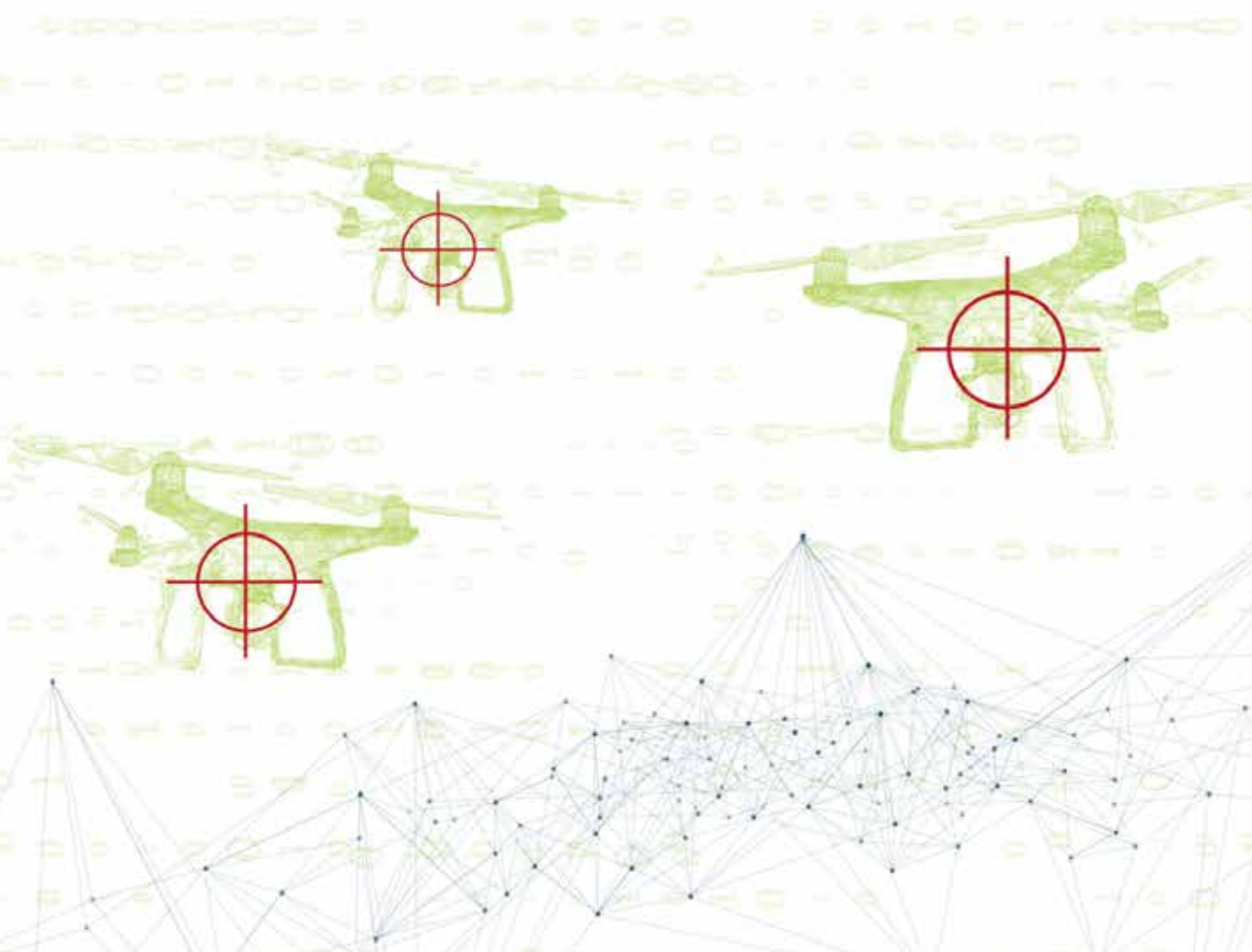


SITUACIÓN Y TENDENCIAS EN EL USO DE LA INTELIGENCIA ARTIFICIAL EN EL SECTOR DE LA DEFENSA



© 2025, de la presente edición: Foro de Empresas Innovadoras

© Diseño de cubierta: Panico Estudio / Alberto Solís

© Diseño y maquetación: Panico Estudio / Alberto Solís

Imprime: Estrella Servicios Gráficos, S. L.
28991 Torrejón de la Calzada (Madrid).

ISBN: 978-84-09-75701-5

Queda rigurosamente prohibido, sin la autorización escrita de los titulares del Copyright, bajo la sanción establecida en las leyes, la reproducción parcial o total de esta obra por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático y la distribución de ejemplares de ella mediante alquiler o préstamo público.

Situación y tendencias en el uso de la inteligencia artificial en el sector de la defensa

septiembre de 2025

Con la colaboración de:



UNIVERSIDAD
POLITÉCNICA
DE MADRID



TABLA DE CONTENIDO

CONTENIDO

PRÓLOGO 13

COMPOSICIÓN DEL GRUPO DE TRABAJO 17

CAPÍTULO 1.

CONTEXTO Y OBJETIVOS 25

1.1 Oportunidad de elaboración del informe 25

1.2 Enfoque metodológico 28

1.3 Objetivos concretos del informe 32

1.4 Método empleado para la elaboración del informe.....34

1.5 Breve descripción de la estructura del informe.....35

CAPÍTULO 2.

CONTEXTO DE LA IA EN EL SECTOR DE LA DEFENSA 41

2.1 IA en el contexto de la digitalización 44

2.2 Relevancia geopolítica de la IA.....44

2.3 Soberanía tecnológica europea en el sector de la defensa 47

2.3.1 Necesidad de conseguir la máxima autonomía estratégica 47

2.3.2 Impulso civil-militar ligado al control de la tecnología 49

2.3.3 Aceleración de los acontecimientos.....52

CAPÍTULO 3.

DIMENSIÓN TECNOLÓGICA DE LA IA COMO TECNOLOGIA DUAL.....59

3.1 Situación de la tecnología de la IA 59

3.1.1 Máquinas con capacidades cognitivas 59

3.1.2 Tipos de inteligencias artificiales.....60

3.1.3 De los datos a la toma de decisiones 61

3.1.4 Modelos computacionales en inteligencia artificial 68

3.1.5 Representación del conocimiento y razonamiento 69

3.1.6 Aprendizaje automático y profundo 71

3.1.7 La revolución de la inteligencia artificial generativa 77

3.1.8 Una mirada al futuro: Inteligencia artificial neurosimbólica.....86

3.2 Hardware/Chips para IA aplicada a la defensa 87

3.2.1 Evolución de las tecnologías de semiconductores.....88

3.2.2 Chips para aplicaciones en Defensa 92

3.2.3 Tipos de chips para la Defensa 96

3.2.4 Tipos de chips para su uso en IA	98
3.2.5 ASICs y aceleradores IA	107
3.2.6 Uso avanzado de chips para IA en Defensa	110
3.2.7 Evolución y tendencias de Chips IA	114
3.2.8 Proyectos de financiación pública de chips IA para Defensa	118
3.2.9 Conclusiones sobre chips IA	119

CAPÍTULO 4.

DIMENSIÓN SOCIOECONÓMICA DE LA IA EN EL SECTOR DE LA DEFENSA 123

4.1 Estructura del mercado internacional de la IA en defensa.	123
4.1.1 Segmentación	126
4.1.2 Mercados por región	128
4.1.3 Relevancia de IA en el mercado de Defensa	129
4.2 Tecnología Industrial	133
4.3 Estructura del ecosistema de defensa relacionado con la IA en la UE y en España	137
4.3.1 Caracterización del sector industrial de IA defensa.	139
4.3.2 Actores Industriales de defensa en Europa	140
4.3.3 Actores Industriales de defensa en España	142
4.3.4 Ecosistema industrial de IA en Defensa en España	148
4.3.5 Programas de I+D de IA en Defensa	151
4.3.6 Desarrollos en IA militar en diversos países.	163
4.3.7 I+D de IA en Defensa en España	167
4.4 Evolución estimada del sector de la defensa hasta 2030.	173

CAPÍTULO 5.

