USOS, RETOS Y OPORTUNIDADES DE LA INTELIGENCIA ARTIFICIAL EN EL EJÉRCITO

Uses, challenges and prospects of Artificial Intelligence for the Army

MIGUEL MANUEL PAREJA PÉREZ[1]

RESUMEN: La inteligencia artificial recientemente se ha convertido en objeto de múltiples especulaciones, más o menos fundamentadas, y se ha visto rodeada de un halo de miedo y misterio basado en la visión que las obras de ciencia ficción literarias y cinematográficas han proyectado sobre esta tecnología sustentada en la computación y la gestión masiva de datos.

Este artículo pretende mostrar las ventajas que la inteligencia artificial aporta al Ejército y los retos a los que éste ha de hacer frente para que su empleo esté de acuerdo con las leyes y usos de la guerra, entendida ésta como un fenómeno que no por indeseado ha de obviarse, como bien demuestra la actualidad y la historia.

Partiendo de una situación ficticia para enmarcar el escenario operativo futuro, se describen las estrategias que la OTAN y España están desarrollando para integrar la inteligencia artificial en las operaciones militares así como las áreas concretas de aplicación que se consideran prioritarias y que ya se están llevando a cabo en el ámbito de la industria de defensa.

Finalmente, se abordan los retos éticos que el uso de esta tecnología plantea, reconociendo que el imperio de la ley, como en todas las esferas de actividad humana, habrá de establecer sus límites. Uso ético y responsable y respeto al Derecho Internacional Humanitario han constituido siempre la vocación y la norma de actuación del Ejército español.

PALABRAS CLAVE: Inteligencia Artificial, Big Data, Estrategia, Disuasión, Defensa, Guerra, Conflicto, OTAN, Ejército, Ciberdefensa, Ciberespacio, MADOC, DIDOM, Tecnología, Ámbito Cognitivo, Espacio, Robots, Autonomía, Armas Autónomas, Vehículos Autónomos, Mando y Control, Multidominio.

ABSTRACT: Artificial intelligence has recently become the object of multiple speculations, more or less founded, and is surrounded by a halo of fear and mystery based upon the vision that sci-fi artwork either literary or film has projected on this technology sustained by computing and big data.

This article tries to show the advantages of artificial intelligence for the Army and the challenges that the latter needs to tackle to achieve its use according to the laws and customs of war, understanding war as an undesirable but real phenomena, as present and history well prove.

Departing from a fictional situation to frame the future operating environment, NATO and Spain's strategies for the integration of artificial intelligence in military operations are described, as well as prioritized specific applications of this technology in defense industry.

[1] Coronel de Infantería DEM, Dirección de Investigación, Doctrina, Orgánica y Materiales, Mando de Adiestramiento y Doctrina, Granada. E-mail: mparper@gmail.com

Finally, the ethical challenges posed by artificial intelligence are presented, recognizing that the rule of law will have to establish its boundaries, as it usually does for all human activity sphere. Ethical and responsible use and respect for the International Humanitarian Law has always been the Spanish Army's foundation and standard of conduct.

KEY WORDS: Artificial Intelligence, Big Data, Strategy, Deterrence, Defense, War, Warfare, Conflict, NATO, Army, Cyber, Cyberdefense, Cyberspace, Technology, Cognitive Domain, Space, Robots, Autonomy, Autonomous Weapons, Autonomous Vehicles, Command and Control, Multidomain.

I. VISIONANDO EL FUTURO…

Tras la segunda guerra contra Timor, Indonesia ha colapsado y devenido en un estado fallido dominado por la anarquía y la fragmentación. En Dhahran, al este de Arabia Saudí, ha detonado una bomba sucia creando un área de dispersión radiológica y provocando un alza masiva del precio del petróleo. Un nuevo yacimiento de gas descubierto en la fosa de las Marianas proporciona seguridad energética a China sin miedo a repercusiones o sanciones de EEUU; China está ahora gobernada por el Directorio, una coalición de hombres de negocios y líderes militares que ha sustituido al Partido Comunista Chino, derrocado por movimientos populares.

China y Rusia han desarrollado una tecnología capaz de detectar y rastrear los buques propulsados por energía nuclear, lo que en la práctica les permite neutralizar la flota submarina nuclear de EEUU. China mantiene sus planes para conseguir el control de la tercera cadena de islas (Aleutianas, Hawái, Kiribati, Samoa americana y Nueva Zelanda)[2] que les asegure el dominio seguro del Pacífico occidental. Mientras tanto, las fuerzas armadas americanas se encuentran desbordadas en personal y material por las operaciones en Afganistán, Yemen y Kenia.

Empleando un virus informático para infiltrarse en los sistemas informáticos de la Agencia de Inteligencia de Defensa, China lanza un ciberataque masivo contra EEUU que daña muchos de sus sofisticados sistemas tecnológicos, incluidos los caza-bombarderos F-35 *Lightning*, de última generación, que se han visto comprometidos por microchips de origen chino infectados en la cadena de suministros. El ataque incluye un amplio uso de armas anti satélite que provocan la caída del Sistema de Posicionamiento Global GPS y la pérdida de varios satélites militares críticos de comunicaciones y reconocimiento.

Los cazas y drones rusos tienen capacidad para lanzar un ataque sobre la base americana de Okinawa, y neutraliza la presencia militar norteamericana en Japón. Con el apoyo de Rusia, China toma finalmente Hawái tras una lucha encarnizada y establece en el archipiélago una Zona Administrativa Especial. Como resultado del ataque, la Flota americana del Pacífico queda prácticamente destruida. Los residentes

[2] Para más información sobre las cadenas de islas del pacífico, consúltese Fallon, 2020.

de la isla de Oahu junto a los militares supervivientes organizan una insurgencia para oponerse a la ocupación china empleando las tácticas aprendidas de los movimientos insurgentes en Irak y Afganistán.

