tanto, al intercambio técnico de información, sino que exige datos fiables, certificación, gobernanza común, confianza, doctrina compartida y criterios comunes sobre supervisión humana y uso responsable[27].

La interoperabilidad algorítmica será, por ello, uno de los grandes desafíos de las operaciones combinadas. No bastará con que los sistemas intercambien datos; será necesario que los mandos comprendan cómo se generan, priorizan y presentan las recomendaciones. En un entorno multinacional, diferentes niveles de tolerancia al riesgo, distintas reglas de enfrentamiento, marcos legales nacionales y políticas de uso responsable de la IA pueden producir fricciones significativas. La coalición deberá poder

[26] NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE. *Artificial intelligence and autonomy in the military: an overview of NATO member states' strategies and deployment* [en línea]. Tallin, NATO CCDCOE, 2021. [Consulta: 25 abril 2026]. Disponible en: https://ccdcoe.org/library/publications/artificial-intelligence-and-autonomy-in-the-military-an-overview-of-nato-member-states-strategies-and-deployment/

[27] NATO. *Summary of NATO's revised artificial intelligence strategy*, op. cit.

operar con sistemas inteligentes heterogéneos sin perder unidad de esfuerzo ni claridad en la atribución de responsabilidades.

Targeting, DIH y cadena cognitiva

El proceso de *targeting* ilustra con especial claridad esta tensión. Una lectura simplificadora reduciría el debate a una alternativa entre prohibir o aceptar sin reservas la IA en el empleo de la fuerza. Sin embargo, algunos análisis sobre IA y *targeting* cinético advierten que el debate ha quedado excesivamente absorbido por los sistemas de armas autónomos letales y el control humano, relegando otros usos potencialmente positivos de la IA en ISR, análisis de información y apoyo al cumplimiento del Derecho Internacional Humanitario. El problema doctrinal no consiste, por tanto, en aceptar o rechazar en bloque la IA, sino en determinar qué funciones puede mejorar, bajo qué controles, con qué límites, con qué trazabilidad y con qué responsabilidad humana[28].

La actualidad ofrece ejemplos que muestran hasta qué punto esta cuestión no es meramente teórica. Según la información publicada por *The New York Times*[29], una investigación militar estadounidense preliminar habría atribuido a EE. UU. el ataque con misil Tomahawk contra la escuela primaria Shajareh Tayyebeh, en Minab, Irán, como consecuencia de un error de fijación de objetivos basado en datos desactualizados. La noticia señala que se examinó si algún modelo de IA, programa de procesamiento de datos u otros medios técnicos habían contribuido a recopilar inteligencia defectuosa, aunque los funcionarios citados consideraban poco probable que el error se debiera a una nueva tecnología y más probable que reflejara un fallo humano común en tiempo de guerra. Precisamente por eso el caso resulta relevante: no prueba un fallo de IA, pero sí ilustra la vulnerabilidad crítica de cualquier arquitectura de *targeting* apoyada en datos. Si la información de partida es errónea, obsoleta o insuficientemente validada, la precisión del arma no evita el fracaso moral, jurídico y estratégico del ataque.

[28] ROBERTS, Ashley y VENABLES, Adrian. «The Role of Artificial Intelligence in Kinetic Targeting from the Perspective of International Humanitarian Law». En JANČÁRKOVÁ, T.; LINDSTRÖM, L.; VISKY, G. y ZOTZ, P., eds. *2021 13th International Conference on Cyber Conflict: Going Viral*. Tallin, NATO CCDCOE Publications, 2021, pp. 43-57.

[29] *The New York Times*. «EE. UU. es responsable del bombardeo a una escuela en Irán, según una investigación preliminar» [en línea]. *The New York Times*, 11 de marzo de 2026. [Consulta: 25 abril 2026]. Disponible en: https://www.nytimes.com/es/2026/03/11/espanol/estados-unidos/iran-ataque-escuela-responsable.html

La lección doctrinal es clara: calidad del dato, trazabilidad de la fuente, actualización de la información, revisión humana y auditabilidad del proceso no son aspectos administrativos, sino condiciones esenciales de legitimidad y eficacia militar. En un entorno crecientemente asistido por IA, esa exigencia se multiplica, porque los sistemas algorítmicos pueden acelerar el ciclo de *targeting* y conferir apariencia de certeza a inferencias que siguen dependiendo de datos falibles. La cuestión central no es solo quién aprieta el gatillo, sino quién valida la cadena cognitiva que convierte una información en objetivo.