DIMENSIÓN TÁCTICA, OPERATIVA Y

ESTRATÉGICA DEL USO DE LA IA EN DEFENSA 181

5.1 Introducción progresiva de la IA en operaciones militares	181
5.2 Evolución hacia un campo de batalla inteligente	183
5.2.1 Introducción progresiva de nuevas tecnologías.	183
5.2.2. Niveles de automatización	187
5.3 Tendencias del uso de la IA en un campo de batalla inteligente	188
5.3.1 IA en el campo de batalla	188
5.3.2 IA en la frontera y el continuo Edge-Fog-Cloud	190
5.3.3 Robots de combate terrestres y marítimos	194
5.3.4 Uso de la IA generativa en aplicaciones de defensa	196
5.3.5 Visión multidominio.	199
5.3.6 Uso de la IA en los sistemas de mando y control.	201

5.3.7 Nube de combate inteligente	205
5.3.8 IA en la guerra electrónica.....	207
5.3.9 Sistemas de armas inteligentes.....	212
5.3.10 Enjambres de sistemas militares no tripulados.....	220
5.3.11 Consecuencias tácticas.....	232
5.4 Relevancia de la IA en la guerra híbrida y cognitiva	236
5.4.1 Concepto y contexto de guerra híbrida	236
5.4.2 Concepto de guerra cognitiva	243
5.4.3 Evolución de la guerra cognitiva	248
5.4.4 Relevancia de la IA en la generación y lucha contra la desinformación en la guerra cognitiva	252
5.4.5 Análisis de sentimientos con herramientas de IA	259
5.4.6 Uso de la IA en la negociación de conflictos militares.....	260
5.4.7 Responsabilidades y límites en la detección de noticias falsas para los proveedores de plataformas digitales	260
5.4.8 IA y cibercrimen	262
5.4.9 Evolución tecnológica futura de la guerra cognitiva	264
5.4.10. Estimación de la aparición de eventos disruptivos relacionados con la guerra cognitiva hasta 2030	274
5.4.11. Consideraciones finales sobre la IA en la guerra híbrida y cognitiva	277
5.5 IA en el sector espacial de la defensa	279
5.5.1 Situación del sector espacial militar	280
5.5.2 Aplicación de la IA en el sector espacial de defensa	284
5.5.3 Optimización de comunicaciones militares espaciales	298
5.5.4 Simulación basada en IA e interoperabilidad de datos espaciales.....	302
5.5.5 Plataformas pseudo satelitales a gran altitud	303
5.5.6 Gemelos digitales de sistemas espaciales	304
5.5.7 Robótica espacial potenciada por la IA.....	304
5.5.8.Situación de Europa en el uso de la IA espacial en defensa	307
5.5.9 Apoyo a nuevas empresas de base tecnológica en el sector espacial	312
5.5.10 Competitividad europea en el contexto del sector espacial.....	313
5.6 Un marco de uso en defensa de la IA en rápida evolución	313
5.6.1. Avance sin consenso	313
5.6.2 Consecuencias para España.....	314
5.7 Conclusiones	316

CAPÍTULO 6.

DIMENSIÓN ÉTICA Y REGULATORIA DE LA IA EN DEFENSA 323

6.1 Contexto del marco ético de la IA en defensa.....	323
6.1.1 Perspectiva histórica de la ética militar	323
6.1.2 Interacción entre el marco ético y el regulatorio de la IA militar	333
6.2 Uso responsable de la IA en el ámbito militar.....	336
6.2.1 Marco jurídico.....	336
6.2.2 IA Responsable en el Ámbito Militar (REAIM)	337
6.3 Regulación dual de la IA	340
6.3.1 Evolución de la regulación civil a la militar de la IA.....	340
6.3.2 Regulación de la IA en la UE	344
6.3.3 Pasos hacia una regulación de la IA en el ámbito militar	348
6.4 Regulación de IA en defensa.....	351
6.4.1 Empleo de las reglas de enfrentamiento (ROE) para el uso de la IA	355
6.5 Necesidad de regulación del uso militar de la IA en la UE	358
6.5.1 Regulación para el uso de sistemas de armas inteligentes.....	360
6.5.2 La ética militar entre la IA y la neurotecnología (NT)	362
6.5.3 Aspectos éticos y regulatorios asociados a la neurotecnología	363
6.6 Riesgos éticos en el ámbito militar derivados del uso de la IA	369
6.7 Conclusiones y previsible evolución.....	370

CAPÍTULO 7.

VALORACIÓN DE LA SOBERANÍA TECNOLÓGICA

DE LA UE EN IA DESDE LA PERSPECTIVA DE LA DEFENSA 375

7.1 Contexto.....	375
7.2 Posicionamiento geopolítico de la UE	376
7.3 Análisis de la soberanía tecnológica en IA de la UE	383
7.4 Geopolítica y semiconductores para IA.....	396
7.4.1 Situación de la UE en el mercado mundial de semiconductores	396
7.4.2 Uso de hardware abierto en el ámbito militar.....	398
7.4.3 Geopolítica de la fabricación de semiconductores	400
7.4.4 Soberanía tecnológica europea en semiconductores para la defensa.....	402
7.5 Geopolítica y plataformas digitales para la IA.....	404
7.6 Desafíos para el futuro	406

CAPÍTULO 8.	
CONCLUSIONES Y RECOMENDACIONES	413
8.1 Contexto	413
8.2 Conclusiones	414
8.2.1 Conclusiones sobre la dimensión científico-tecnológica de la IA	414
8.2.2 Conclusiones sobre la dimensión socioeconómica de la IA	418
8.2.3 Conclusiones sobre la dimensión táctica, operativa y estratégica del empleo de la IA por las Fuerzas Armadas	423
8.2.4 Conclusiones sobre la dimensión ética y regulatoria de la IA	427
8.2.5 Conclusiones sobre la soberanía tecnológica europea en IA	430
8.3 Recomendaciones de actuación	435
8.4 Reflexión final	445
REFERENCIAS	447
ANEXOS	487
Anexo 1. Listado de acrónimos	487
Anexo 2. Evolución tecnológica del aprendizaje basado en redes de neuronas artificiales	497
A2.1. Aprendizaje automático clásico	497
A2.2. El aprendizaje profundo: del Perceptrón al Transformer	500
Anexo 3. Futura convergencia de la IA con las tecnologías cuánticas y su previsible impacto en el sector de la defensa	513
A3.1. Introducción	513
A3.2. Estado actual de las tecnologías cuánticas	514
A3.3. Utilización de las tecnologías cuánticas en el ámbito de la defensa	529
A3.4. Convergencia entre las tecnologías cuánticas y la IA en Defensa	541

PRÓLOGO

*Es un honor y un placer como presidenta del Foro de Empresas Innovadoras (FEI) y como presidente del Grupo Amper, prologar el **informe sobre la inteligencia artificial en el sector de la defensa**, elaborado por un Grupo de Trabajo creado exprofeso con miembros del FEI, del Grupo Amper y expertos externos pertenecientes a los sectores académico, industrial y de las Fuerzas Armadas.*

Su puesta en marcha ha sido consecuencia de un informe previo y más general del Foro de Empresas Innovadoras y del acuerdo suscrito entre nuestras dos entidades para dar a conocer la situación, y su previsible evolución en los próximos años del uso de la inteligencia artificial en el ámbito de la defensa.

Somos conscientes de la creciente relevancia alcanzada por la inteligencia artificial en la sociedad y su exponencial evolución en un mundo complejo como el que tenemos. De hecho, la situación de la inteligencia artificial ha sido abordada con diferentes enfoques: técnicos, regulatorios, políticos, educativos, militares, sociales, laborales, etc. en docenas de informes elaborados en los últimos años por multitud de instituciones públicas y privadas de todos los países avanzados y también por parte de organismos internacionales, sea cual sea su actividad.

Sin embargo, a nuestro juicio, no se disponía de un análisis riguroso en español, basado en fuentes abiertas, focalizado en el uso de la inteligencia artificial como tecnología habilitadora y dual en el ámbito de la defensa, con énfasis en España y en la Unión Europea. La elaboración del presente informe ha permitido valorar la situación de esta última en un contexto de creciente confrontación geopolítica, en el que la tecnología, y expresamente la inteligencia artificial, juegan un papel determinante para obtener el liderazgo entre sus actores principales.

El uso de la inteligencia artificial en el ámbito militar avanza a un ritmo vertiginoso. Ya sea aplicada en productos civiles adaptados para la defensa o desarrollada específicamente para fines militares, esta tecnología está transformando la manera en que se conciben los conflictos. Gracias a estos avances, se está empezando a configurar lo que algunos llaman un “campo de batalla inteligente”. Esta evolución se ve impulsada por la continuidad de guerras de alta intensidad y por el esfuerzo de muchas potencias por lograr una ventaja en todos los frentes. Mirando al futuro, todo apunta a una creciente integración de la inteligencia artificial con tecnologías aún más disruptivas, como la computación cuántica y la neurotecnología.