En el campo diplomático, la OTAN ha sido disuelta y los antiguos aliados de EEUU deciden mantenerse neutrales en la contienda con la excepción de Australia y de Reino Unido, este último aún resentido por la reciente escisión de Escocia tras un segundo referéndum de independencia llevado a cabo aprovechando la situación de conflicto. Para contrarrestar el sistema de detección de submarinos nucleares, Polonia cede parte de sus submarinos diésel a la Marina americana a cambio de diez bombas termonucleares que le permitan disuadir a Rusia, y la recientemente independiente Groenlandia proporciona a cambio de reconocimiento internacional su flota de rompehielos para facilitar su movimiento a través del Paso del Noroeste.

En el frente civil, compañías privadas como Walmart han establecido una cadena de suministros militares construidos con tecnología de impresión aditiva 3D, y el Gobierno americano ha iniciado un programa de reciclado de viejos microchips para sustituir los infectados proporcionados por China. Un excéntrico multimillonario de Silicon Valley ha puesto a disposición del gobierno su constelación de satélites privados para neutralizar los sistemas espaciales chinos. Simultáneamente, otro magnate está financiando su propia campaña de ciberataques con la colaboración del grupo de *hacktivistas* Anonymous para degradar las redes chinas y deteriorar sus capacidades para la ciberguerra…

Lo que en estos primeros párrafos se describe es una situación ficticia extraída de la trama de la obra "*Ghost Fleet: A Novel of the Next World War*" (Singer y Cole, 2015), de los profesores americanos August Cole y P.W. Singer, en la que emplean un modelo de inteligencia narrativa, al que denominan FICINT (*fiction + intelligence*)[3], para explorar los conflictos del futuro por medio de narraciones, charlas y talleres, que les han llevado a ser un referente en la exploración del futuro y a colaborar con instituciones tan destacadas como el Consejo Atlántico o el Instituto Nobel de Oslo.

Todos los Ejércitos del mundo disponen de sus propios observatorios de conflictos y de institutos de prospectiva que les ayuden a entender cómo será el entorno operativo futuro con la suficiente antelación (normalmente de 15 a 20 años) para poder adaptar sus medios, tácticas, técnicas y procedimientos a las previsibles amenazas que deberán afrontar en caso de conflicto, y de esa manera también prevenirlas y evitarlas.

Este esfuerzo tiene una relevancia enorme puesto que contribuye a la disuasión frente a potenciales adversarios y disminuye las amenazas, algunas existenciales, contra la nación. Por tal motivo, en su consecución las naciones emplean importantes recursos, ya sean humanos, económicos o materiales. Así, el planeamiento de la defensa en España parte del análisis del entorno previsible para determinar qué se necesita para afrontarlo.

[3] Consúltese https://www.augustcole.com/ficint para más información sobre el uso de la ficción para la inteligencia militar.

La Dirección de Investigación, Doctrina, Orgánica y Materiales (DIDOM) del MADOC[4], contribuye a este esfuerzo en el ámbito del Ejército de Tierra. Entre sus análisis destaca la elaboración del Entorno Operativo Terrestre Futuro, cuya última edición comprende el horizonte temporal en torno al año 2035, que pretende servir de documento de reflexión sobre el contexto en el que tendrán que operar las fuerzas terrestres, las estrategias de los potenciales adversarios y qué necesidades de innovación son necesarias para adaptarse a los futuros escenarios de actuación. En su redacción participaron expertos militares y civiles pertenecientes al Grupo de Estudios en Seguridad Internacional de la Universidad de Granada.

Otros estudios de la DIDOM relacionados con la evolución del combate y análisis del conflicto son el documento Tendencias, cuya última edición correspondiente al bienio 2020-2021 recoge los principales elementos de transformación de los ejércitos de nuestro entorno, y los Boletines Informativos sobre los principales conflictos en curso, en particular los correspondientes a la guerra Rusia-Ucrania, de periodicidad quincenal.

II. … Y EL PRESENTE

El actual conflicto entre Rusia y Ucrania ha puesto de manifiesto la inevitable realidad de una guerra a escasos kilómetros de las fronteras aliadas en lo que constituye una amenaza existencial que la propia OTAN acaba de reconocer en la Cumbre de Madrid del 28-29 Junio y que recoge en su Concepto Estratégico para la próxima década (OTAN, 2022).

El nuevo Concepto Estratégico de la OTAN marca la estrategia general de la Alianza Atlántica, clarifica los valores fundamentales que defiende, sus principios y objetivos. La OTAN es una alianza de 30 naciones que protege a mil millones de ciudadanos y necesita una estrategia que evalúe el entorno de seguridad y determine las tareas y prioridades para hacerle frente y cómo cumplir con esa misión juntos como aliados. Algunos elementos del Concepto Estratégico 2010 de Lisboa, como el papel central del vínculo transatlántico en la seguridad común o la importancia de defender los valores compartidos, siguen siendo relevantes. Pero el mundo era distinto en 2010 y desde entonces se han producido grandes cambios en el entorno de seguridad que han obligado a su revisión. La anexión de Crimea y la invasión del este de Ucrania en 2014 por parte de Rusia, el auge del Daesh en medio oriente, la intensificación de la competición estratégica, particularmente con China tras el ascenso en 2013 de Xi Jinping en Pekín, y finalmente la agresión rusa contra Ucrania en 2022, han supuesto el inicio del mundo actual y el regreso a la competencia entre las grandes potencias.

Para la OTAN ahora la Federación Rusa es la amenaza más importante y directa para la seguridad de los Aliados y para la paz y estabilidad en el área euroatlántica. Considera que Rusia busca establecer esferas de influencia y control directo a través de la coerción, la subversión, la agresión y la anexión, empleando medios convencionales,

[4] El MADOC es el Mando de Adiestramiento y Doctrina del Ejército de Tierra, encargado de liderar el apoyo a la preparación de la Fuerza Terrestre.

cibernéticos e híbridos. La Federación Rusa está modernizando sus fuerzas nucleares y amenaza con su empleo con el objeto de desestabilizar el Este y Sur de la Alianza.

