

Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Irrupción de la Inteligencia Artificial en el Ministerio de Defensa, primeros casos de uso

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Francisco Cuartero Lorenzo

DIRECTORES: Norberto Fernández García

Milagros Fernández Gavilanes

CURSO ACADÉMICO: 2023-2024

Universidade Vigo



Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Irrupción de la Inteligencia Artificial en el Ministerio de Defensa, primeros casos de uso.

Máster Universitario en Dirección TIC para la Defensa

Especialidad de Sistemas y Tecnologías de la Información

Universidade Vigo

RESUMEN

La Inteligencia Artificial es considerada la más transcendente de las tecnologías emergentes. En el campo militar está siendo contemplada en todas las estrategias de defensa de nuestro siglo llegando a manifestarse que la geopolítica estará marcada por los países que consigan dominarla. La evolución del escenario estratégico militar está sustituyendo el concepto clásico de operaciones conjuntas por el de operaciones multidominio. Este tipo de operaciones estará caracterizado por una masiva sensorización del campo de batalla y un volumen de información desbordante que superará las capacidades humanas de gestión. El Ministerio de Defensa de España, al igual que otras potencias militares y las Organizaciones Internacionales de Seguridad y Defensa consideran que las aplicaciones de la Inteligencia Artificial podrían suponer la clave de la superioridad en el combate y de la interoperabilidad y, a su vez, una oportunidad para establecer una brecha tecnológica frente a los posibles adversarios.

La transversalidad de la Inteligencia Artificial hace que su aplicabilidad alcance todo el espectro de actividades que se realizan en la sociedad en general y en las Fuerzas Armadas en particular. Este trabajo, guiado por la Estrategia de desarrollo, implantación y uso de la Inteligencia Artificial en el Ministerio de Defensa, de la Secretaria de Estado de Defensa, pretende hacer un recorrido por la aplicabilidad de esta tecnología en los casos de uso concretos documentados en el Ministerio de Defensa, así como otros que se estiman de interés. Los casos de uso se presentan agrupados en las categorías reflejadas en dicha Estrategia según el area de actividad en que repercutirán incluyendo tanto la operativa, como la administrativa o de apoyo.

PALABRAS CLAVE

Inteligencia Artificial, operaciones multidominio, defensa, innovación, aprendizaje automático.

AGRADECIMIENTOS

A los tutores de este trabajo, Norberto Fernández García y Milagros Fernández Gavilanes por su guía y apoyo durante la elaboración de este TFM.

Al Director General del CESTIC por permitirme hacer este Máster.

A mi mujer Macamen y a mis tres hijas por regalarme el tiempo necesario.

PRÓLOGO

2023 ha sido sin duda, el año de la Inteligencia Artificial. Su democratización, traída de la mano de la popularización de una herramienta concreta de procesamiento de lenguaje natural, ha acelerado la implantación de esta tecnología. La IA definirá nuestro siglo porque encierra un inusual potencial transformador de procesos productivos, gracias a nuevos modelos llamados a modificar profundamente los entornos empresariales. Dentro de poco, será difícil asistir a una reunión sin copiloto…

También en el campo de batalla veremos acelerarse esta implantación. Esta tecnología tiene aplicación en muchos aspectos de las operaciones militares, en el frente y en la retaguardia. Pronto será difícil encontrar un aspecto del combate en el que no intervengan sistemas de Inteligencia Artificial, de la misma manera que ya es imposible encontrar un ámbito de la actividad bélica en la que no estén presentes los sistemas de información y comunicaciones.

Es cierto que el uso militar de la Inteligencia Artificial plantea interrogantes específicos: el origen de los datos, su calidad y su cantidad en el campo de batalla, en el que la capacidad de cómputo, o la disponibilidad de recursos en la nube no será siempre la óptima. El sesgo en su interpretación, la eficacia de los modelos; los contenidos visuales de difícil discernimiento entre virtualidad y realidad; la lista es larga.

Tantos son los interrogantes, que no parece rentable preocuparse por aquellos que dibujan las distopías más lejanas: ¿Nos enfrentaremos a algoritmos autónomos? ¿Disponen éstos actualmente de suficiente capacidad para elegir y reconocer fallos cuando se centran en acciones con repercusión vital? ¿Está cercano el momento de la singularidad?

La defensa militar de España necesita una aproximación pragmática que permita la implantación de la IA, sin perder de vista los aspectos éticos, y que vaya resolviendo la incertidumbre a medida que se vaya presentando. Pero consiguiendo que ésta no detenga la ola convertida en galerna de la Inteligencia Artificial.

Ese espíritu práctico es el que destila la Estrategia para el uso, implantación y desarrollo de la IA en el Ministerio de Defensa, documento de alto nivel en cuya redacción participó activamente el Capitán de Fragata Francisco Cuartero. El impulso entusiasmado que le imprimió como Oficial de Estado Mayor, le permitió sortear las muchas dificultades encontradas en su confección; el texto es efectivo, adaptado a una situación cambiante y aporta valor al Ministerio de Defensa y a las Fuerzas Armadas. Es una Estrategia que materializa proyectos, que gestiona realidades. Nuestros planes se ejecutan.

El presente trabajo demuestra nuestros avances en este campo, coordinados con otros muchos elementos indispensables para la adopción de la IA en la realidad tecnológica del Ministerio de Defensa, que es cada vez más compleja. Uno de ellos es la imprescindible modificación de la cultura (digital) del Departamento, sometida una vez más a un exigente proceso de adaptación, de cambio, de transformación.

El Ministerio de Defensa apuesta decididamente por esta tecnología, que ya está siendo decisiva en el campo de batalla actual. Para ello tomamos todas las precauciones necesarias relativas a su uso responsable, pero nuestra vocación es activa: emprendemos todos aquellos proyectos que están a nuestro alcance, porque, como Alicia en el País de las Maravillas, tenemos que correr por lo menos dos veces más rápido, si queremos llegar a algún sitio.

Animo al Capitán de Fragata Cuartero a seguir profundizando en el conocimiento y en la aplicabilidad de la Inteligencia Artificial en nuestra misión de soldados y marineros, porque sin ella, no será posible la conquista del futuro.

Teniente General José María Millán Martínez
Director General del CESTIC

ÍNDICE

Índice 7

Índice de Figuras 10

Índice de Tablas 12

1 Introducción 13

1.1 Motivación. 13

1.2 Metodología empleada. 15

1.3 Limitaciones al estudio. 15

1.4 Estructura de la memoria. 15

2 Estado del arte 16

2.1 Inteligencia Artificial y era digital. 16

2.2 Referencias en el entorno del Ministerio de Defensa. 27

2.2.1 En la Administración General del Estado. 27

2.2.2 En la Organización del Tratado del Atlántico Norte. 28

2.2.3 En la Unión Europea. 29

2.2.4 En las principales potencias militares. 32

2.2.5 Adaptación tecnológica e innovación TIC en el Ministerio de Defensa. 37

2.2.6 La Estrategia de IA del MDEF. 38

2.3 La guerra de Ucrania, “sandbox” para la IA. 39

2.3.1 Particularidades de la Guerra de Ucrania. 40

2.3.2 La IA en Ucrania 41

2.4 Categorías y clasificación de la IA. 43

2.5 El dilema ético. 46

2.5.1 Agencia Española de Supervisión de la IA. 47

2.5.2 Uso responsable de la IA en la OTAN (DARB). 48

3 Casos de uso 50

3.1 Casos de uso militar. 50

3.2 Movilidad militar. 51

3.2.1 Planeamiento y apoyo del transporte, estratégico, operacional y táctico. 51

3.2.2 Optimización de rutas de transporte. 51

3.2.3 Seguridad de conductores y pasajeros. 51

3.2.4 Proyecto ARCO: Aplicación robótica de un convoy operativo. 51

3.3 Inteligencia. 52

3.3.1 Interpretación de imágenes, análisis de datos y documental. Traducción automática. 52

3.3.2 Interpretación de imágenes. 53

3.3.3 Proyecto SATELLITE DATA AI (SEDA) para el procesado automático de imágenes satélite. 53

3.3.4 Proyecto de Sistemas Inteligentes para el procesamiento de imágenes y la detección de amenazas en escenarios de conflicto (CUSTODES). 54

3.3.5 Proyecto de reconocimiento de imágenes y asistencia a reacciones tácticas. 55

3.3.6 Análisis de datos y documental. Traducción automática. 56

3.3.7 Herramienta PALANTIR. 57

3.3.8 Traductores e intérpretes. 58

3.4 Guerra electrónica. 59

3.4.1 Planeamiento y apoyo a las operaciones de Guerra Electrónica. 59

3.4.2 Proyectos CIA2 – Armada. 59

3.5 Sistemas no tripulados. 61

3.5.1 Autonomía en el comportamiento de sistemas no tripulados. Desarrollo de funciones autónomas no letales en sistemas no tripulados terrestres, navales y aeroespaciales. 61

3.5.2 Proyecto SAFETERM 63

3.6 Apoyo logístico y alistamiento operativo. 64

3.6.1 Mantenimiento predictivo y sostenimiento. Bases logísticas inteligentes. 64

3.6.2 Mantenimiento predictivo en la Armada 64

3.6.3 Proyecto CESADAR – SOPRENE – ATAVIA – MAPRE. 65

3.6.4 Proyecto Gemelo Digital F-110. 66

3.6.5 Ejército del Aire y del Espacio. Proyecto BACSI. 67

3.6.6 Proyecto PANGEA. 67

3.6.7 Proyecto IMAGIA. Análisis de datos de Rayos-X y ultrasonidos. 68

3.6.8 Mantenimiento predictivo para EUROFIGHTER. 69

3.6.9 Proyecto BLET del Ejército de Tierra. 70

3.6.10 Proyecto SILPRE 71

3.7 Conocimiento y vigilancia del entorno. 71

3.7.1 Proyecto NELSON (UK). 71

3.8 Ciberdefensa. 72

3.8.1 Identificación y actuación frente a ciberamenazas. 72

3.8.2 Detección y mitigación de vulnerabilidades en los sistemas militares. 73

3.8.3 Threat Hunting, caza de amenazas. 73
3.8.4 Herramientas de visualización y trazado de un ciberataque. 73
3.8.5 Herramientas de simulación de APT (Advanced Persistent Threats). 73
3.8.6 Detección de malware. 74
3.8.7 Detección y bloqueo automático de “phishing”, “spam”, intrusiones en la red o actuaciones fraudulentas. 74
3.8.8 Desarrollo de software seguro. 74
3.8.9 Identificación y autenticación de usuarios. 74
3.9 Apoyo a la toma de decisiones 75
3.10 Análisis geoespacial, meteorológico y oceanográfico. 76
3.10.1 Proyecto SIAAMETOC-OM. 76
3.11 Gestión de la Información, de la infraestructura y los servicios CIS/TIC. 76
3.12 Gestión del talento y formación. 77
3.12.1 Proyecto GNOSS. 77
4 Conclusiones y líneas futuras 78
4.1 Conclusiones. 78
4.1.1 Sobre la aplicabilidad de la IA. 78
4.1.2 Sobre la Estrategia de IA del MDEF. 78
4.1.3 Sobre los casos de uso de IA. 79
4.2 Líneas futuras. 80
5. Bibliografía 81

ÍNDICE DE FIGURAS

Figura 1-1. Ámbito de aplicación de una tecnología. 13
Figura 2-1Robot ruso FEDOR 17
Figura 2-2 Relevancia Geopolítica asociada a la maduración tecnológica. 18
Figura 2-3 Concepto I2D2. Fuente: STO Tech Trends report NATO 20
Figura 2-4 Campo de batalla del siglo XXI.. 22
Figura 2-5 Valor relativo de la "autonomía". 22
Figura 2-6 Ideograma de la transformación Digital. 23
Figura 2-7 Cronograma IA generativa. 26
Figura 2-8 Planes incluidos en Plan España Digital 2026. 27
Figura 2-9 Presentación de la NATO´s Artificial intelligence Strategy. 28
Figura 2-10 “Decison advantage outcomes” del enfoque ágil. US DoD. 33
Figura 2-11 Pirámide de la IA. 34
Figura 2-12 Defence AI Centre Architecture. 35
Figura 2-13 Flujo de incorporación de tecnologías TIC al MDEF. 38
Figura 2-14 Representación del Mulidominio. 40
Figura 2-15 Reconocimiento de vehículos militares. 41
Figura 2-16 Reconocimiento de vehículos militares desde UAV. 42
Figura 2-17 Elementos de la IA. 43
Figura 2-18 Tecnologías usadas en sistemas de IA. 44
Figura 2-19 Relación entre IA, ML, y DS. 44
Figura 2-20 Foto oficial DARB (febrero 2023). 48
Figura 3-1. Proyecto ARCO. 52
Figura 3-2. Oferta de curso IMINT. 53
Figura 3-3. Proyecto SEDA I. 54
Figura 3-4. Proyecto CUSTODES ET 55
Figura 3-5. Proyecto SEDA II. 56
Figura 3-6. Ciclo OODA. 56
Figura 3-7. Capacidades de PALANTIR. 57
Figura 3-8 Reunión multilingüe. 58
Figura 3-9. Proyecto de clasificación de señales. 59
Figura 3-10. Proyecto de lanzamiento señuelos antimisil. 60

Figura 3-11 VISTA X-62A. 63
Figura 3-12 Esquema y visualización proyecto SAFETERM. 63
Figura 3-13 Evolución del mantenimiento predictivo en la Armada. 65
Figura 3-14 Herramientas de SOPRENE (2022). 66
Figura 3-15. Ilustración Proyecto Gemelo Digital F-110.. 67
Figura 3-16 Proyecto IMAGIA. Analisis de Rayos X. 69
Figura 3-18. Proyecto NELSON (UK). 72
Figura 3-19 IA empleada en ciberdefensa: 72

ÍNDICE DE TABLAS

Tabla 2-1 Tipos de IA para Arend Hintze. Fuente: Michigan State University 25
Tabla 2-2 Tipos de IA para Russell y Norving. Fuente: IA: Un Enfoque Moderno 25
Tabla 2-3 Startups de IA por países de 2013 a 2022. Fuente: AI Index Report 2023 - Stanford Universitty. 32
Tabla 2-4 Extracto de: *"Lead country and technology monopoly risk"*. Fuente: ASPI. 36
Tabla 3-1 Categorías de casos de uso militar de la IA ESP – OTAN 50
Tabla 3-2 Proyecto ARCO 52
Tabla 3-3 Proyecto SEDA I 54
Tabla 3-4 Proyecto CUSTODES 54
Tabla 3-5 Proyecto SEDA II 55
Tabla 3-6 Proyecto de clasificación de señales CIA 2 60
Tabla 3-7. Proyecto de lanzamiento de señuelos antimisil. 60
Tabla 3-8 Drones en el MDEF (ET, AR, EA, UME) 62
Tabla 3-9 Proyecto CESADAR- SOPRENE - ATAVIA - MAPRE 65
Tabla 3-10 Proyecto gemelo Digital F-110. 66
Tabla 3-11 proyecto PANGEA. 68
Tabla 3-12 Proyecto IMAGIA (END). 69
Tabla 3-13 Proyecto de mantenimiento predictivo para el Eurofighter. 70
Tabla 3-14 Proyecto SILPRE. 71
Tabla 3-15 Proyecto SIAAMETOC_OM. 76
Tabla 3-16 Proyecto GNOSS. 77
Tabla 4-1 Valoración categorías IA. 79

1 INTRODUCCIÓN

"La Inteligencia Artificial es la más trascendente de las tecnologías actuales, también en lo militar, campo en el que está siendo esencial en las estrategias de defensa de nuestro siglo. La geopolítica estará marcada por los países que consigan dominarla."

Teniente General José María Millán

1.1 Motivación.

Desde que el hombre abandonó la idea de resolver sus conflictos únicamente por medios pacíficos y se le ocurrió lanzarle una piedra a su oponente, para no entrar en su alcance físico, tomó conciencia de que la técnica y el ingenio son la mejor ayuda para imponer la propia voluntad a la del adversario.

De esta manera, en el llamado "arte de la guerra", el componente tecnológico ha sido un factor determinante para la resolución de cualquier conflicto armado. Las potencias militares de la era moderna no han escatimado esfuerzos en la búsqueda de la ventaja tecnológica. A su vez, la ciencia ha sido beneficiaria de múltiples descubrimientos y desarrollos que, naciendo con un fin bélico, fueron trasladados a otros campos del conocimiento, como la medicina, la construcción, la producción de energía o el transporte.

Avanzando ya en la tercera década del siglo XXI, muchos autores consideran que se ha invertido el orden, la Dirección General de Armamento y Material lo denomina "*Aprovechamiento del empuje tecnológico Civil*" [1]. Ya no son las aplicaciones militares las que impulsan el desarrollo tecnológico de la sociedad, sino que más bien, son los avances nacidos y desarrollados en el ámbito civil los que son incorporados a la carrera armamentística. Tal vez ARPANET, surgida de una necesidad militar, fue uno de los últimos grandes avances en el sentido de lo militar a lo civil. El profesor Gonzalo León [2] , en su artículo sobre el papel dual de la Inteligencia Artificial señala que: "*La dimensión de defensa ha adquirido gran relevancia dado que la inteligencia artificial es inherentemente una tecnología dual que se ha incorporado en múltiples sistemas de armas inteligentes.*"

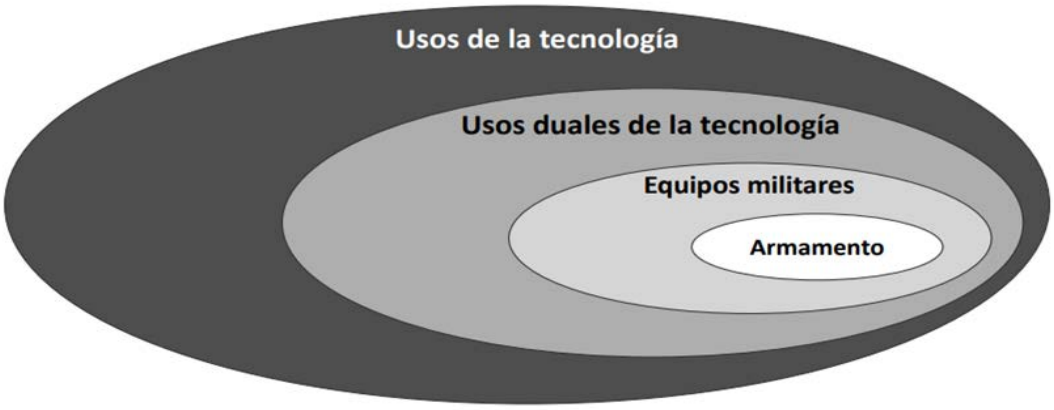


Figura 1-1 Ámbito de aplicación de una tecnología.

Cuando hablamos de tecnologías de uso militar, la línea de pensamiento, la OTAN establece una clasificación de tecnologías a las que denomina Tecnologías Emergentes y Disruptivas (EDT) en función de su aplicabilidad al ámbito militar y el plazo previsible en que esto ocurra. En el estudio *"Science & Technology Trends"* para el periodo 2023-2043 de la NATO Science&Technology Organization [3] se identifican estas tecnologías, agrupándolas en áreas. Este estudio clasifica como las

tres primeras: las relacionadas con los datos, la inteligencia artificial y finalmente los robots y sistemas autónomos.

El Ministerio de Defensa de España, participa activamente en la comunidad científica y se mantiene atento a todos los avances que la ciencia plantea. En los últimos años, ante el conocido como "tsunami" digital y el ímpetu transformador de la Administración General del Estado, el Departamento ha respondido emitiendo normativa y financiando proyectos, convencionales y de I+D+i en función de la madurez en la tecnología a aplicar.

La Política CIS/TIC en vigor [4] fue redactada en 2015. Aunque sus principios de cabecera permanecen vigentes: orientación a servicios, centralización, interoperabilidad y otros, el avance tecnológico global en estos ocho años transcurridos ha sido muy significativo. Para mantener actualizadas las infraestructuras y servicios TIC, la Secretaría de Estado de Defensa tomó la decisión de incorporar las nuevas tecnologías, ya de uso común, mediante un proceso estandarizado, cuyos pasos son: participación en la comunidad científica, elaboración de una estrategia departamental, definición de casos de uso y ejecución de proyectos piloto. De esta manera el Ministerio de Defensa ha incorporado en el ámbito TIC la tecnología de nube, de comunicaciones 5G, las últimas técnicas de desarrollo ágil de software y Dev-Sec-Ops, y por último de desarrollo, implantación y uso de la Inteligencia Artificial [5] a la que se dedica este Trabajo Fin de Máster.

Importancia de la Inteligencia Artificial para la defensa y seguridad.

La última Estrategia de Seguridad Nacional de 2021 [6] es el documento que pretende configurar el marco político estratégico de la Política de Seguridad Nacional. Este documento incluye numerosas referencias a la Inteligencia Artificial entre las que destacan:

En el capítulo 3 dedicado a los Riesgos y Amenazas. En él se lee: *"La superficie de confrontación geopolítica encuentra áreas de intersección con la tecnología y la economía, dibujando así un mapa de riesgos más complejos y muy interrelacionados. Adicionalmente, amenazas derivadas del uso de tecnologías de nueva generación, como la Inteligencia Artificial o el acceso al espacio ultraterrestre, añaden complejidad y dificultan la protección de los derechos individuales ante un eventual uso malicioso"*. Afortunadamente, el documento no se queda en los aspectos negativos de la Inteligencia Artificial y así, en el capítulo cuatro, titulado Planeamiento Estratégico Integrado, se menciona el uso a favor: *"…En particular es necesario tomar conciencia del potencial estratégico de la Inteligencia Artificial y la importancia de esta tecnología como puntal de la Seguridad Nacional"*. Ese potencial señalado en 2021, ya empieza a ser tangible en 2023.

Si nos vamos al plano de las Fuerzas Armadas en particular, el Concepto de Empleo de las Fuerzas Armadas [7] es el documento en que el Jefe del Estado Mayor de la Defensa define el marco estratégico militar. En el capítulo cinco, dedicado a diseñar la Fuerza Conjunta se indica que: *"Las Fuerzas Armadas tienen que acceder a las nuevas tecnologías emergentes y disruptivas, como la Inteligencia Artificial, cuyo desarrollo puede suponer la clave de la superioridad en el combate y de la interoperabilidad"*. Queda por tanto demostrado el interés que la Inteligencia Artificial ha despertado en el contexto de la seguridad y defensa en general y del Ministerio de Defensa de España en particular. Este trabajo pretende elaborar una recopilación ordenada de las iniciativas emprendidas para su incorporación transversal a múltiples áreas de actividad, desde lo puramente administrativo hasta sus aplicaciones en el campo de batalla.

El autor, como Oficial de Estado Mayor destinado en el Area de Planes y Políticas de la Dirección General CESTIC, es conocedor de las expectativas y ambiciones que ha despertado en el Ministerio de Defensa la que ha denominado "irrupción de la Inteligencia Artificial" y espera que este trabajo ofrezca una visión global sobre su aplicabilidad en este entorno.

1.2 Metodología empleada.

Este trabajo seguirá una metodología cualitativa basada en la revisión bibliográfica. Se han analizado los documentos relevantes sobre la materia publicados por instituciones académicas de primer nivel y fuentes oficiales del Ministerio de Defensa.

Para recopilar información sobre casos de uso concretos, actualmente en desarrollo, el autor recurrió a las fuentes primarias responsables de proyectos que incluyen Inteligencia Artificial en el Ministerio de Defensa y su entorno.

El estudio se complementa con documentación procedente de las Organizaciones Internacionales de Seguridad y Defensa (OTAN y UE), y de otras fuentes militares internacionales publicadas por potencias extranjeras relevantes en el ámbito militar y de la seguridad.

1.3 Limitaciones al estudio.

Este trabajo recoge únicamente información “no clasificada” de uso público.

1.4 Estructura de la memoria.

El trabajo se estructura en cuatro capítulos de los que esta introducción constituye el primero de ellos. Los tres restantes son:

- Capítulo 2. Estado del arte, que profundiza en los posibles usos de la Inteligencia Artificial en aplicaciones militares.
- Capítulo 3. Dedicado a los casos de uso específicos identificados agrupados según las categorías señaladas en la Estrategia de desarrollo, implantación y uso de la Inteligencia Artificial en el Ministerio de Defensa.
- Capítulo 4. En este se recogen las conclusiones del trabajo y se plantean posibles líneas futuras de actuación para el Ministerio de Defensa.

2 ESTADO DEL ARTE

"Mi peor miedo es que esta tecnología salga mal. Y si sale mal, puede salir muy mal"

Sam Altman

2.1 Inteligencia Artificial y era digital.

Será muy difícil en los próximos años encontrar un campo de la actividad humana que se mantenga al margen de la Inteligencia Artificial (IA), tal vez el arte, aunque sobre esto también hay discusión. La Directora de Google para España y Portugal, Fuencisla Clemares, afirma que: *"La Inteligencia Artificial es el gran desafío tecnológico del futuro. Va a ser comparable al descubrimiento del fuego"* [8]. Sin llegar a este extremo de posible exageración, lo que ofrece poca discusión es la transversalidad de esta tecnología en la sociedad y podríamos decir que en la humanidad. En el ámbito militar que nos ocupa, la irrupción de esta tecnología, se ve como un poder capaz de cambiar los equilibrios con la misma dimensión que tuvo en su momento la aparición del armamento nuclear.

El uso militar de la IA plantea interrogantes específicos. Uno de estos interrogantes son los posibles conflictos éticos que el uso de esta tecnología pueda conllevar, pero no es el único. Existen otros de gran importancia como: el origen de los datos, la mitigación del sesgo, el alcance de los algoritmos y su entrenamiento, por citar algunos. El Ministerio de Defensa, con el liderazgo de la Secretaria de Estado, ha elaborado una Estrategia para guiar la integración de esta tecnología. Publicada en 2023, dicha Estrategia tiene por finalidad establecer la base para el desarrollo, implantación y uso de soluciones de Inteligencia Artificial en el Ministerio de Defensa, que permitan incrementar la eficacia en las misiones y cometidos del Departamento. Se tratará en detalle más adelante.

La Organización del Tratado del Atlántico Norte (OTAN) ha reconocido a la IA como una de las EDT que pueden potenciar las Capacidades de la Alianza y apoyar el desarrollo de sus misiones. En ese orden de cosas, en octubre de 2021 los Ministros de Defensa de la OTAN aprobaron la Estrategia de la Alianza en esta materia, *NATO's Artificial Intelligence Strategy* [9].

En el plano militar, la evolución del escenario estratégico está sustituyendo el concepto clásico de operaciones conjuntas por el de operaciones multidominio, en las cuales son imprescindibles unos sistemas de gestión de la información, mando y control capaces, seguros e interoperables. Así lo señala el Coronel Caride Abalde en su reciente artículo sobre el Entorno Operacional Multidominio [10]: "*Este entorno operacional multidominio genera una ingente cantidad de información de combate a integrar dentro de una posible nube de combate multidominio, facilitadora de un conocimiento completo de la situación, en todos los niveles de la fuerza táctica operativa, para actuar en todo momento con una mayor resolución y sincronización sobre los efectos buscados. La interconectividad de los sistemas de armas y de los diferentes nodos de los dominios, junto con el proceso y gestión de la información por sistemas de IA, son elementos posibilitadores de tal proceso".*

En este sentido, es muy posible que los avances en las tecnologías de la información y de las aplicaciones militares de la IA, vayan a marcar la evolución del diseño y conducción de las operaciones.

Influencia directa previsible de la IA en el campo de batalla.

Se prevé que la IA tenga una gran influencia en la forma en la que se configurará el campo de batalla. Las aplicaciones de la IA tendrán un impacto directo en todas las áreas que lo componen, destacando el de la gestión de la información sobre el terreno, los procesos de obtención y explotación de inteligencia, la capacidad de disuasión, la toma de decisiones y el propio enfrentamiento.

En un reciente estudio del Centro Conjunto de Desarrollo de Conceptos, el Coronel Gómez de Agreda [11] señala que, *"El aspecto más sensible de la IA para uso militar, –al menos de cara a la opinión pública– es el de la utilización de la robótica en el campo de batalla"*, señalando a continuación que la literatura y el cine han influido mucho en esta percepción.