Precisamente por ello, el debate sobre sistemas de armas autónomos conserva plena relevancia. El Comité Internacional de la Cruz Roja ha definido estos sistemas como aquellos que disponen de autonomía en funciones críticas —selección y ataque de objetivos— sin intervención humana, y ha recomendado prohibir los sistemas impredecibles y aquellos concebidos para aplicar la fuerza contra seres humanos, así como regular estrictamente los sistemas no prohibidos mediante límites de objetivo, tiempo, espacio, escala, situación de uso y requisitos de supervisión e intervención humana. La cuestión de fondo no es solo técnica, sino moral y jurídica: preservar la responsabilidad humana allí donde el empleo de la fuerza afecta directamente a la vida, la integridad y la dignidad de las personas[30].

La doctrina, por tanto, deberá evolucionar en tres planos complementarios. En primer lugar, el conceptual, para definir con precisión qué significa mandar, decidir y asumir responsabilidad en un entorno asistido por IA. En segundo lugar, el procedimental, para adaptar procesos de planeamiento, conducción, inteligencia, *targeting*, evaluación de daños y sostenimiento. Y, en tercer lugar, el formativo, para preparar a los cuadros de mando a ejercer juicio militar en un ecosistema en el que la información será más abundante, las recomendaciones más rápidas y la tentación de delegar más intensa.

Impacto en la inteligencia

La inteligencia es probablemente uno de los ámbitos más transformados por la IA. Durante décadas, el problema principal fue obtener información. Hoy, en muchos

[30] COMITÉ INTERNACIONAL DE LA CRUZ ROJA. *ICRC position on autonomous weapon systems* [en línea]. Ginebra, Comité Internacional de la Cruz Roja, 2021. [Consulta: 25 abril 2026]. Disponible en: https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems

dominios, el desafío es discriminar, verificar, interpretar y priorizar cantidades masivas de datos heterogéneos. La IA ofrece capacidades extraordinarias para detectar patrones débiles, correlacionar señales dispersas, traducir grandes volúmenes de texto, analizar imágenes, explotar fuentes abiertas y generar escenarios prospectivos.

La centralidad del dato aparece igualmente en la estrategia revisada de IA de la OTAN, que considera la disponibilidad y gestión de datos de calidad preparados para IA como requisito previo para desarrollar y emplear sistemas seguros, fiables y responsables. Esta idea resulta decisiva para la inteligencia militar: si los datos son incompletos, sesgados, obsoletos o manipulados, la IA no corrige el problema, sino que puede acelerarlo y conferirle una apariencia de certeza técnica[31].

El cambio fundamental consiste en el paso de la acumulación a la anticipación. La inteligencia apoyada en IA no se limita a ordenar información existente; puede ayudar a identificar anomalías, inferir tendencias, simular comportamientos adversarios y detectar indicadores tempranos. En el ciberespacio, esto se traduce en la posibilidad de descubrir vulnerabilidades antes que el adversario. Pero, como muestra Mythos, la misma capacidad que fortalece la defensa puede alterar el equilibrio ofensivo si reduce drásticamente el coste de encontrar y explotar fallos.

El segundo cambio afecta al papel del analista. La IA no elimina al analista, pero transforma su función. El analista deja de ser únicamente productor de informes para convertirse también en supervisor de sistemas, formulador de preguntas, validador de resultados, detector de sesgos y garante de contexto. La calidad de la inteligencia dependerá cada vez más de la calidad de la interacción entre humanos y sistemas automatizados. Preguntar bien será tan importante como interpretar bien.

El tercer cambio afecta a la inteligencia de fuentes abiertas. Internet ya obligó a comprender que la información militar no procedía solo de fuentes clasificadas. Hoy, la IA multiplica esa realidad. La explotación automatizada de redes sociales, imágenes satelitales comerciales, bases de datos públicas, foros técnicos, repositorios de código, publicaciones académicas y flujos financieros abre un espacio enorme de oportunidad, pero también de intoxicación. La abundancia informativa facilita tanto la anticipación como el engaño.

[31] NATO. *Summary of NATO's revised artificial intelligence strategy*, op. cit.

Esta línea se ve reforzada por el *Cuaderno de Inteligencia 3*, coordinado y elaborado bajo la responsabilidad del Departamento de Inteligencia de la ESFAS. Dedicado precisamente a la transformación de la inteligencia a través de la innovación, incluye trabajos sobre IA como factor transformador, análisis de fuentes abiertas, conciencia situacional cibernética y ciberdefensa[32]. La IA no solo acelera el ciclo de inteligencia; modifica la relación entre obtención, análisis, anticipación, validación y difusión.

El cuarto cambio se produce en el dominio cognitivo. La ETID 2026 reconoce expresamente esta expansión al definirlo como el ámbito de confrontación en torno a la narrativa y la percepción pública, la desinformación, la manipulación mediática y el empleo de redes sociales como armas. La detección de campañas hostiles, el análisis semántico y la protección del capital cognitivo aparecen así como líneas de evolución tecnológico-operativa en las que la IA adquiere un papel central[33].