La decisión de la puesta en marcha del Grupo de Trabajo a finales de 2024 respondía al convencimiento de que la Unión Europea debe reaccionar con urgencia en todos los sectores de actividad: política, económica y social, como se establecía claramente en los diversos informes elaborados por Enrico Letta, Mario Draghi y Sauli Niinistö, publicados en el contexto de la puesta en marcha de la nueva Comisión Europea. El de defensa, como ya se percibe sin contradicción alguna, era uno de ellos. Así, los acontecimientos acaecidos en el primer semestre del presente año corroboraban esa urgencia. El Libro Blanco para la defensa europea, publicado por la Comisión Europea el 18 de marzo, supone el marco para la toma

de decisiones, por partir de las instituciones comunitarias y de los Estados miembros. Poco a poco, decisiones del Consejo de la Unión y de los Estados miembros reflejaban con incrementos presupuestarios y con medidas de fortalecimiento de la industria de defensa, el convencimiento colectivo de que era el momento para prepararse para cualquier eventualidad.

La elaboración del informe durante el primer semestre de 2025 continúa y focaliza en el ámbito de la defensa el informe realizado por el FEI durante el año 2024, dirigido a conocer la situación de la soberanía tecnológica europea en inteligencia artificial. Ya en ese informe, se destacaba el ámbito temático de la defensa y seguridad como uno de los más relevantes por sus implicaciones en la seguridad colectiva, pero no se profundizaba en él.

No se ha pretendido, en el desarrollo del informe, dar cuenta de todos los posibles usos de la inteligencia artificial en el ámbito de la defensa, ni de los productos de uso militar que los incorporan, pero sí permitir al lector obtener una visión global desde dimensiones de análisis complementarias: la científica y tecnológica, la socioeconómica, la militar, la ética y regulatoria, y, sobrevolando todas ellas, la necesidad de incrementar la soberanía tecnológica europea en inteligencia artificial.

El FEI, en su labor de impulsar una reflexión y debate público sobre temas de políticas de innovación, y el Grupo Amper consideran que es el momento oportuno para analizar las consecuencias de la inteligencia artificial desde la perspectiva española y proponer algunas medidas de actuación que aseguren un papel relevante de la Unión Europea y de España y potenciar la contribución de España a la soberanía tecnológica europea en inteligencia artificial.

Estamos convencidos de que España debe, y este informe refleja que puede, jugar un papel relevante en la mejora de la soberanía tecnológica de España y de la Unión Europea en inteligencia artificial para la defensa. Pero ello obliga a actuar con la máxima decisión política, económica e institucional, y en el plazo más breve posible, y seleccionar aquellas áreas en las que el esfuerzo sea más eficaz.

Deseamos que todas aquellas personas que accedan a este documento encuentren respuestas, pero también se les susciten preguntas, que es, sin duda, uno de los mejores modos de avanzar. Este documento, como el objeto sobre el que trata, son elementos vivos acerca de unas tecnologías que avanzan a extraordinaria velocidad: su comprensión y su control permitirán su utilización sin los enormes riesgos que, sin dichas comprensión y control, comportarían para la humanidad.

Quisiéramos, para finalizar reconocer y, por supuesto, agradecer al Grupo de Trabajo y muy especialmente a su coordinador, Prof. Gonzalo León, y, como no, a todos los invitados externos, su excelente trabajo y su dedicación y esfuerzo.

En Madrid a 30 de septiembre de 2025

Carmen Vela

Presidenta FEI

Pedro Morenés

Presidente Grupo Amper

COMPOSICIÓN DEL GRUPO DE TRABAJO

Gonzalo León (Coordinador)

- Catedrático emérito - Universidad Politécnica de Madrid.
 - Miembro de la Comisión Ejecutiva del Foro de Empresas Innovadoras.
 - Vicepresidente de la Fundación Círculo de Tecnologías para la Defensa y Seguridad.
 - Miembro correspondiente de la Real Academia de Doctores de España y de la Academia de las Ciencias y las Artes Militares.
 - Secretario General de Política Científica en el Ministerio de Ciencia y Tecnología (2002-2004).
 - Vicerrector de Investigación de la UPM (2004-2013) y director del Centro de Apoyo a la Innovación tecnológica (CAIT) (2014-2021).
-

Asunción Gómez Pérez

- Catedrática de Inteligencia Artificial - Universidad Politécnica de Madrid (2007 -)
 - Vicerrectora de Investigación, innovación y doctorado de la UPM (2016 - 2025)
 - Directora del Departamento de Inteligencia Artificial de la UPM (2008 -2016)
 - Académica de la Real Academia Española y de la Real Academia de Ingeniería
-

Juan Carlos Dueñas

- Catedrático de Ingeniería Telemática de la Universidad Politécnica de Madrid.
 - Vicerrector Adjunto de Investigación de la UPM (2016-2025).
 - Director del Centro tecnológico mixto Santander-UPM “Center for Open Middleware” (2012-2016).
 - Editor jefe del área de Cloud Computing en la revista Journal of Systems and Software, Elsevier (2015-2024).
 - Presidente del capítulo español de Computación del Institute of Electrical and Electronic Engineers (IEEE) (2009-2014).
-

Luis Fernando Álvarez-Gascón

- Vicepresidente del Foro de Empresas Innovadoras.
 - Director General de Secure eSolutions en GMV.
 - Vicepresidente de Ametic (2017-2024)
 - Vicepresidente de la Comisión de I+D+i de CEOE (2016-2019).
-

Txema Báez Cristóbal

- Director de operaciones en economía y competitividad, innovación y crecimiento sostenible en NOVADAYS S.L.

- Miembro del Foro de Empresas Innovadoras.
 - Director de programas de la FECYT.
 - Miembro de la Delegación española en la ESA.
-

Ángel Gómez de Agreda

- Coronel en la reserva del Ejército del Aire y del Espacio.
 - Doctor en Ingeniería de Organización por la UPM.
 - Director de Desarrollo de Negocio para Oriente Medio de EUROPAVIA.
 - Agregado Militar en Corea del Sur (2021 - 2024).
-

Luis Vázquez Martínez

- Catedrático emérito de la Universidad Complutense de Madrid.
 - Miembro del Foro de Empresas Innovadoras.
 - Miembro correspondiente de la Real Academia de Ciencias Exactas, Físicas y Naturales, y de la Real Academia de Doctores de España.
 - Vicedecano de Investigación de la Facultad de Ciencias Físicas (1989 – 1995)
 - Vicerrector Adjunto de investigación de la UCM (1995 – 1999).
-

José María Insenser Farré

- Doctor en Economía y Gestión de la Innovación por la UCM, UAM y UPM e Ingeniero de Telecomunicación por la UPC.
 - Miembro Junta Directiva FEI.
 - Ingeniero de diseño microelectrónica en el CIE de Telefónica (Centro de Investigación y estudios de Telefónica) (1979 - 1987).
 - Fundador y CEO de la empresa SIDSA (Semiconductores Investigación y Diseño) (1992-2012).
 - Lead del Workstream Communications del IPCEI – Microelectronics/Communication Technology e Industrial Point of Contact (Ministerio de Industria /AMETIC) del IPCEI-ME/CT (2021 – 2024).
-

Juan Bosco Morales de los Ríos

- Director Corporativo de Tecnología del Grupo AMPER.
 - CEO de la empresa Swarming TS.
 - Jefe de la División Aeroespacial de Everis.
-

David Ramírez Morán

- Analista Principal del Instituto Español de Estudios Estratégicos. Centro Superior de Estudios de la Defensa Nacional - Ministerio de Defensa (2013 -).

- Registro de Empresas de Interés para la Defensa Nacional. DGAM (2009-2013)
 - Ingeniero de Telecomunicaciones (UPM) (Técnico 1995-1999, Superior 1999-2001, DEA 2003)
-

Luis Guerra

- Presidente de la Plataforma Aeroespacial española.
- Miembro del Foro de Empresas Innovadoras.
- Director de Espacio de Airbus.

La participación de los miembros del GT mencionados se realiza a título personal y las opiniones vertidas en el informe no tienen por qué corresponderse con las posiciones oficiales, si las hubiere, de las entidades a las que pertenecen.