Si recordamos la narración con la que comenzábamos este artículo, muchos de sus elementos están presentes en la guerra de Ucrania:

- La importancia del factor económico. Por mucho empeño que un país ponga en su defensa, necesita unas cantidades ingentes de recursos económicos para sostener el esfuerzo bélico. En el caso de Ucrania, el presidente Zelenski los ha estimado en 5.000 millones de dólares mensuales (Brown y Ahmedzade, 2022). En relación con el otro bando, las sanciones contra Rusia buscan debilitarla con el doble objeto de mostrar determinación por parte de la comunidad internacional y disminuir la capacidad rusa de financiar su campaña militar, si bien su eficacia se ve limitada debido a la inmensa cantidad de recursos naturales de Rusia y a sus alternativas comerciales; China, África o la India siguen siendo compradores netos de recursos energéticos o material militar. Las maniobras europeas para conseguir la seguridad energética autónoma de Rusia forman también parte de esta estrategia.
- La resistencia civil y militar de los ucranianos está siendo admirable. Seguramente este es el primer factor del éxito que la lucha contra la invasión rusa tuvo en las primeras semanas del conflicto, cuando se detuvo la ofensiva generalizada y obligó a Rusia a cambiar su estrategia y centrarse en las regiones del Dombás y la costa del Mar Negro y Mar de Azov.
- A pesar del heroico comportamiento de la población y del ejército ucraniano, sin apoyo internacional Ucrania habría sucumbido hace mucho tiempo. Muchas naciones, incluida España, están proporcionando ayuda económica, diplomática, humanitaria y militar a este país. Aquí la clave será mantener el compromiso y sostener el apoyo a pesar del alargamiento del conflicto. Nadie sabe cuánto durará la guerra ni cuál será el resultado; por eso es crítico adoptar una postura decidida y tomar medidas a largo plazo desde el principio.
- Difíciles de atribuir y contrarrestar, se sabe que ambos bandos han hecho uso de diversas acciones cibernéticas contra su adversario y contra países y organizaciones colaboradoras, como la OTAN o la UE en el lado ucraniano. En la práctica, las acciones rusas han sido menos eficaces de lo esperado y se han centrado en: ataques rusos muy puntuales a infraestructuras críticas y servicios esenciales de Ucrania; ataques masivos rusos a sitios web de Ucrania (fundamentalmente, DDoS[5]); numerosos *defacements*[6] en sitios oficiales de Ucrania; campañas de *phishing*[7] y suplantaciones de identidad a media escala

[5] DDoS es el acrónimo de denegación distribuida de servicios, un tipo de ciberataque que interrumpe o degrada un servicio virtual, por ejemplo una página web, por medio de su saturación enviándole una avalancha de peticiones que no es capaz de atender. Véase https://www.incibe.es/protege-tu-empresa/blog/medidas-prevencion-ataques-denegacion-servicio para más información.

[6] El *defacement* es un tipo de ciberataque que se realiza contra un sitio web, en el que se modifica la apariencia de alguna de sus páginas. Véase https://www.incibe.es/aprendeciberseguridad/defacement para más información.

[7] El *phishing* es una técnica que consiste en el envío de un correo electrónico a un usuario simulando ser una entidad legítima, con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo. Véase https://www.incibe.es/aprendeciberseguridad/phishing para más información.

en redes sociales; distribución limitada de malware ruso de sofisticación media-baja (Cubeiro Cabello, 2022). Asombrosamente, el ámbito de actividad de estas acciones ha quedado principalmente circunscrito a Ucrania. Del lado ucraniano, Anonymous y otros grupos hacktivistas han tomado partido contra Rusia, si bien con escaso impacto hasta la fecha. De cualquier manera, la dificultad a la hora de atribuir las acciones cibernéticas y el secreto que rodea a sus verdaderos efectos, no permiten asegurar qué eficacia real han tenido. Lo que sí parece es que el ciberespacio no está jugando el papel decisivo que muchos pensábamos, quizás porque Ucrania se había preparado muy bien en los aspectos de ciberseguridad. Pero puede que muchas de las capacidades cibernéticas de ambos contendientes estén aún por desplegar y que la importancia del ciberespacio en los conflictos futuros sea cada vez mayor.

- Las guerras no las hacen (solo) los soldados. Toda la sociedad y todos los sectores civiles se ven implicados de una forma u otra y tienen mucho que aportar. Tradicionalmente hablamos de los cuatro instrumentos de poder de una nación (diplomático, informativo, militar y económico), como el conjunto de herramientas que determinan la capacidad de influencia de un país sobre los demás. En la dinámica geopolítica actual de competición o incluso de conflicto, las Fuerzas Armadas no siempre serán el instrumento más importante para defender los intereses nacionales. Hoy en día cualquier actuación en el ámbito de seguridad y defensa para tener éxito requiere de la acción integrada de los instrumentos del Estado y también de los sectores sociales. En lo diplomático, la OTAN permanece dispuesta a mantener abiertos los canales de comunicación con Moscú para gestionar y mitigar los riesgos, evitar la escalada y aumentar la transparencia, y advierte que cualquier cambio en la relación con Rusia depende de que detenga su comportamiento agresivo, sus políticas y acciones hostiles y cumpla plenamente con el derecho internacional.
- En el caso del conflicto Rusia-Ucrania, ha sido muy destacado el uso de la constelación de satélites privados de Elon Musk para proporcionar cobertura de comunicaciones e internet a los militares y a la población ucraniana sin depender de la infraestructura dañada por los ataques rusos. Podemos ver otros ejemplos de participación del sector civil en las redes de ayuda humanitaria que han dado soporte a refugiados o en las acciones cibernéticas que algunos grupos privados han llevado a cabo.
- Si atendemos a los aspectos cognitivos del conflicto, la guerra de Ucrania ocurre en tiempo real en el mundo digital; recibimos infinidad de mensajes visuales a través de las redes y medios pero esa información está llena de datos falsos, medias verdades, imágenes trucadas, vídeos manipulados, etc. (Marín Gutiérrez, 2022). Mucha de la información recibida también es verdadera pero es necesario cribarla. El Centro de Resiliencia Informativa con sede en Reino Unido trabaja con un centenar de voluntarios para verificar lo que se difunde en las redes sociales, desacreditar las campañas de desinformación rusa y extraer datos útiles para la población y el estado ucraniano. El resultado final es un mapa de monitorización de Ucrania en el que se recoge y clasifica toda la información geolocalizada por tipo y fechas. La realidad es que se trata de un trabajo ingente y exhaustivo pero de una utilidad evidente incluso desde el punto de vista de la inteligencia militar, y de hecho ambos bandos hacen uso de