Esta dimensión coincide con la preocupación expresada por la OTAN ante la desinformación y las operaciones de información habilitadas por IA. La generación de contenidos sintéticos, la segmentación de audiencias, la personalización de mensajes, la automatización de narrativas y la difusión masiva de materiales verosímiles obligan a ampliar la concepción tradicional de la inteligencia. Ya no se trata solo de comprender al adversario, sino de comprender cómo el adversario intenta modelar nuestra percepción y, cada vez más, cómo puede contaminar los sistemas de IA que utilizamos para interpretarla. A medida que mandos, analistas y organizaciones confíen en herramientas inteligentes para filtrar información, resumir fuentes o detectar tendencias, el envenenamiento de datos podrá dirigirse no solo contra las personas, sino también contra los sistemas que condicionan lo que esas personas llegan a considerar relevante, fiable o probable[34].

En este mismo sentido, el IEEE ya ha advertido sobre el empleo de la IA en la guerra híbrida como arma de desinformación, subrayando el papel de *fake news*, *deepfakes*, infoxicación y campañas digitales como amenazas para las sociedades democráticas[35].

[32] IEEE. *Cuaderno de Inteligencia 3: La transformación de la inteligencia a través de la innovación*. Madrid, Instituto Español de Estudios Estratégicos, 2025. Coordinado y elaborado bajo la responsabilidad del Departamento de Inteligencia de la Escuela Superior de las Fuerzas Armadas.
[33] MINISTERIO DE DEFENSA. *Estrategia de Tecnología e Innovación para la Defensa: ETID 2026*, op. cit.
[34] NATO. *Summary of NATO's revised artificial intelligence strategy*, op. cit.
[35] RODRÍGUEZ LORENZO, E.; MORALES, R.; CRESCENTE, D.; CABELLO, M. I. y PAZ, I. «La inteligencia artificial en la guerra híbrida como arma de desinformación». Documento de Opinión IEEE 61/2023, 16 de junio.

Esta dimensión confirma que la IA no solo actúa sobre sistemas técnicos, sino también sobre percepciones, narrativas y legitimidad.

Todo ello obliga a reforzar una idea clásica: más información no equivale necesariamente a mejor inteligencia, y más automatización no equivale necesariamente a mejor comprensión. La IA puede acelerar el análisis, pero también amplificar errores si se emplea sin control, sin contraste de fuentes o sin comprensión del contexto. La inteligencia militar deberá integrar capacidades algorítmicas sin abdicar del juicio crítico.

Impacto en la disuasión

La disuasión descansa tradicionalmente sobre tres pilares: capacidad, credibilidad y comunicación. La IA afecta a los tres.

Afecta a la capacidad porque puede mejorar la detección, la atribución, la defensa activa, la respuesta y la resiliencia. En el dominio ciberespacial, modelos capaces de identificar vulnerabilidades a gran escala pueden fortalecer la protección de infraestructuras críticas, pero también generar incertidumbre sobre la capacidad ofensiva de quien los posee. Si un Estado o una gran empresa tecnológica dispone de sistemas que encuentran vulnerabilidades desconocidas en software ampliamente utilizado, su posición estratégica cambia.

Afecta a la credibilidad porque introduce una forma nueva de opacidad. La disuasión, y especialmente la nuclear, nunca ha sido plenamente transparente; de hecho, la ambigüedad deliberada sobre umbrales, escenarios y voluntad de empleo ha formado parte de su eficacia. Pero en la disuasión nuclear clásica las capacidades estratégicas básicas eran relativamente identificables: arsenales, vectores, doctrinas declaradas, pruebas, despliegues o sistemas de alerta. En la disuasión algorítmica, por el contrario, la capacidad real puede ser invisible, secreta, distribuida y difícil de verificar. Un actor puede exagerar capacidades para disuadir, ocultarlas para explotarlas o comunicarlas parcialmente para condicionar comportamientos. El caso Mythos muestra precisamente esa ambigüedad: la comunicación de la capacidad produce efectos estratégicos aunque los detalles técnicos completos permanezcan restringidos.

Afecta a la comunicación porque la IA puede alterar las señales. En un entorno donde decisiones defensivas, alertas tempranas, atribuciones de ataque o recomendaciones de

respuesta se apoyan en sistemas automatizados, aumenta el riesgo de interpretación errónea. La velocidad puede reducir el tiempo de deliberación política. La opacidad puede dificultar la atribución. La automatización puede generar escaladas no intencionadas.

De ahí que podamos hablar de nuevas modalidades de disuasión: disuasión por superioridad informativa, disuasión por resiliencia algorítmica, disuasión por capacidad de descubrimiento de vulnerabilidades, disuasión cognitiva y disuasión por velocidad de decisión. Ninguna sustituye por completo a las formas clásicas, pero todas las complementan y complican.