Sin caer en una distopía cinematográfica, sí parece claro que la aparición de "Sistemas de Armas Letales Autónomos" (SALAS) es una realidad que ya está presente en el campo de batalla. Tras un sangriento siglo XX, la aversión a las bajas humanas en todos conflictos pronostica un empleo progresivo de robots. Cabe esperar que estos dispositivos tengan capacidad de aprendizaje y evolución, tal vez más allá del marco del conjunto de datos con el que han sido adiestrados. Esta realidad preocupa y dará lugar a normativa internacional inspirada por una "ética" de la guerra difícil de acordar. En el campo de la legítima defensa, la protección de las fuerzas propias es otra capacidad que se verá incrementada. El uso de Robots Inteligentes en primera línea, en ambiente hostil y para cometidos extremadamente peligrosos permitirá aumentar la supervivencia de las tropas. Tal es el caso por ejemplo de FEDOR, véase Figura 2-1, el robot humanoide ruso que incluso ha sido enviado a la Estación Espacial Internacional durante 10 días realizando *"cinco o seis tareas secretas"* [12] y que nació como un soldado.



Figura 2-1 Robot ruso FEDOR. Fuente: Twitter.

Cuando hablamos del planeamiento y la conducción de operaciones, un mejor conocimiento de la situación basado en IA descargará a los mandos de la desbordante avalancha de datos del campo de batalla moderno, extraordinariamente sensorizado (IoT militar), permitiendo que los mandos se concentren en la toma de decisiones.

La guerra electrónica, más allá de lo visible, y por supuesto las operaciones en el ciberespacio, no pueden ni plantearse sin el apoyo de la IA allí donde la velocidad de evaluación y reacción del ser humano es claramente insuficiente.

Influencia indirecta previsible de la IA en el campo de batalla.

Dwight D. Eisenhower declaró: *"No encontrarás difícil demostrar que las batallas, las campañas e incluso las guerras se han ganado o perdido, principalmente, por la logística"*, y todo el que no lo ha interpretado así, ha podido ganar alguna batalla pero ninguna guerra. Esta será, por tanto, un área principal para el desarrollo de aplicaciones basadas en IA que permitan mejorar la eficacia y eficiencia de los procesos logísticos. En este campo encontraremos desarrollos para mejorar el sostenimiento de la fuerza, la movilidad militar y la sanidad.

Finalmente, a nadie se le escapa, que toda gran organización, y las Fuerzas Armadas de cualquier estado lo son, necesita de otros procesos de apoyo fundamentales para su funcionamiento. Entre estos se encuentran los puramente administrativos o la enseñanza. Estas imprescindibles funciones también se verán beneficiadas por la llegada de la IA, como mínimo por la reducción de la demanda de personal para las mismas que podrá ser empleado en las fuerzas de combate, aunque estas últimas probablemente también tiendan a reducirse.

Convergencia tecnológica.

En una reciente conferencia impartida como parte del Curso de Acceso al empleo de General en el CESEDEN el Profesor León advertía a los alumnos sobre el singular momento histórico en el que nos encontramos. Señalaba que la tecnología siempre ha tenido un factor geopolítico, el arma de fuego o la energía nuclear, por citar dos ejemplos. Lo excepcional en esta década es la convergencia tecnológica de la maduración simultánea de varias tecnologías de claro uso militar cuya relevancia sobre los conflictos armados se vislumbra transcendental. León lo reflejaba con la siguiente Figura 2-2:

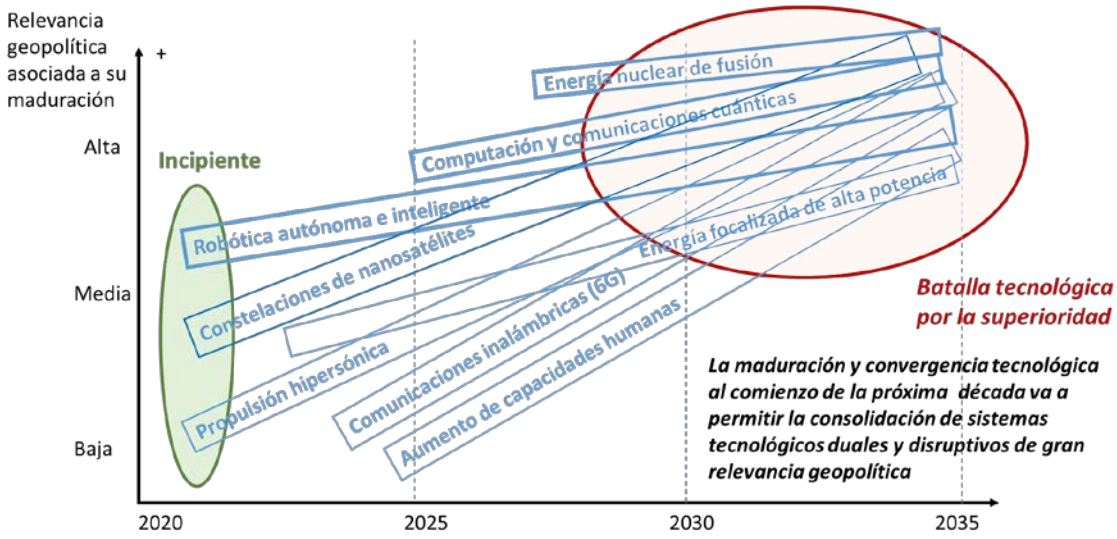


Figura 2-2 Relevancia Geopolítica asociada a la maduración tecnológica. Fuente: Gonzalo León.

Esta idea, es reflejada en el artículo titulado, *"Soberanía tecnológica para la defensa y la seguridad de España en la UE: entre lo deseable y lo posible"* [13] donde los autores señalan que la competencia internacional por la hegemonía tiene, por tanto, una dimensión tecnológica creciente que, como ha sucedido en otras etapas históricas, resulta en políticas de bloques determinadas por la capacidad de acceso a la tecnología de uno u otro actor dominante. El proceso se acelera cuando se produce una situación de convergencia tecnológica en periodos de tiempo muy reducidos como ocurre en la actualidad. Señala León que: *"El desarrollo simultáneo de sistemas de armas que combinan las comunicaciones celulares de banda ancha, la nanoelectrónica, los nanomateriales, los sistemas autónomos, la IA, la propulsión hipersónica, la ciberseguridad, las tecnologías de energía dirigida y,*

en un futuro muy próximo, las tecnologías cuánticas o la propulsión por reactores de fusión, entre otras, ha acelerado la dimensión tecnológica de la hegemonía, y la consiguiente carrera hacia la superioridad en nuevos sistemas de armas".

En caso de cumplirse esta predicción sobre las tecnologías que actualmente se encuentran en un estado "incipiente", donde destaca especialmente la "robótica autónoma e inteligente", en la próxima década asistiremos a una nueva "carrera" armamentística donde el dominio tecnológico marcará el dominio geopolítico. Como señalaba León: *"La maduración y convergencia tecnológica al comienzo de la próxima década va a permitir la consolidación de sistemas tecnológicos duales y disruptivos de gran relevancia geopolítica"*.

Es más que probable que el avance o ventaja no se deba a una tecnología concreta, sino a una combinación de ellas. En este aspecto podemos afirmar que la gran mayoría de ellas se reforzarán combinándose con la IA. Estas combinaciones son reflejadas en el estudio ya mencionado de "*Science & Tecnology Trends*" para el periodo 2023-2043 de la OTAN que dedica un capítulo a la Convergencia, Interdependencias y Sinergias (*Convergence, Inter-Dependencies and Synergies)* referido a las EDTs.

Las combinaciones reflejadas en este documento que incluyen a la IA son:

- Datos-IA-Autonomía
- Datos-IA-Biotecnología
- Datos- IA-Nuevos materiales
- Energías-Nuevos materiales- IA

¿Cuál va a ser el "futuro" cercano del campo de batalla?

Desde el punto de vista militar es importante visualizar las características del espacio de batalla futuro y el papel que jugará la IA. Volviendo al mencionado documento de la OTAN *"Science & Technology Trends 2023-2043"* [3] encontramos que sigue estableciendo, como lo hacía en su versión 2020-2040, que el concepto I2D2 (inteligente, interconectado, descentralizado y digital), véase Figura 2-3, seguirá vigente las próximas décadas y definirá el avance de las tecnologías militares. Las tecnologías militares existentes se fusionarán con las EDTs para crear nuevas formas y medios de participar en los conflictos.

Más adelante se tratará el matiz entre lo "inteligente" y lo "autónomo" que son dos conceptos que no se superponen totalmente. Lo que puede asumirse es que el futuro tecnológico de equipos y sistemas en el campo de batalla estará caracterizado por los atributos señalados por el S&T Trends 2023-2043, (traducido y adaptado del original por el autor):

- Concepto 1 - Inteligente: El desarrollo tecnológico explotará la IA integrada, las capacidades analíticas centradas en el conocimiento y la simbiosis de la inteligencia humana y la artificial para proporcionar aplicaciones disruptivas en todo el espectro tecnológico.

    - Autonomía: Los sistemas autónomos basados en IA serán capaces de funcionar de forma independiente para tomar decisiones. Dichos sistemas autónomos pueden ser robóticos, basados en plataformas o en agentes digitales.
    - Inteligencia colaborativa: La integración de los sistemas psicosociales y tecnológicos respaldará la mejora de los equipos humano-máquina y su comportamiento sinérgico.
    - Análisis del conocimiento: Los métodos analíticos avanzados (incluida la IA) manejarán grandes volúmenes de datos y explotarán matemáticas avanzadas, proporcionando conocimiento y recomendaciones, ideas y consejos.

- Concepto 2 - Interconectado: La tecnología explotará redes a través de dominios virtuales, biológicos y físicos, incluyendo redes de sensores, organizaciones, individuos y agentes autónomos, vinculados a través de nuevos métodos de cifrado y tecnologías distribuidas.

    - Comunicaciones confiables: el uso de tecnologías distribuidas como "Blockchain", la distribución de claves cuánticas (QKD), la criptografía postcuántica y los ciberagentes de IA garantizarán las comunicaciones fiables y el intercambio de información.
    - Sistemas sinérgicos: El desarrollo de sistemas de sistemas complejos mixtos (físicos o virtuales) creará ecosistemas novedosos como las ciudades inteligentes.
    - Sistemas biológico-físicos: Las tecnologías explotarán los sistemas humanos, mecánicos, biológicos y físicos a través de IA, interfaces hombre-máquina y manipulación del genoma.

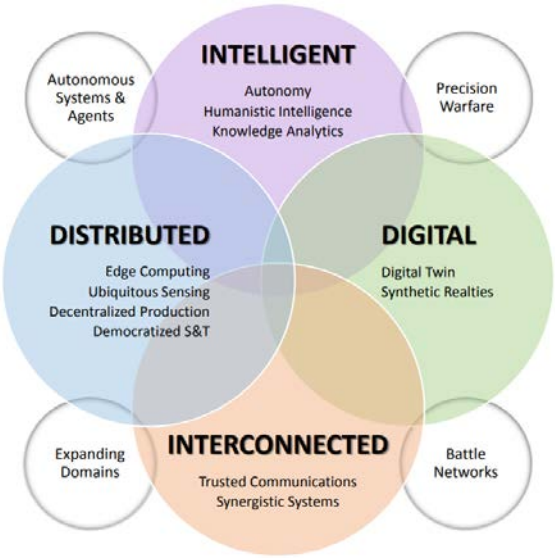


Figura 2-3 Concepto I2D2. Fuente: STO Tech Trends Report NATO

- Concepto 3 - Descentralizado: Dispondremos de sensores, capacidad de almacenamiento y computación distribuida y ubicua a gran escala.

    - Computación en el borde - Edge Computing: El almacenamiento de datos, la computación y la capacidad de análisis/IA se integrarán en agentes y objetos cercanos a las fuentes de información.
    - Sensorización ubicua: sensores de bajo coste crearán grandes redes a través de los dominios humano, físico y de la información.
    - Producción descentralizada: La fabricación y producción digital in situ explotará el diseño asistido por IA, nuevos materiales y tecnologías de impresión 3D/4D.
    - Democratización tecnológica: La amplia disponibilidad de información científica y tecnológica y el fomento de la innovación serán el resultado de capacidades computacionales aumentadas de alto rendimiento y ampliamente disponibles, costes de diseño y producción reducidos y la innovación científica.

- Concepto 4 - Digital: Nuevos efectos disruptivos (positivos y negativos) resultarán de la fusión digital de productos de los dominios biológico, físico y de la información.

- Gemelo digital: Simulacro digital de entidades físicas, biológicas o de información, digitalmente vinculado (a menudo casi en tiempo real) al original respaldará el análisis predictivo, la experimentación y la evaluación.
- Realidad sintética: Se crearían nuevas realidades cognitivas o físicas percibidas a partir de la integración de sistemas psico-socio-tecno. Estas realidades podrán ser aumentadas, virtuales, sociales o culturales.

Una vez más, la combinación de estos atributos o características será la que proporcionará nuevas capacidades militares como las siguientes que resultan de la combinación de dos atributos:

- Acción autónoma inteligente-----Inteligente y Descentralizado.
- Dominio cognitivo----------Interconectado y Digital.
- Dominios ampliados----------Interconectado y Descentralizado.
- Combate de precisión----------Inteligente y Digital

Para intentar bajar estos conceptos teóricos al terreno podemos recurrir a las reflexiones sobre el nuevo entorno operacional multidominio [10] o a la visualización que hace el profesor Steve Blank del *"Modern War Institute at West Point"* [14] en su clase sobre Autonomía y Defensa en el siglo XXI.

Previamente, tal y como se citó anteriormente, cabe señalar que inteligente y autónomo no es el mismo concepto. Según el US Defence Science Board [15] entenderemos que, para ser autónomo, *"un sistema debe tener la capacidad de establecer y seleccionar de forma independiente entre diferentes cursos de acción para lograr objetivos basados en su conocimiento y comprensión del mundo, de sí mismo y de la situación"* y se contemplan dos tipos de autonomía:

- Autonomía en reposo: sistemas que "operan virtualmente, en software, e incluyen sistemas de planificación y asesoramiento experto". Por ejemplo, en el ámbito cibernético, donde las reacciones deben producirse a la velocidad de una máquina.
- Autonomía en movimiento: sistemas que "tienen presencia en el mundo físico". Estos incluyen robótica y vehículos autónomos, misiles y otros efectos cinéticos.

Para Steve Blank, los sistemas inteligentes combinan autonomía en reposo y autonomía en movimiento con la aplicación de IA a un problema o dominio particular. Preguntándose el ¿por qué el US DoD necesita sistemas autónomos en el campo de batalla?, Blank recurre a la figura 2-4 de la que señala que podría semejarse al estrecho de Taiwán o a las proximidades de la península de Corea.

En este semi-imaginario espacio de batalla, podemos ver a la izquierda una fuerza conjunta compuesta por: un portaaviones y su grupo naval de escolta, aviones AWACS y comunicaciones por satélite. A la derecha, las fuerzas agresoras en las burbujas naranjas están empleando amenazas cibernéticas, amenazas cinéticas, perturbación del GPS y las comunicaciones denegadas. Todo esto podría asemejarse al espacio de batalla actual. La diferencia radica en que en estos entornos multidominio, el tiempo de reacción humana puede ser insuficiente para sobrevivir.

Debajo de la Figura 2-4 podemos observar algunas de las características que marcarán los nuevos escenarios:

- Se incrementa la velocidad y precisión de la decisión.
- Se necesitan nuevas tácticas y conceptos operacionales que requieren mayor resiliencia.
- Es necesario reducir el riesgo de bajas civiles y militares.
- Han de posibilitarse las operaciones en entornos hostiles de Guerra Electrónica y Cíber.
- Ser capaz de operar plataformas no tripuladas en caso de denegación de comunicaciones.
- Ser capaz de operar plataformas si los operadores humanos mueren o son heridos.

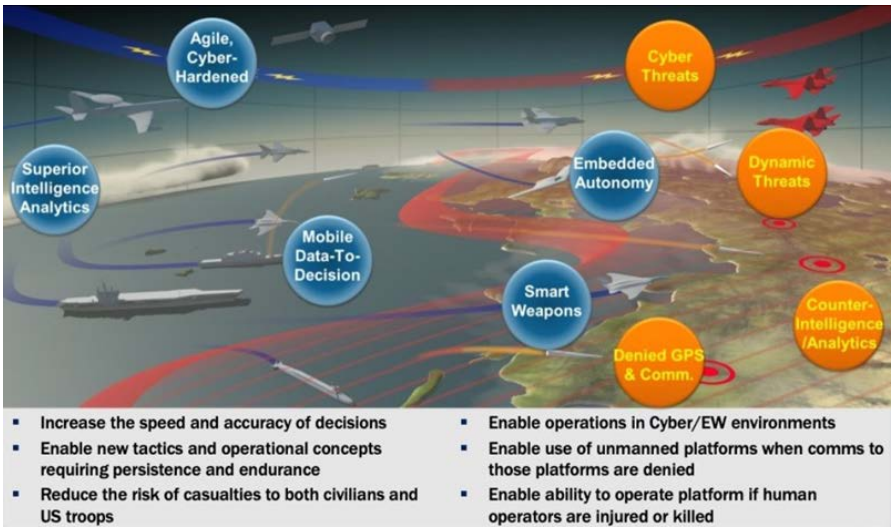


Figura 2-4 Campo de batalla del siglo XXI. Fuente: Modern War Institute at WEST Point.

Estas necesidades pueden resumirse en lo expresado por el Teniente General Millán cuando, al referirse al cambio cultural que debe acompañar a la transformación digital en la clausura del Máster Universitario en Dirección TIC para la Defensa en enero del 2023, señalaba que: *"en el combate multidominio al que nos enfrentamos, el margen de error se ha reducido, el ciclo de decisión se ha acortado y la superficie de exposición ha crecido"*.

Es en estas condiciones cuando lo "autónomo" y su evolución hacia lo "inteligente" toman un valor fundamental. Blank recurre a la siguiente Figura 2-5 para expresar el valor de la autonomía en función de la situación y plantea varios escenarios.



Figura 2-5 Valor relativo de la "autonomía". Fuente: Modern War Institute at West Point

Es decir, lo autónomo aportará ventaja respecto al humano cuando:

- Sea necesario decidir con rapidez, como por ejemplo, ciberoperaciones o defensa antimisil.
- Cuando haya un gran volumen de datos o sean heterogéneos (inteligencia de imágenes.).
- Si no hay buen enlace de datos.
- Si la acción es compleja (centro de operaciones aéreas).

- Si el peligro es alto (operaciones NBQR).
- Si es necesaria gran persistencia y resistencia (vehículos no tripulados de vigilancia).

En resumen, se dará una tendencia a que las máquinas o robots realicen las tareas más difíciles y arriesgadas en el campo de batalla. Cabría una consideración sobre los efectos que tendría un combate entre máquinas, sin intervención humana, probablemente pocos. Pero ese escenario distópico podrá dar lugar a estudios posteriores. En conclusión, podría parecer a primera vista que en el combate multidominio queda menos hueco para los humanos, lo que en principio parece una muy buena noticia. Veremos que no es así, en la "niebla de la guerra" y el caos del combate la experiencia y el juicio humano aun juegan un papel decisivo, y es esperable que así sea al menos durante unas décadas más.

Visión de la Transformación Digital del Ministerio de Defensa.

El Ministerio de Defensa, circunscribe la adopción masiva de la IA al proceso de transformación digital en curso. Más allá de la publicación de la Estrategia de desarrollo, implantación y uso de la IA que se tratará más adelante, la visión de la transformación digital expresada en diferentes foros por el Teniente General Millán, Director General del CESTIC desde octubre 2019, se refleja en la siguiente Figura 2-6:

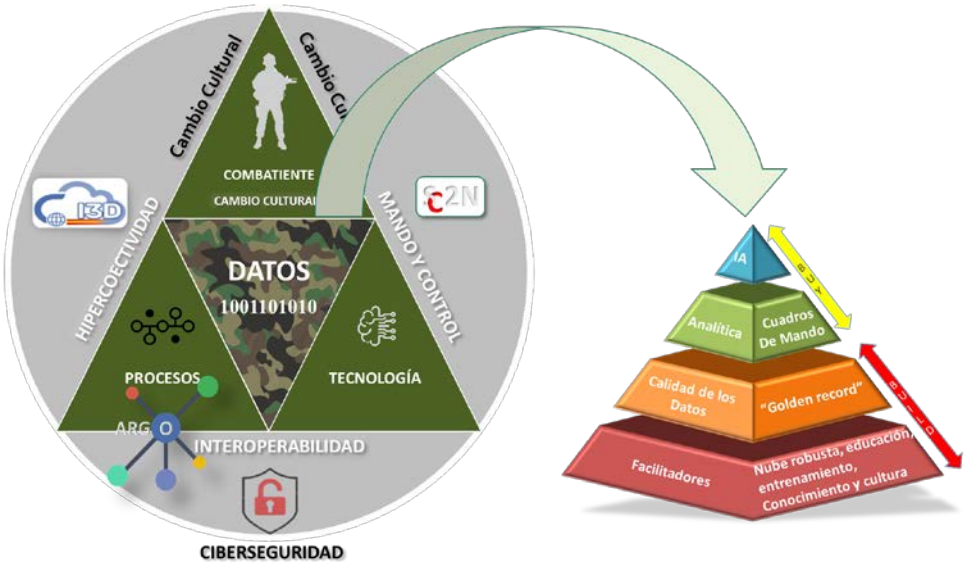


Figura 2-6 Ideograma de la transformación Digital.
Fuente: CESTIC

Esta visión es una adaptación del conocido "triángulo mágico de la transformación digital" en el que en los vértices bajos están representados los procesos y la tecnología, en el vértice superior las personas y en el centro los datos. Existen numerosas imágenes del mismo concepto, el cual implica que debemos actuar sobre los tres vértices sin olvidar que es la información, los datos, el eje sobre el que pivota y da sentido a la transformación.

Mediante los artículos de la saga "el viaje inaplazable", publicados en la Revista Española de Defensa [16], José María Millán pretendía hacer llegar al departamento su visión sobre el proceso de transformación digital en el que nos hemos visto voluntaria y forzosamente embarcados. El segundo artículo, de un total de tres, titulado "Gasolina para el viaje inaplazable" [17] se refleja la centralidad de los datos y el valor intrínseco que tienen para la transformación digital, los datos son la gasolina para este viaje. En el tercero y último, publicado en noviembre 2022, titulado; "La Inteligencia del vIAje

inaplazable" [18], está dedicado a la IA a la que califica como la reina de las tecnologías disruptivas. En este artículo Millán fija que los pilares de la IA, en adelanto de la posterior estrategia, serán: los datos, el talento y la seguridad, y que además la Infraestructura Integral de Información para la Defensa (I3D) habrá de prepararse para albergar aplicaciones de IA dotándose de las capacidades de almacenamiento y computación necesarias para ello. También adelanta la necesidad de regular el uso responsable de esta tecnología.

Referente a la preparación del Ministerio de Defensa para la llegada de la IA, el Director General del CESTIC señalaba que si bien determinadas capacidades, podremos adquirirlas del mercado, como por ejemplo: motores de IA, herramientas de inteligencia de negocio y análisis; otras, como las relacionadas a la calidad de los datos, su limpieza y almacenamiento, y su etiquetado deberemos adquirirlas como propias.

Etapas de desarrollo de la IA.

No se dispone de un consenso científico sobre las etapas de desarrollo de la IA y menos sobre en cual nos encontramos. El criterio más común para determinar las etapas es su nivel de inteligencia como capacidad para imitar al ser humano y sus habilidades. En torno a este criterio se definen tres etapas, por sus siglas en inglés ANI, AGI y ASI que significan:

- ANI, IA débil o estrecha.
- AGI, IA general.
- ASI, súper IA.

Las capacidades que se suponen a cada etapa son:

- ANI (IA Estrecha o Débil), se centra en tareas específicas y limitadas enfocada a una sola tarea. Los sistemas ANI generalmente se entrenan con un gran conjunto de datos. Su técnica principal es el Machine Learning (ML). Dentro de esta categoría se encuentran los robots que pueden vencer al campeón del mundo de ajedrez, Siri, Alexa o el traductor de Google, la conducción autónoma o el mismísimo ChatGPT. Estos sistemas no pueden operar fuera del rango definido por sus programadores y no pueden tomar decisiones por su cuenta. Estos desarrollos están diseñados para realizar tareas específicas con una gran eficacia y una más que discutible eficiencia. Carecen de comprensión y conciencia de sí mismos, aunque podamos percibirlos como tal, es solo una ilusión. No pueden crear conocimiento o aprender de manera independiente fuera de sus áreas de especialización.
- AGI (IA General), el concepto es que en esta etapa los sistemas de IA son capaces de aprender y aplicar conocimientos de manera similar a un humano. Es decir, la máquina adquiere capacidades cognitivas de nivel humano y es capaz de realizar cualquier tarea que realiza una persona y lo fundamental, en cualquier ámbito. Alcanzado este nivel es cuando empiezan a surgir el "miedo" sobre unos posibles riesgos para la sociedad e incluso para la humanidad. Algunos expertos entienden que las máquinas podrían aprender nuevas habilidades por sí mismas y ahí reside su peligro.
- ASI (Súper IA), llegado a este nivel, la IA supera ampliamente la inteligencia humana en cualquier aspecto. La teoría que sostiene este concepto es que, cuando la máquina logre tener una inteligencia similar a la humana, sumándole la capacidad de multiplicar esa inteligencia de forma exponencial mediante su propio aprendizaje autónomo hará que en poco tiempo se alcance la ASI. Existen ciertas dudas de si una máquina podrá en esta etapa llegar a "sentir" o ser capaz de adquirir habilidades sociales. Lo que sí que parece posible es que en esta etapa habría que replantearse el trabajo humano.

Existen otras clasificaciones de IA:

Arend Hintze, profesor de Biología Integrada y Ciencias de la Computación de la Universidad de la Michigan establece una clasificación, que recoge el Foro Económico Mundial en una colaboración del Profesor Hintze [19] basada en la capacidad predictiva y en los niveles de complejidad que pueden alcanzar las máquinas reflejadas en las columnas de la Tabla 2-1:

- Máquinas reactivas.
- Memoria limitada.
- Teoría de la mente.
- Autoconciencia.

AI Type	Follows Rules	Can Learn	Has Memories	Knows Other Minds Exist	Aware of Emotion	True AI
Reactive Machines	✓					
Limited Memory	✓	✓	limited			
Theory of Mind	✓	✓	✓	✓	✓	
Self Aware	✓	✓	✓	✓	✓	✓

Tabla 2-1 Tipos de IA para Arend Hintze. Fuente: Michigan State University

Stuart Russell y Peter Norving, de la Universidad de Berkeley, han publicado cuatro ediciones de su libro *"IA: Un enfoque moderno"* [20]. Su clasificación original establece estas cuatro categorías basadas en la comparación con los seres humanos. En la Tabla 2-2 pueden observarse la clasificación en cuatro grupos y la descripción de cada uno de ellos:

Tipos de Inteligencia Artificial	
Según Tipos de Sistemas de IA	**Descripción**
1. IA que piensa como humanos	Automatizan actividades como la toma de decisiones, la resolución de problemas y el aprendizaje. Un ejemplo son las redes neuronales artificiales.
2. IA que actúa como humanos	Se trata de computadoras que realizan tareas de forma similar a como lo hacen las personas. Es el caso de los robots.
3. IA que piensa racionalmente	Intentan emular el pensamiento lógico racional de los humanos, es decir, se investiga cómo lograr que las máquinas puedan percibir, razonar y actuar en consecuencia. Los sistemas expertos se engloban en este grupo.
4. IA que actúa racionalmente	Idealmente, son aquellos que tratan de imitar de manera racional el comportamiento humano, como los agentes inteligentes.

Tabla 2-2 Tipos de IA para Russell y Norving. Fuente: IA: Un Enfoque Moderno

¿Dónde nos encontramos respecto a la evolución de la IA?

No encontraremos una respuesta unificada y académica a esta pregunta. No cabe duda de que aunque la IA ya está presente en nuestras vidas, y en nuestros trabajos, todavía nos encontramos ante una tecnología incipiente dando sus primeros pasos.