Asimismo, el GT ha contado con la colaboración técnica de:

Aureliano da Ponte Vainman

- Doctor en Economía y Gestión de la Innovación por la UCM, UAM y UPM.
 - Consultor en temas relacionados con la industria de defensa global, I+D en defensa y asuntos de seguridad internacional e inteligencia tecnológica (2020-)
 - Director de Política Industrial en el Ministerio de Defensa de Argentina (2016-2019).
-

José Luis Sousa Freitas

- Country Manager en Portugal de Amper Sistemas y responsable por el equipo de I+D en IA
 - Ha sido director del departamento de Aerospace & Security en Thales Portugal
 - Ingeniero informático, doctorado en Sostenibilidad y Desarrollo Social
- Durante las reuniones mantenidas por el Grupo de Trabajo se ha invitado a las siguientes personas, con objeto de incrementar las perspectivas por parte del Grupo de Trabajo:

Manuel Pérez Cortés

- Director General de Defensa y Seguridad de GMV
 - Profesor Titular de la Universidad de la UPM
 - Director de la Escuela Española de Ensayos en Vuelo y Aeronavegabilidad (E4A)
-

Ricardo Sáenz

- Ingeniero de ICAI
 - Director de programas de Defensa y Seguridad de GMV desde 2013
 - Responsable de proyectos Internacionales de OTAN, EDA, y Fondo Europeo de Defensa
-

Guillermo Ramírez Altozano

- General de División del Ejército de Tierra
 - Jefe de la Jefatura de los Sistemas de Información, Telecomunicaciones y Asistencia Técnica (JCISAT) del E.T. (MINISDEF).
-

Roberto Villanueva Barrios

- General de Brigada del Ejército de Tierra (Reserva)
 - Fue Jefe del Estado Mayor del Mando Conjunto de Ciberdefensa
 - Responsable de la Jefatura de Ciberseguridad del CESTIC
 - Ha presidido el Grupo de Trabajo del Comité Militar de la UE
-

• Claudio Feijóo

- Doctor ingeniero de telecomunicaciones y licenciado en economía. Catedrático en la UPM
 - Director Cátedra Jean Monnet en Diplomacia Tecnológica y Soberanía Digital.
 - Codirector del Campus Sino-Hispánico de la UPM en Shanghai.
-

D. Juan A. Moliner González

- General de división del Ejército del Aire y del Espacio (R).
 - Doctor en Seguridad Internacional por la UNED/IUGM y Licenciado en Psicología por la Universidad de Granada.
 - Vicepresidente de la Academia de Ciencias y las Artes Militares (ACAMI)
 - Su principal línea de investigación es la Ética Militar y la importancia de la Dimensión Humana en guerras y conflictos.
-

Asimismo, también han participado en algunas reuniones del G.T. **D^a Carmen Vela** (Presidenta del Foro de Empresas Innovadoras) y **D. Pedro Morenés** (Presidente del Grupo Amper).

Capítulo 1

CAPÍTULO 1.

CONTEXTO Y OBJETIVOS

1. Oportunidad de elaboración del informe

Los diversos enfoques tecnológicos englobados en la **inteligencia artificial (IA)**, aunque con un origen que se remonta a la segunda mitad del siglo XX, han sufrido en la última década un **crecimiento acelerado** que ha impulsado su penetración en todos los eslabones de la sociedad. Hoy día, **afecta de forma consciente o inconsciente a miles de millones de personas** y a entidades de todos los países mediante el uso de aplicaciones basadas en IA para el desarrollo de su actividad diaria, proceso que se intensificará aún más en el futuro.

Sin embargo, de manera diferente a lo sucedido con otros cambios tecnológicos cuya penetración e impactos en la sociedad han sido más limitados, se trata, en este caso, de reconocer la existencia de un **impacto global de la IA potenciado por su integración con otras tecnologías** como son la microelectrónica, la robótica, la neurotecnología, la sensórica, los sistemas de comunicaciones en banda ancha, los servicios digitales en la nube, y otros, con especial énfasis en su implicación para el ciudadano con el uso masivo de las redes sociales. Todos ellos refuerzan el **carácter disruptivo de la IA en la sociedad** en una evolución cuyo alcance y consecuencias no son sencillas de determinar.

Atendiendo a esta relevancia, el **Foro de Empresas Innovadoras (FEI)** ha desarrollado durante el año 2024 una intensa actividad relativa a la elaboración de un **informe para conocer la situación de España y de la Unión Europea (UE) en relación con la IA** denominado “*Contribución de España a la soberanía tecnológica europea en Inteligencia Artificial: Análisis y recomendaciones de actuación*”⁰⁸.

El objetivo pretendido con la elaboración del citado informe, desarrollado por un Grupo de Trabajo específico constituido por miembros del FEI, fue **evaluar la soberanía tecnológica de la UE en Inteligencia Artificial y la forma en la que España podría contribuir a ella** en los próximos años indicando algunas actuaciones que deberían impulsarse por las administraciones públicas para este fin.

El informe elaborado en 2024 planteó el análisis desde una **perspectiva multidimensional** abordando, a su vez, la dimensión tecnológica, socioeconómica, legislativa/regulatoria y de defensa y seguridad; todas ellas, fuertemente interrelacionadas.

⁰⁸ Los documentos generados pueden encontrarse en la página Web del FEI. Informe completo (<http://foroempresasinnovadoras.com/wp-content/uploads/2024/10/2024-10-15-Informe-FEI-sobre-autonomia-estrategica-en-IA-VCON-PORTADA.pdf>) y resumen (http://foroempresasinnovadoras.com/wp-content/uploads/2024/10/2024-10-15-RESUMEN-Documento_IA_Paginas_individuales-COMPRIMIDO.pdf)

Aunque no se pretendía enfatizar ningún sector socioeconómico concreto en las recomendaciones, se identificaron como relevantes para España en la aplicación de la IA los sectores de **salud, educación, administraciones públicas, industria, agroalimentación, y defensa y seguridad** en los que se describieron brevemente algunos proyectos españoles relevantes desde el punto de vista del desarrollo y uso de aplicaciones de la IA en cada uno de los sectores indicados.

Tras el trabajo realizado en 2024, el FEI ha considerado necesario **profundizar el esfuerzo realizado** mediante la elaboración de un informe detallado⁰⁹ sobre un sector socioeconómico de máxima actualidad en los que el impacto de la IA y su relevancia para la soberanía tecnológica europea son máximos: **el sector de la defensa**¹⁰. Para ello, se ha constituido un *Grupo de trabajo* (GT) específico.

El **contexto geopolítico** que rodea en el momento actual la elaboración de un informe como el planteado sobre el sector de la defensa, y, parcialmente, cuando es relevante, sobre el sector de seguridad, es extraordinariamente complejo y, a la vez, sumamente relevante para el futuro desde la UE y de España¹¹. El análisis de **los condicionantes y evolución geopolítica mundial influye en el impacto del uso y despliegue de la IA en el sector de la defensa** tanto desde la perspectiva tecnológica como de la socioeconómica, así como de la potencial revolución táctica y operativa que conlleva en la conducción de las operaciones militares.

La decisión de abordar la realización de este **informe sobre la IA en defensa** en el año 2025 no es, por tanto, casual. Responde a una preocupación y a un amplio debate sobre la situación de la UE tras la evolución de la guerra en Ucrania en la que la tecnología de IA está siendo probada en los diversos dominios, así como a las posiciones adoptadas por la nueva Administración de Estados Unidos. Ambos factores refuerzan la **necesidad de acelerar la mejora de la capacidad de defensa de la Unión acelerando el proceso de innovación tecnológica**.

Como se indica en el **Libro Blanco sobre el futuro de la defensa europea** presentado por la Comisión Europea en marzo de 2025, las rivalidades geopolíticas no solo conducen a una nueva carrera armamentística sino también a una **competición tecnológica global**. Tecnologías disruptivas como son la inteligencia artificial, la computación en la nube, las tecnologías cuánticas, y los sistemas autónomos (por ejemplo, los drones autónomos), ya están conformando con luces y sombras el **nuevo campo de batalla**.

09 Expresamente para el desarrollo de este análisis detallado, el FEI ha firmado un acuerdo con el Grupo AMPER para su patrocinio y colaboración en la elaboración del informe y en su edición y presentación.

10 El informe realizado por el FEI en 2024 contenía una sección sobre la defensa y la seguridad, en la que se abordaba de manera sucinta la utilización de la IA y la situación en España. En el presente documento se ha acotado el ámbito para focalizarse en los temas de defensa, aunque en algunas secciones se abordan diversos aspectos del uso de la IA en seguridad necesarios para enmarcar el contenido, y con fronteras borrosas entre ambos dominios.

11 Aunque no sea objeto del informe elaborado describir en detalle la situación geopolítica alrededor de la IA, no es posible ignorarlo puesto que condiciona las decisiones políticas y de inversión adoptadas en torno a la IA.

Para destacar el reto actual de la UE basta reconocer que la perentoria necesidad de **conseguir un nivel de autonomía estratégica mayor** del que goza actualmente deberá sustentarse en una **mejora sustancial de su soberanía tecnológica**. En este escenario, estamos convencidos de que, como ha ocurrido repetidamente en la historia en periodos convulsos, **el desarrollo tecnológico se va a acelerar aún más durante la presente década, y la IA**, como tecnología habilitadora y dual, apoyada y convergiendo con la microelectrónica para la ejecución eficiente de sus algoritmos, **jugará un papel preeminente** en todos los sistemas de armas avanzados y de toma de decisiones en el ámbito militar.