> estos resultados ya sea para localizar o identificar objetivos o para verificar la eficacia de los ataques realizados. Este doble uso obliga a medir muy bien el alcance de las acciones cognitivas ya que pueden tener un efecto indeseado. Lo que parece claro es que la desinformación y propaganda rusa está perdiendo efectividad por ser ya demasiado conocidas y por las medidas activas aplicadas en las redes sociales, así como por el bloqueo a las agencias Sputnik y Russian Today (RT), de modo que, de hecho, la opinión pública está de forma abrumadora a favor de Ucrania.

Afortunadamente, no todo el escenario que los autores describían en 2015 se ha materializado. Por ejemplo, la OTAN no se ha disuelto sino que, por el contrario, se ha fortalecido y unido más aun frente a las amenazas que se vislumbran y que se están materializando. Como organización defensiva que es, la OTAN no trata de rearmarse sin más sino de demostrar su determinación de defender cada centímetro de territorio aliado, preservar la soberanía e integridad territorial de todos sus miembros y prevalecer contra cualquier agresor ante la posibilidad de ser atacados, que no se descarta.

III. USOS DE LA INTELIGENCIA ARTIFICIAL

Entre los compromisos suscritos en la cumbre de Madrid, los 30 países aliados acordaron la creación de un fondo de innovación con un importe inicial de mil millones de dólares con el objeto de desarrollar nuevas tecnologías, entre las que destaca la inteligencia artificial (IA). El fondo del asunto es que se percibe que potencias como China están superando las capacidades aliadas en un ámbito que se considera esencial para mantener la disuasión y la capacidad de respuesta. La ventaja tecnológica, que siempre ha sido uno de los objetivos de la transformación de los ejércitos, es ahora más crítica por la velocidad con que se desarrollan nuevos avances y por su capacidad para producir cambios estratégicos disruptivos que inclinen la balanza del poder militar hacia quienes los posean.

La inteligencia artificial es una de las siete áreas tecnológicas que la OTAN ha priorizado por su relevancia para la seguridad y defensa. Las otras seis son la computación cuántica, la autonomía, el *big data*, la biotecnología y mejora del rendimiento humano (*human enhancement*), las armas supersónicas y la tecnología espacial. De todas estas tecnologías de doble uso, la IA es conocida por ser la dominante cuando se combina con otras como big data, autonomía o biotecnología.

En efecto, el campo de la inteligencia artificial ha avanzado a un ritmo cada vez mayor en las últimas dos décadas. Los sistemas que incorporan tecnologías inteligentes prometen ventajas potenciales en las capacidades necesarias para la defensa nacional. Un número cada vez mayor de vehículos robóticos y armas autónomas puede operar allá donde el riesgo para nuestras fuerzas es elevado, ya sea por las condiciones ambientales o por la exigencia del teatro de operaciones.

Los sistemas defensivos asistidos por inteligencia artificial son cada vez más capaces de detectar, analizar y responder a los ataques con más rapidez y eficacia que los

operadores humanos. Los sistemas de análisis masivo de datos para apoyar a la toma de decisiones ya son capaces de digerir volúmenes de información que ningún grupo de analistas humanos jamás ha sido capaz de gestionar.

La inteligencia artificial, entendida como la capacidad de los sistemas informáticos para realizar tareas que normalmente requieren inteligencia humana, tiene una potencial aplicación directa en todos los sistemas que en un presente o futuro se adquieran para cubrir las funciones de las operaciones conjuntas[8].

La primera y más extendida aplicación de la IA es la fusión de información y su presentación al operador. La fusión de información o fusión de datos procesa exhaustivamente información de múltiples fuentes y bases de conocimiento para obtener una descripción y una comprensión más precisas y fiables.

Otras iniciativas se dirigen a mejorar la conciencia situacional del teatro de operaciones en todos sus niveles. La conciencia situacional se puede definir como la percepción y la comprensión en profundidad de los elementos del entorno, tiempo y espacio, incluyendo las intenciones de los diversos actores y sus objetivos. Con el desarrollo de la tecnología de la información, la traslación del combate individual al combate conjunto integrado es cada vez más intensa. En la actualidad, el "Combate Multidominio" tiende a configurar un espacio de combate multidimensional, con múltiples fuerzas de combate y un mando y control centralizado, aportando sus capacidades junto a otros dominios no militares. En la actualidad, para que el Comandante pueda tener un mando en tiempo real del campo de batalla, depende en gran medida de una variedad de sistemas, y de la fusión de información de los mismos, con el objetivo de que sea capaz de entender la situación del teatro de operaciones de una forma integral.

El Ejército entiende que invertir en IA es estratégico e irrenunciable y por tanto de vital importancia para no situarse en desventaja frente a potenciales adversarios. En un contexto de creciente competencia mundial, la integración progresiva de las tecnologías de IA en el ET es una cuestión estratégica de primer orden y puede constituir un importante multiplicador de la potencia de combate de la Fuerza Terrestre.

Así, el Ejército ha identificado las siguientes categorías de aplicación de la IA en su proyecto Fuerza 35[9]:

- Mando y Control.