Si nos vamos a la primera clasificación nos encontramos claramente en la IA Débil o Estrecha y en opinión del autor, bastante más lejos de la "General" de lo que pregona más la prensa especializada que la comunidad científica. La aparición de ChatGPT en 2022, disparó el interés y noticias alrededor de la IA llamada generativa y los modelos LLM *(Large Language Model)*. David Hurtado, Director de Innovación de Microsoft ES, en una conferencia a la asociación Larsen Digital Leaders presentaba el cuadro evolutivo de la Figura 2-7 basado en el "GPT-4 Technical Report" (OpenAI), *"Sparks of Artificial General Intelligence"* (Microsoft Research).

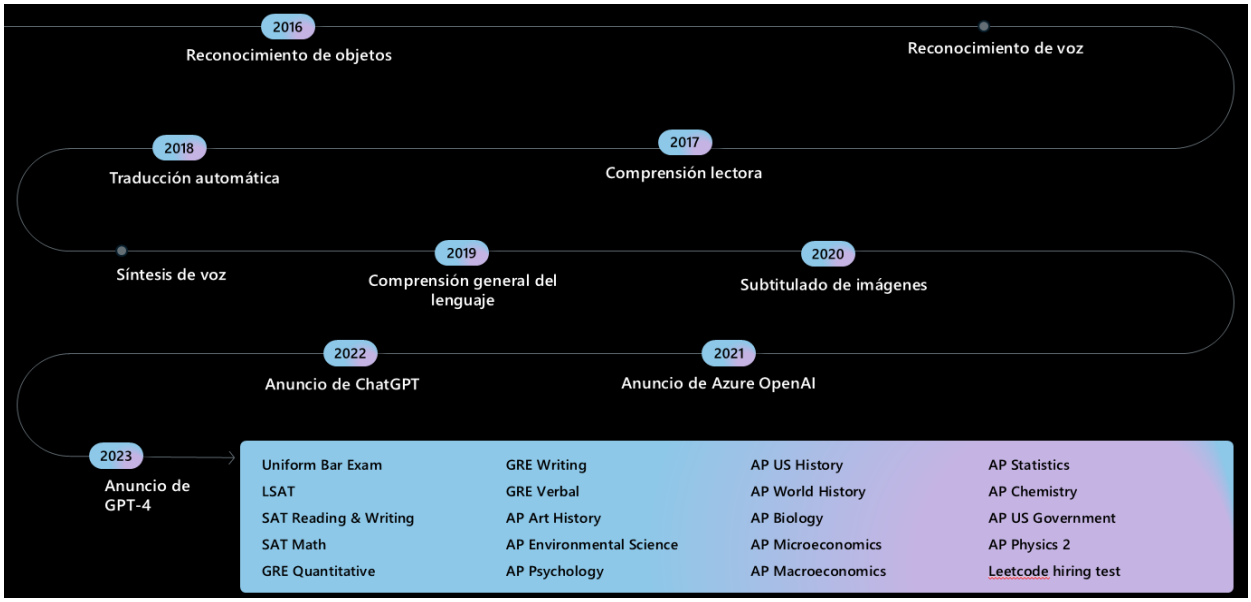


Figura 2-7 Cronograma IA generativa. Fuente: David Hurtado - Microsoft ES

El gráfico comienza en 2016 con el "reconocimiento de objetos" y continúa presentando las diferentes habilidades que han ido adquiriendo las aplicaciones de Inteligencia Artificial. Por lejano que parezca, ChatGPT fue anunciado en octubre de 2022, apenas hace un año. A partir de ese momento, se ha disparado el número de aplicaciones, aunque según señalaba Hurtado son aplicaciones sectoriales, cada campo de actividad tiene su propia Inteligencia Artificial generativa. Probablemente todas usen básicamente el mismo el mismo "motor" adaptado a las particularidades de esa parte del conocimiento. Así podemos encontrar una Inteligencia artificial que nos apoye en: "*History (US or World), Chemistry, Biology"* etc, pero no encontráremos una que sea buena en todo. Con la prudencia que implica que solamente conocemos los desarrollos "comercializados" por los gigantes tecnológicos, cabe deducir que finalizando 2023 nos encontramos todavía en la etapa de IA Estrecha.

2.2 Referencias en el entorno del Ministerio de Defensa.

En este apartado se analizarán las principales organizaciones de referencia del Ministerio de Defensa de España y su relación con la IA y su aplicabilidad.

2.2.1 *En la Administración General del Estado.*

La Agenda España Digital 2025/2026 y la ENIA

La Estrategia Nacional de IA [21], publicada el 2 de diciembre de 2020, por el Ministerio de Asuntos Económicos y Transformación Digital es un marco de referencia que orienta los planes sectoriales, estatales y estrategias regionales en esta materia en el periodo 2020-2025, en línea con las políticas desarrolladas por la Unión Europea, e impulsa la transformación de los diferentes sectores económicos mediante la cooperación público-privada.

La ENIA es uno de los ejes de la Agenda España Digital 2025, aprobada en julio de 2020, y a su vez uno de los componentes del Plan de Recuperación, Transformación y Resiliencia (PRTR). En la edición España Digital 2026 [22] se engloba en el Eje 4 *"Economía del Dato e IA"*. Cabe señalar que dentro del PRTR la inversión directa en la Estrategia Nacional de IA es la menor de los ocho planes sectoriales de impulso a la digitalización con 600 millones de euros. El presupuesto asociado a cada uno de los ocho planes está reflejado en la Figura 2-8.

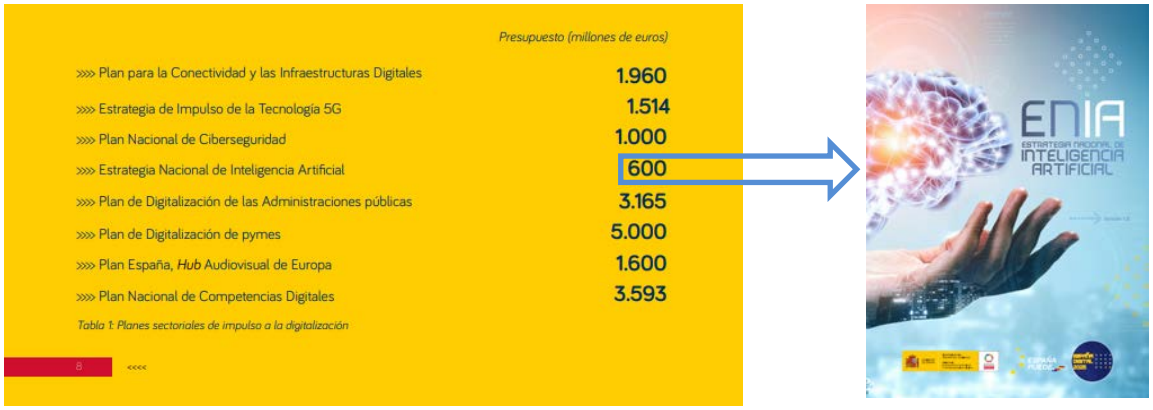


Figura 2-8 Planes incluidos en Plan España Digital 2026. Fuente: Gobierno de España.

En el prólogo de la ENIA, el Presidente del Gobierno señala que: *"La IA ha sido identificada a nivel mundial como una de estas tecnologías con mayor proyección e impacto en todas las áreas de actividad. La IA actúa como un catalizador de la investigación y la innovación, haciendo de la generación, almacenamiento y procesado masivo de datos (Big Data) un sector económico en sí mismo en el nuevo escenario digital y de desarrollo tecnológico."*

Unos párrafos más adelante se señala lo que se denomina como la "cuestión central" que no es otra que la cuestión ética: *"la cuestión central que subyace en el desarrollo y la extensión de la IA es la cuestión ética. El uso extendido y la gestión de los datos mediante la acción de los algoritmos y sistemas autónomos tiene múltiples implicaciones en el plano ético y moral que exige procesos y mecanismos de control que protejan nuestros valores, principios y derechos"*.

La ENIA establece un plan de acción que se desarrolla en seis ejes estratégicos:

1. Impulsar la investigación científica, el desarrollo tecnológico y la innovación en IA.
2. Promover el desarrollo de capacidades digitales, potenciar el talento nacional y atraer talento global en IA.
3. Desarrollar plataformas de datos e infraestructuras tecnológicas que den soporte a la IA.

4. Integrar la IA en las cadenas de valor para transformar el tejido económico.
5. Potenciar el uso de la IA en la administración pública y en las misiones estratégicas nacionales.
6. Establecer un marco ético y normativo que refuerce la protección de los derechos individuales y colectivos, a efectos de garantizar la inclusión y el bienestar social.

Las alusiones a la Defensa y Seguridad son escasas en el documento y se circunscriben al Eje 4 donde se recogen las iniciativas de I+D+i asociadas a la defensa desde el punto de vista nacional y europeo. No obstante, la ENIA, sus principios y ejes estratégicos han constituido la primera referencia de la estrategia propia del Ministerio de Defensa. En especial cabe señalar que el último eje estratégico desarrolla la necesidad de establecer un marco ético y normativo que refuerce la protección de los derechos individuales y colectivos, a efectos de garantizar la inclusión y el bienestar social.

Las acciones previstas en este eje estratégico se articulan en tres ámbitos, considerados clave, sobre los que incide la IA:

- Jurídico. Para proteger los derechos fundamentales ya reconocidos e identificar las lagunas jurídicas existentes.
- Socio-tecnológico. Para establecer metodologías y estándares con los que desarrollar aplicaciones de la IA.
- Ético. Para aseguras que el uso de la IA acompaña a los valores de la sociedad.

A lo señalado anteriormente hay que añadir que el Gobierno de España ha constituido un Comité de Expertos para la elaboración de una Carta de Derechos digitales con el fin de identificar un conjunto de principios fundamentales que inspiren la producción normativa para adaptarla a las nuevas situaciones y circunstancias del ámbito digital, en particular, las relativas a la extensión de la IA.

2.2.2 *En la Organización del Tratado del Atlántico Norte.*

En octubre 2021 la OTAN aprobó su estrategia sobre IA tras haberla reconocido como la EDT de mayor transcendencia para potenciar las capacidades de la Alianza y apoyar el desarrollo de sus misiones. Fue presentada como la “first-ever”, primerísima estrategia de IA como aparece en la Figura 2-9. La Alianza considera que la IA afectará a todas las actividades que realiza la organización y apoyará sus tres misiones esenciales: la defensa colectiva, la gestión de crisis y la seguridad cooperativa.



Figura 2-9 Presentación de la NATO´s Artificial Intelligence Strategy. Fuente: NATO.

Para la OTAN, la IA está cambiando el entorno global también en defensa y seguridad. A la vez manifiesta que ofrece oportunidades sin precedentes para fortalecer nuestra ventaja tecnológica en una

declaración de optimismo poco habitual, pues también reconoce que aumentará la capacidad de las amenazas que enfrentamos.

Es importante señalar que la OTAN asume la definición de IA del NATO STO (2020) [23] ya señalado en este capítulo, y que la expresa como *"la capacidad de las máquinas para realizar tareas que tradicionalmente requieren inteligencia humana, por ejemplo: reconocer patrones, aprender de la experiencia, sacar conclusiones, hacer predicciones, o tomar acciones, ya sea digitalmente o mediante el software inteligente detrás de los sistemas físicos autónomos."*

Según se recoge en la página web oficial de la OTAN, esta estrategia persigue cuatro objetivos:

1. Proporcionar una base para que la OTAN y sus aliados lideren y fomenten el desarrollo y uso de la IA de manera responsable para fines asociados a la defensa y seguridad de los Aliados.
2. Acelerar e incorporar la adopción de la IA en el desarrollo y la entrega de capacidades, mejorando la interoperabilidad dentro de la Alianza, a través de propuestas de casos de uso de IA, nuevas estructuras y programas.
3. Proteger y monitorizar nuestra tecnología de IA y la capacidad propia de innovar, abordando consideraciones de seguridad como la puesta en práctica de nuestros principios de uso responsable.
4. Identificar y protegerse contra las amenazas del uso malicioso de la IA por parte de actores estatales y no estatales.

Es importante señalar el carácter comparativo que da la Alianza a la IA cuando señala que "nuestros" adversarios, tanto estatales como no estatales están desarrollando IA y desafían a la Alianza en una carrera para su adopción, algo parecido a una nueva carrera espacial. Por lo que manifiesta que es necesario mantener la "brecha tecnológica" respecto a nuestros potenciales adversarios para lo que la Alianza debe consolidar los esfuerzos realizados por las diferentes estructuras de la OTAN, promoviendo un foro de consulta entre los aliados y un vehículo de desarrollo empresarial de aplicaciones basadas en IA, y promoviendo la adopción de estándares y permitiendo su interoperabilidad.

El documento destaca los principios y la base legal para un uso seguro y responsable de la IA. Para ello orienta una hoja de ruta estableciendo unas normas compartidas por los aliados de acuerdo con la legislación internacional vigente y los valores de la Alianza. Estas normas se plasman en seis principios, basados en compromisos legales y éticos para el que denominan "uso responsable de la IA" que son: legitimidad, responsabilidad, trazabilidad y sencillez, fiabilidad, gobernabilidad y mitigación de posibles sesgos. Todos estos principios han sido asumidos por España y trasladados por el Ministerio de Defensa a su normativa propia.

La estrategia de la OTAN ha propiciado un gran número de iniciativas dentro de la Alianza y de los estados miembros entre la que destaca la creación del "NATO´s Data and Artificial Intelligence Review Board" (DARB) para canalizar los objetivos propuestos en la Estrategia. El Ministerio de Defensa de España participa activamente en este organismo y constituye una de las principales referencias tanto en la generación de normativa como en el desarrollo de casos de uso.

2.2.3 *En la Unión Europea.*

El Libro Blanco sobre la IA [24] es el documento que acompaña a la estrategia digital de la Unión Europea con una visión de cinco años, lo cual refleja que en este campo del conocimiento casi nadie se atreve a hacer planes a largo plazo. Durante este periodo la Comisión se centrará en:

- Diseñar el futuro digital de la UE a través de una tecnología que redunde en beneficio de las personas, impulsando la adquisición de competencias digitales, protegiendo de ciberamenazas,

asegurando que la IA respete los derechos de las personas, acelerando el despliegue de banda ancha ultra rápida y aprovechando la supercomputación.
- Apostar por la excelencia y confianza en la IA, mediante un liderazgo mundial, que fomente su uso de forma segura, a través del aprovechamiento de los centros de investigación.

Para ello en el citado Libro Blanco la Comisión propone un marco para una IA fiable. Este proyecto es fruto del trabajo llevado a cabo por un grupo de expertos de alto nivel, que presentó sus directrices éticas para una IA fiable en abril 2019. Con este documento la UE pretende movilizar a la sociedad europea y buscar sinergias entre los sectores público y privado para acelerar la implantación de la IA en todos los sectores.

En abril 2022 la UE publicó la Revisión del Plan Coordinado de IA y la Propuesta de Reglamento Europeo de IA. El borrador de este Plan recogía las acciones conjuntas entre la Comisión y los estados miembros en materia de inversiones; y la propuesta de Reglamento pretende ser el marco regulatorio para garantizar su uso fiable, ético y centrado en el ser humano, sin que ello suponga un lastre excesivo a la innovación y a las empresas. Tras largas sesiones de discusión y negociación, a finales de 2023 se llegó a un consenso sobre el citado Reglamento.

AI Act – Reglamento de IA de la Unión Europea.

El viernes 8 de diciembre de 2023, los negociadores del Parlamento y del Consejo llegaron a un acuerdo provisional sobre el Reglamento de IA de la Unión Europea. Este reglamento tiene como objetivo garantizar que los derechos fundamentales, la democracia, el Estado de derecho y la sostenibilidad ambiental estén protegidos contra la IA de alto riesgo, al tiempo que pretende impulsar la innovación y convertir a Europa en un líder global en este campo. El Reglamento establece obligaciones para hacer uso de la IA en función de sus riesgos potenciales y su nivel de impacto. El texto acordado, del que solo se dispone de las versiones previas, tendrá que ser aprobado formalmente tanto por el Parlamento como por el Consejo para convertirse en ley de la UE. La propuesta legislativa de Reglamento establece cuatro categorías de riesgos para sistemas y aplicaciones:

- Prohibidos, cuando los riesgos son inaceptables, como técnicas subliminales, aprovechamiento de vulnerabilidades, clasificación social, identificación biométrica.
- Regulados, cuando los riesgos son altos, como es el caso de la salud y la seguridad o que caen en las áreas de identificación biométrica y categorización de personas, gestión y operación de infraestructuras críticas, educación y formación, empleo, fuerzas de seguridad, servicios privados y públicos esenciales, migración y control de fronteras y administración de justicia y procesos democráticos.
- Transparencia, cuando los riesgos son limitados, como sistemas que interactúan con humanos, sistemas de reconocimiento de emociones, sistemas de caracterización biométrica y sistemas de manipulación de imagen, audio y vídeo.
- Sin obligaciones, cuando los riesgos son bajos o mínimos.

En función de estos riesgos, los legisladores de la Unión Europea reconociendo la amenaza potencial para los derechos de los ciudadanos y la democracia que plantean determinadas aplicaciones de la IA, acuerdan prohibir:

- Sistemas de categorización biométrica que utilizan características sensibles: *"un sistema de IA destinado a asignar a personas físicas a categorías concretas, como un sexo, edad, color de pelo, color de ojos, tatuajes, origen étnico u orientación sexual o política, en función de sus datos biométricos"*

- Extracción no dirigida de imágenes faciales de Internet o secuencias de CCTV para crear bases de datos de reconocimiento facial.
- Reconocimiento de emociones en el lugar de trabajo y en las instituciones educativas.
- Puntuación social basada en comportamiento social o características personales.
- Sistemas de IA que manipulan el comportamiento humano para eludir su libre albedrío.
- IA utilizada para explotar las vulnerabilidades de las personas (por su edad, discapacidad, situación social o económica).

Respecto a las exenciones de aplicación de la ley, los borradores disponibles señalan que esta regulación no se aplica a los sistemas desarrollados y empleados exclusivamente para usos militares, así como en el marco de acuerdos internacionales para las fuerzas de seguridad y cooperación judicial.

Los negociadores acordaron una serie de salvaguardias y excepciones concretas para el uso de sistemas de identificación biométrica en espacios de acceso público con fines policiales, sujetos a autorización judicial previa y para listas de delitos estrictamente definidas. La identificación biométrica "post-remota" se utilizaría estrictamente en la búsqueda selectiva de una persona condenada o sospechosa de haber cometido un delito grave.

Para los sistemas de IA clasificados como de alto riesgo (debido a su importante daño potencial a la salud, la seguridad, los derechos fundamentales, el medio ambiente, la democracia y el Estado de derecho), se acordaron compromisos que incluyen una evaluación obligatoria del impacto sobre los derechos fundamentales. Se les exige una evaluación de conformidad ex ante y el registro del sistema en una base de datos europea antes de que salga al mercado, además del cumplimento de la legislación de seguridad ya aplicables. Deben cumplir una serie de requisitos relativos a la gestión de riesgos, pruebas, robustez técnica, datos de entrenamiento y gobernanza de datos, trasparencia, supervisión humana y ciberseguridad. Se ha acordado que los sistemas de IA de propósito general, y los modelos en los que se basan, tendrán que cumplir con requisitos de transparencia. Estos incluyen la elaboración de documentación técnica, el cumplimiento de la ley de derechos de autor de la UE y la difusión de resúmenes detallados sobre el contenido utilizado para el entrenamiento.

Los Estados Miembros deben designar una entidad supervisora de la aplicación e implementación de la regulación, que para España es la Agencia Española de Supervisión de la IA (AESIA), y la European Artificial Intelligence Board formada por los Estados Miembros y la Comisión. Las autoridades nacionales tendrán acceso a la información confidencial, incluido el código de la IA, y podrían exigir medidas correctivas prohibiendo, restringiendo o retirando ese software e imponiendo severas sanciones económicas.

La Estrategia de desarrollo, implantación y uso de la IA en el Ministerio de Defensa, contempla dentro de sus principios varios aspectos alineados con los preceptos de los que ha emanado la necesidad de la Ley / Reglamento de IA de la Unión Europea. Entre ellos destacan:

- Legalidad: las aplicaciones de IA se desarrollarán y emplearán de acuerdo con el derecho nacional e internacional que sea de aplicación, incluida la Declaración Universal de Derechos Humanos y el Derecho Internacional Humanitario.
- Responsabilidad humana y rendición de cuentas: cualquier desarrollo de IA, así como su utilización, deberá permitir una clara supervisión humana con el fin de garantizar la debida rendición de cuentas y la atribución de responsabilidades.

También, en la Estrategia del MDEF se incluye un apartado específico de Resolución de conflictos éticos.

Será fundamental analizar el texto final cuando se apruebe definitivamente y entre en vigor, con especial atención a la redacción final que se dé a la exención para "usos específicamente militares", dado el impacto sobre las aplicaciones del MDEF. De hecho está pendiente de concreción la cuestión de cómo se tratan las aplicaciones de IA de doble-uso y militares.

Críticas a la Unión Europea

No son pocos los expertos que critican el excesivo afán regulador de la Unión Europea frente a potencias tecnológicas como Estados Unidos y China, menos obsesionadas en la regulación y más proclives a fomentar la innovación. Así lo expresa el Catedrático Andrés Pedreño en su libro; *"Europa frente a EEUU y China – Prevenir el declive en la era de la IA"* [25] cuya idea principal es que Europa se está convirtiendo en una economía cada vez más secundaria y dependiente tecnológicamente de otras potencias, y esto se está haciendo más evidente si cabe con la llegada de la IA.

2.2.4 *En las principales potencias militares.*

Dada la dimensión del trabajo, se estudiaran únicamente las tres potencias más sobresalientes en IA en el campo militar, que coinciden con aquellas que lideran el desarrollo de IA a nivel global. Son las que más invierten, las que más innovan: Estados Unidos, China y Reino Unido. Como muestra, son también las que disponen de más *"start-ups"* como señala la tabla 2-3:

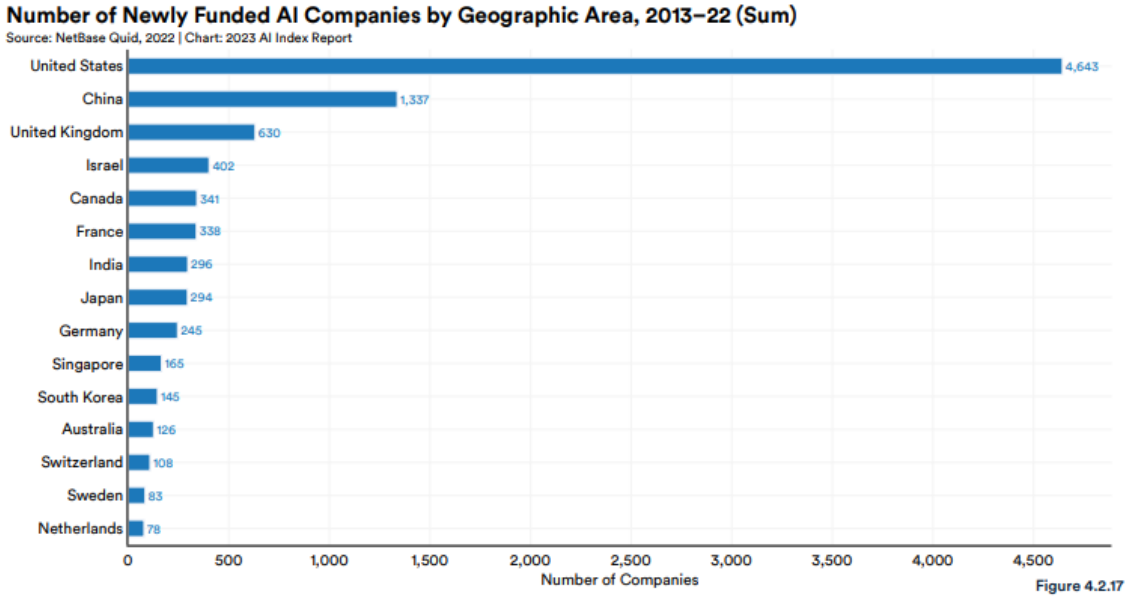


Tabla 2-3 Startups de IA por países de 2013 a 2022. Fuente: AI Index Report 2023 - Stanford Universitty.

Estados Unidos

En 2018 el DoD de los Estados Unidos publicó su propia Estrategia de IA [26] con el subtítulo *"Harnessing AI to Advance Our Security and Prosperity"* (Aprovechar la IA para mejorar nuestra seguridad y prosperidad). En la introducción del documento se señala que esta tecnología está cambiando el campo de batalla y las amenazas a las que los Estados Unidos deben hacer frente y que: *"Aprovecharemos el potencial de la IA para transformar positivamente todas las funciones del Departamento, apoyando y protegiendo así a los miembros de las fuerzas armadas estadounidenses, salvaguardando a los ciudadanos estadounidenses, defendiendo a los aliados y socios, y mejorando la asequibilidad, eficacia y rapidez de nuestras operaciones."*

En una situación que recuerda a la "guerra fría" expone que otras naciones, en particular China y Rusia, están realizando importantes inversiones en IA con fines militares, incluso en aplicaciones cuestionables en relación al derecho internacional y a los derechos humanos. Manifiesta que estas inversiones amenazan con debilitar la ventaja tecnológica y podría desestabilizar el orden mundial. Su intención es que los Estados Unidos, junto con sus aliados y socios, incorpore la IA para mantener su posición estratégica, prevalecer en los futuros campos de batalla y salvaguardar el orden.

En el documento se argumenta que la IA beneficiará al Departamento, su Ministerio de Defensa, y a la nación mediante:

1. Apoyar y proteger a los militares y civiles de todo el mundo: Mejorar el mantenimiento de los equipos, reducir los costes operativos y mejorar la preparación. Mejorar la exactitud de las evaluaciones militares y la precisión de las misiones. Reducir el riesgo de víctimas civiles y daños colaterales.
2. Proteger el país y a los ciudadanos: Mejorar la capacidad de predecir, identificar y responder a las amenazas cibernéticas y físicas. Desalentar los intentos de perturbar infraestructuras estadounidenses como redes financieras y eléctricas, procesos electorales y sistemas médicos.
3. Crear una organización eficiente y racionalizada: Simplificar los flujos de trabajo y aumentar la velocidad y la precisión de tareas repetitivas.
4. Convertirse en un líder en IA: Identificar y aplicar nuevos enfoques organizativos, estableciendo estándares y atrayendo el talento en esta tecnología.

En junio de 2023 un nuevo documento del DoD revisa y actualiza la Estrategia anterior. Esta vez lo titulan *"Data, Analytics, and Artificial Intelligence Adoption Strategy"* [27]. En esto no son los primeros que establecen una relación directa entre la Gestión de Datos y la IA. Como subtítulo esta vez *"Accelerating Decision Advantage"*, "acelerando la ventaja en la toma de decisión" con lo que se invoca a la señalada "carrera" geopolítica por el liderazgo en IA.

En este documento se señala que los últimos avances en tecnologías de datos, análisis e IA permiten a los líderes tomar mejores decisiones con mayor rapidez, en una sala de juntas y en el campo de batalla. Por este motivo, ven acelerar la adopción de esta tecnología como una oportunidad sin precedentes para proporcionar a los líderes de todos los niveles del Departamento los datos que necesitan y aprovechar todo el potencial del proceso de toma de decisiones de los miembros del Departamento.

Para adquirir esta **ventaja en la toma de decisiones** establece que será necesario: Tomar conciencia y comprender el espacio de batalla, disponer de un proceso de planeamiento adaptativo, disponer de cadenas de suministro rápidas y resilientes y hacer más eficientes los procesos. La figura 2-10 muestra visualmente los objetivos a conseguir con las diferentes tecnologías.