El *GT* admite que en el primer semestre de 2025 **múltiples acontecimientos relevantes relacionados con la defensa europea** se han sucedido a un ritmo vertiginoso¹²; por lo cual advierte que algunas **recomendaciones de actuación específicas** contenidas en el presente informe pueden verse **superadas por la realidad** en poco tiempo. Es el precio que se debe pagar por abordar un tema de enorme actualidad si se desea **influir a tiempo en el debate sobre el futuro tecnológico de la UE en defensa focalizado en la IA** y las medidas potenciales que la UE y España, desde una base realista, deberían adoptar.

A partir del **Libro Blanco de la Defensa de la UE**, la discusión en los Estados miembros de la UE y en las instituciones comunitarias sobre las prioridades políticas, tecnológicas y presupuestarias relacionadas con estos asuntos adquieren un mayor protagonismo; sucede en un momento en el que dan los primeros pasos de la **discusión sobre el próximo marco financiero plurianual 2028-2034 de la Unión**. Por ello, informar al conjunto de la sociedad de la relevancia que ha adquirido la tecnología de IA para la defensa y seguridad común, conocer sus posibilidades y limitaciones, así como la necesidad de implicarse con decisión en su desarrollo se ha convertido en una cuestión esencial en la formulación de las políticas públicas.

Asimismo, en la segunda mitad del año 2025 comenzará el **debate sobre la estructura y prioridades del nuevo programa marco de investigación e innovación** (Horizonte Europa, HE 2028-2034) en el contexto del futuro **Fondo de Competitividad**. En este contexto se espera un mayor esfuerzo en el desarrollo de **tecnologías duales** entre las que se encuentra la IA.

La estructura, prioridades y presupuestos de un programa HE 2028-2034 estrechamente interconectado con otros programas comunitarios son factores clave ante los que **el gobierno español deberá posicionarse en el marco de la discusión sobre las nuevas perspectivas financieras plurianuales a partir de 2028**. Además, debe tenerse en cuenta que, en el contexto español, el *Ministerio de Defensa* deberá elaborar en 2025 la actualización de la

¹² La información de base contenida en el informe de IA en defensa y seguridad para su análisis se ha cerrado a finales de junio de 2025.

“Estrategia Tecnología e Innovación para la Defensa” (ETID)¹³ en la que, a buen seguro, la IA jugará un papel habilitador muy relevante.

El GT ha sido consciente de que la realización de un documento como el presente focalizado en la IA debe tener en cuenta que, tanto los **avances científico-tecnológicos** como la introducción en el mercado de **productos y servicios basados en IA**, se está produciendo a un ritmo muy rápido. Es una evolución difícil de estimar a largo plazo en la que anuncios relevantes se suceden prácticamente cada semana, y otros muchos se preservan en laboratorios o proyectos restringidos por razones de confidencialidad.

Por este motivo, es pertinente **delimitar el marco temporal** considerado como referencia para la elaboración del informe y sus recomendaciones. El GT considera que su utilidad no sería máxima si se analizase únicamente la situación actual (2025) del uso de la IA en defensa¹⁴ sin abordar su previsible evolución; pero también asume que una tecnología como es la IA en la que avances disruptivos se suceden de forma acelerada, **el horizonte temporal de análisis no puede ser muy lejano** porque el nivel de incertidumbre aumenta exponencialmente.

La opción adoptada por el GT es fijar el **horizonte temporal de análisis en el año 2030**, y tener en cuenta algunas previsiones o estimaciones hasta 2035 relevantes desde la perspectiva de la defensa cuando se dispone de una base documental para ello.

2. Enfoque metodológico

Dado que el ámbito potencialmente cubierto por el desarrollo y uso de la IA en la sociedad es muy amplio y su uso es dual, **el presente informe ha acotado su alcance al ámbito de la defensa** y, únicamente en ciertos casos, a aspectos relacionados con la **seguridad** (por ejemplo, la ciberseguridad y la desinformación en los conflictos híbridos o en aplicaciones críticas como sucede con la navegación satelital).

Asimismo, el GT ha partido del reconocimiento de que el **desarrollo científico y tecnológico de la IA se sigue impulsado, en gran medida, desde los mercados civiles**. Las inversiones del sector empresarial, apoyadas por las Administraciones Públicas (AAPP) con amplias divergencias temáticas y geográficas, se han constituido en el **factor crucial para su desarrollo**. Sin embargo, el **carácter dual de una tecnología habilitadora** como la IA y su relevancia para conseguir la supremacía frente al adversario, está influyendo decisivamente en su rápida adopción por las Fuerzas Armadas (FAS) y contribuye al crecimiento

13 La ETID actual para el periodo 2021-2027 puede encontrarse en: <https://www.tecnologiaeinovacion.defensa.gob.es/es-es/estrategia/Paginas/Defensa.aspx>

14 Los datos empleados más actualizados disponibles se refieren a los años 2023 y 2024.

y configuración de los mercados militares. Por este motivo, se ha prestado atención a casos de uso, productos y servicios basados en IA del mundo civil que pudieran adaptarse a aplicaciones militares.

La complejidad conceptual del uso de la IA en defensa obliga a **considerar su análisis desde dimensiones complementarias**. Concretamente, se adopta en el informe una **visión multidisciplinar** que integra las dimensiones tecnológica, socioeconómica, industrial, táctica-operativa, y ética y regulatoria. Brevemente en el anexo 3, esas dimensiones abordan los siguientes elementos:

Dimensión tecnológica. Tiene en cuenta la evolución tecnológica de la IA en aquellos ámbitos que tengan o puedan tener una relevancia para la defensa con la perspectiva temporal de 2030.

Se ha prestado atención desde esta dimensión no solo a las técnicas propias de la IA, sino también a su **convergencia con otras tecnologías emergentes** relacionadas con ella como son la microelectrónica, la robótica, las comunicaciones y sensórica cuántica, la neurotecnología, la ciberseguridad, la computación en el borde, la simulación (empleando, por ejemplo, gemelos digitales), etc. El anexo 2 complementa el análisis histórico de su evolución hacia la IA generativa.

La relación de la IA con la computación cuántica se ha analizado brevemente, dado que su uso real en defensa, no sólo experimental, estará, muy probablemente, fuera del ámbito temporal de análisis fijado hasta 2030. El Anexo 3 analiza la futura convergencia de la IA con las tecnologías cuánticas y su previsible impacto en el sector de la defensa

Dimensión socioeconómica. El análisis realizado parte de la valoración del volumen del mercado de la IA en defensa partiendo de la situación existente en 2024 y con estimaciones de su evolución previsible hasta 2030 de acuerdo con diversos informes de entidades oficiales y de empresas de consultoría, y los cambios relativos a su configuración en diversos países.

Dado que el FEI **no ha realizado estudios específicos de mercado** para la elaboración del informe se hace referencia a informes de mercado elaborados por diversas entidades externas, no necesariamente coincidentes en sus estimaciones, empleando la documentación pública accesible sobre los mismos.

Esta información se complementa con el detalle del sector industrial de la defensa y su relación con el de IA desde una visión de **ecosistema de innovación**. Para ello, se identifican los principales actores en el contexto nacional, europeo y global, tanto desde el punto de

vista de grandes empresas como de pequeñas y medianas empresas (PYMES) y, especialmente, de la emergencia y papel jugado por startups tecnológicas.

Es importante indicar que la **estructura del sector empresarial en defensa relacionado con la IA** está evolucionando de forma muy rápida con frecuentes reconfiguraciones, fusiones y adquisiciones entre sus actores principales. Entre los factores que influyen se destaca la necesidad de acceso a los mercados internacionales, tanto para la provisión de herramientas, sistemas y componentes, la cooperación en el desarrollo de sistemas, como la comercialización internacional de productos y servicios.

Desde esta dimensión se ha realizado un análisis sobre la **forma en la que la IA en defensa se aborda en diferentes programas de I+D en el contexto nacional e internacional**, con especial énfasis en los de la UE y la OTAN y sus consecuencias en el caso específico de la participación de entidades españolas en los mismos.

Dimensión táctica, operativa y estratégica. Desde esta dimensión se aborda la forma en la que el “*campo de batalla*” sometido a un proceso acelerado de digitalización, evoluciona desde un **campo de batalla digital** (proceso en marcha, pero no completado) a un **campo de batalla inteligente** (proceso incipiente) con profundos cambios en los niveles estratégicos, tácticos y operativos.

Desde esta dimensión se ha prestado especial atención a la forma en la que la IA se está empezando a usar en conflictos militares abiertos; se hace referencia, especialmente, a la experiencia de su uso en el caso de Ucrania y Oriente Medio, y también en relación con la denominada “guerra híbrida”, con creciente impacto en las decisiones militares en todos los niveles.