La IA acelerará el ciclo de decisión, contribuyendo así a la agilidad del Sistema de Mando y Control. Las futuras capacidades de obtención de información excederán ampliamente de las de análisis, debido a la progresiva sensorización del campo de batalla. Será necesario contar con aplicaciones de IA en todos los niveles de mando

[8] Las actividades que realizan las Fuerzas Armadas de cara a su utilización en combate se agrupan en una serie de Funciones Conjuntas: Mando y Control, Maniobra, Fuegos, CIMIC (Cooperación Cívico-Militar), Inteligencia, Información, Apoyo Logístico, Protección de la Fuerza.

[9] Consúltese https://ejercito.defensa.gob.es/estructura/briex_2035/resumen_ejecutivo_fuerza_35.html para más información sobre el proyecto Fuerza 35.

para compilar la información de forma ágil, favoreciendo una explotación inmediata y autónoma. La cantidad de sensores de inteligencia en el campo de batalla obligará a automatizar los procesos ISTAR[10].

La aplicación de IA a alguna parte del proceso de adquisición de objetivos podría adquirir cierto grado de autonomía, evitando los retrasos producidos por la intervención humana y proporcionando gran velocidad al proceso en su conjunto.

- Apoyo Logístico.

Vehículos, materiales, centros logísticos, personal, talleres, almacenes, rutas, situación y posicionamiento, municionamiento, etc. aportarán grandes volúmenes de datos en tiempo real que, debidamente tratados con procesos de IA, permitirán tener capacidad de predicción para optimizar las funciones logísticas.

Así, será posible disponer de capacidad de anticipación en la identificación de necesidades, gracias a la sensorización, al trabajo en red y al tratamiento de datos apoyado en IA y en las técnicas de Big Data, y obtener una logística de carácter predictivo y capacidad de autodiagnóstico, gracias a la creciente monitorización de la información, la sensorización de los materiales y a la introducción de aplicaciones de IA.

El análisis de errores, la estimación de la durabilidad de diferentes componentes de los sistemas de armas o las actividades de planeamiento para una misión concreta, son posibles aplicaciones de IA que permitirían llevar a cabo el mantenimiento predictivo de los equipos, consiguiendo al tiempo optimizar los periodos de mantenimiento y de reparación, así como aumentar la disponibilidad de los sistemas en las operaciones.

- Operaciones en el ciberespacio.

El aumento del tráfico de datos, la complejidad de los despliegues y las amenazas de los ciberataques dotan de un carácter prioritario y fundamental al hecho de disponer de una gestión adecuada de las redes tácticas. La aplicación de desarrollos de IA a la Ciberdefensa permitiría hacer más efectivas sus acciones, permitiendo seleccionar la más adecuada o los posibles objetivos en función de los efectos deseados.

Los sistemas de IA apoyarían en la detección de incidentes, el análisis de vulnerabilidades, en la capacidad predictiva y en las actividades de respuesta y recuperación.

- Operaciones de información.

Las tecnologías de Big Data posibilitarán la explotación del inmenso volumen de datos existente en internet. La IA puede facilitar la personalización de la información para cada audiencia y contribuir a ahorrar importantes recursos para la monitorización de internet.

[10] El acrónimo ISTAR corresponde a las actividades relacionadas con Inteligencia, Vigilancia, Adquisición de Objetivos y Reconocimiento.

Los desarrollos de IA serán también muy importantes como herramienta de información y decepción, permitiendo crear capacidades, redes, imágenes o videos falsos, haciendo que cada vez sea más difícil distinguir entre realidad y ficción en el campo de batalla.

- Vehículos autónomos.

Los vehículos autónomos, tanto terrestres como aéreos, ofrecen nuevas posibilidades para operar en diferentes tipos de escenarios, aumentando la seguridad del personal en las situaciones más comprometidas (entornos urbanos, operaciones en el subsuelo, zonas minadas). Las posibilidades de la IA para este tipo de plataformas irán dirigidas a dotarles de autonomía en el cumplimiento de su misión, sin intervención humana, pudiendo superar las dificultades a las que deban enfrentarse (posibles ataques u obstáculos del terreno).

Se consideran de especial interés aquellos desarrollos dirigidos a conformar un enjambre de robots terrestres o aéreos, funcionando de forma sincronizada, pudiendo combinar plataformas tripuladas con otras no tripuladas e implementando configuraciones en las que el vehículo/robot líder pueda ser controlado a distancia desde una plataforma terrestre u otra ubicación.

- Sistemas de armas autónomos.

Partiendo de la premisa, como luego se dirá, de que el ET no contempla el uso de Sistemas de Armas letales completamente autónomas, es decir, sin intervención humana, el empleo de sistemas asistidos por IA permite un aumento en su rendimiento y eficacia, mejorando parámetros relativos a localización exacta y la selección de objetivos, alcance, precisión y graduación de efectos, así como a la reducción de huella. Se considera que la aplicación de la IA puede contribuir a la optimización de acciones clásicas tales como: selección de objetivos, analizando el terreno para encontrar posibles zonas hostiles, o selección de las armas más adecuadas, teniendo en cuenta diferentes parámetros (tipo de terreno, estimación del número de fuerzas enemigas y su equipamiento, evaluación de efectos generados, minimización de daños colaterales).

También han de considerarse los sistemas de armas autónomos que tengan como objetivo contrarrestar los sistemas autónomos que pueda emplear un posible adversario. La principal dificultad aquí está en identificar estos sistemas y reducir el riesgo de un uso letal accidental.

En resumen, esta visión coincide con la perspectiva sobre IA recogida en la “Estrategia de Tecnología e Innovación para la Defensa” (Secretaría de Estado de Defensa, 2020), en la que se identifica la Estrategia de I+D+i en IA como una de las iniciativas a nivel nacional más relevante y con más sinergia para la defensa. Además, la reciente Estrategia “España Nación Emprendedora” (Alto Comisionado para España Nación Emprendedora, 2021) sitúa a la IA como una de las tecnologías habilitadoras digitales con capacidad disruptiva y de alto impacto para el desarrollo y la transformación de la economía y la sociedad en su conjunto.