En el ciberespacio, esta lógica resulta particularmente compleja. Como se ha señalado desde el Mando Conjunto del Ciberespacio, la disuasión tradicional encuentra límites importantes en este dominio por la dificultad de atribución, la actuación en zona gris y la ausencia de estructuras jurídicas plenamente eficaces. Ello obliga a combinar resiliencia, defensa activa, inteligencia, capacidad de respuesta y cooperación público-privada, especialmente cuando la IA puede acelerar tanto la detección defensiva como la explotación ofensiva de vulnerabilidades.

Esta dimensión de la disuasión tecnológica no puede separarse de la soberanía tecnológica, la autonomía industrial y la cadena de valor de la IA. La ETID advierte que la falta de apoyo al desarrollo de tecnologías emergentes puede traducirse en nuevas dependencias estratégicas futuras. En materia de IA, esa dependencia no afectaría solo a equipos o componentes, sino a modelos, datos, capacidades de entrenamiento, infraestructura computacional y control del ciclo de vida de sistemas críticos. La prospectiva tecnológica nacional añade otros factores de vulnerabilidad: dependencia de tecnologías importadas, falta de autonomía en sistemas críticos, escasez de especialistas en IA, ciberseguridad y sistemas autónomos, y ausencia de una regulación internacional suficientemente madura sobre usos militares de la IA. En la misma línea, el IEEE ha subrayado que la IA no es un producto aislado, sino una arquitectura compleja que integra materias primas, semiconductores, infraestructura digital, datos, algoritmos, capital humano y aplicaciones. Los cuellos de botella en cualquiera de estas capas pueden convertirse en vulnerabilidades estratégicas[36].

[36] Véanse MINISTERIO DE DEFENSA. *Estrategia de Tecnología e Innovación para la Defensa: ETID 2026*. Madrid, Secretaría de Estado de Defensa, Dirección General de Estrategia e Innovación de la Industria de Defensa, marzo

En consecuencia, la disuasión en la era de la IA no dependerá únicamente de disponer de mejores algoritmos. Exigirá preservar la libertad de uso, modificación y sostenimiento de las capacidades que condicionan la decisión y la acción militar; controlar, al menos en grado suficiente, la cadena de valor; formar talento propio; asegurar la explicabilidad; y garantizar que el empleo de la IA se mantiene dentro de marcos doctrinales, éticos y jurídicos robustos.

El riesgo principal es la inestabilidad. Si los actores creen que la ventaja pertenece a quien actúa primero, la IA puede incentivar comportamientos preventivos o preemptivos en el ciberespacio. Si las vulnerabilidades descubiertas superan la capacidad humana de parcheo, el sistema se vuelve más frágil. Si modelos equivalentes proliferan sin control, actores no estatales pueden acceder a capacidades antes reservadas a servicios especializados. Y si la defensa se automatiza sin gobernabilidad suficiente, los errores pueden escalar con rapidez.

La integración de IA en ámbitos de alta sensibilidad estratégica, como el nuclear, refuerza la necesidad de preservar la supervisión humana. La reflexión publicada por el IEEE sobre armas nucleares e inteligencia artificial sitúa precisamente la estabilidad estratégica en el equilibrio entre automatización tecnológica y capacidad de decisión humana, alertando de que los beneficios en alerta temprana, análisis y ciberseguridad no eliminan los riesgos asociados a su empleo en decisiones críticas[37].

La disuasión en la era de la IA exigirá, por tanto, no solo capacidades, sino también mecanismos de confianza, normas de comportamiento responsable, canales de comunicación, acuerdos entre aliados y criterios claros de control humano. La seguridad no dependerá únicamente de tener mejores algoritmos, sino de integrar esos algoritmos en arquitecturas políticas y doctrinales prudentes.

Esta necesidad de control y gobernanza ha sido formulada con particular fuerza por Henry A. Kissinger y Graham Allison al proponer una reflexión sobre el control de armamentos en inteligencia artificial inspirada, aunque no calcada, en las lecciones de

de 2026; FUNDACIÓN CÍRCULO DE TECNOLOGÍAS DE LA DEFENSA Y LA SEGURIDAD. *Áreas tecnológicas y científicas de especial relevancia para la defensa: resumen de los informes finales de los grupos de trabajo del año 2024*. Madrid, Fundación Círculo de Tecnologías de la Defensa y la Seguridad, noviembre de 2025; y GARCÍA RETUERTA, Óscar y GARCÍA-RETUERTA, David. «La cadena de valor de la inteligencia artificial: estrategias de autonomía para España». Documento de Opinión IEEE 03/2026, 12 de enero.