Dado que la dimensión militar del uso de la IA es muy amplia y no es posible cubrirla en su totalidad, el análisis se ha focalizado exclusivamente en tres ámbitos de indudable relevancia actual: el **sector espacial** de la defensa, la **guerra cognitiva** (en el contexto de la guerra híbrida), y en el creciente uso de la IA en los sistemas de toma de decisión ligados a **sistemas de armas autónomos o semiautónomos**. Otros usos de la IA como son los de la logística, la automatización de procesos administrativos o la formación no son, en esencia, muy diferentes de sus usos civiles.

Dimensión ética y regulatoria. Desde esta dimensión el énfasis se ha situado en los **problemas éticos derivados de los procesos de toma de decisión** en las que el ser humano puede verse desplazado por el creciente uso de algoritmos de IA en contextos de incremento masivo de la información a manejar, y a la reducción del tiempo disponible para tomar decisiones; requisitos difíciles de cumplir con las capacidades limitadas del ser humano.

Esta dimensión ha adquirido gran relevancia en los últimos años debido a las **consecuencias éticas**, en algunos casos ante situaciones derivadas del uso de la IA en la identificación automática de objetivos o en su uso en sistemas de armas semiautónomos, y, pensando en el final de la década, en circunstancias potenciales que pueden encontrarse en el futuro ante la integración de sistemas de IA más potentes.

Se analiza también la **falta de un consenso legislativo y regulatorio compartido** para abordarlo de forma responsable. El GT admite que, ante la falta de un consenso global, existen diferencias apreciables entre las regulaciones disponibles en diversos países en el uso de la IA en defensa y sus consecuencias en el uso real en operaciones militares. Sin embargo, se ha podido hacer un análisis comparado con la situación existente en diversos países y su previsible evolución.

Se trata de **dimensiones interrelacionadas** teniendo en cuenta que la evolución de una de ellas afecta a las demás por lo que **deberán analizarse de manera global**. Con esa amplia visión, se pretende facilitar el debate sobre su contenido y recomendaciones entre los actores más relevantes.

En la figura 1.1 se describe de forma esquemática la **relación entre las dimensiones indicadas** y algunos de los **elementos o factores clave identificados** en cada una de ellas; la situación actual de estos elementos y su previsible evolución futura se detallarán en los diferentes capítulos del informe.



Figura 1.1 Relación entre las dimensiones utilizadas en la elaboración del informe.

Fuente: elaboración propia

3. Objetivos concretos del informe

Con la expansión de las aplicaciones de la IA ya no es el humano el único agente implicado en la toma de decisión en muchos ámbitos de la sociedad. Ni siquiera se trata de que algoritmos complejos realicen en forma digital computaciones de modelos complejos con mayor eficiencia y velocidad aprovechando sistemas de altas prestaciones, extrayendo “inteligentemente” datos tanto de servidores que almacenan petabytes de información como del conjunto de Internet a través de redes de banda ancha; se trata de **sistemas que son capaces de “aprender de su entorno y evolucionar por sí mismos”**; algunas veces en direcciones desconocidas y sorprendentes para los humanos que participaron en su desarrollo inicial.

En los últimos años hemos presenciado la irrupción en la sociedad de la **inteligencia artificial generativa**, primero focalizada en la interacción, análisis y elaboración de texto en lenguaje natural, y en los últimos tres años profundizando en el análisis y la generación de contenido con un carácter multimodal (incluyendo audio, imágenes, video y programas de ordenador). Este proceso va camino de **alterar la barrera entre la realidad y la ficción** con consecuencias sociales muy relevantes.

En un fenómeno de evolución tecnológica que se potencia con la paulatina integración de **sistemas de realidad virtual y de realidad aumentada** que, impulsados por su maduración y abaratamiento, comienzan a penetrar en los mercados de consumo masivo y también en los profesionales. Lejos de detenerse ahí, previsiblemente, continuarán en los próximos años integrando **sistemas holográficos y herramientas derivadas de la neurotecnología**, aún en estado experimental. Todas ellas también son tecnologías inherentemente duales que se integrarán en productos y servicios comercializados en mercados civiles y militares como ya se está empezando a experimentar.

Expresamente, en relación con el **impacto de la IA en el ámbito de la defensa** que es el objeto del presente informe, se ha indicado repetidamente que estamos a las puertas de una **transformación de la naturaleza del conflicto militar** en la que el humano coexistirá y, en cierto modo, compartirá decisiones con máquinas y algoritmos previamente entrenados, pero que aprenderán de su propio comportamiento. El interrogante que se deriva, tal como ha sido sugerido, puede enunciarse del siguiente modo: ¿Nos encaminamos “aceleradamente” desde un **“campo de batalla digital”**, proceso en el que estamos inmersos desde hace una década, y aún no culminado, a otro que podemos denominar **“campo de batalla inteligente”** que ya se atisba en el horizonte?

La transición hacia el campo de batalla inteligente, probablemente, no será tan rápida como algunos preconizan, pero tampoco tan lenta como para no pensar en sus efectos y anticiparse a la forma de gestionarlos. **La segunda mitad de la actual década y la próxima de los años treinta del siglo XXI será testigo de esta transición** en la que el acceso a sistemas muy po-

tentes de IA estará a disposición de todos los ejércitos del mundo, aunque las capacidades de desarrollo de los sistemas más avanzados sí estén limitadas a algunas potencias tecnológicas.

De hecho, se puede objetivar cómo el **incremento de conflictos militares** interestatales abiertos, al mismo tiempo que la emergencia de otros de carácter asimétrico con implicación de estados, organizaciones terroristas o paraestatales, está provocando una **aceleración del empleo de la IA** tanto en su incorporación a sistemas de armas como en otros muchos aspectos de la defensa.

En el contexto descrito, los **objetivos concretos** de este informe son los siguientes:

- Analizar las **bases tecnológicas de la IA aplicada al ámbito de la defensa y la seguridad**, y su relación con otras tecnologías.
 - El objetivo es determinar la situación tecnológica de la IA y tecnologías habilitadores asociadas, así como su previsible evolución en un horizonte temporal hasta 2030 y, en algunos casos, de diez años (hasta 2035).
 - No se pretende elaborar un informe científico-técnico detallado orientado a expertos en IA, sino indicar la situación actual, tendencias y eventos disruptivos que puedan suceder, y valorar su trascendencia en el ámbito de la defensa y la seguridad, en el supuesto de que éstos tengan lugar. Aun así, se ha realizado un esfuerzo para introducir las bases necesarias para comprender la situación y previsible evolución de la IA.
- Evaluar la **forma en la que la IA se está empezando a utilizar en los conflictos militares** en base a información procedente de *fuentes abiertas*.
 - Se pretende para ello recabar información de casos de uso avanzados que utilicen la IA en sistemas de toma de decisión, el desarrollo de sistemas autónomos o semiautónomos, ya sean individuales o en enjambre, armados o no, sistemas de desinformación con generación de información sintética, etc.
 - Analizar las consideraciones éticas y reglamentarias que condicionen su uso en el ámbito de la defensa.
- Analizar la **situación actual en la UE del uso de sistemas basados en IA relacionadas con la defensa** con análisis de las interdependencias con países proveedores, y su previsible evolución en los próximos años.
 - Se desea analizar el grado de soberanía tecnológica en IA existente en el sector de la defensa en la UE y las interdependencias más relevantes en componentes, subsistemas, adquisiciones y operación y mantenimiento.
 - Debe tenerse en cuenta que la adquisición de un sistema de armas complejo suele estar condicionado a determinados controles sobre su uso y operatividad por parte del país proveedor.

- Determinar las **capacidades españolas** en la IA para la defensa y su previsible evolución en el contexto de la UE adoptando una posición realista indicando las áreas tecnológicas en las que existen debilidades, fortalezas, amenazas y oportunidades que contribuyan a mejorar la posición española.
 - ▀ Desde la perspectiva de las Fuerzas Armadas y cuerpos de seguridad.
 - ▀ Desde la perspectiva de la industria.
 - ▀ Desde la perspectiva de las universidades y centros de investigación.
- Elaborar un **conjunto de recomendaciones de actuación** para las Administraciones Públicas y las empresas españolas que puedan servir de base para acordar medidas en los respectivos ámbitos competenciales.
 - ▀ Para la Administración General del Estado.
 - ▀ Para las entidades empresariales.

4. Método empleado para la elaboración del informe

El método seguido para la elaboración del informe se ha basado en la puesta en marcha de un **grupo de trabajo de once personas** durante un período de seis meses tras su constitución en diciembre de 2024.