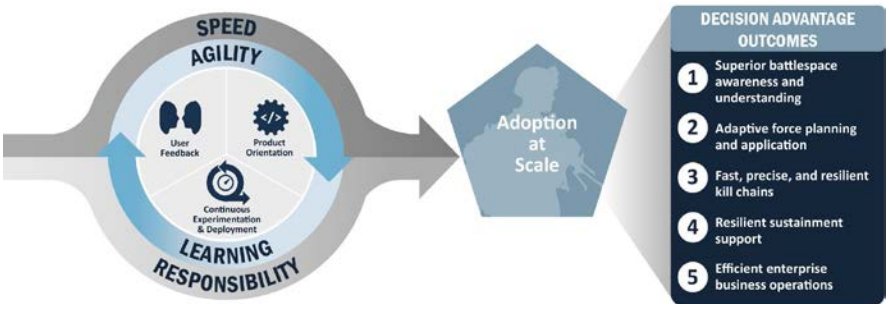


Figura 2-10 *"Decison advantage outcomes"* del enfoque ágil. Fuente: US DoD.

En lo que se refiere específicamente a la IA, el DoD afirma que centrará sus esfuerzos estratégicos en varios objetivos interdependientes que apoyan la Jerarquía de Necesidades de IA del DoD. Esta, se representa por la pirámide de la figura 2-11 cuyos cimientos son los datos de calidad.

En la cúspide de la pirámide se encuentra la IA responsable, que es el enfoque del Departamento para el diseño, desarrollo, despliegue y uso de las capacidades de IA de acuerdo con los principios éticos del DoD. Las capas de la jerarquía se apoyan en sólidos conjuntos de procesos: el de la calidad de los datos y el análisis que se logran mediante una gobernanza eficaz de los datos. Los procesos de garantía para la prueba, evaluación, validación y verificación son imprescindibles para la IA responsable.

Finalmente, alrededor de la pirámide se representan los facilitadores, como la gestión del talento digital, que ayudan a sostener la jerarquía de necesidades; además de otros como la eliminación de barreras y las inversiones en mejorar la interoperabilidad.

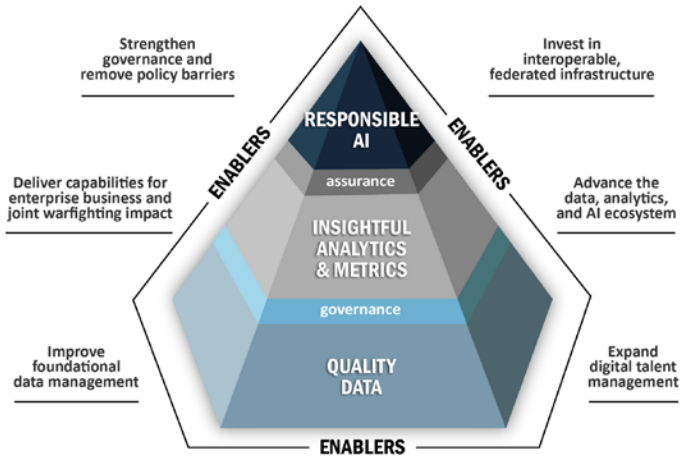


Figura 2-11 Pirámide de la IA. Fuente: US DoD.

El documento, de muy alto nivel y que no contempla casos de uso específicos, concluye que la dimensión y responsabilidades del DoD son únicas, pero que grandes organizaciones de todos los sectores han superado retos similares y han aprovechado las ventajas de la transformación digital. Su objetivo es conseguir que los líderes del DoD tengan acceso a datos de alta calidad, análisis avanzados y capacidades de IA para tomar decisiones oportunas y bien informadas para defender la patria, disuadir la agresión y ganar en los conflictos. Recuerda otra vez que sus competidores militares están integrando estas mismas tecnologías para su propio beneficio: *"No podemos permitirnos esperar y, además, no podemos lograrlo solos. Aplicar este enfoque ágil y centrarse en las actividades y en los objetivos descritos en esta estrategia permitirá al Departamento adoptar capacidades de datos, análisis e IA al ritmo y a la escala necesarios para crear una ventaja duradera en la toma de decisiones"*.

La influencia de los Estados Unidos en la OTAN y en sus aliados es evidente, más aun teniendo en cuenta su liderazgo en esta tecnología, por lo que los documentos del US DoD han sido tenidos en cuenta en la elaboración de la normativa nacional

Reino Unido

El Ministerio de Defensa del Reino Unido publicó en junio de 2022 su *"Defence Artificial Intelligence Strategy"* [28] apenas un año después de una *"Integrated Review"* sobre el mismo tema. Este nuevo documento está motivado según afirma el Secretario de Estado de Defensa en su prólogo por la invasión ilegal de Ucrania por parte de Rusia: *"Los trágicos acontecimientos que se están produciendo en Ucrania nos recuerdan con crudeza la importancia de garantizar que nuestras fuerzas armadas puedan hacer frente desafío militar convencional que esperábamos que nuestro continente hubiera*

dejado atrás en el siglo XX", convencional pero*; "…dar prioridad a la investigación, el desarrollo y la experimentación, mantener la ventaja estratégica explotando conceptos innovadores y avances tecnológicos de vanguardia - y la IA es una de las tecnologías esenciales para la modernización de la Defensa"*.

El UK MoD pretende con esta estrategia transformarse en una organización *"AI ready"* colaborando a nivel internacional en promover avances en su desarrollo y también con la industria británica de IA. Su visión es que, en términos de IA, pretenden ser la organización de Defensa más eficaz, eficiente, confiable e influyente del mundo, que no parece un objetivo menor:

- Eficaz, gracias a la capacidad de combatir y a las funciones de apoyo, y mejorando la capacidad de colaborar y asociarnos con los aliados del Reino Unido y el ecosistema de IA.
- Eficiente, mediante el uso innovador de la tecnología para proporcionar capacidades, conducir operaciones y mejorar la productividad en la organización.
- Confiable, para la sociedad, nuestros socios y nuestro personal, gracias a la seguridad y fiabilidad de nuestros sistemas de IA, y nuestro claro compromiso con el uso legal y ético de esta tecnología en consonancia con nuestros valores fundamentales.
- Influyente, colaborando con el desarrollo global de las tecnologías de IA y la gestión de los problemas asociados a esta tecnología, trabajando colaborativamente y predicando con el ejemplo.

La estrategia señala como resultados prioritarios a obtener que sus Fuerzas Armadas se modernicen y pasen rápidamente de una Fuerza Conjunta de la era industrial a una ágil Fuerza Integrada de la Era de la Información. A continuación, se resumen estos resultados prioritarios:

- Ventaja en la toma de decisiones, acelerando el proceso.
- Eficiencia, mejorando en flexibilidad, productividad y disponibilidad mediante la automatización inteligente.
- Desbloquear nuevas capacidades, garantizar la ventaja operacional desarrollando nuevas formas de operar, mejorando los efectos militares y protegiendo a nuestros soldados.
- Empoderar a toda la fuerza, reducir las cargas y concentrar el talento humano en las funciones de mayor valor que requieren ingenio, pensamiento contextual y criterio.

Al igual que la estrategia española, establece la necesidad de contar con una infraestructura TIC de base sólida, robusta y resiliente, su *"Digital Backbone"* equivalente a nuestra I3D nacional como se muestra en la Figura 2-12.

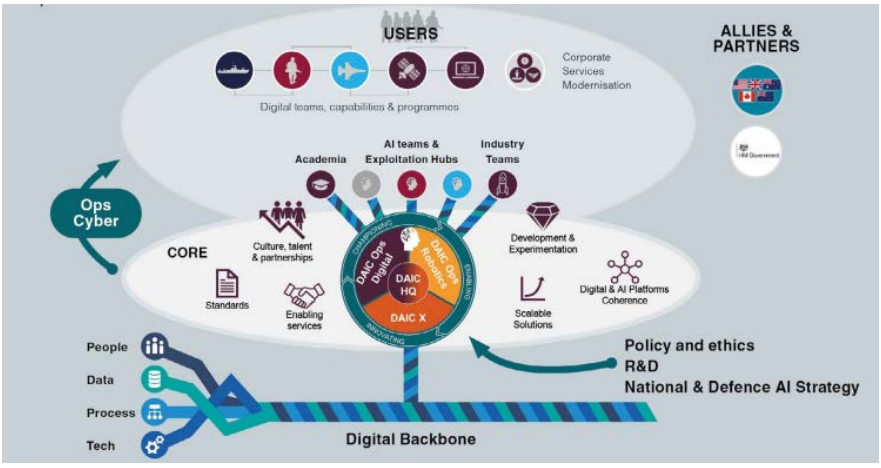


Figura 2-12 Defence AI Centre Architecture. Fuente: UK MoD.

También es compartida con el UK MoD la visión multidominio de las operaciones militares. En líneas generales comparte con otras estrategias aliadas incluidas la de la propia OTAN y la española la visión de transversalidad que presenta esta tecnología y los beneficios y desafíos que trae consigo. Asimismo, coincide en la necesidad de colaborar con todo el ecosistema de IA.

China

El Instituto Australiano de Política Estratégica, ASPI, es un grupo de expertos en políticas estratégicas y de defensa financiado el gobierno australiano. Regularmente pública un informe bajo el título, *"ASPI's Critical Technology Tracker. The global race for future power"* [29] que constituye una referencia global en la carrera geopolítica de la tecnología. Según la edición de 2023 del citado informe, China va por muy por delante en IA, hipersónica, drones y baterías eléctricas, mientras que solamente Estados Unidos le discute el liderazgo global aferrándose a la fabricación de chips y la informática de alta velocidad.

El informe además refleja que, según puede verse en la Tabla 2-4, China es ahora líder mundial en 37 de las 44 tecnologías clave, y ocupa el primer puesto mundial en tecnologías relacionadas con la defensa y el espacio en términos de investigación de alto impacto. Este estudio es únicamente un informe más de los muchos que reflejan la búsqueda de China de la hegemonía tecnológica mundial. En esta hegemonía buscada, la IA es uno de los principales, sino el primero, ejes de actuación del Gobierno chino.

Technology	Lead country	Technology monopoly risk
Artificial intelligence, computing and communications		
13. Advanced radiofrequency communications (incl. 5G and 6G)	China	high
14. Advanced optical communications	China	medium
15. Artificial intelligence (AI) algorithms and hardware accelerators	China	medium
16. Distributed ledgers	China	medium
17. Advanced data analytics	China	medium
18. Machine learning (incl. neural networks and deep learning)	China	low
19. Protective cybersecurity technologies	China	low
20. High performance computing	USA	low
21. Advanced integrated circuit design and fabrication	USA	low
22. Natural language processing (incl. speech and text recognition and analysis)	USA	low
Defence, space, robotics and transportation		
39. Advanced aircraft engines (incl. hypersonics)	China	medium
40. Drones, swarming and collaborative robots	China	medium
41. Small satellites	USA	low
42. Autonomous systems operation technology	China	low
43. Advanced robotics	China	low
44. Space launch systems	USA	low

Tabla 2-4 Extracto de: *"Lead country and technology monopoly risk"*. Fuente: ASPI.

En el caso de China es difícil encontrar documentos estratégicos militares. No obstante, en el ámbito civil, si es que existe esa diferenciación en el caso de la República Popular de China, el Gobierno Chino dio difusión en 2017 a su Plan de desarrollo de IA de nueva Generación cuya traducción realizada por la Universidad de Stanford [30], está disponible en la red.

Los principios básicos que guían esta estrategia son:

- Dirección tecnológica. Captar la tendencia de desarrollo global de la IA, destacar el despliegue de la investigación y el desarrollo orientados al futuro, explorar la disposición en dominios fronterizos clave, el apoyo a largo plazo, y esforzarse por lograr avances transformacionales y disruptivos en teoría, métodos, herramientas y sistemas; mejorar exhaustivamente la capacidad de innovación original en IA.

- Disponibilidad de sistemas. Aprovechar plenamente las ventajas del sistema socialista para concentrar las fuerzas en las grandes empresas, promover la planificación y la disposición de los proyectos, las bases y la reserva de talentos, vincular orgánicamente los grandes proyectos ya desplegados y las nuevas misiones.
- Dominar del mercado. Seguir las reglas del mercado, incentivar las posibilidades de las empresas en la línea tecnológica y el papel principal en el desarrollo de estándares de productos comerciales. Acelerar la comercialización de la tecnología y los resultados de la IA y crear una ventaja competitiva.
- Compartir conocimiento. Defender el concepto de compartición del conocimiento con la industria, la academia y la comunidad de innovación. Y lo que es más importante para este trabajo, traducción directa: *"Seguir la ley de desarrollo coordinado para la construcción económica y de defensa nacional; promover la conversión y aplicación bidireccional de los logros científicos y tecnológicos militares y civiles y la construcción conjunta y el uso compartido de los recursos de innovación militares y civiles; formar un nuevo modelo de integración civil-militar de todos los elementos, multidominio y altamente eficiente. Participar activamente en la investigación y el desarrollo globales y en la gestión de la IA, y optimizar la asignación de recursos innovadores a escala global."* Intención que marca claramente la intención "dual" del apoyo gubernamental al desarrollo de IA.

Posteriormente el documento fija los objetivos estratégicos en tres fases, con el fin de alcanzarlos progresivamente en 2020, 2025 y 2030. Por su trascendencia quedémonos en los programados para 2030, porque los anteriores, a juzgar por el informe ASPI y otros similares ya se han cubierto.

Estos objetivos son que para 2030:

1- Las teorías, tecnologías y aplicaciones de IA de China deberían alcanzar niveles de liderazgo mundial, convirtiendo a China en el principal centro de innovación de IA del mundo, logrando resultados visibles en aplicaciones de economía y sociedad inteligentes, y sentando una base importante para convertirse en una nación líder en innovación y una potencia económica.
2- China habrá formado un ecosistema teórico y tecnológico de IA de nueva generación más maduro. El país logrará grandes avances en inteligencia inspirada en el cerebro humano, inteligencia autónoma, inteligencia híbrida, inteligencia de enjambres y otras áreas, lo que tendrá un impacto importante en el ámbito de la investigación internacional.
3- La competitividad de la industria de la IA alcanzará el nivel de liderazgo mundial. La IA debe profundizarse y expandirse en gran medida en la producción y el sustento, la gobernanza social, la construcción de la defensa nacional, y en todos los aspectos de las aplicaciones, se convertirá en una tecnología central expansiva para los sistemas clave, las plataformas de apoyo y la aplicación inteligente de una cadena industrial completa y clústeres industriales de gama alta.
4- China habrá establecido una estructura de centros de innovación tecnológica y formación de personal de IA líderes en el mundo, y habrá elaborado leyes y reglamentos de IA más completos, así como un sistema de normas éticas y políticas.

Cabe concluir que la comunidad "occidental" debería acelerar en esta carrera geopolítica y unir esfuerzos para competir con China en el desarrollo de la IA y discutir su liderazgo. La opción contraria nos llevaría a un desequilibrio de inquietantes consecuencias geopolíticas.

2.2.5 *Adaptación tecnológica e innovación TIC en el Ministerio de Defensa.*

Desde la Secretaría de Estado de Defensa, bajo el liderazgo de la Dirección General CESTIC, ante la necesidad de incorporar las EDT en el ámbito TIC se inició en 2019 un sencillo esquema de actuación que está reflejado en un flujo de tareas, véase Figura 2-13, que comienza con la participación en la

comunidad tecnológica, atendiendo a foros de investigación y conferencias, en resumen "adquirir conocimiento" sobre la materia. Posteriormente, elaborar un documento estratégico que aúne las ambiciones e intereses del departamento y fije principios y líneas estratégicas de actuación. En tercer lugar, crear una estructura que permita la colaboración y suma de esfuerzos entre los ámbitos y busque recursos allá donde se encuentren.

Superados los tres primeros pasos, definir unos casos de uso iniciales y promover, ya dentro del campo de la innovación unos primeros proyectos piloto. Estos también podrán ser; pruebas de concepto, demostradores tecnológicos o directamente proyectos y programas llamados a ser puestos en producción en un periodo razonable.

Con esta sencilla línea de trabajo se pretende crear un marco de colaboración interdepartamental y también con el ecosistema nacional e internacional de innovación. Tres "consejos" se añaden a esta idea:

- Asegurar siempre un uso finalista de la tecnología, el departamento dispone de limitados recursos para investigar y deberá centrarse en las necesidades identificadas.
- Regirse por el paradigma ABC (*Adapt, Buy, Create*) y priorizar opciones de uso dual disponibles en el mercado.
- Huir de la solución mágica y la tener paciencia mínima que requiere la innovación.



Figura 2-13 Flujo de incorporación de tecnologías TIC al MDEF. Fuente: DG CESTIC.

Siguiendo este esquema, la Secretaría de Estado de Defensa, a propuesta de la Dirección general CESTIC, ha promovido entre 2021 y 2023 la incorporación de estas tecnologías apoyándose en las estrategias que se señalan:

- Estrategia de Explotación de la Nube en el Ministerio de Defensa.
- Estrategia de Comunicaciones Móviles de Quinta Generación (5G) del Ministerio de Defensa
- Estrategia de Desarrollo de Software en el Ministerio de Defensa.
- Estrategia de Desarrollo, Implantación y Uso de la IA en el Ministerio de Defensa.

2.2.6 *La Estrategia de IA del MDEF.*

Todas las referencias anteriores son citadas en el preámbulo de la "Estrategia de desarrollo, implantación y uso de la IA" [5] publicada por la Secretaría de estado de Defensa en el marco de la Transformación Digital.

A continuación, se señalan los aspectos más destacables de este documento de alto nivel. De la exposición de motivos cabe destacar las siguientes afirmaciones: "*En el plano militar, la evolución del escenario estratégico está sustituyendo el concepto clásico de operaciones conjuntas por el de operaciones multidominio, en las cuales son imprescindibles unos sistemas de gestión de la información, mando y control capaces, seguros e interoperables. En este sentido, los avances en las tecnologías de*

la información y de las aplicaciones militares de la IA, van a marcar la evolución del diseño y conducción de las operaciones."

Sobre la influencia que tendrá la IA en la configuración del campo de batalla, se indica: *"Las aplicaciones de la IA tendrán un impacto directo en todas las áreas que lo componen, destacando el de la gestión de la información, los procesos de obtención y explotación de inteligencia, la capacidad de disuasión, la toma de decisiones."*

Definición de IA para el Ministerio de Defensa.

Debido a la dificultad de encontrar una definición consensuada de IA, el Ministerio de Defensa opta por asumir la redactada por la Comisión Europea y que es citada en la ENIA [21]. Con esta definición se intenta acotar el alcance del término: *"Sistemas de software, y posiblemente también de hardware, diseñados por humanos que, ante un objetivo complejo, actúan en la dimensión física o digital percibiendo su entorno, a través de la adquisición e interpretación de datos estructurados o no estructurados, razonando sobre el conocimiento, procesando la información derivada de estos datos y decidiendo las mejores acciones para lograr el objetivo dado. Los sistemas de IA pueden usar reglas simbólicas o aprender un modelo numérico, y también pueden adaptar su comportamiento al analizar cómo el medio ambiente se ve afectado por sus acciones previas"*.

Pilares del desarrollo implantación y uso de la IA.

Para emprender actuaciones que preparen al Ministerio de Defensa para la incorporación extensiva de IA en el desarrollo de sus misiones, se determinan los siguientes cuatro pilares:

- Gestión del dato.
- Infraestructuras para la IA.
- Investigación, desarrollo e innovación.
- Formación, captación y retención del talento.

Principios de uso responsable de la IA.

Claramente inspirados en los *"NATO Principles of responsible Use of Artificial Intelligence in Defence"* [9], el Ministerio de Defensa traslada a su propia estrategia los siguientes siete principios *"Con el fin de lograr que la IA sea una tecnología fiable dirigida al cumplimiento de las misiones y cometidos del MDEF en general y de las Fuerzas Armadas en particular…"*:

- Legalidad.
- Responsabilidad humana y rendición de cuentas.
- Inteligibilidad y trazabilidad.
- Fiabilidad y trasparencia.
- Gobernabilidad.
- Mitigación del sesgo.
- Privacidad.

2.3 La guerra de Ucrania, "sandbox" para la IA.

Todavía es pronto en términos de análisis, pero tal y como señala Fojón [31] en un artículo publicado en el "IEEE", *"El teatro de operaciones ucraniano se ha convertido en un banco de experimentación de armas y procedimientos con especial relevancia para la valoración del impacto de las nuevas tecnologías y la digitalización en las operaciones militares presentes y futuras."* Un centro de experimentación "sandbox" para los bandos en disputa y sus aliados.

El empleo de nuevas tecnologías ha sido la oportunidad del supuesto contendiente débil, el ucraniano, para poder competir en el conocimiento de la situación y la coordinación de acciones ha concedido libertad de acción a las fuerzas propias.

La guerra de Ucrania podría considerarse como el primer gran conflicto de operaciones multidominio. Para representar este concepto multidominio, el Director General del CESTIC, expuso recientemente en el CESEDEN la visión de "semiesfera digital". La semiesfera de la Figura 2-14 pretende representar, frente a la tradicional representación por planos, que la información y los datos, representados en código binario, rodean a todos los dominios tradicionales. La esencia de las operaciones multidominio es que se ven envueltas por una capa o componente digital que ejerce una notable influencia y del que no es posible aislarse.

El volumen de información a procesar para conseguir la ansiada "superioridad de información" que nos permita vencer es de tal volumen y crecimiento exponencial que las capacidades humanas se ven sobrepasadas. En este contexto entra en juego la IA en los conflictos actuales y la guerra de Ucrania en febrero 2022 es para muchos el primer conflicto militar a gran escala donde esta tecnología está jugando un papel relevante.

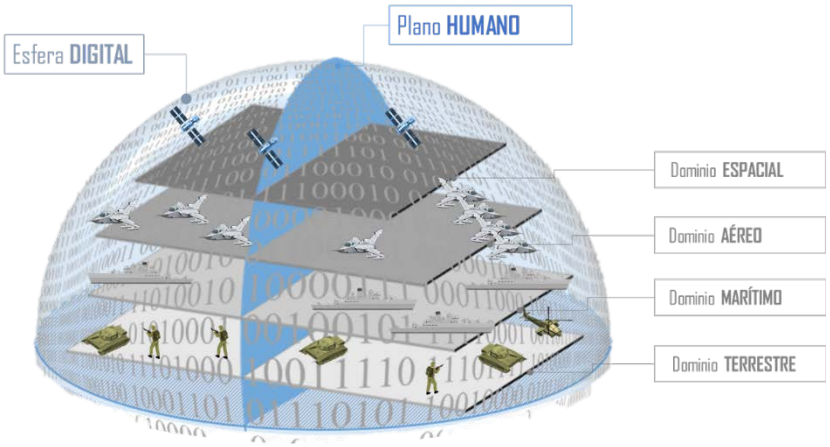


Figura 2-14 Representación del Mulidominio. Fuente: CESTIC.

2.3.1 *Particularidades de la Guerra de Ucrania.*

El hecho de que este es un conflicto distinto se podría apoyar en una serie de acontecimientos donde las tecnologías digitales han jugado un papel protagonista, siete de ellos son los que se señalan a continuación:

1. Semanas antes de atacar militarmente a Ucrania, la Federación Rusa ya se encontraba realizando ataques a las cuentas bancarias de funcionarios de alto mando y a los servidores del gobierno ucraniano intentando sembrar el caos y desestabilizar las instituciones gubernamentales y a su población. Horas antes de la invasión, Ucrania sufrió ataques cibernéticos como hackeos, malware, ataques de denegación de servicio (DDoS), y de hecho, los sitios web del Ministerio de Relaciones Exteriores, el Ministerio de Defensa y los principales bancos de Ucrania se encuentran funcionando de manera intermitente.
2. La primera persona que dio a conocer la invasión en los medios, no fue un militar o diplomático, lo descubrió a través de Maps. Días antes del ataque, un tecnólogo llamado Jeffrey Lewis se encontraba monitoreando la frontera de Rusia y Ucrania mediante Google Maps, a raíz de haber recibido unas fotografías donde se veían vehículos militares rusos "en fila y listos para salir". Un día antes de la invasión, se dio cuenta que había bloqueos inusuales en las calles y un tráfico muy pesado cerca de las fronteras. Inmediatamente determinó, que era porque Rusia comenzaba

a invadir, fue el primero en notar esto, sus predicciones fueron tristemente ciertas. Tras este descubrimiento, y en vista de la situación, Google desactivó la geolocalización en Ucrania para evitar que los rusos rastrearan los movimientos ucranianos.

3. Sanciones económicas vía Internet. La primera de ellas es la expulsión de algunos bancos rusos al sistema "SWIFT", un protocolo que permite que compartan información y activos financieros a nivel internacional, y también se limitó el acceso de Apple Pay y Google Pay.
4. Ucrania pidió a las BigTech US que le negasen actualizaciones de software a los rusos.
5. Las noticias falsas "fake news" adquieren un nivel de uso sin precedentes, por los dos bandos. Es probable que nadie se crea nada, pero quedan en el subconsciente imágenes que podrían condicionar el comportamiento humano.
6. Elon Musk apoya a Ucrania con su constelación de satélites de baja órbita STARLINK permitiendo la conectividad a Internet de las fuerzas ucranianas y su población. Por otro lado, AZURE de Microsoft migra a la nube a la gran mayoría de instituciones gubernamentales ucranianas en tiempo record.
7. El empleo de drones de todo tipo y la vertiginosa adaptación de desarrollos civiles para su uso militar está marcando al curso de la guerra y equilibrando a bandos inicialmente desnivelados.

2.3.2 *La IA en Ucrania*

La mayoría de los drones utilizados han sido pilotados remotamente por lo que no se puede considerar en sí mismo como aplicaciones de IA. No obstante, sí que han empleado aplicaciones puramente IA, algunas fueron presentadas por el "DELTA TEAM" *(From Innovation to Battle-Winning Capability)*, acompañado de vídeos representados en las figuras 2-15 y 2-16. Representantes de las Fuerzas Armadas ucranianas mostraron a la comunidad militar y de innovación varias destacadas aplicaciones entre las que se destacan las siguientes:

- Utilización de ML para reconocimiento de vehículos terrestres desde cámaras en superficie *(Road cameras)*.



Figura 2-15 Reconocimiento de vehículos militares. Fuente: UKR Delta Team.

- Utilización de ML para reconocimiento de vehículos terrestres desde cámaras en drones (UAV).



Figura 2-16 Reconocimiento de vehículos militares desde UAV. Fuente: UKR Delta Team.

También se han empleado otras aplicaciones que merecen ser destacadas por originales:

Triage, priorización de pacientes.

Un artículo recogido en prensa digital [32] informa que *"investigadores ucranianos desarrollaron un sistema de triage basado en IA para ayudar a clasificar a los heridos de metralla en función de la gravedad de su estado"*. El equipo de la Universidad Nacional Radioelectrónica de Karkov desarrollo un sistema capaz de analizar tomografías computerizadas (TAC) de heridas de metralla, determinar su localización en el cuerpo, el tipo de materia y el nivel de urgencia para una posible intervención. Un correcto triage salva muchas vidas en el campo de batalla, pues permite optimizar los recursos médicos disponibles siempre saturados. En Ucrania, según señala el artículo, *"…los médicos de su país atienden hasta tres nuevos heridos de metralla al día y que la mayor dificultad es encontrar los pequeños fragmentos de menos de cinco milímetros que se alojan en el cuerpo y la extracción segura de los que están cerca de las arterias. Este modelo de IA, esperan, ayudará a los médicos a estimar rápidamente el nivel de gravedad de los pacientes"*.

Llama la atención especialmente el método de obtener datos, llamémosle etiquetados, *"Entrenar una IA requiere una gran cantidad de datos que ayudan al sistema a aprender una tarea en concreto. Para poder establecer el nivel de peligro de una herida de metralla, la IA ucraniana tiene que aprender primero a determinar qué tipo de material es el que ha provocado las heridas. El equipo de científicos ucraniano, liderado por el profesor Kyrylo Smelyakov, obtiene sus datos al insertar diferentes materiales de metralla en un tejido muy similar al del cuerpo humano, el de los cerdos. Sin embargo, este método no ha dado buenos resultados ya que, según explican, el movimiento del tejido animal al desplomarse y hundirse durante los TAC ensucia la calidad de los datos recogidos."* Ante esta mala calidad de los datos han recurrido a, *"…sus colegas de la Universidad de Warwick,…, que están especializados en el diseño de modelos de distintas partes del cuerpo humano con impresión 3D"*. Con estos datos esperan que el modelo dé mejores resultados, *"En el mejor de los casos, (la IA) podrá predecir con una precisión del 100% cuál es el resultado para ese paciente, qué tratamiento necesita, si es inmediatamente crítico, si necesita que se lo extirpen o si se puede dejar dentro e ingresarlo en un pabellón durante un tiempo"*.