[37] RODRÍGUEZ LA BARRERA, Luciana Alejandra. «Armas nucleares e inteligencia artificial: un equilibrio entre la automatización y el factor humano». Documento de Opinión IEEE 10/2026, 29 de enero.

la era nuclear. Su planteamiento parte de una advertencia: la IA podría erosionar mecanismos esenciales de estabilidad estratégica, debilitar monopolios estatales sobre determinadas formas de violencia masiva o facilitar a actores reducidos capacidades de daño hasta ahora reservadas a grandes potencias. Sin embargo, los propios autores subrayan que la analogía nuclear tiene límites decisivos: mientras la tecnología nuclear fue desarrollada principalmente por Estados, la IA avanza impulsada por empresas privadas; mientras las armas nucleares son objetos físicos relativamente contables, la IA es digital, conceptual y difícil de verificar; y mientras el control nuclear se desarrolló durante décadas, la IA evoluciona y se difunde a una velocidad que estrecha dramáticamente los márgenes de negociación.

De ahí que el control de la IA estratégica exija instrumentos nuevos: diálogo entre las principales potencias tecnológicas, cooperación entre gobiernos y empresas, pruebas de estrés de modelos antes de su despliegue, mecanismos de transparencia adecuados al carácter digital de la tecnología, canales de comunicación científica y política, y eventualmente marcos internacionales capaces de limitar sus aplicaciones más peligrosas. La lección no es que la IA sea “la nueva arma nuclear”, sino que, como ocurrió con la energía atómica, determinadas tecnologías obligan a pensar la seguridad más allá de la ventaja inmediata y a reconocer que incluso los competidores estratégicos pueden compartir un interés superior: evitar una catástrofe que ninguno podría controlar[38].

El CESEDEN y la ESFAS ante el cambio: formar para decidir en la era de la IA

Si la inteligencia artificial transforma la forma de observar, orientar, decidir y actuar, la enseñanza militar superior no puede limitarse a incorporar módulos técnicos sobre nuevas tecnologías. Debe formar mandos capaces de comprender su alcance estratégico, sus límites, sus riesgos y sus implicaciones éticas. El reto no consiste solo en conocer la herramienta, sino en formar criterio para emplearla, supervisarla y limitarla cuando sea necesario.

El CESEDEN no se aproxima ahora por primera vez a esta cuestión. Su propia actividad reciente muestra una búsqueda permanente de conocimiento, en sentido amplio, sobre

[38] KISSINGER, Henry A. y ALLISON, Graham. «The Path to AI Arms Control: America and China Must Work Together to Avert Catastrophe» [en línea]. *Foreign Affairs*, 13 de octubre de 2023. [Consulta: 25 abril 2026]. Disponible en: https://www.foreignaffairs.com/united-states/henry-kissinger-path-artificial-intelligence-arms-control.

el impacto de la tecnología en la defensa. Así lo evidencian tanto la presentación de la *Estrategia de Tecnología e Innovación para la Defensa 2026* como la de los trabajos de prospectiva tecnológica nacional desarrollados en torno a las áreas científicas y tecnológicas de especial relevancia para la defensa. Ambos documentos, presentados recientemente en el CESEDEN, confirman que la inteligencia artificial debe entenderse dentro de una transformación más amplia: tecnológica, doctrinal, industrial, formativa y cultural[39] [40].

Como se ha señalado, ya en 2019 organizó, junto con la Universidad Politécnica de Madrid, un curso de verano dedicado al impacto de la inteligencia artificial en defensa y seguridad, y la producción reciente del IEEE ha abordado la IA desde perspectivas complementarias: defensa, automatización, robótica, inteligencia, guerra híbrida, desinformación, planeamiento operacional, autonomía estratégica, cadena de valor digital y estabilidad nuclear. La cuestión, por tanto, no es iniciar la reflexión, sino avanzar desde la reflexión hacia la implantación doctrinal, formativa y cultural. En términos clásicos, ha llegado el momento de pasar de las musas al teatro[41].

En este punto, el CESEDEN y la ESFAS ocupan una posición singular dentro de las Fuerzas Armadas españolas. La ESFAS forma a los oficiales de Estado Mayor, capacita en inteligencia y planeamiento operacional, prepara a oficiales para la alta gestión administrativa de recursos logísticos, financieros, humanos y patrimoniales, y actualiza conocimientos de coroneles y capitanes de navío con potencial de ascenso al generalato. Esa configuración convierte a la Escuela en un espacio privilegiado para anticipar cambios, absorber innovación, generar doctrina práctica y modelar la cultura profesional de quienes deberán ejercer el mando y asesorar al nivel político-militar.