Tras la reunión de arranque celebrada en diciembre de 2024, la elaboración del informe se ha realizado en base a un **número limitado de encuentros presenciales** en 2025, uno al mes (enero, febrero, marzo, abril, mayo y junio), y uno final en el mes de julio para la aprobación del informe final. Se ha facilitado la participación por videoconferencia a aquellos miembros del GT que no pudieron asistir presencialmente a alguna reunión específica.

El informe elaborado corresponde a un **trabajo colectivo** basado en las aportaciones elaboradas por miembros del GT, ya sea individualmente o en pequeños subgrupos, y su presentación y discusión en sucesivas oportunidades.

Con objeto de complementar la experiencia y conocimiento de los miembros del Grupo de Trabajo se decidió invitar a diversos **expertos civiles o militares** a las reuniones con el fin de proporcionar visiones complementarias a la experiencia y conocimiento en temas específicos de los miembros del GT.

La actividad realizada ha contado con un **repositorio de información** con acceso para los miembros del GT en el que se han almacenado las contribuciones realizadas, la documentación de referencia empleadas, las decisiones adoptadas por el GT en sus reuniones, y

las diversas presentaciones elaboradas para la discusión de los temas procedentes de los miembros del GT o de los expertos invitados.

Un elemento esencial que debe tenerse en cuenta es que **el informe se ha elaborado empleando fuentes abiertas y no clasificadas**. Esto supone que la información puede no reflejar el grado de desarrollo en el que se encuentran algunos de los sistemas de defensa mencionados, ni tampoco los datos reales derivados de su uso (p.ej. prestaciones y eficiencia relativa) en el campo de batalla al tratarse de información clasificada.

No se han empleado **informes comerciales completos de mercado sobre la IA en defensa y seguridad** proporcionados por diversas empresas consultoras con estimaciones de la situación actual y de su evolución en los próximos años. En este sentido, se ha empleado la información abierta y accesible de datos procedentes de varios de ellos, lo que, si bien enriquece las visiones obtenidas, al mismo tiempo, muestra las diferencias de estimaciones entre ellos.

Por razones del tiempo y de recursos disponibles, **tampoco se han realizado encuestas estadísticamente significativas a expertos españoles o europeos**, y tampoco se han empleado **técnicas de prospectiva tecnológica** como serían estudios Delphi, señales débiles, análisis de escenarios o análisis DAFO detallados. En todo caso, sí se han empleado múltiples referencias sobre estudios relacionados cuando era pertinente.

El trabajo realizado ha dado origen no sólo a la redacción del **informe final** tal y como se presenta en este documento, sino a un conjunto de **documentos adicionales** realizados por algunos miembros del FEI en el GT con información más detallada sobre los temas tratados y con una visión autocontenida cuya longitud y nivel de detalle no permitían su incorporación completa en el informe final. Los **documentos adicionales generados** son:

- Relevancia de la IA en el sector espacial de la defensa
- Relevancia de la IA en la guerra híbrida y cognitiva
- Microelectrónica de IA para la defensa

El presente informe final **ha incorporado únicamente una parte de estos documentos**. En todo caso, los documentos completos con la idea de que sean útiles y accesibles para personas interesadas pueden encontrarse en la página Web del FEI.

5. Breve descripción de la estructura del informe

El **informe final** se ha estructurado en diversos capítulos y un conjunto de anexos. Tras este **primer capítulo** (*Contexto y objetivos*), el resto del informe consta de los siguientes capítulos, indicando sus secciones más relevantes.

El **capítulo 2** (*Contexto de la IA en defensa*) tiene como objetivo proporcionar una visión de la relevancia actual de la IA en el contexto de la UE y la necesidad de incrementar la soberanía tecnológica europea en IA para la defensa. Aun así, se acepta como punto de partida la necesidad de mantener un **enfoque de interdependencias tecnológicas controladas**. Para ello se abordan los siguientes temas: el papel de la IA en el contexto de la digitalización, la relevancia geopolítica de la IA y la situación de la soberanía tecnológica europea en el sector de la defensa.

El **capítulo 3** (*Dimensión tecnológica de la IA en defensa*) tiene como objetivo presentar los aspectos técnicos más relevantes que permitan evaluar la situación actual, las áreas de desarrollo científico-tecnológico más activas, y los previsibles avances esperables para los próximos años. Se ha pretendido que este capítulo proporcione la información tecnológica necesaria para todo el informe sin perder de vista la necesidad de que el detalle técnico empleado permita que sea accesible a no expertos en áreas de IA. Para ello, los temas principales tratados son la situación de la tecnología de la IA, el desarrollo hardware y microelectrónica para la IA y la relación entre la IA y otras tecnologías para la defensa.

El **capítulo 4** (*Dimensión socioeconómica de la IA en el sector de la defensa*) describe las grandes cifras del mercado de la IA, y desvela la estructura del sector de la IA desde el punto de vista empresarial. El foco geográfico se pone en la UE y su competitividad comparada con otros grandes bloques. Para ello se describe la estructura del mercado internacional de la IA en defensa y los actores relevantes de la IA en la UE.

El **capítulo 5** (*Dimensión táctica, operativa y estratégica de la IA en defensa*) presenta desde la perspectiva del GT la forma en la que la IA se está empleando actualmente por las Fuerzas Armadas en diversos ámbitos y las tendencias a lo largo de la presente década. En tal virtud, se analiza la evolución hacia el campo de batalla inteligente, los sistemas autónomos para la decisión, los enjambres de sistemas autónomos, el impacto de la IA en la guerra cognitiva, la relevancia en la denominada “guerra híbrida” y, por último, el uso de la IA en el sector espacial de la defensa.

El **capítulo 6** (*Dimensión ética y regulatoria de la IA en defensa*) aborda los retos éticos y regulatorios a los que se enfrenta el uso de la IA en el sector de la defensa y los esfuerzos que se están realizando en el contexto internacional en estos momentos con especial atención a la situación en la UE. Por eso, discute la problemática de la regulación de la IA en defensa y revisa la situación regulatoria internacional.

El **capítulo 7** (*Valoración de la soberanía tecnológica de la UE en IA desde la perspectiva de la defensa*) parte del posicionamiento geopolítico de la UE para analizar sus fortalezas y debilidades en relación con la IA. Al respecto, el punto de partida es el posicionamiento geopolítico de la UE y las dependencias críticas del bloque en función de los proveedores no europeos. Seguidamente, se analiza la geopolítica y gobernanza tecnológica en IA y se-

miconductores para terminar con una apreciación sobre la evolución actuales y previsibles de las capacidades de IA en la UE.

El **capítulo 8** (*Conclusiones y recomendaciones*) recoge un conjunto limitado de conclusiones y recomendaciones que permitan mejorar la situación española en el ámbito del desarrollo y uso de la IA en aplicaciones de defensa.

El informe incorpora un amplio conjunto de **referencias** bibliográficas empleadas en el texto (485) acompañado de múltiples **notas a pie de página** (más de 480) que, conjuntamente, permiten al lector obtener información más detallada de los aspectos tratados.

Finalmente, el documento cuenta con tres **anexos que complementan el contenido del informe principal**. El **Anexo 1** incluye el Listado de **acrónimos** empleados, el **Anexo 2** resume la **evolución tecnológica del aprendizaje basado en redes de neuronas artificiales** desde los primeros trabajos con el *Perceptrón* hasta la arquitectura *Transformer*. Finalmente, el **Anexo 3** se reflexiona sobre la futura **convergencia de la IA con las tecnologías cuánticas** y su previsible impacto en el sector de la defensa.

Capítulo 2

CAPÍTULO 2.

CONTEXTO DE LA IA EN EL SECTOR DE LA DEFENSA

2.1 IA en el contexto de la digitalización

El uso de la inteligencia artificial (IA) se ha extendido rápidamente a todos los sectores económicos en la última década transformando profundamente la sociedad; pero no se trata de un fenómeno aislado. Concretamente, **no puede desligarse la relevancia de la IA del proceso de digitalización** del que forma parte, iniciado años antes, y que se representa esquemáticamente en fases u oleadas en la figura 2.1.

Estas tres fases u oleadas no suponen procesos finalizados que dan paso a la siguiente fase, sino **evoluciones del proceso de digitalización** que continúan cada una siguiendo sus propias especificidades, pero al mismo tiempo con **impactos cruzados** en sus respectivos desarrollos. A la informática se le agregaron las comunicaciones y, a ambas, la etapa actual donde la IA adquiere una creciente centralidad lo cual ha generado dinámicas paralelas donde predomina una lógica orientada por lo sectorial, pero también un creciente número de casos donde se destaca la convergencia. Por lo tanto, la esquematización se propone a los fines analíticos, pero no implica compartimentar o dar por finalizada ninguna de las fases.