Reconocimiento facial.

La sección de tecnología del diario ABC [33] se hacía eco en el pasado mes de marzo 2022 de una información de la Agencia Reuters que afirmaba que *"la empresa estadounidense Clearview AI, que cuenta con una base de datos de 10.000 millones de imágenes faciales, estaba prestando sus servicios al gobierno de Zelenski de forma gratuita"*.

Apoyándose en la inmensa base de datos de Clearview, el ejército ucraniano puede localizar a espías rusos, realizar controles o identificar soldados caídos en combate. No es descartable que la controvertida empresa, de la que se han puesto en duda los métodos utilizados para obtener las imágenes faciales de redes sociales, fotografías policiales y medios de comunicación esté intentando lavar su imagen corporativa. Esta aplicación, que muy probablemente se estará utilizando, presenta números conflictos éticos, pero según señala un jurista mencionado en el mismo artículo, *"Ucrania no es un miembro de la UE, no tiene nuestra normativa. Aunque dudo mucho de que les preocupe mucho en la situación en la que se encuentran"*. De la base de datos existente se estima que 2.000 millones de imágenes procederían de VKontake, la plataforma más popular de Rusia. Estas imágenes son las que sirven para detectar soldados rusos. Sin duda, si eres un joven ucraniano y te pareces a un joven ruso, preocúpate mucho por los errores en las técnicas de reconocimiento facial, que se producen con frecuencia. *"El año pasado, un grupo compuesto por más de 70 académicos y juristas españoles enviaron una carta al Gobierno español solicitando una moratoria en el uso de estos sistemas. Un error de esta tecnología en zona de combate, o en un control policial, podría motivar que ciudadanos corrientes corriesen graves riesgos"*

2.4 Categorías y clasificación de la IA.

Consensuar una definición de IA, está siendo objeto de múltiples discusiones en foros académicos, empresariales e incluso militares. Aunque no es el motivo de este trabajo, se considera necesario al menos establecer unos conceptos de básicos y definiciones que nos permitirán después agrupar los posibles casos de uso militar.

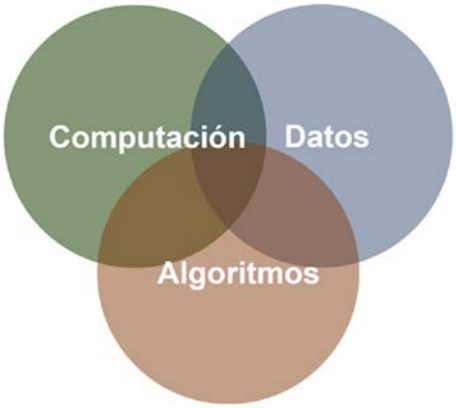


Figura 2-17 Elementos de la IA. Fuente: IEEE

En el Documento de Investigación 01/2022 del Instituto Español de Estudios Estratégicos Oliver y Corchado exponen [34] los que considera componentes de la IA: *"la IA se podría definir esquemáticamente como una estructura de sistemas complejos que usan avanzadas tecnologías digitales de procesamiento electrónico, manipulan complejos algoritmos y, a su vez, gestionan enormes volúmenes de datos estructurados y no estructurados, todo ello realizado a gran velocidad."* En el mismo documento, más adelante encontramos identificadas un conjunto de tecnologías que se reconocen como agrupadas bajo el concepto de IA. Es una clasificación bastante extendida y proviene de una

traducción de un estudio de M. Ziyad de la Universidad Británica de Egipto. Considerándola lo suficientemente completa para las necesidades de este trabajo se tomará como referencia. En la Figura 2-18 se refleja la versión en inglés y su traducción al español.

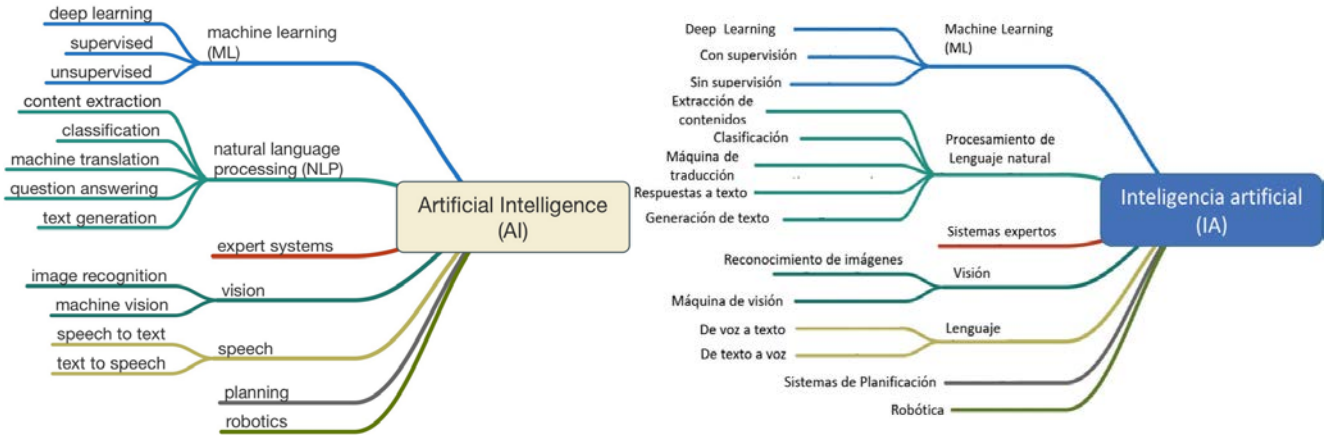


Figura 2-18 Tecnologías usadas en sistemas de IA. Fuente: IEEE

Aunque son áreas del conocimiento muy próximas e íntimamente relacionadas, no conviene confundir la IA con el *"Data Science"* (DS) o el *"Data Management"* (DM). La ciencia de los datos es un campo multidisciplinar que combina estadística, matemáticas, informática y conocimientos especializados para extraer conocimientos sobre datos recogidos o extraídos. La IA en cambio persigue mediante técnicas y teorías desarrollar computadoras, hardware y software, para que puedan llevar a cabo tareas que inicialmente requerían inteligencia humana o al menos biológica. En la Figura 2-19 del *"Defense Science and Technology Laboratory (DSTL)"* [35] podemos ver la relación entre IA y DS, y la consideración del Machine Learning como un subconjunto de la IA.

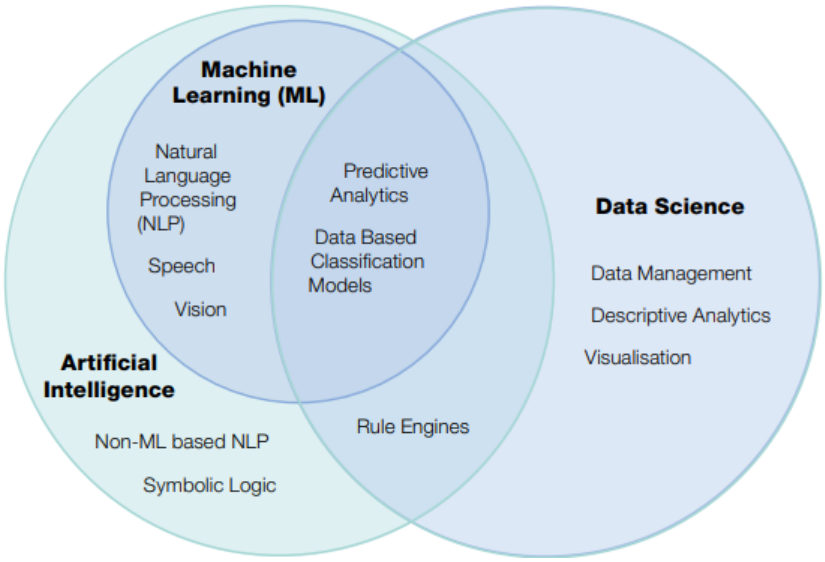


Figura 2-19. Relación entre IA, ML, y DS. Fuente: The DSTL Biscuit Book.

Llegados a este punto, se considera conveniente establecer algunas definiciones con vistas a poder clasificar posteriormente los diferentes proyectos de IA.

El Machine Learning (ML) o aprendizaje automático, "es una rama de la IA y la informática que se centra en el uso de datos y algoritmos para imitar la forma en la que aprenden los seres humanos, con una mejora gradual de su precisión"[1]. Se basa en el proceso de alimentar una computadora con datos (información, en principio en cualquier formato). Esta máquina utilizará diferentes técnicas de análisis sobre estos datos para aprender y será capaz de realizar una tarea, por ejemplo clasificar tipos documentales. La ventaja que ha aportado el ML es que para conseguir esto, no necesita una programación específica con gran cantidad de esfuerzo de desarrollo.

El ML se subdivide en varios tipos:

- ML supervisado. El aprendizaje supervisado se basa en datos etiquetados (preparados) a partir de los cuales se generan modelos para predecir el resultado de salida. Se basa en ejemplos históricos conocidos. Para ello utiliza algoritmos y características de los datos de entrenamiento. A medida que se introducen datos de entrada en el modelo, este se adapta sus pesos hasta que se haya ajustado correctamente. El aprendizaje supervisado permite a las organizaciones resolver una amplia variedad de problemas del mundo real.
- ML no supervisado. El aprendizaje no supervisado se define como el aprendizaje de soluciones (conocidas como modelos) que no están obtenidas a partir de datos supervisados o etiquetados por alguien, es decir, no se le ha dicho a la máquina lo que tiene que aprender. El modelo se ajusta a la observación de los datos sobre los que no hay un conocimiento previo.
  La familia más popular de ML no supervisado son los algoritmos de agrupamiento o *"clustering"*. Esta técnica consiste en encontrar grupos de datos similares entre sí y relaciones que pueden estar ocultas en nuestros datos, algo que puede no ser obvio. Se usa para explorar datos desconocidos y revelar patrones sobre grandes volúmenes de información.

Si nos vamos a un nivel más puro, que algunos autores reconocen como la auténtica IA, aparece el Deep Learning (DL).

- Deep Learning (DL), aprendizaje profundo, es un tipo de ML que está inspirada en la arquitectura del cerebro humano y sus redes neuronales. A partir de una gran cantidad de datos y con numerosas capas de algoritmos busca que la máquina profundice y termine aprendiendo por cuenta propia de manera similar a como lo haría un humano. En el DL, el sistema aprende de los datos y aumenta su precisión si se le proporciona más datos. A priori, cuantos más estímulos reciba del objetivo, mejor será su predicción.
- Deep Reinforcement Learning (DRL), aprendizaje profundo por refuerzo, es una nueva generación de las técnicas de DL, que evoluciona la forma en que una máquina aprende a realizar una tarea. Busca implementar algoritmos que permitan a un agente aprender a tomar decisiones a partir de su interacción con el entorno. Se basa en obtener recompensas ante el aprendizaje de una nueva tarea, es decir, consiste en entrenar modelos para la toma de decisiones sin requerir datos para el entrenamiento.
  Así pues, los datos se generan a través de un método de prueba y error, donde se marcan con una etiqueta. Durante las fases de entrenamiento el algoritmo recibe marcas de recompensa cuando lleva a cabo la función correcta. Tras repetir la experiencia y verificar las recompensas recibidas, aprende por sí mismo. En el aprendizaje profundo por refuerzo el modelo es generado y realimentado automáticamente en cada nueva ejecución del algoritmo. A la máquina se le programan una serie de reglas básicas que regirán cada ejecución y una

[1] ibm.com

función de recompensa como resultado de la misma. La recompensa puede ser una función calculada por la propia máquina o bien recibir el visto bueno de una persona externa. La máquina aprenderá con cada ejecución si las decisiones que ha tomado le han reportado una mejor recompensa y en base a eso tomará mejores decisiones en el futuro.

Además del ML, si volvemos a la Figura 2-18 encontramos otras técnicas incluidas dentro del campo de la IA.

Natural Lenguaje Processing (NLP), Procesamiento del Lenguaje Natural, es una rama de la IA que consiste en la habilidad de una máquina para procesar información comunicada mediante el uso del lenguaje natural. El NLP combina la lingüística computacional, modelado basado en reglas del lenguaje humano, con modelos matemáticos estadísticos y de aprendizaje automático y profundo. Combinando estas tecnologías los ordenadores son capaces de procesar el lenguaje humano en forma de datos de texto o voz e incluso llegar a percibir su significado completo, y el sentimiento del emisor.

Expert Systems (ES), Sistemas Expertos, aunque hay cierta controversia sobre el asunto, muchos expertos incluyen esta técnica dentro de la IA. En todo caso fueron los pioneros de allá por la década de los 60 o incluso antes. Consisten en programas informáticos cuyo objetivo es solucionar un problema concreto y utilizan diferentes técnicas para simular el razonamiento de un ser humano. El nombre de *expertos* se debe a que originalmente pretendían imitar la actuación de un profesional en la materia con el objetivo de sustituirlo.

Los tipos más importantes son: RBO *"Rule Based Reasoning"*, basados en reglas previamente establecidas y abordan las situaciones más complejas a través de dichas reglas deterministas, CBR *(Case Based Reasoning)*, basados en casos, buscan soluciones haciendo una analogía de problemas anteriores y basados en Redes de Bayes, que emplean variables conocidas y su probabilidad para deducir una solución.

Robótica, esta rama del conocimiento está muy relacionada con la IA y ha de ser estudiada, más aún en el campo de lo militar. Pero no son pocos los que consideran que son dos campos de la ciencia y la tecnología muy relacionados, pero con elementos diferenciales. La robótica es esencialmente la disciplina que se encarga de diseñar máquinas capaces de automatizar tareas. Mientras que la IA es una rama de la computación que estudia la forma de que las máquinas imiten los procesos cognitivos de los humanos, que puedan aprender y razonar. La robótica se centra en la manipulación física, mientras que la IA se orienta a la parte interna o digital.

2.5 El dilema ético.

A pesar de no ser esta la motivación de este trabajo, no puede obviarse su importancia o al menos su repercusión. Aunque tal vez esta cuestión pueda ser considerada más propagandística que científica, la realidad es que mucho se ha publicado sobre la cuestión ética de la IA. En los últimos meses ha llegado a los medios una visión apocalíptica sustentada principalmente en opiniones escasamente documentadas. Poco ayuda que, con cierto oportunismo, medios de gran difusión rescatan en 2023, declaraciones de 2018 de científicos ya fallecidos como Stephen Hawking que señaló que *"Puede ser el fin de la raza humana"* [36] sacando esta frase del contexto en que la dijo el científico años antes.

La realidad es que "Terminator" es una buena película de 1984, dónde la computadora "SkyNet" entraba en línea en el futuro el 4 de agosto de 1997, tomaba conciencia de si misma el 29 de agosto, a las 2:14 y provocaba el apocalipsis global. Afortunadamente ese futuro, del que han pasado 25 años todavía no se ha producido y se ha quedado en una buena saga de películas con alta probabilidad de una quinta entrega (Terminator Génesis).

No obstante, todas las organizaciones están fijando postura ante los posibles dilemas éticos que podría presentar el uso de la IA. Sin necesidad de tomar conciencia de sí mismo, hoy es totalmente posible que un algoritmo de IA se conecte a un arma, letal o no, y ese es el caso principal que conviene regular a priori. En un segundo nivel, deberemos asegurar el respeto a los derechos de las personas y su privacidad.

La Estrategia de desarrollo, implantación y uso de la IA en el MDEF [5], zanja el asunto en su artículo octavo sobre "*Resolución de conflictos éticos"* señalando que: "*La utilización de IA en sistemas de armas estará condicionada a la clara e inequívoca posibilidad de identificar a la persona responsable de su empleo directo y de la decisión de uso, de acuerdo con las directrices que establezca el MDEF en esta materia*". A continuación, designa las autoridades responsables en los diferentes ámbitos de aplicación.

Estemos más o menos cerca de enfrentarnos a conflictos éticos derivados del uso de esta tecnología, la misión de los responsables, en el ámbito del MDEF, será garantizar que se cumplen los principios de desarrollo, implantación y uso responsable de la IA en la Defensa, recogidos en el apartado séptimo de la Estrategia (señalados en el punto 2.2.6. de este trabajo) para "*lograr que la IA sea una tecnología fiable dirigida al cumplimiento de las misiones y cometidos del MDEF en general y de las Fuerzas Armadas en particular*".

Para completar este punto se citan a continuación varios organismos surgidos para asegurar el uso ético de esta tecnología.

2.5.1 *Agencia Española de Supervisión de la IA.*

Después de numerosas controversias, es muy probable que la futura sede de la Agencia Española de Supervisión de IA se establezca en La Coruña. Según señaló en la prensa la Alcaldesa Inés Rey [37]: *"Continuamos trabajando en la creación del Patronato para gestionar la sede de la AESIA en A Coruña que, como nos comprometimos, estará en marcha antes de finales de año"*. No cabe duda de que la sede de esta Agencia situará a Galicia en la vanguardia tecnológica y científica en el prometedor campo de la IA convirtiendo a España en el primer país de la Unión Europea en crear una agencia estatal de supervisión de la IA.

El pasado 2 de septiembre se publicó en el BOE el Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el *"Estatuto de la Agencia Española de Supervisión de IA"* [38]. A partir de esta publicación, la administración dispone de un plazo máximo de tres meses para la efectiva puesta en funcionamiento de la AESIA con la constitución del Consejo Rector. La AESIA estará presidida por la persona titular de la Secretaría de Estado de Digitalización e IA. En cuanto al Consejo Rector, se compondrá de un Director y siete vocalías, de las cuales seis serán ejercidas por representantes de ministerios: cuatro del Ministerio de Asuntos Económicos y Transformación Digital, una de Hacienda y otra de Industria, Comercio y Turismo.

Si bien el MDEF no estará representado en el Consejo Rector, a propuesta del departamento el Real Decreto de creación recoge en su Disposición Adicional cuarta respecto a la colaboración con órganos de responsabilidad en materia de IA del MDEF que: *"En el desarrollo de las funciones que tiene atribuidas la Agencia Española de Supervisión de IA, para el cumplimiento de sus objetivos y fines, se articularán canales y procedimientos de colaboración y de coordinación de actividades de carácter permanente entre la Agencia y los órganos con responsabilidad en materia de IA del MDEF"*.

Funciones de la AESIA

El artículo 10 del Estatuto de la AESIA establece las competencias de la agencia de las que se destacan las siguientes:

- *La promoción de entornos de prueba que permitan una correcta adaptación de sistemas innovadores de IA a los marcos jurídicos en vigor.*
- *El apoyo al desarrollo y uso de sistemas de IA desde una doble perspectiva ambiental y sostenible.*
- *La creación de conocimiento, formación y difusión en relación con la IA ética y humanista.*
- *El impulso de la colaboración público-privada…*
- *La supervisión de los sistemas de IA para garantizar el cumplimiento de la normativa, tanto nacional como europea.*

La promoción de entornos de prueba que permitan la adaptación de sistemas innovadores de IA a los marcos jurídicos en vigor debe considerarse una función importantísima, que permitirá a las empresas desarrollar herramientas orientadas a cualquier sector en un entorno seguro. El impulso de la colaboración público-privada, la coordinación con iniciativas de terceros y la ayuda a la ejecución de programas a través de acuerdos o convenios, son una gran oportunidad para empresas, instituciones y Universidades y también, por qué no, para el sector público incluido el MDEF. Cabe concluir que las funciones de la AESIA van mucho más allá de la de mero supervisor. Su creación temprana y la atribución de competencias de dinamización y asesoramiento en IA tienen potencial para que la AESIA se convierta en aliado estratégico del sector y en un polo de atracción de empresas y talento relacionado con la IA en España y Europa y redunde en beneficio del MDEF.

2.5.2 *Uso responsable de la IA en la OTAN (DARB).*

En la mencionada NATO´s Artificial Intelligence Strategy [9], los Aliados y la propia estructura de la OTAN se comprometían a garantizar que las aplicaciones de IA que se desarrollen se ajusten a seis Principios de Uso Responsable (PRU) recogidos: *"legalidad; responsabilidad y rendición de cuentas; explicabilidad y trazabilidad; fiabilidad; gobernabilidad; y mitigación de sesgos"*, todos ellos trasladados a la estrategia nacional. Para dar cumplimiento a este mandato se creó el Comité de Revisión de Datos e IA (DARB, por sus siglas en inglés), cuyos representantes pueden verse en la Figura 2-20. El DARB sirve de foro para los Aliados para guiar el desarrollo y uso responsable de la IA y promueve el cumplimiento de los PRU.



Figura 2-20 Foto oficial DARB (febrero 2023). Fuente: NATO

El DARB se estableció con los siguientes objetivos:

- Generar confianza entre la comunidad, los innovadores y los usuarios operativos para dirigir los esfuerzos de innovación responsable en defensa de acuerdo con los valores de la Alianza y el derecho internacional.
- Guiar la adopción responsable de la IA (RAI), trasladando los PRU en normas y mejores prácticas que ofrezcan a la OTAN y a sus aliados una base común para crear controles de calidad, mitigar los riesgos y adoptar sistemas de IA fiables e interoperables.
- Actuar como foro para compartir las mejores prácticas e intercambiar puntos de vista.

La Alianza insta al DARB a que se asegure de que sus resultados no levanten barreras innecesarias a la adopción de la IA a la velocidad necesaria. La misión del DARB es colaborar a que, los Aliados y la OTAN, consigan desarrollar sistemas más fiables, interoperables y seguros, contribuyendo a proporcionar una ventaja cualitativa en relación con competidores estratégicos y potenciales adversarios.

La primera misión del DARB es determinar un conjunto de herramientas, *"Practical RAI Toolkits"*, que se pondrá a disposición de los Aliados que deseen utilizarlos. Otra de las solicitudes al DARB es el desarrollo del estándar de certificación RAI, *"RAI Standard Certification"*, que será una norma basada en un "proceso" que asegure el cumplimiento de los principios a través de un flujo de trabajo basado en la experiencia de los casos de uso propios y en las mejores prácticas en los sectores público, privado y académico, así como la sociedad civil y otros actores internacionales. Los primeros borradores de ambos objetivos ya están circulando entre los aliados, pero de momento su clasificación de seguridad no permite su publicación. Básicamente el proceso pretende ir comprobando el cumplimiento de todos los PRU en todas las fases del proceso lo cual implica revisar la ingesta de datos, los algoritmos, las herramientas utilizadas incluyendo su proceso de contratación, el despliegue y finalmente el uso.

3 CASOS DE USO

¿Por qué esta magnífica tecnología científica, que ahorra trabajo y nos hace la vida más fácil nos aporta tan poca felicidad? La respuesta es esta, simplemente: porque aún no hemos aprendido a usarla con tino.

Albert Einstein

3.1 Casos de uso militar.

Para estudiar los casos de uso potenciales, o en desarrollo, en el MDEF, se tomará como referencia los recogidos en el apartado undécimo de la estrategia de 2023 que como señala el Capítulo 1: *"Se basan e inspiran en los fijados en las Organizaciones Internacionales de Seguridad y Defensa y tienen en cuenta la disponibilidad de las infraestructuras de datos que permiten la adopción de IA"*. Son los recogidos en la siguiente tabla:

	Estrategia MDEF	**NATO's Artificial Intelligence Strategy**
1	Movilidad militar	Military Mobility Capability
2	Inteligencia	Intelligence
3	Guerra electrónica	-
4	Autonomía en sistemas no tripulados	-
5	Apoyo logístico y alistamiento operativo	Logistics Support and Operational Readiness
6	Conocimiento y vigilancia del entorno	lnformation Environment Assessment
7	Ciberdefensa	Cyber Defence and influence
8	Apoyo a la toma de decisiones	Assisted Decision-Making
9	Análisis geoespacial, meteorológico y oceanográfico	AI for climate analysis
10	Gestión de la información y CIS/TIC	-
11	Talento y formación	-

Tabla 3-1 Categorías de casos de uso militar de la IA ESP – OTAN

3.2 Movilidad militar.

3.2.1 *Planeamiento y apoyo del transporte, estratégico, operacional y táctico.*

El despliegue de fuerzas requiere de su proyección, o movimiento y transporte, desde la zona donde se encuentran estacionadas a la zona donde van a ser empleadas. Esta es una operación compleja donde el empleo de la IA se estima que podría ser ventajoso. El planeamiento de los movimientos y transportes exige tratar numerosos datos para adaptar las capacidades disponibles a las necesidades de movimiento y su coordinación. La exploración de muchas posibilidades en muy breve tiempo permite recomendar cuáles serán las más eficaces o eficientes, según los criterios marcados.

A la hora de controlar el movimiento, la capacidad de proceso de datos procedentes de los distintos medios de transporte permitirá tener una imagen precisa de la situación. De esta forma, se podrán corregir las desviaciones o reaccionar ante incidencias. Esto es fundamental en el caso de transportes multimodales.

3.2.2 *Optimización de rutas de transporte.*

En el ámbito civil, la IA está desempeñando un papel cada vez más relevante en el transporte de mercancías, impulsando la optimización, la eficiencia y la rentabilidad en las operaciones logísticas. La industria del transporte utiliza IA para la optimización de rutas y la gestión de flotas con seguimiento en tiempo real.

El US Army colabora con IBM para optimizar rutas de transporte, en combate o en el aprovisionamiento habitual diario de sus acuartelamientos y unidades desplegadas. El objetivo no es únicamente reducir los tiempos de transporte, sino también el consumo de combustible y las necesidades de mantenimiento de sus vehículos. Ya en 2017, Parsons publicaba en Defense Daily [39] , *"Army Enlists IBM's Watson To Streamline Logistics, Vehicle Maintenance"*.

3.2.3 *Seguridad de conductores y pasajeros.*

En el ámbito de la seguridad, la IA ofrece soluciones innovadoras para evitar accidentes humanos en la conducción: monitorizando el cansancio del conductor o sus constantes. Por su parte, la conducción autónoma está cerca de ser una realidad que pronto será regulada y admitida por la sociedad. No se tiene conocimiento de algún proyecto específico apoyado por IA, actualmente en desarrollo en el MDEF, que pretenda explotar esta vía de investigación.

3.2.4 *Proyecto ARCO: Aplicación robótica de un convoy operativo.*

Este proyecto [40] tiene como objetivo lograr el control a distancia, y en una segunda evolución autónomo, del primer vehículo de un convoy militar en zona de operaciones para reducir riesgos de IED u otras amenazas. Se pretendía hacer un demostrador funcional capaz de operar en entornos de operaciones militares, y de superar situaciones de GNSS denegado o con comunicaciones degradadas. Para ello se transformaron unos camiones tácticos en vehículos semiautónomos mediante equipamiento de sensorización y automatización.

Los resultados obtenidos hasta el momento en entornos representativos, equivalentes a las Zonas de Operación reales del Ejército de Tierra, han provocado optimismo sobre el posible desarrollo de un prototipo inspirado en el proyecto ARCO.