IV. RETOS QUE LA INTELIGENCIA ARTIFICIAL MILITAR PLANTEA

La estrategia OTAN para la inteligencia artificial publicada en octubre 2021 (OTAN, 2021) subraya las líneas principales para su empleo en el área de seguridad y defensa y se compromete a un uso responsable de acuerdo con las leyes internacionales y los valores éticos de la alianza. También reconoce las amenazas que plantean su utilización por parte de potenciales adversarios y el liderazgo del sector civil y académico en su desarrollo.

En cuanto a la robótica y el uso de armas autónomas, el Ministerio de Defensa español aboga por un abierto control de armamento y medidas de fomento de la confianza y seguridad, incentivando la transparencia y el intercambio de información relativa a los sistemas de armas letales autónomas, y por la prohibición de uso militar de cualquier sistema cuya acción sea contraria a los Derechos Humanos y al Derecho Internacional Humanitario. Además, considera necesario avanzar en la acotación de la definición técnica de sistemas de armas letales autónomas para un mejor entendimiento común; entiende la diferencia entre autónomo y automatizado, advirtiendo que la automatización es una característica indispensable en los sistemas militares ante los limitados tiempos de reacción disponibles para responder a una agresión, y que el aislamiento de este tipo de tecnologías podría afectar negativamente a la seguridad de las Fuerzas Armadas ante sus adversarios, así como suponer una merma en determinadas capacidades necesarias para el cumplimiento de sus misiones.

Por ello, la postura del Ministerio de Defensa de España es proseguir en el estudio y aplicación de la IA en sus sistemas, apoyando el empleo de sistemas con un cierto grado de autonomía y capaces de proyectar una fuerza letal siempre que exista la participación de un operador humano o un control humano en el proceso.

Las aplicaciones militares de la IA son diversas y generan retos tanto tecnológicos como éticos. Diversos proyectos se han orientado hacia el apoyo a la toma de decisiones en el campo militar, tanto estratégico, como operacional o táctico. Ahora bien, todos los que han tenido una aplicación práctica, se han desarrollado para mejorar las capacidades humanas, manteniendo el control humano y la decisión final, preservando los dilemas éticos de que una decisión automatizada pueda conllevar pérdidas humanas o materiales en un escenario de combate[11].

Uno de los dilemas que se plantean es la propia información que alimenta a la IA. La información en cualquier entorno de combate siempre contiene un grado de imperfección. En una situación de confrontación, la información obtenida es siempre limitada, y su autenticidad no está garantizada. En todos los conflictos se toman y se han tomado decisiones en función de información imprecisa, pero han partido de análisis originados en grupos humanos. Incluso si el ser humano es quien toma la última decisión, no puede obviarse el dilema ético de que decidamos sobre vidas humanas en función de las opciones, planteadas por una máquina, basadas en información que escapa a nuestro control.

[11] Programas como el "*Commander's Virtual Staff*", "*Alpha AI*", "*The Third Offset Strategy*" o el "*Project Maven*". Fuente: DARPA https://www.darpa.mil

Otra preocupación general en la aplicación de IA militar es el control de la escalada en un conflicto. Dónde y con qué intensidad se producen las acciones de fuerza son decisiones de enorme transcendencia basadas en gran manera en la percepción de los decisores. En el uso de la IA, sobre todo al comienzo, existe el riesgo de que los operadores y líderes militares confíen demasiado en sus sistemas de IA. El "sesgo de automatización", es decir, confiar en los resultados de la IA incluso cuando no parecen tener sentido, está presente. Este sesgo se intensifica en los sistemas en los que el procesamiento algorítmico es tan complejo que sus resultados son inexplicables. Además, si la IA acaba reduciendo la atrición propia, los jefes de fuerza podrían asumir mayores riesgos o actuar con mayor agresividad, alimentando una dinámica de escalada.

Como consecuencia de todo ello, el Ejército de Tierra, consciente de la creciente inquietud por el uso de sistemas militares autónomos, dedicó su última Jornada anual "El Ejército de Tierra y los Retos Futuros"[12] al marco ético y jurídico del proceso de la decisión en la era digital, jornada que se celebró en Granada el pasado 18 de Mayo con la colaboración de la Universidad de Granada. Asimismo, MADOC, junto a la UGR e ISDEFE, llevó a cabo en 2021 dos interesantes estudios titulados "Análisis de Tendencias en Inteligencia Artificial aplicadas a la Fuerza 2035" y "Estudio para la Implantación de la Inteligencia Artificial en el ET", que abordan el empleo militar de esta tecnología.

En la citada jornada se alertó de los riesgos del mundo digital virtual, no solo por la dificultad creciente de distinguirlo del mundo real, sino sobre todo por la extensión de su poder aparentemente sin límites, condicionando, cuando no determinando, las decisiones que se adopten en todos los niveles. Precisamente, las Fuerzas Armadas, cuyo principio de actuación se basa en la aplicación de valores éticos al comportamiento de sus miembros, están llamadas a constituir un referente en cuanto a la manera de integrar la IA en este proceso evitando que sean las máquinas las que finalmente tomen las decisiones.

El General Amador Enseñat y Berea, Jefe de Estado Mayor del Ejército (JEME), señaló la digitalización como factor clave en el proceso de transformación del Ejército, reconociendo que las nuevas tecnologías habrán de incorporar la inteligencia artificial para mantener la capacidad de disuasión y respuesta ante las amenazas reales y emergentes que se vislumbran para nuestra nación. En esta labor, el ET es consciente de la necesidad de que su empleo se haga dentro de un marco normativo que haga frente a dilemas morales y éticos que afectan a toda la sociedad. La ausencia de controles en su aplicación al campo militar reviste especiales peligros por las dramáticas consecuencias de un uso inapropiado de la fuerza armada. El empeño de compatibilizar algoritmos con humanismo en el campo militar debería ser un esfuerzo de la comunidad internacional en su conjunto y su posible solución impulsaría, sin duda alguna, la renovación del derecho internacional humanitario.