Esa función no se limita a la docencia reglada. La coordinación y elaboración del *Cuaderno de Inteligencia 3* por el Departamento de Inteligencia de la ESFAS, junto con varios trabajos de fin de máster de alumnos del curso de Estado Mayor dedicados a la

[39] MINISTERIO DE DEFENSA. *Estrategia de Tecnología e Innovación para la Defensa: ETID 2026*, op. cit.
[40] FUNDACIÓN CÍRCULO DE TECNOLOGÍAS DE LA DEFENSA Y LA SEGURIDAD. *Áreas tecnológicas y científicas de especial relevancia para la defensa*, op. cit.
[41] Véanse CESEDEN y UNIVERSIDAD POLITÉCNICA DE MADRID. *Impacto de la inteligencia artificial en Defensa y seguridad*. Programa del curso de verano de la Cátedra Ingeniero General D. Antonio Remón y Zarco del Valle, 2-4 de julio de 2019; IEEE. *Cuaderno de Estrategia 226: La inteligencia artificial en la geopolítica y los conflictos*, op. cit.; ROLDÁN TUDELA, José María. *La inteligencia artificial aplicada a la defensa*, op. cit.; y CCDC. *Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R)*, op. cit.

IA[42], muestran que la Escuela puede actuar también como foco de producción intelectual aplicada, conectando enseñanza, inteligencia, innovación y reflexión doctrinal. En un ámbito como la inteligencia artificial, esa capacidad de generar pensamiento desde la experiencia docente y profesional resulta especialmente valiosa[43].

La inteligencia artificial tendrá un impacto enorme en el nivel táctico, donde puede automatizar tareas, acelerar procesos, mejorar sensores, fuegos, protección, logística, mantenimiento, reconocimiento, vigilancia o análisis inmediato del entorno. En ese nivel, la ventaja estará muy vinculada a la rapidez, la precisión, la automatización y la capacidad de operar bajo saturación informativa. Pero a medida que se asciende al nivel operacional y estratégico-militar, el problema cambia de naturaleza. Allí donde aparece el arte —arte operacional, pensamiento estratégico, conducción de campañas, articulación de medios y fines— el factor humano no disminuye, sino que aumenta.

La razón es sencilla: ninguna guerra futura será igual a la anterior. No lo será solo por la evolución material de los sistemas de armas, sino porque la guerra es siempre combinación singular de factores políticos, humanos, morales, tecnológicos, geográficos, logísticos, económicos y culturales. La IA puede analizar precedentes, identificar patrones, generar opciones y simular escenarios; pero la creatividad militar consiste precisamente en combinar factores de un modo no previsto, en interpretar lo excepcional, en convertir restricciones en oportunidades y en producir sorpresa allí donde el adversario espera regularidad. La victoria rara vez procede de aplicar mecánicamente una solución anterior; nace de comprender una situación concreta mejor que el adversario y actuar sobre ella con decisión, oportunidad y sentido.

La experiencia del XXIV Curso de Capacitación para el Desempeño de los Cometidos de Oficial General resulta ilustrativa. En aquella clausura se subrayaba que los concurrentes estaban llamados a ejercer el mando de grandes unidades, dirigir órganos de planeamiento, gestionar programas principales, ocupar puestos de alta responsabilidad en estados mayores nacionales y multinacionales y auxiliar al Gobierno en la gestión de la Defensa. Esa es precisamente la generación de mandos que deberá decidir en

[42] En los últimos cursos de Estado Mayor se han presentado diversos trabajos de fin de máster relacionados con inteligencia artificial, planeamiento, inteligencia, mando y control o transformación tecnológica. Se citan aquí como indicio de la incorporación progresiva de esta línea de reflexión a la actividad académica de la ESFAS.
[43] IEEE. *Cuaderno de Inteligencia 3: La transformación de la inteligencia a través de la innovación*, op. cit.

entornos crecientemente condicionados por la IA: no para delegar el juicio en el sistema, sino para utilizarlo como apoyo sin abdicar de su responsabilidad.

El reto formativo no consiste en convertir a todos los oficiales en ingenieros de inteligencia artificial. Consiste en formar jefes capaces de hacer las preguntas correctas: qué datos alimentan el sistema, qué sesgos contiene, qué grado de explicabilidad ofrece, qué margen de error admite, qué decisiones pueden automatizarse, cuáles requieren intervención humana directa, qué riesgos introduce su uso y qué ocurre si el sistema falla, es manipulado o no está disponible.

La formación aparece, así, como condición de posibilidad de la implantación responsable de la IA. La *Visión de la Inteligencia Artificial en las FAS* señala la necesidad de captar y retener personal especializado, pero también de formar y concienciar al usuario no especializado. La estrategia revisada de IA de la OTAN apunta en la misma dirección al reclamar una fuerza laboral aliada preparada para la IA, programas de reciclaje, alta especialización y una integración más profunda de expertos técnicos en operaciones militares. Para la ESFAS, esto confirma que la enseñanza militar superior debe formar mandos capaces de comprender la IA sin convertirse necesariamente en técnicos, dialogar con especialistas y ejercer juicio militar responsable en entornos asistidos por sistemas inteligentes[44][45].