Nombre	ARCO
Año	2022 (Programa coincidente)
Agencia/Organismo	Ministerio de Defensa
Ámbito MDEF	DGAM / Ejército de Tierra
Área tecnológica	Robótica
Área de aplicación	Movilidad militar
Presupuesto	-
Avance	I+D+i
Resultados	Demostrador tecnológico
URL	https://publicaciones.defensa.gob.es/media/downloadable/files/links/b/o/bot_73.pdf

Tabla 3-2 Proyecto ARCO

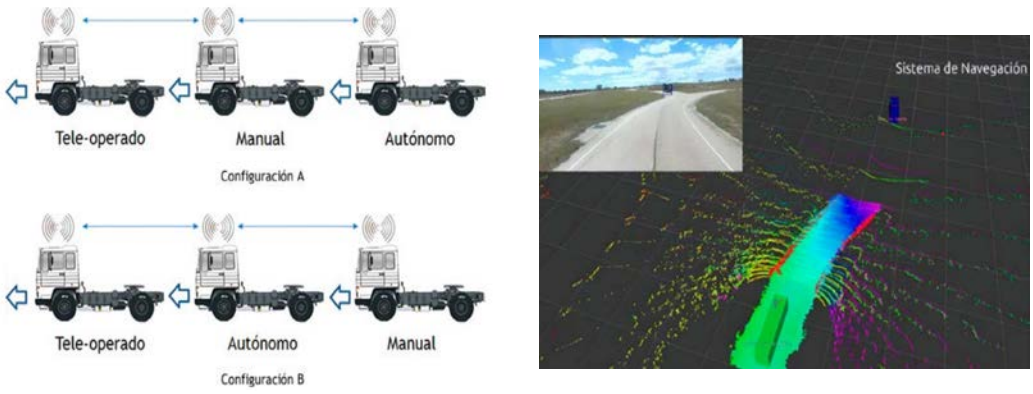


Figura 3-1 Proyecto ARCO. Fuente: Boletín Tecnológico Defensa

3.3 Inteligencia.

3.3.1 *Interpretación de imágenes, análisis de datos y documental. Traducción automática.*

Según la doctrina para el empleo de las Fuerzas Armadas [41], *"la función conjunta de inteligencia está formada por actividades que permiten tener, de forma continua, coordinada y oportuna, una visión integral, apropiada y actualizada del entorno operativo"*. El fin de la inteligencia militar es proporcionar a todos los niveles de mando y conducción de las operaciones una posición de ventaja en la toma de decisiones, a través del conocimiento y de la capacidad de hacerlo llegar al que lo necesita en tiempo y forma.

Se espera que la IA sea especialmente útil en labores de inteligencia debido a los grandes conjuntos de datos disponibles para el análisis. La sensorización de las Fuerzas Armadas presenta una tendencia de crecimiento que parece imparable, crece mucho más rápido que la capacidad para procesar la información recolectada. Ante la imposibilidad de analizarlo todo con medios humanos, las herramientas avanzadas de análisis y la IA se presentan como la tecnología que ayudará, más que sustituirá, a las personas "analistas" a realizar esta tarea. Las tecnologías innovadoras empleadas han de permitir al

combatiente superar a sus adversarios, física y cognitivamente, y así ganar ventaja militar, conocer mejor el entorno y al adversario, anticipándose a sus decisiones. Para no saturar al combatiente, pensemos en la primera línea, será necesario aligerar su carga cognitiva que traducido es "que tenga que pensar poco", lo cual en el fin último se tratará de marcar objetivos priorizados y distinguir entre "amigo o enemigo".

3.3.2 *Interpretación de imágenes.*

Este es sin duda un campo dónde la aplicación de la IA parece inmediata. Una de las más evidentes es la identificación de material militar a través de información recogida a lo largo del tiempo por distintos sensores, desde satélites hasta los propios combatientes en el campo de batalla y fuentes abiertas. Disponiendo de datos previamente etiquetados, podremos aplicar la técnica más eficaz para el reconocimiento e identificación de aeronaves, buques, vehículos terrestres o hasta personas. En el ámbito civil son herramientas de uso común, "Google lens" es un ejemplo.

Estás aplicaciones están muy extendidas, en el ambiente militar se conocen como técnicas de IMINT, Inteligencia de Imágenes, y constituye una especialización a la acceden analistas de todos los empleos en unidades de primera línea y estados mayores. Tal es el interés que presenta esta aplicación que ya se ofrecen incluso cursos en el sector civil, véase Figura 3-2, para conocer y aplicar diferentes técnicas al "reconocimiento e identificación de material" como el ofrecido por el LISA Institute, entidad educativa internacional especializada en Seguridad, Inteligencia, Ciberseguridad y Geopolítica.



Figura 3-2 Oferta de curso IMINT. Fuente: LISA Institute.

En el MDEF ya se están desarrollando casos de uso como los indicados en las siguientes secciones:

3.3.3 *Proyecto SATELLITE DATA AI (SEDA) para el procesado automático de imágenes satélite.*

El objetivo de este proyecto, Tabla 3-3 y Figura 3-3, era llevar a cabo la definición, desarrollo e implementación de una plataforma web de inteligencia geoespacial para la defensa. La plataforma está basada en diferentes técnicas de IA que permiten la colección, fusión y análisis de información adquirida por satélites procedentes de fuentes abiertas y operadores privados y por otro lado, lo que resulta militarmente más interesante, la detección automática de anomalías y cambios en las imágenes adquiridas.

Nombre	SEDA I
Año	2018 (Programa Coincidente)
Agencia/Organismo	Ministerio de Defensa
Ámbito MDEF	DGAM / Armada
Área tecnológica	Deep Learning
Área de aplicación	Guerra electrónica
Presupuesto	358.182 €
Avance	I+D+i
Resultados	Demostrador tecnológico
URL	Boletín de Observación Tecnológica en Defensa. Nº 74, 3º Trimestre de 2022

Tabla 3-3 Proyecto SEDA I

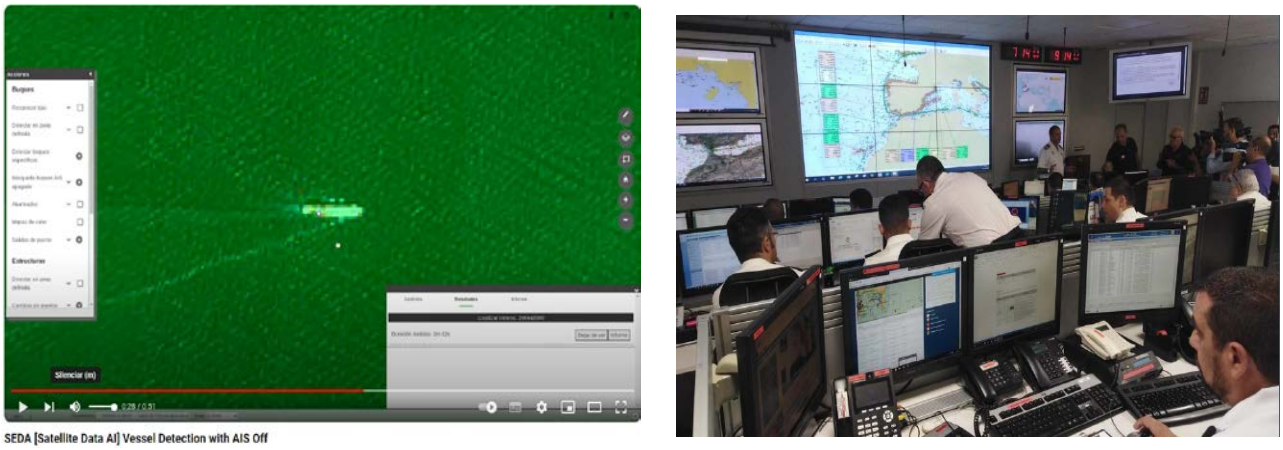


Figura 3-3 Proyecto SEDA I. Fuente: Boletín Tecnológico Defensa

3.3.4 *Proyecto de Sistemas Inteligentes para el procesamiento de imágenes y la detección de amenazas en escenarios de conflicto (CUSTODES).*

Nombre	CUSTODES
Año	2020
Agencia Organismo	MDEF – Universidades de Jaén y Granada
Ámbito MDEF	Ejército de Tierra
Área tecnológica	Machine Learning – Deep learning
Área de aplicación	Interpretación de imágenes
Presupuesto	458.142 €
Avance	-
Resultados	-
URL	https://diariodigital.ujaen.es/

Tabla 3-4 Proyecto CUSTODES



Figura 3-4 Proyecto CUSTODES ET

El proyecto, Tabla 3-4, Figura 3-4) pretende:

- Fusionar de forma automática la información disponible, de diferentes fuentes y tipología y aplicar métodos de preprocesamiento de imágenes y la anotación / construcción de características útiles para la extracción de conocimiento.
- Identificar de forma automatizada objetos de interés en imágenes estáticas o de vídeo mediante la obtención de modelos basados en técnicas DL.
- Recuperar de forma automática las imágenes disponibles de un determinado objeto de interés.
- Detectar anomalías con algoritmos para procesar imágenes y detectar cambios y en las mismas.

3.3.5 *Proyecto de reconocimiento de imágenes y asistencia a reacciones tácticas.*

Nombre	SEDA II
Año	2018 (Programa coincidente)
Agencia/Organismo	Ministerio de Defensa
Ámbito MDEF	DGAM / Armada
Área tecnológica	Deep Learning
Área de aplicación	Guerra electrónica
Presupuesto	358.182 €
Avance	I+D+i
Resultados	Demostrador tecnológico
URL	Boletín de Observación Tecnológica en Defensa. Nº 74, 3º Trimestre de 2022

Tabla 3-5 Proyecto SEDA II

Desde el Centro de IA de la Armada (CIA 2) se está trabajando en el SEDA II (Tabla 3-5, Figura 3-5) proyecto que incorpora IA para el procesado de imágenes procedentes de diferentes sistemas optrónicos. El proyecto se lleva a cabo en colaboración con NAVANTIA (SEPI) en el marco de los proyectos QuickWin de IA para el desarrollo de un modelo cuya implementación permitiría a los sistemas de vigilancia optrónicos (SVO) la detección y clasificación de unidades de superficie, aeronaves y misiles.



Figura 3-5 Proyecto SEDA II. Fuente: CIA2.

3.3.6 *Análisis de datos y documental. Traducción automática.*

Ante la desbordante acumulación de información, para conseguir inteligencia, es fundamental aumentar "mucho" la velocidad a la que se procesará la información, utilizando métodos tecnológicos avanzados, incluyendo IA, realidad virtual, modelización, análisis avanzado de datos y simulación. Si no hacemos esto, como ya se ha demostrado en muchos conflictos, se seguirán produciendo bajas aun disponiendo de la información necesaria para evitarlo, al no ser capaces de procesar y distribuir la información a tiempo. Necesitamos hacer que el ciclo OODA, representado en el Figura 3-6, sea más rápido que el del adversario y, en caso de ser posible, intentar atacar su ciclo o infectarlo con datos "malos" para conducirle a tomas acciones erróneas o a nuestro favor.



Figura 3-6 Ciclo OODA. Fuente: infodiagram.co.uk

No se ha encontrado información cuyo nivel de clasificación permita su publicación en este trabajo. A efectos de la investigación cabe señalar que existen herramientas ya disponibles en el mercado que permiten la necesaria centralización de los datos para mejorar la capacidad de explotar fuentes de inteligencia múltiple; nacionales, comerciales, privadas y de las llamadas fuentes abiertas mediante el análisis avanzado de datos y la IAIA. Entre estas herramientas disponibles destacan las siguientes:

3.3.7 *Herramienta PALANTIR.*

La empresa de tecnología Palantir, fundada por Peter Thiel, está tomando medidas para ampliar su alcance de mercado más allá de los servicios de vigilancia nacional para el Servicio de Inmigración y Control de Aduanas de los Estados Unidos.

En los últimos meses está tomando una cuota importante de mercado con su herramienta AIP que combina las técnicas de IA más importantes de las conocidas y pretende aplicarlas a todo tipo de clientes, con atención muy especial al sector de seguridad y defensa a nivel internacional. En su página web afirma disponer de una herramienta "AI-Powered" para cualquier decisión según muestra en su página web, Figura 3-7.

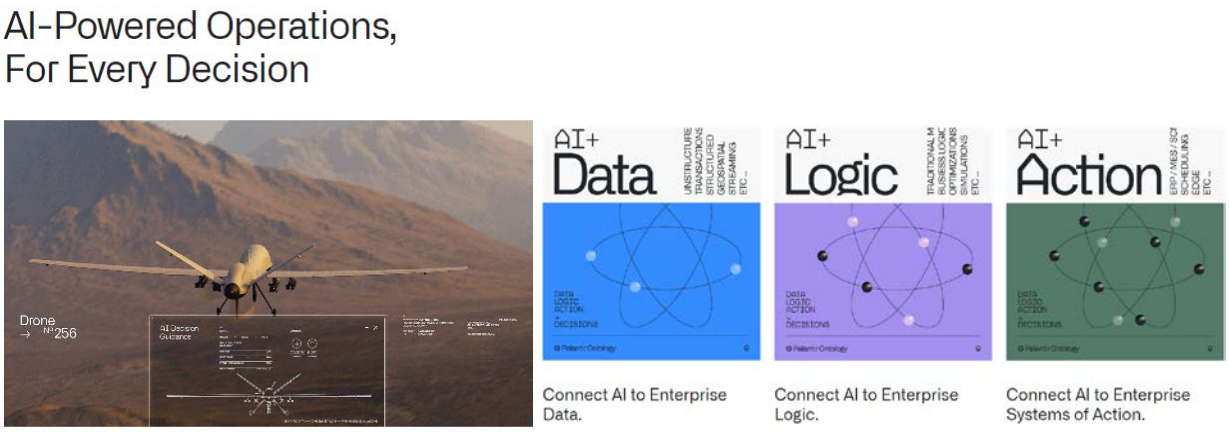


Figura 3-7 Capacidades de PALANTIR. Fuente: palantir.com

En un vídeo promocional de la empresa se muestra cómo su software podría ser utilizado en escenarios de guerra actuales. En el vídeo[2] un operador utiliza un Chatbot (LLM) para ordenar el reconocimiento de drones, generar planes de ataque y coordinar la interferencia de las comunicaciones enemigas, fusionando toda la información disponible en diferentes fuentes y sistemas.

Aunque las habilidades de la herramienta AIP parecen eficaces y eficientes para su empleo militar en la comunidad de inteligencia, el proveedor reconoce la importancia de controlar la aplicación de LLM y algoritmos en situaciones delicadas pudiendo garantizar su uso ético y legal. También existen preocupaciones sobre cómo evitar que los LLM generen datos y detalles falsos.

El tiempo dirá si esta herramienta u otra similar se hace con el mercado de la inteligencia militar, lo que no cabe duda es que no hay analistas "humanos" suficientes para fusionar toda la información disponible.

[2] https://www.youtube.com/watch?v=XEM5qz__HOU

3.3.8 *Traductores e intérpretes.*

Llama la atención que no se haya podido documentar ningún proyecto que intente explotar la capacidad de traducción que aporta la IA y los modelos de procesado del lenguaje natural. En casi cualquier misión militar, exceptuaremos las que son exclusivamente aéreas, tanto en tierra como en la mar, interactuar con la población local es imprescindible. La tarea de intérpretes y traductores, muchas veces reclutados "in situ", es fundamental para permitir que la comunicación sea efectiva. La misión de estos intérpretes es a menudo arriesgada, es necesario establecer una relación de confianza mutua que permita asegurar la integridad de la comunicación. A menudo crea unos vínculos de responsabilidad en el contratista que una vez finalizada su misión tiene que hacerse cargo del propio traductor y a veces incluso de su familia por miedo a represalias por parte de la comunidad local.

En el sector civil y empresarial esta aplicación de la tecnología está alcanzando un desarrollo del que cabe pronosticar que en poco tiempo reduzca o incluso acabe con la necesidad de traductores humanos. Un reciente artículo en la sección de tecnología de un importante diario nacional Santos [42] señalaba refiriéndose a uno de las aplicaciones de traducción más exitosas que: *"Aunque la voz suena un tanto robótica y hay un ligero retraso comparado con una traducción realizada por una persona, el resultado sigue siendo sorprendente. Mientras que una interpretación humana suele tener un retraso de 5 a 7 segundos, la experiencia artificial ronda los 10"*, teniendo en cuenta el tiempo de desarrollo empleado, cabe pensar que ese "gap" ira reduciéndose poco a poco en los próximos años o meses según se señala en el mismo artículo, *"el avance de la IA es inevitable y que los progresos que originalmente se pensaba que tardarían de 5 a 10 años, se han logrado en cuestión de meses"*.

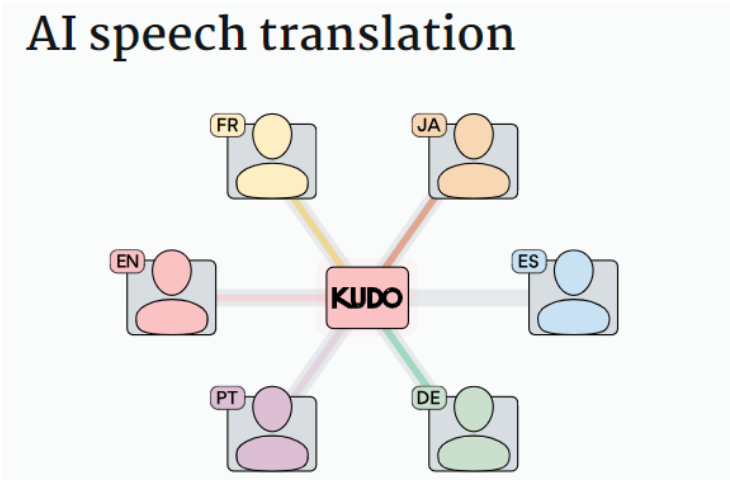


Figura 3-8 Reunión multilingüe. Fuente: kudoway.com

Lo que se está planteando en el sector empresarial no es una conversación en dos idiomas. El escenario propuesto es disponer de la capacidad de hacer una reunión en la que puedan participar al casi al unísono varios interlocutores, cada uno en su propia lengua, y ser capaz de entenderse, la empresa kudoway representa en la Figura 3-8, una posible conversación multilingüe. En el ambiente de operaciones multinacional en el que se desarrollan habitualmente las operaciones militares esta capacidad sería muy valorada.

La empresa META presentó en el verano de 2022 su proyecto NLLB-200, acrónimo cuyas siglas responden a la expresión en inglés *"No Languaje Left Behind"*, traducido, no dejar ninguna lengua atrás que nos recuerda a "no dejaremos ningún hombre atrás" lema característico militar como el recogido en el decálogo del soldado de nuestro Ejército de Tierra "*Jamás abandonaré a un compañero que necesite*

ayuda". El modelo basado en IA, se entiende que principalmente LLM, es capaz de traducir a doscientos idiomas diferentes. Actualmente traduce a cincuenta y cinco idiomas africanos, incluyendo lenguas como por ejemplo el "igbo" que se habla por un grupo étnico del centro y sureste de Nigeria que, aunque es un grupo de los más grandes de África, no parece fácil encontrar traductores en el seno de los estados miembros de la OTAN.

Según recoge Europa Press [43], *"La compañía ha publicado en código abierto el modelo NLLB-200 para que los investigadores puedan ampliar su trabajo a más idiomas y diseñar tecnologías más inclusivas. Con ello, ha anunciado que quiere conceder subvenciones de hasta 200.000 $ a organizaciones sin ánimo de lucro (ONG) que quieran aplicar esta nueva tecnología en entornos reales"*. Existen estas y otras herramientas ya disponibles para su incorporación como servicio de Software y uso inmediato en el MDEF allí donde sea necesario. Cabría pensar en una colaboración de las Fuerzas Armadas en el desarrollo de estas aplicaciones en sus zonas de misión con el fin de aprovecharse de ellas en el futuro y reducir la dependencia de traductores e intérpretes o al menos cumplimentarla. Además, la capacidad de percibir el comportamiento y el sentimiento humano en la comunicación, la mentira y el engaño, serían líneas de investigación a explorar, obviamente respetando los principios de uso responsable autoimpuestos.

3.4 Guerra electrónica.

3.4.1 *Planeamiento y apoyo a las operaciones de Guerra Electrónica.*

Como se expuso en el capítulo 2, el espacio de batalla del siglo XXI es híbrido y complejo. La llegada de las comunicaciones 5G y el IoT militar (Internet Of Things), el empleo de satélites, drones de todo tipo y el cada vez más sofisticado armamento configuran un entorno sobresaturado de señales electromagnéticas, propias a proteger y enemigas a quienes intentaremos negarles el uso a su favor del espectro electromagnético.

El avance y la utilización combinada de la inteligencia electrónica "ELINT", la inteligencia de señales "SIGINT" y los sistemas de guerra electrónica o contramedidas "ECM" están presentes en todos los dominios de las operaciones tradicionales; terrestres, marítimas y aéreas. La aplicación de la IA en la Guerra Electrónica Cognitiva tendrá el objetivo de combinar el uso de sensores avanzados con aplicaciones de gestión de grandes volúmenes de datos, en principio etiquetados y herramientas de aprendizaje automático (ML y DL) que permitan reaccionar a la altísima velocidad que las operaciones requieren.

3.4.2 *Proyectos CIA2 – Armada.*

Desde el Centro de IA de la Armada (CIA 2) se está trabajando en una prueba de concepto (Tabla 3-6, Figura 3-9) junto con ISDEFE que demuestra la bondad de las técnicas de ML en la clasificación de señales electromagnéticas en el espectro radar.

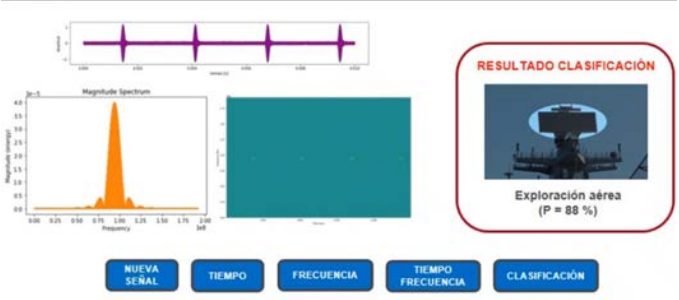


Figura 3-9 Proyecto de clasificación de señales. Fuente: CIA2.

Nombre	Clasificación de señales
Año	2023
Agencia/Organismo	Ministerio de Defensa
Ámbito MDEF	Armada
Área tecnológica	Machine Learning
Área de aplicación	Guerra electrónica
Presupuesto	-
Avance	I+D+i
Resultados	Prueba de concepto
URL	-

Tabla 3-6 Proyecto de clasificación de señales CIA 2

Otro proyecto significativo del CIA2 (Tabla 3-7, Figura 3-10) es el que se desarrolla para el empleo de IA en la determinación de la mejor solución de lanzamiento de señuelos, conocidos como “chaff” en la reacción antimisil, es un asunto recurrente de investigación en la Armada Española y en muchas otras desde hace décadas. Se busca facilitar a los operadores la elección del mortero y la secuencia de lanzamiento del señuelo ante el estresante acercamiento de un misil “inbound”. Si la reacción es automática, mucho mejor:

Nombre	Señuelos antimisil
Año	2023
Agencia/Organismo	Ministerio de Defensa
Ámbito MDEF	Armada
Área tecnológica	Machine Learning
Área de aplicación	Guerra electrónica
Presupuesto	-
Avance	I+D+i
Resultados	Prueba de concepto
URL	-

Tabla 3-7. Proyecto de lanzamiento de señuelos antimisil.

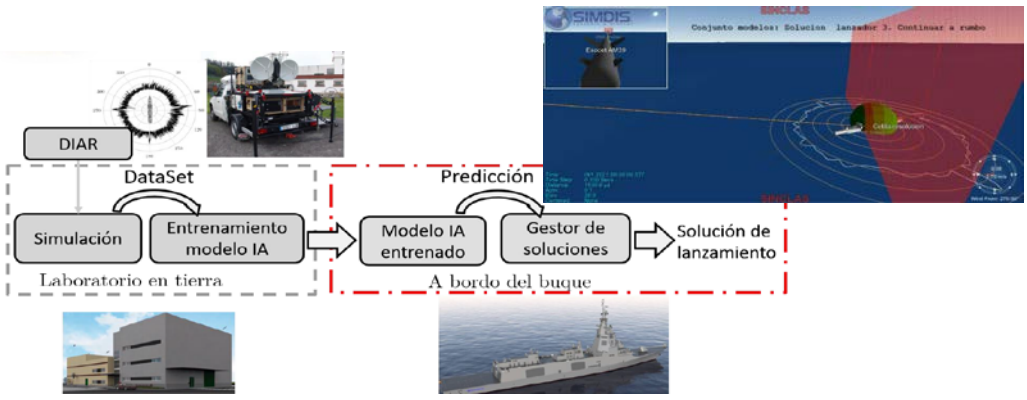


Figura 3-10 Proyecto de lanzamiento señuelos antimisil. Fuente: CIA2.

3.5 Sistemas no tripulados.

3.5.1 *Autonomía en el comportamiento de sistemas no tripulados. Desarrollo de funciones autónomas no letales en sistemas no tripulados terrestres, navales y aeroespaciales.*

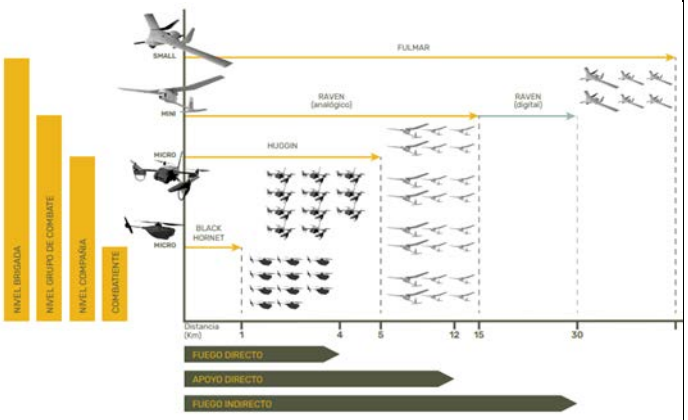
Este apartado, en sí mismo, merecería uno o varios trabajos pues sin duda alguna es el campo donde los avances y proyectos, ya operativos, han alcanzado su empleo más significativo por lo que únicamente se mencionarán algunos usos identificados y probados relacionados con la autonomía de sistemas no tripulados. A este respecto, desarrollaremos a lo largo de los siguientes párrafos las funciones autónomas no letales en sistemas no tripulados tanto terrestres, como navales y aeroespaciales.

Comencemos por el ámbito aéreo. En este sentido, volar será siempre una actividad peligrosa y formar a un piloto una misión extremadamente costosa. La posibilidad de dejar a los humanos en tierra y que vuelen sistemas *"unmaned"* sin hombre, a los que hemos traducido como autónomos, una palabra que no aclara tanto el concepto como el termino en inglés. Todo lo que vuela sin personas no es igual, conviene al menos distinguir entre RPAS *"Remotely Piloted Air Systems"* y UAV *"Unmaned Air Systems"* entendiéndose que los RPAS son sistemas controlados a distancia por personas que sustituyen a los que antes iban a bordo, en este caso será crucial asegurar las comunicaciones. El caso que nos interesa más, es el de los UAV, que los entenderemos como aquellos que realizan una misión de forma más o menos independiente. Aquí entra el concepto SALAS "Sistemas de Armas Letales Autónomos" sobre los que existe una notoria controversia y necesidad de regulación como ya se ha mencionado.

Conviene puntualizar que si nos vamos al concepto dron, "aeronave no tripulada" según la RAE, nos cabe casi cualquier elemento que vuela de forma autónoma, y nos estamos refiriendo a la actividad del vuelo y no de la misión, considero conveniente hacer esta puntualización. Hoy ya se encuentran en servicio multitud de drones en los ejércitos y la Armada, e incluso en la UME, se muestran a continuación algunos ejemplos en la Tabla 3-8.

Ejército de Tierra





1 Intelligence, Surveillance, Target Acquisition, Reconnaissance.

"Como medios propios de obtención, la unidad de Inteligencia de la «Brigada 35» dispondrá de plataformas aéreas tripuladas remotamente, con alcances de hasta 150 km, que le permitirán generar inteligencia de imágenes hasta los límites máximos de su área de responsabilidad"

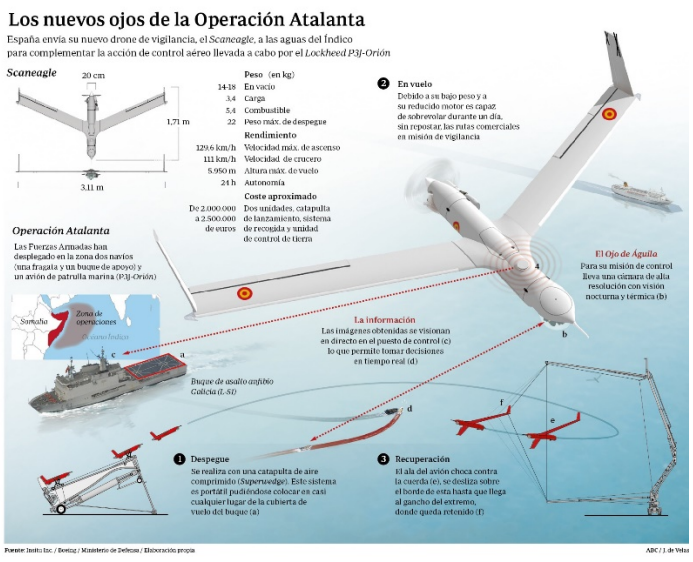
VISIÓN JEME FUERZA 2035

Armada



Alpha 900 en el BAM Furor. Fuente: verticalmag.com

"Alpha Unmanned Systems fabricante de helicópteros no tripulados con sede en Madrid, ha completado con éxito la integración de sus UAV en los sistemas de combate del BAM "Furor (P-46)" de la Armada Española."