Entendiendo que muchos de los desarrollos normativos y legislativos que tratan de poner un gobierno sobre la inteligencia artificial no son de aplicación a sus usos

[12] Consúltese https://ejercito.defensa.gob.es/eventos/retos_futuros/index.html para más información sobre la Jornada Retos Futuros.

militares o tratan tan solo de establecer códigos de buenas prácticas, el ET no renuncia en principio a las ventajas que esta tecnología proporciona.

Es cierto que el Derecho Internacional Humanitario no acaba de pronunciarse al respecto, pero ello no quita para que el Ejército entienda que, de acuerdo con sus principios y valores éticos seculares, ha de establecerse una graduación o escala de riesgo en el uso de sistemas militares que empleen alguna forma de IA, a la manera en que el futuro Reglamento Europeo[13] propone. Parece claro que deberían existir unos usos militares prohibidos, en los que entrarían las armas que produzcan un efecto letal sobre las personas de manera completamente autónoma sin intervención humana, o aquellos sistemas que no ofrezcan garantías de protección a las personas no combatientes o directamente incumplan las reglas del derecho internacional humanitario. Habría, no obstante, que delimitar en este punto los sistemas que dispongan de algún tipo de asistencia de IA, como las que facilitan la identificación de objetivos, el guiado de las armas o la respuesta ante armas autónomas enemigas, cuya utilización no debería plantear ninguna restricción siempre que exista una posibilidad de intermisión por parte humana en algún momento de la acción.

En un estudio reciente publicado por el *Journal of Artificial Intelligence Research* (Zhang et al, 2021) se explica la preocupación de los investigadores acerca de la ética en el desarrollo de sistemas IA militares. Los resultados muestran claramente que la preocupación se centra en el desarrollo de algoritmos que alimenten procesos en los sistemas de armas letales autónomos (SALA).

Así pues, entre los sistemas letales completamente autónomos y los usos no letales de la IA, de bajo riesgo o nulo riesgo, puede establecerse una gradación todo lo complicada que se desee, y en ello está trabajando el grupo de expertos gubernamentales de la Convención de las Naciones Unidas sobre Ciertas Armas Convencionales (UN CCW) (Oficina de Naciones Unidas en Ginebra, 2014), que lleva desde 2020 debatiendo los retos derivados de los sistemas de armas letales autónomas[14]. Las reuniones del grupo de expertos se centran en definir los SALA, el papel del humano en el uso de la fuerza letal y las posibles opciones para abordar los desafíos humanitarios y de seguridad a futuro y cómo intervienen las tecnologías asociadas a la IA y los SALA.

La postura de países como Estados Unidos, Rusia, Reino Unido o Israel es que no son las características tecnológicas que potencian las capacidades de los sistemas de armas las que deberían estar en el centro del debate, sino el uso que de esas capacidades se vaya a hacer en los conflictos, en lo que se refiere al cumplimiento del Derecho Internacional Humanitario.

España mantiene una postura conservadora, relacionando los dilemas éticos y legales que suponen los SALA al sometimiento del sistema al control humano. Así entiende que, dado el desarrollo de una mayor autonomía en los sistemas de armas, deberían

[13] Véase https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52021PC0206 para más información sobre el proyecto de reglamento europeo para la inteligencia artificial.

[14] Consúltese https://geneva.usmission.gov/2020/09/30/group-of-governmental-experts-on-lethal-autonomous-weapons-systems-laws-agenda-item-5e/ para más información sobre el grupo de expertos gubernamentales sobre armas letales autónomas.

prohibirse los sistemas de armas que operan sin un control humano significativo. Mientras los sistemas de armas autónomos sigan bajo control humano significativo, no existe ninguna razón para asumir que, por definición, estas armas deben estar incluidas en una de las categorías de armas prohibidas por el Derecho Internacional Humanitario.

En estas consideraciones acerca del control humano en el uso de fuerza letal, la postura española también entiende que un excesivo control humano podría repercutir en la capacidad del sistema de manera negativa. Es decir, la clave está en definir qué grado de autonomía y qué instrumento de control humano se considera suficiente para cumplir los objetivos de los SALA, al mismo tiempo que se asegura el cumplimiento de los preceptos éticos y legales del Derecho Internacional Humanitario.

Otros asuntos que entran en este debate son la necesidad de algún tipo de autoridad de acreditación de sistemas militares para determinar a qué categoría pertenece un sistema asistido por IA y el grado de control que precisa. También será preciso que las Reglas de Enfrentamiento (ROE), que regulan el empleo de la fuerza en función de las circunstancias en cada escenario, y los planes operativos que se elaboren para cada misión, determinen qué medios están autorizados, quiénes son los responsables de su uso y en qué condiciones.

Finalmente, en el uso de la IA, como en el de cualquier medio militar, ha de predominar el principio de responsabilidad, no renunciable ni compartible para un jefe militar ni para el operador de un medio susceptible de producir daño. Será aconsejable, pues, que los sistemas cuenten con algún tipo de registro que asegure que su uso ha sido autorizado y garantice la aplicación de este principio.

V. CONCLUSIONES

La naturaleza brutal, violenta, perturbadora y desestabilizante de la guerra no ha cambiado, pero la IA tiene la capacidad de alterar fundamentalmente el carácter de la misma. Su aplicación a las capacidades que actualmente aseguran que el Ejército cumpla sus misiones tendrá un efecto multiplicador, siendo posible que la IA esté imbricada en gran parte de los sistemas militares en un futuro próximo.

A pesar de que algunos sectores en la comunidad internacional albergan cierto temor de que los Estados y sus Fuerzas Armadas se sientan cada vez más presionados para integrar la IA en las aplicaciones militares y se apresuren a desarrollar y utilizar nuevas tecnologías sin control, lo cierto es que España y las demás naciones aliadas están comprometidas a poner las necesarias restricciones humanitarias y de seguridad para un uso militar responsable de los nuevos avances.

Para abordar algunos de los riesgos de la IA militar, se está desarrollando un consenso en varios foros sobre la necesidad de que los humanos mantengan el control sobre el desarrollo, el despliegue y el uso de sistemas de IA militar. Sin embargo, todavía hay muchas preguntas abiertas sobre el grado de control necesario, qué forma debe adoptar y cómo pueden aplicarse esas salvaguardas a nivel nacional e internacional.