Esta necesidad de incorporar la IA a la formación de los futuros líderes militares ha sido abordada también en publicaciones recientes del IEEE. Soriano Morales ha señalado que la inteligencia artificial puede contribuir a transformar la formación de oficiales mediante herramientas de simulación, análisis de decisiones, personalización del aprendizaje y apoyo al liderazgo, siempre que su empleo se oriente a mejorar el criterio profesional y no a sustituir la responsabilidad del mando[46]. Esta perspectiva refuerza la idea de que la enseñanza militar superior debe integrar la IA no solo como objeto de estudio, sino como instrumento pedagógico y como desafío ético-profesional.

[44] ESTADO MAYOR DE LA DEFENSA. *Visión de la inteligencia artificial en las FAS*, op. cit.
[45] NATO. *Summary of NATO's revised artificial intelligence strategy*, op. cit.
[46] SORIANO MORALES, Pedro. «ESFAS. Revolucionando el liderazgo militar: implementación de la inteligencia artificial en la formación de oficiales» [en línea]. CESEDEN, 30 de mayo de 2025. [Consulta: 25 abril 2026]. Disponible en: https://www.defensa.gob.es/ceseden/-/esfas/revolucionando_el_liderazgo_militar_implementacion_de_la_inteligencia_artificial_en_la_formacion_de_oficiales

La ESFAS debe actuar, por tanto, como motor de adaptación doctrinal. No porque deba resolver por sí sola todos los retos tecnológicos, sino porque forma a quienes integrarán esos retos en el planeamiento, el mando, la gestión y el asesoramiento estratégico. La enseñanza militar superior no solo transmite conocimiento: construye criterio. Y en la era de la IA, el criterio será más necesario que nunca.

Esta exigencia de juicio no es nueva. La tradición militar española cuenta con una referencia particularmente valiosa en el marqués de Santa Cruz de Marcenado[47], cuyas *Reflexiones militares* de inicios del siglo XVIII comienzan, significativamente, por las virtudes morales, políticas y militares del general[48]. Marcenado no se detiene en las cualidades que dependen de la naturaleza o de la fortuna, sino en aquellas que pueden adquirirse mediante diligencia, disciplina y formación. Su advertencia sobre la necesidad de que el jefe sea dueño de sus pasiones conserva plena vigencia en la era de la inteligencia artificial: el mando debe dominar no solo el temor, la ira o la ambición, sino también la fascinación por la velocidad, la automatización y la aparente certeza del sistema.

El propio Marcenado advertía al lector contra el rechazo precipitado de las novedades militares, recordando que las mutaciones en la calidad de las armas y en la formación de las tropas demostraban que no era temerario proponer cosas nuevas cuando se sometían al examen de sus motivos y pruebas[49].

La vigencia de Marcenado no reside en haber anticipado técnicamente la inteligencia artificial, sino en haber situado el conocimiento, la previsión y el dominio racional de las pasiones en el centro del mando. Cuando defendía que el general podía aprender por la lectura de las historias lo que la experiencia directa tardaría años en enseñarle, estaba subrayando una idea que conserva plena actualidad: la experiencia militar no debe limitarse a lo vivido personalmente, sino que puede y debe ampliarse mediante el estudio sistemático de los precedentes. La IA puede hoy multiplicar esa capacidad de búsqueda,

[47] Se cita el prólogo «Al lector» por la edición original de 1730 y el cuerpo de las *Reflexiones militares* por la edición de la Comisión Española de Historia Militar de 1984. Para la recepción e influencia de la obra, véase FERNÁNDEZ GARCÍA, Pelayo. *Las Reflexiones militares del marqués de Santa Cruz de Marcenado y su influencia más allá de las fronteras nacionales*. Madrid, Ministerio de Defensa, 2015.

[48] NAVIA-OSORIO Y VIGIL, Álvaro de. *Reflexiones militares*. Madrid, Consejo Superior de Investigaciones Científicas / Comisión Española de Historia Militar, 1984. ISBN 978-84-00-05818-0.

[49] NAVIA-OSORIO Y VIGIL, Álvaro de. *Reflexiones militares del marqués de Santa Cruz de Marzenado, mariscal de campo de los exércitos de su magestad cathólica* [en línea]. [S. l.], Imprenta de Simón Langlois, 1730. [Consulta: 25 abril 2026]. Disponible en: https://archive.org/details/bub_gb_wnEPgoRKenAC

comparación y explotación de datos, pero no reemplaza la comprensión histórica que permite distinguir entre analogías útiles y semejanzas engañosas[50].