Scaneagle de la Armada en servicio desde 2014. Fuente: abc.com

Ejército del Aire y del Espacio



MQ-9 Predator B en servico en el EA desde 2019

Unidad Militar de Emergencias

"El objetivo de la UME es contar con más de medio centenar de drones: 30 aéreos, 15 terrestres y 10 acuáticos que van a suponer toda una revolución tecnológica dentro de la UME, que obtendrá más información real de lo que está pasando y podrá intervenir de forma más eficiente." [44]





Tabla 3-8 Drones en el MDEF (ET, AR, EA, UME)

Pero, siendo puristas no ha sido hasta diciembre de 2021, cuando en un vuelo de prueba en la Base de la USAF Edwards (California), un avión de combate Lockheed Martin F-16 (VISTA X-62A), véase Figura 3-11, se convertía en el primer avión táctico controlado totalmente por IA durante diecisiete horas [45]. El piloto IA combinaba dos de los sistemas autónomos de Lockheed Martin: el Algoritmo de Seguimiento del Modelo (MFA) y el Sistema para el Control Autónomo de la Simulación (SACS). No se ha encontrado más información sobre la técnica o el mecanismo de aprendizaje utilizado. Lo esperado es que los cazas de 6ª generación, todavía faltan decadas para que entren en servicio, tengan la opción de volar y realizar misiones sin piloto.



Figura 3-11 VISTA X-62A. Fuente: la razon.es

3.5.2 *Proyecto SAFETERM*

Merece la pena hacer mención a este proyecto que la empresa GMV ha desarrollado mediante un contrato de la Agencia Europea de Defensa y la empresa AERTEC. Con el nombre de SAFETERM *"Safe Flight Termination System"* este proyecto [46] pretende mejorar los sistemas y procedimientos actuales de terminación de vuelo de drones de altitud media y larga duración mediante la aplicación de tecnologías de aprendizaje automático (ML) y así aumentar el nivel de seguridad en situaciones de emergencia o en caso de fallo de comunicaciones. Según recoge la página web de AERTEC[3], *"El sistema tiene como objetivo proporcionar herramientas para que la aeronave determine de forma autónoma las Áreas de Terminación de Vuelo Alternativas (AFTA) donde se pueda minimizar el riesgo para terceros. Se trata de que, ante la pérdida de comunicación con la aeronave y la posterior identificación de una emergencia que impida alcanzar las Áreas de Terminación de vuelo planificadas, la aeronave identifique rápidamente un área segura para aterrizar, evitando edificios, carreteras o áreas habitadas."*

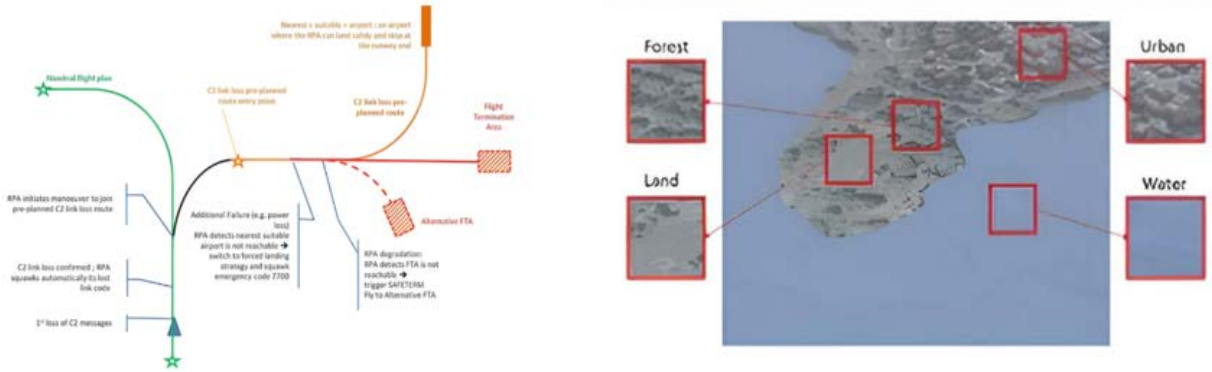


Figura 3-12 Esquema y visualización proyecto SAFETERM. Fuente: GMV.

[3] aertecsolutions.com

Según se recoge en el informe de Javier Ferrero [46] (Ferrero, 2023), los vuelos de captación de datos y validación se realizaron en el centro Atlas, en Villacarrillo (Jaén) y en la fase final se utilizó el UAS TARSIS 75 con el sistema SAFETERM embarcado.

Para desarrollar el algoritmo de control del sistema se utilizaron distintas técnicas de IA: aprendizaje automático (ML), aprendizaje profundo (DL) tradicional y de transferencia. Según señala Ferrero: *"El aprendizaje automático requiere un entrenamiento desde cero, que es computacionalmente caro y requiere una gran cantidad de datos para lograr un alto rendimiento. Sin embargo, el aprendizaje por transferencia es un método automático en el que reutilizamos un modelo preentrenado como punto de partida para un modelo en una nueva tarea."*

3.6 Apoyo logístico y alistamiento operativo.

3.6.1 *Mantenimiento predictivo y sostenimiento. Bases logísticas inteligentes.*

La incorporación de la IA en las tareas de mantenimiento del material militar está demostrando ser una herramienta muy valiosa para optimizar la eficacia de la estructura logística y para reducir los costes asociados a la reposición del material y su sostenimiento.

Fundamentalmente, el aprendizaje automático (ML) puede ayudar a predecir fallos en los equipos haciendo uso del denominado mantenimiento preventivo. Este permite a los técnicos de mantenimiento tomar medidas preventivas antes de que se produzca una costosa avería catastrófica que implicaría además una pérdida de operatividad de la unidad. Estas son técnicas que proceden de la industria civil que analizan grandes cantidades de datos, procedentes de una sensorización masiva, para identificar patrones y tendencias que a menudo superan las capacidades humanas, bien por la sensibilidad o por el volumen de datos a analizar con un personal disponible siempre limitado.

Todos los ámbitos están ejecutando proyectos similares en este campo, algunos de los cuales se describen a continuación.

3.6.2 *Mantenimiento predictivo en la Armada*

Según escribe Lamas en la Revista General de Marina [47], *"Tras el establecimiento del CESADAR en 2011 como Centro de Supervisión y Análisis de Datos de la Armada, se han sucedido diversos hitos en la evolución de sus capacidades. Durante los primeros años, la capacidad de análisis de datos en el centro fue muy limitada y se basaba en análisis visual de variables"*. Y en 2017, *"se reafirmó la necesidad de ser capaces de aplicar modelos de IA sobre nuestros datos y adaptar la capacidad de análisis a las nuevas tecnologías y modelos inteligentes. La IA cobraba más importancia y era un objetivo prioritario como capacidad para ser adquirida"*.

La Armada no ha dejado de invertir personal y recursos para avanzar en esta línea. Ya iniciada la segunda década del siglo el sistema SOPRENE está totalmente incorporado a la actividad de buques y arsenales de apoyo. Está constituido por varias herramientas específicas en función del usuario, localización y misión. Actualmente y en formato de demostrador tecnológico, la evolución a MAPRE (Mantenimiento Predictivo) busca la predicción y clasificación de anomalías. Según se refleja en la Figura 3-13, MAPRE, que incorpora técnicas de IA, es entrenado en tierra y ejecutado a bordo.



Figura 3-13 Evolución del mantenimiento predictivo en la Armada. Fuente: RGM.

3.6.3 *Proyecto CESADAR – SOPRENE – ATAVIA – MAPRE.*

Como se ha reflejado en el punto anterior, la Armada comenzó en la primera década del siglo a recoger datos de los muchos equipos sensorizados a bordo de sus buques. El CESADAR comenzó entonces con un proyecto de Data Science, ver Tabla 3-9, que no ha parado de evolucionar desde entonces y que está siendo trasladado a otros ámbitos del MDEF. En la Figura 3-13 se muestran las herramientas que incorpora SOPRENE en 2022 en sus diferentes fases de tratamiento de datos y explotación.

Nombre	CESADAR SOPRENE ATAVIA MAPRE
Año	2012-2024
Agencia/Organismo	MDEF – ARMADA - DGAM
Ámbito MDEF	Armada
Área tecnológica	Data Science – ML - DL
Área de aplicación	Apoyo logístico
Presupuesto	-
Avance	En producción
Resultados	Medibles
URL	https://armada.defensa.gob.es/archivo/rgm/2022/07/rgmjul2022cap08.pdf

Tabla 3-9 Proyecto CESADAR- SOPRENE - ATAVIA - MAPRE

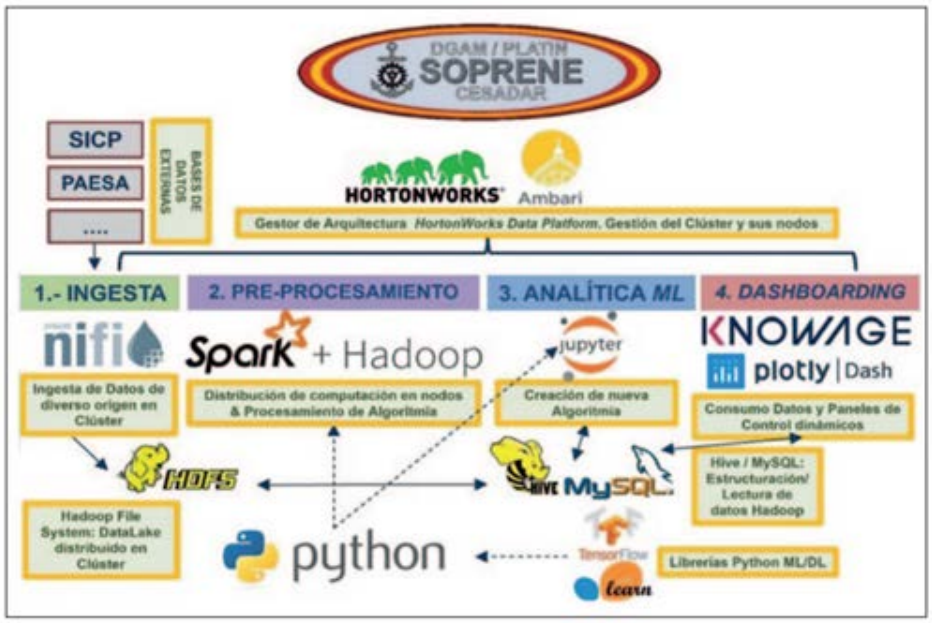


Figura 3-14 Herramientas de SOPRENE (2022).

3.6.4 *Proyecto Gemelo Digital F-110.*

El futuro en la Armada está representado por el Gemelo Digital Avanzado ligado al programa de obtención de las nuevas fragatas de la clase F-110, de hecho este proyecto ha sido presentado como una de las grandes innovaciones de esta serie respecto a su antecesora clase F-100 en servicio desde 2001. Se pretende que el gemelo incorpore herramientas que permitan modelar el comportamiento en un grupo de sistemas críticos incorporando IA que actúe de forma autónoma o asesore a los operadores a tomar decisiones relativas a la gestión de estos sistemas, tiempo hasta el fallo y plazo de subsanación de la avería. Se espera que el primer buque de esta serie entre en servicio antes de que acabe la década.

Nombre	Gemelo Digital F-110
Año	2023
Agencia/Organismo	DGAM- NAVANTIA
Ámbito MDEF	Armada
Área tecnológica	Data Science - ML
Área de aplicación	Apoyo Logístico y Alistamiento Operativo
Presupuesto	-
Avance	Proyecto
Resultados	-
URL	https://armada.defensa.gob.es/archivo/rgm/2020/06/rgmjunio20cap7.pdf

Tabla 3-10 Proyecto gemelo Digital F-110.

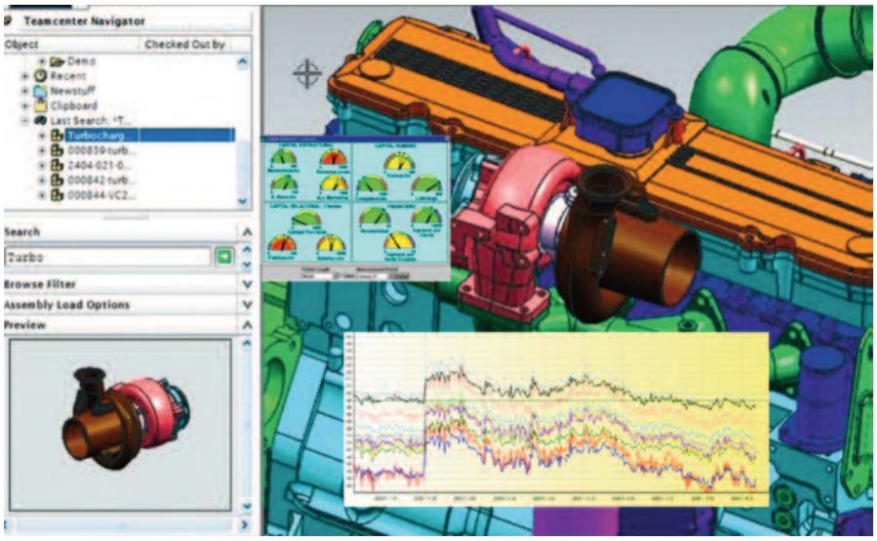


Figura 3-15 Ilustración Proyecto Gemelo Digital F-110. Fuente: NAVANTIA.

3.6.5 *Ejército del Aire y del Espacio. Proyecto BACSI.*

Los proyectos del Ejercito del Aire y del Espacio, están enmarcados en un gran programa denominado BACSI, Base Aérea Conectable Sostenible Inteligente. Con él se pretende dar un paso en su transformación, aprovechando la evolución tecnológica ligada a la Industria 4.0, la IA, y otros avances vinculados a la llamada Cuarta Revolución Industrial, mediante numerosos sub-proyectos de investigación y desarrollo, con el fin de que éste sea implantado en todas las bases aéreas del Ejército del Aire y del Espacio progresivamente. El proyecto obedece a tres objetivos principales: potenciar los recursos y aumentar la productividad y la operatividad de una base aérea, responder al compromiso del MDEF con el medioambiente y conseguir bases más seguras en todos los ámbitos, tanto en la seguridad física, como cibernética y de sus trabajadores.

A continuación se muestran varios proyectos dirigidos a la optimización de procesos de mantenimiento en el Ejército del Aire asociados al proyecto BACSI.

3.6.6 *Proyecto PANGEA.*

PANGEA es un proyecto que emplea algoritmos de IA/ML para la optimización de procesos de mantenimiento de tercer escalón, ver Tabla 3-11 y Figura 3-16. Coordina las entradas, trabajos y materiales de un taller de mantenimiento de aeronaves y pretende conseguir:

- Mejor aprovisionamiento de materiales de repuesto.
- Reducción de tiempos de mantenimiento.
- Mayor disponibilidad de la flota.
- Mejorar la distribución de horas/trabajador.

Nombre	PANGEA
Año	2023
Agencia/Organismo	Ministerio de Defensa
Ámbito MDEF	Ejército del Aire y del Espacio
Área tecnológica	Machine Learning
Área de aplicación	Apoyo Logístico y Alistamiento Operativo
Presupuesto	1.440.000 €
Avance	-
Resultados	En aplicación.
URL	-

Tabla 3-11 proyecto PANGEA.

Trabaja sobre diferentes algoritmos:

- Predicción. Adelantando la necesidad de piezas de repuesto.
- Programación: Planificación macro de las tareas de mantenimiento y optimización de los trabajos de taller/hangar.



Figura 3-16 Proyecto PANGEA.

3.6.7 *Proyecto IMAGIA. Análisis de datos de Rayos-X y ultrasonidos.*

Este proyecto tiene como objetivo el análisis de "Ensayos No destructivos" (END), empleado desde hace años para inspeccionar aeronaves, Tabla 3-13, Figura 3-17. Mediante ML supervisado, se entrena un algoritmo con información existente de las continuas revisiones de los aviones. IMAGIA, procesa diferentes tipos de información; de ultrasonidos (Pulso-Echo y Transmisión), radiografías y termografías. Al aprovechar la IA, los especialistas en END pueden tomar decisiones mejor informadas, mejorar la eficiencia y garantizar materiales y estructuras más seguras y fiables.

Nombre	IMAGIA
Año	2021
Agencia/Organismo	Ministerio de Defensa
Ámbito MDEF	Ejército del Aire y del Espacio
Área tecnológica	Robótica - Machine Learning
Área de aplicación	Apoyo Logístico y Alistamiento Operativo
Presupuesto	-
Avance	-
Resultados	En aplicación.
URL	https://ejercitodelaire.defensa.gob.es

Tabla 3-12 Proyecto IMAGIA (END).



Figura 3-17 Proyecto IMAGIA. Análisis de Rayos X.

3.6.8 *Mantenimiento predictivo para EUROFIGHTER.*

Este proyecto es el resultado de la colaboración entre el Ejército del Aire y del Espacio con la empresa Indra para desarrollar en un nuevo sistema de IA que dote al Caza de Combate Eurofighter de *"capacidad para autodiagnosticar el estado de cerca de una veintena de sistemas críticos de aviónica y reforzar con ello la seguridad en vuelo y la superioridad del que es uno de los aviones de combate más sofisticados del planeta"* [48].

Este sistema, que se desarrolla dentro del área funcional de Sostenimiento 4.0 del Proyecto BACSI, permitirá detectar de forma anticipada un posible fallo de los elementos críticos y comprobará que el avión se encuentra en perfecto estado antes de cada despegue. Se trata de un mantenimiento inteligente que no solo eleva la seguridad, sino que también ahorra costes y extiende la vida útil de cada plataforma, asegurando la máxima disponibilidad de la flota.

Nombre	Mantenimiento Predictivo Eurofighter
Año	2022
Agencia/Organismo	Ministerio de Defensa
Ámbito MDEF	Ejército del Aire y del Espacio
Área tecnológica	Machine Learning
Área de aplicación	Apoyo Logístico y Alistamiento Operativo
Presupuesto	-
Avance	-
Resultados	En aplicación.
URL	https://ejercitodelaire.defensa.gob.es

Tabla 3-13 Proyecto de mantenimiento predictivo para el Eurofighter.

3.6.9 *Proyecto BLET del Ejército de Tierra.*

En línea con los proyectos BACSI del Ejército del Aire y del Espacio y el Arsenal Inteligente de la Armada, el Ejército de Tierra ha lanzado el Proyecto BLET, Base Logística del Ejército de Tierra. Con este proyecto el Ministerio ha lanzado recientemente diferentes proyectos que buscan convertir la futura base, ubicada en Córdoba en un motor tecnológico, de creación de empleo regional y de I+D+i nacional, a la vez que persigue la optimización de los procesos logísticos y de mantenimiento del Ejército apoyándose en las nuevas tecnologías digitales dando un gran peso a la IA. La intención es incorporar IA tanto a las tareas de mantenimiento como a las de gestión e la propia base así como a su seguridad física y cibernética. La BLET representa un ambicioso proyecto a largo plazo del Ejército de tierra con un gran apoyo institucional y un presupuesto estimado superior a los 200 millones de €.



Figura 3-18 Proyecto BLET.

3.6.10 *Proyecto SILPRE*

Como ya se mencionó al tratar los proyectos de la Armada, el Ejército de Tierra en su búsqueda de un modelo de mantenimiento predictivo de sus vehículos se ha fijado en MAPRE y ha puesto en marcha el desarrollo del Sistema de logística predictiva (SILPRE).

Según se recoge en Infodefensa [49],*"Navantia liderará el diseño del nuevo sistema logístico del Ejército de Tierra"*. Con SILPRE, el Ejército da continuidad a su proyecto MANPREDIC y apuesta decididamente por el mantenimiento predictivo para sus vehículos logísticos y también en sus sistemas de armas. Además de Navantia, se ha incorporado al proyecto la Universidad de Córdoba.

Nombre	SILPRE
Año	2023
Agencia/Organismo	ET – Navantia – Universidad Córdoba DGAM
Ámbito MDEF	Ejército de Tierra
Área tecnológica	Data Science – ML - DL
Área de aplicación	Apoyo logístico y Alistamiento Operativo
Presupuesto	3.900.000 €
Avance	En ejecución
Resultados	-
URL	Ejército de tierra (defensa.gob.es)

Tabla 3-14 Proyecto SILPRE.

3.7 Conocimiento y vigilancia del entorno.

En los ámbitos terrestre, marítimo, aeroespacial, ciberespacial y cognitivo. Análisis masivo de datos, información y desinformación. En esta aplicabilidad de la IA se echa de menos un gran proyecto de fusión de información, bien para un ámbito concreto, Ejército de Tierra, Armada, Ejercito del Aire y del Espacio o incluso dentro de la estructura conjunta del Estado Mayor de la Defensa. Tal vez, en este campo de aplicación podrían haberse ubicado los proyectos CUSTODES, SEDA y la herramienta PALANTIR, pues su objetivo es recopilar información de diferentes fuentes y sensores y fusionarla sobre una misma plataforma.

Como ejemplo de este gran proyecto podríamos fijarnos en NELSON de la Royal Navy (UK) del que se muestran unas ideas.

3.7.1 *Proyecto NELSON (UK).*

La Royal Navy ha puesto el nombre de Nelson, brillante Almirante inglés caído en batalla contra el reino de España, al programa de transformación digital de su fuerza naval. Es un esfuerzo de colaboración en el que participan la Royal Navy y un equipo de expertos de "*BAE Systems Applied Intelligence*" para garantizar que su flota pueda hacer un uso más eficiente de sus datos en el mar y en tierra. El equipo de NELSON ha desarrollado la plataforma de datos "*Navy Mind*", creada con un diseño centrado en el usuario, que permite a los operadores proponer mejoras en su entorno de trabajo. NELSON incorpora desarrollos de IA y ciencia de datos, así como una gran capacidad para el desarrollo de software que permite desarrollar rápidamente las aplicaciones demandadas por los usuarios. Como resultado, los operadores de la Armada pueden trabajar con mayor rapidez y eficacia. No se tiene

conocimiento del avance del proyecto pero si de su ambición. El alcance del proyecto queda reflejado en un vídeo corporativo de carácter futurista[4] y otro comercial de BAE[5]. En una presentación abierta a miembros de la OTAN mostraban las premisas guía del proyecto que muestra la Figura 3-20.

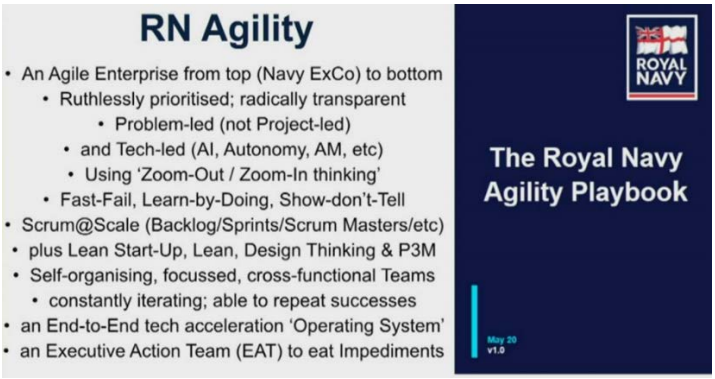


Figura 3-19 Proyecto NELSON (UK).

3.8 Ciberdefensa.

3.8.1 *Identificación y actuación frente a ciberamenazas.*

El campo de la ciberdefensa es sin duda uno de los usos principales de la IA. Por motivos de clasificación los casos de uso asociados a esta aplicación no pueden ser detallados. Por este motivo se indicarán únicamente las aplicabilidades potenciales. En las V Jornadas de Ciberdefensa: ESPDEF-CERT de diciembre 2023, un representante de la Jefatura de Apoyo Técnico a Operaciones del Mando Conjunto del Ciberespacio expuso su visión sobre los "puntos fuertes de la IA en Ciberdefensa". Según el punto de vista de I.M.U. son los siguientes: Detección de patrones, clasificación, automatización y procesamiento del lenguaje como refleja la diapositiva de la Figura 3-21.



Figura 3-20 IA empleada en ciberdefensa: Fuente: MCCE.

El volumen de información en el ciberespacio, y la velocidad de las transacciones, hacen imposible acometer estas tareas con capacidades humanas claramente desbordadas. La IA es a la vez amenaza, riesgo y la única solución viable.

[4] https://vimeo.com/356840946
[5] https://www.youtube.com/watch?v=LokA1-KxDR0

A continuación se hace referencia a algunas aplicaciones de IA en beneficio de tareas de ciberdefensa sin hacer mención explícita a proyectos concretos en desarrollo por motivos de confidencialidad de la información.

3.8.2 *Detección y mitigación de vulnerabilidades en los sistemas militares.*

La detección y mitigación de vulnerabilidades en los sistemas son tareas que pueden resultar complicadas y que requieren la inversión de mucho tiempo para los administradores de seguridad de los sistemas. La automatización es imprescindible y, para sistemas y redes complejas, la aplicación de soluciones apoyadas en IA se vislumbra como la única forma de poder acometer estas tareas de forma eficiente en un futuro cercano. La IA aplicada a este aspecto puede proporcionar un conocimiento de la situación de seguridad del sistema dinámico y en tiempo real, apoyando la evaluación de las medidas de mitigación, reduciendo los tiempos (que son tiempos de exposición a la amenaza), y facilitando su despliegue.

Así, el aprendizaje automático puede ayudar a acabar con ciertas vulnerabilidades, especialmente las relacionadas con las amenazas de tipo día cero. Los "*exploits*" (scripts) de día cero no se pueden detectar por medios convencionales, como antimalware o dispositivos de detección y prevención de intrusiones, porque aún no se han creado las firmas. Esto significa que la prevención debe lograrse monitorizando el tráfico y las actividades de los usuarios, con base en el comportamiento de referencia para detectar anomalías, para lo que las técnicas de ML son las más apropiadas.

3.8.3 *Threat Hunting, caza de amenazas.*

Los servicios de caza de amenazas tienen el objetivo de explorar a través de todas las redes y comprobar si dentro de algún elemento existe algún agente malicioso que suponga un riesgo o ciberamenza que pueda causar problemas dentro de una red y su sistema de seguridad. Para realizar una campaña de "*threat hunting*" se necesita definir una hipótesis que establezca los posibles ataques o agentes maliciosos que pueden existir. Una hipótesis puede incluir las tácticas del atacante, las técnicas y los procedimientos que puede utilizar.

La IA puede dar apoyo a la generación de hipótesis en aspectos como los siguientes:

- Detección de anomalías en logs: Mediante ML no supervisado, se puede llevar a cabo un filtrado que reduzca los logs analizados a aquellos considerados más amenazantes.
- Detección de elementos que se están comportando de manera anómala: Mediante algoritmos de ML se puede identificar, por ejemplo, una máquina que se está comportando de manera diferente a como suele hacerlo.
- Detección de elementos que se están comportando de manera similar a campañas conocidas: Mediante modelos de clasificación basados en aprendizaje supervisado, como redes neuronales, se puede identificar comportamientos similares a campañas maliciosas conocidas.

3.8.4 *Herramientas de visualización y trazado de un ciberataque.*

Mediante técnicas de ML sobre datos existentes, se puede determinar probabilísticamente la evolución de un ciberataque, pudiendo predecir los siguientes pasos que va a dar una vez es detectado. El objetivo es determinar los parámetros desconocidos (u ocultos) a partir de los parámetros observables.