Nuestro planteamiento es que en cualquier rama de la tecnología podrían desarrollarse sistemas individuales que violaran estas normas. De hecho, casi todas las armas podrían utilizarse de forma que violaran el Derecho Internacional Humanitario, por lo que la consideración importante es cómo se utilizan. En cuanto al riesgo de fallo, siempre ha estado ahí y ningún sistema está libre de él al cien por cien. Para mitigarlo, de nuevo es necesario mantener un cierto nivel de acción humana sobre estos sistemas.

Por último, la visión catastrofista sobre el dominio de las máquinas que en muchos se ha impuesto, es en gran medida fruto de la creatividad de escritores y guionistas cuyo objeto, sin menospreciar su valor artístico y literario, es más alimentar la imaginación humana que aportar rigor al análisis de lo que esta nueva tecnología supone. Por el contrario, el buen uso de la IA está produciendo y seguramente va a permitir grandes avances para la humanidad, incluso en el ámbito militar, reduciendo el número de errores que los humanos normalmente comentemos, mejorando la precisión de nuestros sistemas de todo tipo, ahorrando vidas propias, eliminando o minimizando los daños colaterales, anticipándose y enfrentándose a las amenazas y agresiones que nos puedan afectar, y, en definitiva, aportando más seguridad a nuestra sociedad.

VI EPÍLOGO

En la noche, el sistema de asistencia de combate inteligente Delphi identificó un vehículo de combate enemigo a 150 metros del flanco oeste. Obviando el protocolo, abrió un enlace a la soldado más próxima y envió una imagen fija del vehículo a su visor… “Dispara tan pronto como lo tengas en tu mira” fue su mensaje. Mientras el vehículo zigzagueaba alrededor de un muro de ladrillo, la soldado, impulsada por su exoesqueleto, se situó en posición de tiro a pocos metros de su objetivo… La voz “¡ahora, al suelo y dispara!” sonó en su auricular.

La soldado aceptó el juicio de Delphi y sintió el impacto del brazo de su exoesqueleto al tirarse al suelo mientras el vehículo se movía en una nube de polvo. Las cámaras de su casco mantenían la imagen fija del vehículo enemigo en la pantalla cuando hizo fuego. El sistema de combate automático calculó que el ángulo y dirección de su arma estaban correctamente alineados y la IA tiró del gatillo […]

“Delphi ¿estás ahí?” – preguntó la soldado.

“Aquí estoy”

Estaba amaneciendo. A lo largo de todo el frente norte los supervivientes enemigos se estaban retirando, deteniendo su éxodo tan solo cuando nuestros drones pasaban cerca… La incursión había sido derrotada […]

En sus peores pesadillas, Delphi perdía el contacto por voz con sus soldados. Podía ver al enemigo esperando en una emboscada; podía conocer su posición, sus armas, su alcance… sabía que sus clientes estaban en peligro pero no podía alertarlos.

Mientras la pesadilla de la guerra se desataba frente a sus ojos, lo único que le alentaba era saber que la asistencia y las alertas que les daba podían salvar la vida de sus soldados.[15]

BIBLIOGRAFÍA

- Alto Comisionado para España Nación Emprendedora. (2021). Estrategia España Nación Emprendedora. https://nacionemprendedora.gob.es/sites/default/files/Estrategia_Espana_Nacion_Emprendedora.pdf

- Brown, D. y Ahmedzade, T. (27 mayo 2022). *Ukraine weapons: What military equipment is the world giving?* BBC News. https://www.bbc.com/news/world-europe-62002218

- Cubeiro Cabello, E. (2022). El ciberespacio en la guerra de Ucrania. Documento de Opinión IEEE 32/2022. https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO32_2022_ENRCUB_Ucrania.pdf

- Secretaría de Estado de Defensa. (2020). Estrategia de Tecnología e Innovación para la Defensa. https://publicaciones.defensa.gob.es/media/downloadable/files/links/e/t/etid_estrategia_de_tecnolog_a_e_innovaci_n_para_la_defensa_2020.pdf

- Fallon, J. (2020). Breaking the island chains. *UK Defence Forum.* https://www.defenceviewpoints.co.uk/articles-and-analysis/breaking-the-island-chains

- Marín Gutiérrez, F. (2022). ¿Comprendemos la desinformación?: Rusia y la evolución de las medidas activas. Documento de Opinión IEEE 26/2022. https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO26_2022_FRANMAR_Rusia.pdf

- Nagata, L. (2015). *We can win the war, you must win the peace.* En A. Cole et al, *War stories from the future* (pp. 41-47). The Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/books/war-stories-from-the-future

- Oficina de Naciones Unidas en Ginebra. (2014). *Convention on certain conventional weapons*. United Nations Publication.

- OTAN. (2021). *Summary of the NATO Artificial Intelligence Strategy.* https://www.nato.int/cps/en/natohq/official_texts_187617.htm

- OTAN. (2022). *Strategic concept 2022.* https://www.nato.int/strategic-concept/

[15] Adaptación de la narración NAGATA, 2015, que forma parte del proyecto *The Atlantic Council Art of Future Warfare* dirigido a la prospección de los posibles escenarios de guerra en el futuro.

- Singer, P. W. y Cole, A. (2015). *Ghost fleet.* Nueva York: Houghton Mifflin Harcourt

- Zhang, B. et al. (2021). *Ethics and Governance of Artificial Intelligence: Evidence from a Survey of Machine Learning Researchers*. Journal of Artificial Intelligence Research, 71, 591-666. https://scholar.google.es/scholar_url?url=https://www.jair.org/index.php/jair/article/download/12895/26701&hl=es&sa=X&ei=Kzv2Yr7MJK-Ty9YPpJKV2Ak&scisig=AAGBfm1hMFCbPxQ5lkETAVoA9v7uQtaOGA&oi=scholarr