También resulta sugerente su preferencia por el consejo de los libros frente al consejo sometido a pasiones, intereses o lisonjas[51]. En términos contemporáneos, los sistemas de apoyo a la decisión pueden contribuir a ordenar información, reducir la presión emocional del momento y ofrecer alternativas que el mando quizá no habría considerado. Pero la comparación tiene un límite esencial: la IA no es un consejero moralmente puro, sino un sistema dependiente de datos, modelos, supuestos y criterios de diseño. Por eso, el verdadero heredero del espíritu de Marcenado no sería el mando que obedece al algoritmo, sino el que lo interroga críticamente para decidir mejor.

La lección de 2023 sobre valores del generalato conserva, por ello, plena vigencia. La IA puede proporcionar datos, hipótesis, simulaciones y recomendaciones; puede incluso ayudar a ordenar el pensamiento, acelerar análisis y ampliar perspectivas. Pero no posee conciencia, honor, prudencia ni responsabilidad moral. La tecnología no cambia los valores militares; modifica las competencias necesarias para ejercerlos. Esa distinción debe presidir cualquier incorporación de IA a la formación militar: apertura a la innovación, sí; delegación irreflexiva del juicio, no.

La enseñanza militar superior debe, en definitiva, capacitar técnicamente para comprender la IA, pero también preservar y actualizar las virtudes superiores del mando: carácter, templanza, responsabilidad, sentido ético, creatividad, capacidad de juicio y comprensión histórica de la guerra. Porque la IA podrá acelerar el combate y multiplicar las opciones del mando, pero no puede absolverlo de pensar la guerra.

Conclusiones

Primera. El caso Anthropic/Mythos constituye algo más que una noticia tecnológica. Representa un síntoma de transición: la inteligencia artificial avanzada empieza a producir efectos estratégicos por su mera existencia, por sus capacidades atribuidas, por la forma en que se comunica y por las decisiones de acceso, restricción o colaboración que provoca.

[50] NAVIA-OSORIO Y VIGIL, Álvaro de. *Reflexiones militares*, op. cit.
[51] NAVIA-OSORIO Y VIGIL, Álvaro de. *Reflexiones militares*, op. cit.

Segunda. La IA no es un actor estratégico en sentido pleno, pero tampoco puede ser tratada ya como una herramienta pasiva. Su integración en procesos críticos de ciberseguridad, inteligencia, mando y control, disuasión y gobernanza la convierte en una infraestructura estratégica con efectos cuasi-actoriales.

Tercera. La evolución actual se inserta en una secuencia histórica reconocible: telefonía móvil, Internet, sistemas autónomos e IA generativa. Cada irrupción tecnológica ha sido inicialmente interpretada como instrumento auxiliar y ha terminado modificando vulnerabilidades, procedimientos, estructuras y formas de pensar. La novedad actual es que la IA incide directamente en el proceso cognitivo de la decisión.

Cuarta. En doctrina militar, la IA comprimirá los ciclos de decisión, obligará a redefinir la integración hombre-máquina, introducirá nuevas vulnerabilidades algorítmicas y exigirá una interoperabilidad ética, jurídica y técnica entre aliados.

Quinta. En inteligencia, la IA permitirá pasar de la acumulación masiva de información a la anticipación apoyada en patrones, anomalías y simulaciones. Pero también incrementará los riesgos de intoxicación, sesgo, dependencia y manipulación cognitiva.

Sexta. En disuasión, la IA alterará capacidad, credibilidad y comunicación. Su impacto será especialmente relevante en el ciberespacio, donde la frontera entre defensa y ataque puede estrecharse y donde la velocidad de descubrimiento de vulnerabilidades puede superar la capacidad humana de mitigación.

Séptima. El CESEDEN y la ESFAS deben asumir un papel central como motores de adaptación. La respuesta no puede limitarse a adquirir herramientas, sino que debe formar criterio, doctrina, cultura ética y capacidad de mando en un entorno donde la IA asistirá, condicionará y acelerará la decisión.

Octava. La historia militar recuerda que ninguna innovación tecnológica deroga los planos humanos, políticos y morales de la guerra. La IA puede multiplicar la capacidad de procesamiento, pero no sustituye la razón práctica del mando. Marcenado nos recuerda que la guerra no la gana quien acumula más información, sino quien sabe convertirla en juicio.

La inteligencia artificial no decidirá por sí sola el resultado de los conflictos, pero transformará el entorno en el que los responsables políticos y militares deberán decidir.

Y en la guerra, como en toda competencia estratégica, quien no comprende a tiempo el nuevo entorno acaba decidiendo tarde.

Teniente general Miguel
*Ballenilla y García de Gamarra**
Director del Centro Superior de Estudios de la Defensa Nacional