3.8.5 *Herramientas de simulación de APT (Advanced Persistent Threats).*

Las herramientas que simulan APTs, son utilizadas para la formación y adiestramiento del personal en ciberdefensa, con el objeto de ejecutar cibermaniobras o ciberejercicios, de modo que los usuarios

estudiantes adquieran competencias en materia de ciberseguridad que luego sean aplicables en escenarios reales. Con la incorporación de técnicas de IA con aprendizaje adaptativo, los escenarios pueden adaptarse de forma específica a cada estudiante y enriquecer el entrenamiento.

3.8.6 *Detección de malware.*

Este es, probablemente, el campo al que más se está enfocando la investigación de IA en ciberseguridad, junto con el de detección de ataques, con el que está íntimamente relacionado. La detección de nuevo malware y virus mediante el reconocimiento de patrones anómalos en el funcionamiento de las aplicaciones y el aislamiento de los sistemas antes de ser infectados ha sido objeto prioritario de atención desde los primeros tiempos de la ciberseguridad.

Este es el empleo que por ejemplo señala Holgado [50] en un artículo de 20bits. La noticia señala que la división de Google en España ha lanzado un sistema para analizar malware a través de IA, *"se trata de VirusTotal Code Insight, una herramienta basada en inteligencia artificial enfocada para el análisis de malware. Para llevar a cabo su tarea, la tecnología es capaz de analizar código y resumir fragmentos de código en lenguaje natural"*.

Aceptando la imposibilidad de que los sistemas detectores de malware alcancen algún día la condición de infalibles, resultan absolutamente imprescindibles como elemento esencial de la primera línea de protección perimetral y su perfeccionamiento de la mano de la IA se presenta como la única manera de mejorar sustancialmente las herramientas actualmente disponibles para detectar malware.

3.8.7 *Detección y bloqueo automático de "phishing", "spam", intrusiones en la red o actuaciones fraudulentas.*

Los sistemas de ML analizan un número considerable de correos de phishing, de modo que pueden encontrar, en un nuevo correo, señales lo suficientemente significativas para tacharlo de "sospechoso". La IA puede también analizar los correos para determinar su nivel de amenaza, comparando con el modelo de comportamiento habitual que haya creado para determinar si es "normal" o no. La IA también puede utilizarse en los sistemas de detección de intrusiones, de modo que sean capaces de rechazar, aceptar o redirigir la información de un servidor externo dependiendo de si esta proviene de un servidor infectado, o un servidor limpio.

3.8.8 *Desarrollo de software seguro.*

La IA puede ayudar al propio desarrollo del software. Con la ayuda del ML, el propio software define qué es lo que va a hacer y de qué forma lo hará. Esto permite que los operadores del software puedan delegar en él la responsabilidad de generar nuevas estrategias para procesar datos, ordenarlos, evaluarlos y modificarlos. Se basa en que el procesamiento de los datos que maneja puede variar, y tendrá la capacidad de resolver esa variabilidad de forma inteligente y automatizada.

Además, la IA puede ayudar en la necesaria fase de pruebas, propiciando entornos lo más realistas posibles. Entre la batería de pruebas, resultan especialmente importantes los análisis de código en busca de vulnerabilidades, para lo cual existen ya diferentes herramientas que lo hacen de forma automática, pero que la IA puede mejorar.

3.8.9 *Identificación y autenticación de usuarios.*

La IA puede mejorar la seguridad en el proceso de autenticación y acceso de usuarios a los sistemas. Un ejemplo es el reconocimiento facial. El sistema elabora un modelo avanzado de la cara del individuo para la identificación de correlaciones y patrones claves. Además, tiene la capacidad para adaptarse a los cambios de la cara, como el maquillaje o el crecimiento de vello facial. Es más, la IA puede ponderar

dinámicamente los perfiles de usuario, la criticidad de la aplicación a la que acceden, el emplazamiento de los puntos de acceso a la red, o el nivel de amenaza del momento. Los algoritmos deciden en cada caso solicitar distintos factores de autenticación, analizar el comportamiento del usuario o las características del dispositivo y modificar, si fuera necesario, sus privilegios en el sistema sin intervención humana.

3.9 Apoyo a la toma de decisiones

Incluye la simulación y visualización de escenarios presentes y futuros para apoyar la adopción de decisiones en todos los niveles de conducción de las operaciones militares, estratégica, operacional y táctica.

El tercer puesto del concurso de ensayos de 2023 del *"National Defense University Press"* fue ganado por un ensayo titulado: *"Alexa, Write My OPORD: Promise and Pitfalls of Machine Learning for Commanders in Combat"* escrito por el LtCol Jeffrey Wong [51]. En el plantea como la capacidad de la IA para analizar grandes volúmenes de datos y resolver problemas complejos podría ayudar a la difícil misión del planeamiento y conducción de operaciones. Wong describe un escenario operativo donde un Oficial, sin conocimientos informáticos, hace uso de herramientas de ML para *"apoyar la planificación y ejecución de la operación"*, de lo que deduce que "We´re screwed" que coloquialmente se traduce como "estamos apañados".

Tras presentar varias reflexiones el ensayo concluye que los mandos y sus estados mayores deben comprender que se trata de una herramienta capaz que, si se utiliza con sensatez, mejorará significativamente la capacidad de las fuerzas conjuntas para absorber datos de fuentes dispersas y dar sentido a esa información que proporcionan haciendo uso de la IA, ML fundamentalmente. Afirma que el uso de las capacidades de ML debería formar parte de la fase de *"wargaming"* de un equipo de planeamiento en el que una persona designada tendría la misión de servir de interfaz humana con una herramienta de apoyo a la toma de decisiones como MaL, que es el curioso nombre que Wong le da al desarrollo de LLM de apoyo al planeamiento.

Esta idea de elemento de ayuda al planeamiento operativo está desarrollada en el trabajo de Garat [52] titulado "La Inteligencia Artificial como causa de transformación del Planeamiento Operativo" donde analiza cómo las diferentes tecnologías de IA, *"…pueden contribuir al planeamiento de operaciones militares en el nivel operacional, tomando como referencia el proceso de planeamiento de la OTAN, y centrando el estudio en las fases relacionadas con la generación de conocimiento y toma de decisiones"*.

Dentro de este campo parece claro que cabría emplear técnica de IA, al menos para la fase de "wargaming" del planeamiento. Esta fase según describe Dapena [53], *"Un juego de guerra es un modelo o simulación de guerra que usa reglas, datos y procedimientos, sin emplear fuerzas militares reales, y en el que el desarrollo de los acontecimientos afecta y es afectado por las decisiones tomadas durante el curso de esos acontecimientos por los jugadores, que representan bandos opuesto."* Esta actividad recogida como una de las más importantes de la COPD *"Comprehensive Operations Planning Directive"*, documento guía del planeamiento en la OTAN, se realiza actualmente con medios humanos. Dos o más equipos, que representan a las partes en contienda, ejecutan las posibles COA (Course Of Action) que se plantean al Comandante para su decisión. La aplicabilidad de desarrollos de IA como los que planteaba Wong en su ensayo podrían agilizar y mejorar el planeamiento, en la tarea del wargaming, en la de conocimiento del entorno y probablemente también en el resto, inicialmente a modo de recomendación y análisis.

No se ha encontrado documentación sobre proyectos nacionales que exploten esta vía de aplicación de la IA en apoyo al planeamiento militar más allá de las relacionadas con el conocimiento y vigilancia del entorno y el alistamiento operativo.

3.10 Análisis geoespacial, meteorológico y oceanográfico.

La IA se ha mostrado muy útil para analizar grandes cantidades de datos meteorológicos históricos y en tiempo real para identificar patrones climáticos y reconocer eventos extremos con gran precisión. Esta capacidad tiene un evidente empleo militar donde el factor meteorológico es siempre tenido en cuenta en el planeamiento y desarrollo de las operaciones militares.

Se considera que el uso habitual será la contratación a terceros de servicios de predicción meteorológica específicos para las fuerzas desplegadas pues ya se ofrecen con cobertura global. No obstante se han realizado en el MDEF algún proyecto específico como el descrito a continuación.

3.10.1 *Proyecto SIAAMETOC-OM.*

El Sistema Integrado de Apoyo Automático Meteo-Oceanográfico para Operaciones Marítimas (SIAAMETOC-OM), ver Tabla 3-15, tenía como objetivo la identificación, análisis y explotación de datos meteo- oceanográficos disponibles actualmente a nivel mundial, y su adaptación e interpretación automática para el apoyo a misiones y operaciones marítimas del MDEF. Este proyecto incluía la planificación temprana y segura de maniobras de desembarco anfibio donde la meteorología juega un papel determinante.

Nombre	SIAAMETOC-OM
Año	2019-2021
Agencia/Organismo	Programa Coincidente – IHM – Universidad de Cantabria.
Ámbito MDEF	DGAM
Área tecnológica	Data Science – ML - DL
Área de aplicación	Análisis meteorológico y oceanográfico
Presupuesto	3.830.000 €
Avance	En ejecución
Resultados	Aceptados. Continuidad del proyecto.
URL	https://www.tecnologiaeinnovacion.defensa.gob.

Tabla 3-15 Proyecto SIAAMETOC_OM.

3.11 Gestión de la Información, de la infraestructura y los servicios CIS/TIC.

La estrategia marca que en este apartado se incluyen la asignación autónoma de recursos a servicios CIS/TIC en función de su carga de trabajo y previsión de actuaciones de mantenimiento, reposición y ampliación de los componentes de la infraestructura.

Más allá del uso de software inteligente para la gestión de los recursos de hardware disponibles y la propia red, no se han encontrado proyectos de IA para la gestión de la Infraestructura TIC.

3.12 Gestión del talento y formación.

Se incluyen los Sistemas de gestión del talento, formación y apoyo a las actividades de enseñanza, instrucción y adiestramiento.

3.12.1 *Proyecto GNOSS.*

Este programa pretende ampliar y modernizar el Campus Virtual Corporativo de la Defensa (CVCDEF) existente para dotarlo de nuevas capacidades, ver Tabla 3-16. Este campus virtual está desplegado la nube pública y es accesible vía web para los alumnos del MDEF, principalmente de Tropa y Marinería. La plataforma integra un sistema de gestión de aprendizaje (LMS). Se espera que este embrión de plataforma, ya en producción, continúe desarrollándose en los próximos años y que en un futuro cercano cubra gran parte de las necesidades de formación de los miembros de la Fuerzas Armadas.

Nombre	GNOSS
Año	2022
Agencia / Organismo	DIGEREM – Universidad Autónoma de Madrid
Ámbito MDEF	SUBDEF
Área tecnológica	Data Science – ML - DL
Área de aplicación	Enseñanza y Formación
Presupuesto	2.000.000 €
Avance	En producción
Resultados	Aceptados. Continuidad del proyecto.
URL	https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-5824

Tabla 3-16 Proyecto GNOSS.

4 CONCLUSIONES Y LÍNEAS FUTURAS

4.1 Conclusiones.

4.1.1 *Sobre la aplicabilidad de la IA.*

La IA no es una tecnología más, su relevancia geopolítica hace que vaya apareciendo en la agenda de todos los estados y organizaciones internacionales de seguridad y defensa. Especialmente en el campo de lo militar está llamada a ser la tecnología que ofrezca mayor desarrollo tanto para hacer uso de ella a favor, como para negarle su uso al adversario.

La guerra de Ucrania ha demostrado que las aplicaciones de IA son útiles en situaciones de combate abierto. Estas aplicaciones de vertiginoso desarrollo han contribuido a equilibrar un conflicto inicialmente muy desigual entre los contendientes. Las aplicaciones duales de la tecnología de IA han permitido a los contendientes tener un mayor y más profundo conocimiento del entorno utilizando ML para el reconocimiento de fuerzas enemigas y también para otras aplicaciones en la retaguardia como el triage o la búsqueda de infiltrados. Estos usos improvisados de la IA y otros todavía en desarrollo pasarán pronto a formar parte del modus operandi de las operaciones militares.

El Ministerio de Defensa de España mantiene visibilidad sobre iniciativas relacionadas con la IA en la Administración General del Estado, de donde obtiene aprendizaje y recursos. También permanece atento a las iniciativas de las organizaciones de seguridad y defensa OTAN, y de la UE. España participa activamente en los foros OTAN para buscar la coherencia y la cooperación con los aliados en esta materia con beneficio mutuo. Cabe esperar que el DARB, organismo creado ad-hoc para avanzar en la adopción de IA en la Alianza, consiga sus objetivos de estandarización y puesta a disposición de los aliados de mecanismos que aseguren el uso responsable de la AI de acuerdo a los valores establecidos.

Los posibles conflictos éticos que acompañan a esta tecnología no deben ser, en el estado de madurez que nos encontramos, la principal preocupación para su empleo militar. Todavía estamos lejos de disponer de SALAS (Sistemas de Armas Letales Autónomos), de momento, lo recomendable es seguir avanzando en el conocimiento de la tecnología y participar en los foros donde se desarrolla la normativa. En la gran mayoría de aplicaciones que se han estudiado y las presumibles en los próximos años, la principal preocupación será asegurar, eso sí, que las aplicaciones respetan los derechos individuales de las personas, en cuanto a privacidad, imagen, honorabilidad y en general todos los relacionados con la protección de datos personales.

4.1.2 *Sobre la Estrategia de IA del MDEF.*

Estamos a tiempo de subirnos al tren de la IA, la Estrategia de IA del MDEF es una base normativa útil e indispensable para iniciar un desarrollo coordinado de aplicaciones de IA en el Departamento y no caer en una dispersión de recursos, siempre escasos, y conocimiento.

Los Ámbitos del MDEF, coordinados desde la Secretaría de Estado por la DG CESTIC y por la DGAM, están diseñando e implantando soluciones concretas que dan respuesta a necesidades del MDEF empleando IA de acuerdo a los principios de uso responsable recogidos en la Estrategia. Claramente esto es solo el principio, llegar a tener una red de centros de excelencia y cubrir todos los casos de uso señalados y los nuevos que surjan, ha de ser una ambición del MDEF que además contribuya al crecimiento de la industria nacional del sector tecnológico.

La DG CESTIC está preparando la I3D (Infraestructura Integral de Información para la Defensa) para poder soportar la demanda que traerán consigo las aplicaciones de IA. Al mismo tiempo, todo el MDEF avanza en la necesaria gobernanza del dato, cuestión en la que está poniendo especial énfasis el CIO del MDEF, sin la cual no se podrá aprovechar toda la potencialidad de la IA. No tendremos datos para entrenar los modelos.

El MDEF tiene una capacidad de innovación limitada, en el campo de las TIC y en todos los demás que cada vez tienen más componente digital. Es totalmente necesario apoyarse en el tejido industrial y en la Universidad para emprender proyectos de IA con una cierta viabilidad. Experiencias como la del programa Coincidente muestran el camino, el uso dual de la IA es evidente.

4.1.3 *Sobre los casos de uso de IA.*

En los últimos años se ha escrito mucho sobre IA y su aplicabilidad militar pero la gran mayoría de las veces en genérico. Se considera recomendable comenzar a tratar cada una de las técnicas por separado pues existen diferentes técnicas que se van ramificando conforme avanza la ciencia. Estas diferentes técnicas exigen un tratamiento diferenciado y un conocimiento particular. El MDEF necesitará expertos en Machine Learning, en Redes Neuronales o en Visión Artificial y es imposible dominar todos los campos.

Entre las once categorías de casos de uso señaladas en la Estrategia se han observado diferentes grados de desarrollo de los proyectos asociados a cada una de ellas. En la siguiente Tabla se refleja, a juicio del autor, la madurez alcanzada y el potencial de empleo de la IA que se estima en cada categoría en función del conocimiento de iniciativas en otros estados y organizaciones.

	Categoría caso de uso	**Madurez**	**Potencial**
1	Movilidad militar	Inicial	Medio
2	Inteligencia	Medio	Alto
3	Guerra electrónica	Inicial	Alto
4	Autonomía en sistemas no tripulados	Inicial	Alto
5	Apoyo logístico y alistamiento operativo	Avanzado	Alto
6	Conocimiento y vigilancia del entorno	Inicial	Alto
7	Ciberdefensa	Avanzado	Muy alto
8	Apoyo a la toma de decisiones	Inicial	Muy alto
9	Análisis geoespacial, meteorológico y oceanográfico	Medio	Medio
10	Gestión de la información y CIS/TIC	Inicial	Alto
11	Talento y formación	Inicial	Medio

Tabla 4-1 Valoración categorías IA.

Los resultados obtenidos en las aplicaciones de ML y DL para apoyar la función logística y el alistamiento operativo deben servir de guía para el resto de aplicaciones. Estos desarrollos han demostrado que aunque el camino es largo, los resultados obtenidos producen un aumento significativo de las capacidades y un mejor empleo de los recursos disponibles.

En el caso de las herramientas de ciberdefensa, el empleo de la IA podríamos decir que es irrenunciable en un entorno dónde las capacidades humanas se ven claramente superadas por la velocidad de los acontecimientos y por el volumen de información a analizar.

4.2 Líneas futuras.

Se recomienda que el MDEF persevere en el desarrollo de la Estrategia iniciada en 2023, fortaleciendo sus infraestructuras y promoviendo el gobierno del dato en todo el departamento para permitir el entrenamiento de los modelos de IA.

El MDEF debe adquirir conocimiento experto en IA y fomentar la creación, prevista en el apartado decimoquinto de la Estrategia del MDEF, de la Red de Centros de Referencia para el seguimiento técnico de proyectos de IA, la compartición de resultados de estos proyectos y el establecimiento de entornos de experimentación.

Se considera urgente comenzar a desarrollar herramientas de apoyo a la toma de decisión, especialmente en el planeamiento operativo donde se estima un altísimo potencial.

El proyecto de Gemelo Digital para la F-110 merece ser seguido con atención por su potencial. Nuestro primer Gemelo Digital representa un ambicioso proyecto extrapolable a otras plataformas terrestres o aéreas.

Los proyectos piloto y demostradores tecnológicos que se han considerado viables en su fase inicial, es muy conveniente convertirlos en proyectos o programas con financiación propia o en caso contrario no se conseguirá dar el salto a producción que justifique el esfuerzo investigador realizado.

La colaboración con Universidad y empresas del sector es imprescindible para alcanzar los objetivos planteados en materia de IA por lo que deberán mantenerse y reforzarse los acuerdos y convenios asumidos por el MDEF para impulsar la aplicación de esta tecnología.

5. BIBLIOGRAFÍA

[1] DGAM, «Estrategia de tecnologia e innovación para la Defensa. ETID 2020.,» 2020. [I línea]. Available: https://publicaciones.defensa.gob.es/estrategia-de-tecnologia-innovacion-para-la-defensa-etid-2020-libros-pdf.html.

[2] L. Gonzalo, «El papel dual de la inteligencia artificial en una era de conflictos híbridos 2023. [En línea]. Available: https://www.acami.es/wp-content/uploads/2023/12/El-pape dual-de-la-inteligencia-artificial-web.pdf.

[3] NATO, «Science & Technology Trends,» 2023. [En línea]. Availabl https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf.

[4] Ministerio de Defensa, «Política de los Sistemas y Tecnologías de la Información y l Comunicaciones del Ministerio de Defensa,» 3 diciembre 2015. [En línea]. Availabl https://publicaciones.defensa.gob.es/politica-de-los-sistemas-y-tecnologias-de-la-informacion-y-las-comunicaciones-del-ministerio-de-defensa.html.

[5] Ministerio de Defensa, «Estrategia de desarrollo, implantación y uso de la Inteligenc Artificial en el MDEF,» 6 julio 2023. [En línea].

[6] Departamento de Seguridad Nacional, «Estrategia de Seguridad Nacional 2021,» 202 [En línea]. Available: https://www.dsn.gob.es/es/documento/estrategia-segurida nacional-2021.

[7] Estado Mayor de la Defensa, «Concepto de empleo de las Fuerzas Armadas 2021,» 202 [En línea]. Available: https://emad.defensa.gob.es/Galerias/emad/files/CEFAS_2021.pd

[8] C. Alcántara, «Fuencisla Clemares (Google): "La IA va a ser comparable al descubrimien del fuego",» 30 10 2019. [En línea]. Available: https://murciaplaza.com/la-inteligenci artificial-va-a-ser-comparable-al-descubrimiento-del-fuego.

[9] NATO, «NATO´s Artificial Intelligence Strategy,» 2019. [En línea]. Availabl https://www.nato.int/cps/en/natohq/official_texts_187617.htm.

[10] V. Caride, «Reflexiones sobre el nuevo entorno operacional multidominio,» *Revis Ejército*, nº 987, 2023.

[11] Centro Conjunto de Desarrollo de Conceptos. CESEDEN, «Usos militares de inteligencia artificial, la automatización y la robótica (IAA&R),» 2020. [En línea Available: https://emad.defensa.gob.es/Galerias/CCDC/files/USOS_MILITARES_DE_LA_INTEI GENCIA_ARTIFICIALx_LA_AUTOMATIZACION_Y_LA_ROBOTICA_xIAAxRx. _VV.AA.pdf.

[12] El País, «Fedor, el primer robot humanoide ruso, ya está en el espacio,» 22 08 2019. [I línea].Available:https://elpais.com/tecnologia/2019/08/22/actualidad/1566469024_9557 0.html.

[13] D. R. M. y. G. L. Serrano, «Soberanía tecnológica para la defensa y la seguridad de España en la ue: entre lo deseable y lo posible,» *Economía Industrial,* nº 427, 2023.

[14] S. Blank, «TEACHING TECHNOLOGY, INNOVATION, AND MODERN WAR AT STANFORD, PART 5: AUTONOMY AND DEFENSE IN THE TWENTY-FIRST CENTURY,» 2020. [En línea]. Available: https://mwi.westpoint.edu/teaching-technology-innovation-and-modern-war-at-stanford-part-5-autonomy-and-defense-in-the-twenty-first-century/.

[15] Defensa Sciencce Board, «Summer Study on Autonomy.,» 2016. [En línea]. Available: https://www.hsdl.org/?view&did=794641.

[16] J. M. M. martínez, «El viaje inaplazable,» *Revista española de Defensa,* Enero 2022.

[17] J. m. M. y. F. Cuartero, «Gasolina para el viaje inaplazble,» *Revista Española de Defensa.,* Abril 2022.

[18] J. m. m. Martínez, «La Inteligencia del vIAje inaplazable,» *Revista Española de Defensa,* Noviembre 2022.

[19] World Economic Forum, «weforum.org,» 15 11 2016. [En línea]. Available: https://www.weforum.org/agenda/2016/11/the-four-types-of-ai-what-you-need-to-know/.

[20] S. R. &. P. Norving, Artificial Intelligence: A Modern Approach., 2021.

[21] Ministerio de Asuntos Económicos y Transformación Digital., *Estrategia Nacional de Inteligencia Artificial (ENIA),* 2020.

[22] Gobierno de España, *España digital 2026,* 2022.

[23] NATO Science & Technology Organizatión, Science & Technology Trends, 2020.

[24] Unión Europea, *Libro Blanco sobre la Inteligencia Artificial,* 2020.

[25] L. M. y. A. Pedreño, "Europa frente a EEUU y China – Prevenir el declive en la era de la Inteligencia Artificial".

[26] US Department of Defense, Summary of the 2018 Department of Defense Artificial intelligence Strategy. Harnessing AI to Advance Our Security and Prosperity, 2018.

[27] US Department of Defense, Data, Analytics, and Artificial Intelligence Adoption Strategy. Accelerating Decision Advantage, 2023.

[28] UK Ministry of Defence, Defence Artificial Intelligence Strategy, 2022.

[29] Australian Strategic Policy Institute. ASPI., «ASPI's Critical Technology Tracker. The global race for future power,» 2023.

[30] República Popular China, *China's 'New Generation Artificial Intelligence Development Plan,* 2017.

[31] E. fojón, «Ucrania: la tecnología en la guerra,» *ieee.es,* 1 Diciembre 2022.

[32] O. Kardoudi, «La inteligencia artificial ucraniana que decidirá qué soldados se salvarán primero.,» *El Confidencial,* 2023.

[33] R. Alonso., «El arma tecnológica de Ucrania: así es la polémica Inteligencia Artificial capaz de reconocer soldados rusos.,» *ABC Tecnología,* 2022.

[34] E. O. y. J. M. Corchado, «Inteligencia artificial: aplicaciones a la Defensa,» *ieee.es,* 2022.

[35] Defence Science and Technology Laboratory, The Dstl biscuit Book. Artifcicial intelligence, data Science and (mostly) Machine learnig, 2019, p. 6.

[36] N. Villalba, «Puede ser el fin de la raza humana": la predicción de Stephen Hawking sobre la Inteligencia Artificial que se está cumpliendo,» *La Razón,* 02 mayo 2023.

[37] P. Quintás, «La Aesia sigue adelante en A Coruña: Inés Rey y Nadia Calviño avanzan en su hoja de ruta,» *El Español,* 19 octubre 2023.

[38] Ministerio de la Presidencia, relaciones con las Cortes y Memoria Democrática., *Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto,* 2023.

[39] D. Parsons, «Army Enlists IBM's Watson To Streamline Logistics, Vehicle Maintenance.,» 2017.

[40] J. V. Serrano, «Proyecto ARCO: aplicacion robótica de un convoy operativo,» *Boletín de observación tecnológica DGAM - PLATIN,* vol. 2º trimestre, nº 73, pp. 18-23, 2022.

[41] Estado Mayor de la Defensa., PDC-01 (A) DOCTRINA PARA EL EMPLEO DE LAS FAS, 2018.

[42] E. Santos, «Hablar con un japonés y escucharlo en español: las máquinas ya ganan terreno en la interpretación de idiomas,» *El País,* 2023.

[43] PORTALTIC, «Hablar con un japonés y escucharlo en español: las máquinas ya ganan terreno en la interpretación de idiomas,» 2022.

[44] C. Marcos, «SITEP,» 2023. [En línea]. Available: https://sitep.com/udrume-presentacion-de-aeronaves-y-servicios-dron-para-la-ume/. [Último acceso: 11 1 2024].

[45] A. Biurrun, «larazon.es,» 15 02 2023. [En línea]. Available: https://www.larazon.es/tecnologia/pilota-avion-combate-f16d-primera-vez_2023021563ebf9a62f84b400018a9a35.html.

[46] J. Ferrero, «Sistema SAFETERM: Safe Flight terminatión System,» *Boletín de Observación Tecnológica en Defensa,* nº 77, pp. 14-19, 2023.

[47] F. L. López, «Sensores inteligentes y módulo de manetnimiento predictivo embarcado (MAPRE),» *Revista General de Marina,* 2022.

[48] INDRA, «indracompany.com,» 13 01 2022. [En línea]. Available: https://www.indracompany.com/es/noticia/indra-dotara-inteligencia-artificial-mantenimiento-eurofighter-reforzar-disponibilidad.

[49] Infodefensa, «Navantia liderará el diseño del nuevo sistema logístico del Ejército de Tierra,» 9 diciembre 2023. [En línea]. Available: https://www.infodefensa.com/texto-diario/mostrar/4642239/navantia-liderara-diseno-nuevo-sistema-logistico-ejercito-tierra.

[50] R. Holgado, «20minutos.es,» 26 04 2023. [En línea]. Available: https://www.20minutos.es/tecnologia/ciberseguridad/google-lanza-sistema-analizar-malware-inteligencia-artificial-malaga-5122343/.

[51] J. Wong, «ALEXA, WRITE MY OPORD: PROMISE AND PITFALLS OF MACHINE LEARNING FOR COMMANDERS IN COMBAT,» 20 09 2023. [En línea]. Available: https://cimsec.org/alexa-write-my-opord-promise-and-pitfalls-of-machine-learning-for-commanders-in-combat/.

[52] J. G. González, *La Inteligencia Artificial como causa de transformaión del Planeamiento Operativo.*, 2023.

[53] S. f. Dapena, «On War...gaming: el juego de guerra como apoyo a la toma de deciones.,» *Revista de Aeronautica y Astronaútica.*, 11 2023.

[54] «Web de La Moncloa,» [En línea]. Available: http://www.lamoncloa.gob.es. [Último acceso: 13 enero 2015].