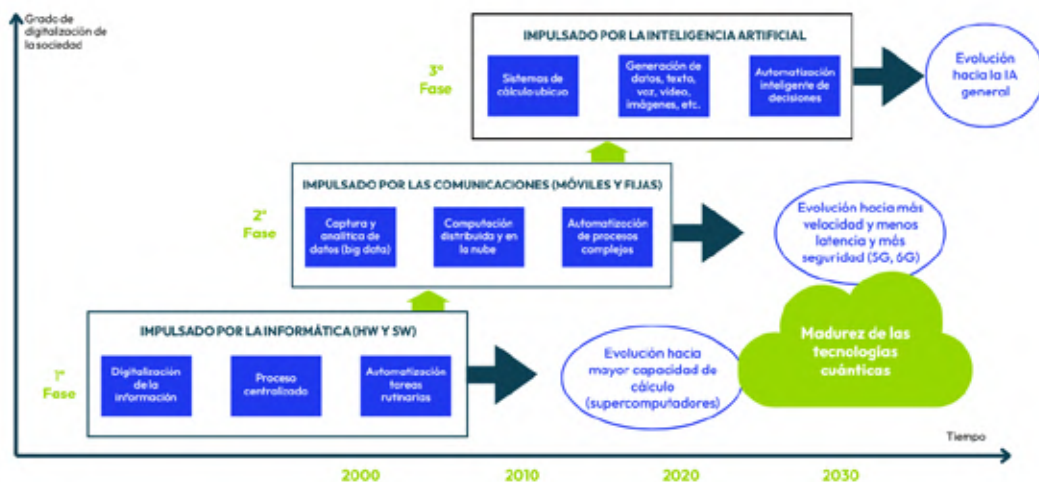


Figura 2.1 Fases principales del proceso de digitalización
Fuente: León (2025).

En la **primera fase**, abarcando un periodo que se extiende hasta entrado el presente siglo, la digitalización estuvo impulsada por la **expansión de la informática** con sistemas hardware y software más baratos y potentes que permitió la democratización de su acceso, alimentada por la progresiva digitalización de la información, la expansión de los centros de cálculo (inicialmente centralizados) y la automatización de tareas sencillas (rutinarias o bien definidas), ya sean éstas administrativas o de cálculo.

Tal como ha sido señalado, esta fase no puede considerarse terminada puesto que, de la mano de las **mejoras en la microelectrónica** (p.ej. miniaturización, nuevos tipos de empaquetado de chips, menor consumo, mayor velocidad, altas frecuencias), y el desarrollo de **nuevas arquitecturas distribuidas de supercomputadores**, las capacidades de procesamiento se superan de forma continua, y se solapa y realimenta con los avances y necesidades surgidas en las siguientes fases de digitalización.

La primera fase posibilitó una **segunda fase** en la que las técnicas de captura y análisis de grandes volúmenes de datos (*big data*), apoyada por el desarrollo de redes de alta velocidad, así como la **sensorización del mundo físico** con el despliegue de redes de sensores, permitieron la generación y el despliegue de sistemas de gestión de bases de datos y procesamiento en la nube, la expansión de sistemas de cálculo distribuidos y ubicuos (como es el caso de los teléfonos móviles inteligentes o en múltiples dispositivos integrados en todo tipo de productos, desde vehículos a electrodomésticos y robots), y la consiguiente capacidad de automatización de procesos administrativos o fabriles de una mayor complejidad. Todas ellas configuran la sociedad actual.

La **tercera fase** comenzó paulatinamente hace veinte años pero se ha acelerado en la última década y seguirá evolucionando de forma muy rápida. Esta fase se apoya en las anteriores, facilitando tres **avances decisivos impulsados por la inteligencia artificial**: la penetración en la sociedad de la **IA generativa**, permitiendo la generación de nueva información de datos (sintéticos), texto, voz, imágenes o videos, la expansión de la **capacidad de procesamiento ubicua** en todo tipo de dispositivos (computación “en el borde” o “en la niebla”), y la **automatización inteligente de las decisiones** con la capacidad de apoyar o sustituir al ser humano en muchas de ellas con la expansión de los denominados **agentes inteligentes**.

Es en esta tercera fase en la que se ha centrado la atención del presente informe. No obstante, debe tenerse en cuenta que **la tercera fase u oleada se apoya en las anteriores que no desaparecen**, profundizando el proceso de digitalización de la sociedad y, en especial, del sector de la defensa, cuyos ritmos de adopción son distintos a los de los sectores civiles. Tampoco la evolución de la digitalización se detendrá en esta fase. La sociedad camina hacia una **cuarta fase de digitalización** más lejana en el tiempo, pero cuyos elementos básicos ya se intuyen. La evolución de la capacidad de computación continuará en la próxima década con la irrupción de la **computación cuántica** (acelerando enormemente la capacidad de procesamiento), con las redes de **comunicaciones móviles 6G** (con muchas mejores prestaciones en velocidad y latencia) cuyo despliegue comenzará al final de esta década, y con

una rápida **evolución de la capacidad de razonamiento de la IA** acercándose, con todas las reservas, hacia la IA general durante la década de 2030.

En algunos de los sectores de la sociedad como es relativo a la **defensa** el uso de la IA ha alcanzado un interés comparativamente mayor porque detrás de su adopción se encuentra la capacidad de sustentar la **supremacía militar** entre las grandes potencias, enfrascadas en una carrera para conseguir a través de la IA la ventaja competitiva deseada.

Este interés se sustenta por las ventajas que pueden obtenerse al **introducir la IA en múltiples sistemas militares** como los de mando y control multidominio, los de guerra electrónica, en la gestión inteligente de la nube de combate, en comunicaciones militares cifradas, en el proceso de diseño de todas las plataformas militares, en constelaciones de satélites, o en los sistemas de armas autónomas letales, por citar algunos de ellos.

No será un proceso rápido; tal y como ha ocurrido con las otras fases de digitalización mencionadas, también en el ámbito de la defensa es necesario que la incorporación de su uso de forma rutinaria en el campo de batalla se produzca al mismo tiempo que la tecnología de IA, y se integre y evolucione junto a las estrategias y tácticas militares.

En la figura 2.2 (Pérez-Martínez, 2024) puede verse como se ha pasado de tener un **campo de batalla tradicional** (analógico y cinético) en el que la superioridad en el combate está impulsada por la capacidad de la fuerza militar, por el despliegue rápido y la maniobra, a otro **campo de batalla digital**, en el que la superioridad se logra impulsada por la captura de datos y su procesamiento en tiempo real para guiar el uso de sistemas cinéticos y ataques híbridos. Ambos modelos de campo de batalla coexisten como se demuestra en el conflicto militar de Ucrania.



Figura 2.2 Evolución del campo de batalla
Fuente: adaptada de Pérez-Martínez (2024)

Pero también, como parte de la tercera fase de la digitalización mencionada anteriormente, se ha comenzado a producir una transición al denominado **“campo de batalla inteligente”** en el que la superioridad en el combate se consigue mediante la sinergia obtenida de la generación masiva de datos en tiempo real (basado en un campo de batalla sensorizado y progresivamente *“transparente”* en el que el movimiento de tropas y equipos es difícil ocultar) y la aplicación de algoritmos basados en IA para la toma de decisiones con el empleo de sistemas de mando y control y múltiples vehículos con funcionamiento autónomo o semiautónomo. Asimismo, estas cuestiones no pueden disociarse de aspectos de **ciberseguridad** que han adquirido una gran relevancia para poder desplegar con confianza estos sistemas.

Como ocurre en todos los periodos históricos dominados por inestabilidades militares de relevancia, el desarrollo tecnológico se acelera, y éste no va a ser distinto como se profundizará en los diferentes capítulos del presente Informe. **Con ello, la transición al campo de batalla inteligente es imparable**, y su expansión va a **transformar la naturaleza del conflicto militar**.

Este proceso, aunque la adopción de la IA pueda parecer **más lenta de lo que ocurre en algunos ámbitos de los sectores civiles**, acabará por expandirse en todos los ejércitos y se superpondrá tanto al campo de batalla convencional como al digital, modificando profundamente la forma de planificar, las tácticas empeladas y la conducción de operaciones.

Más adelante en el horizonte ya se vislumbra la emergencia de un **campo de batalla cognitivo** (la Escuela de Guerra de Estados Unidos acuñó el término de *“guerra tecno-sentiente”*), del que muchos de los eventos asociados a la guerra híbrida y la guerra cognitiva actuales, potenciadas ambas por la IA, en evolución sinérgica con las neurotecnologías y las tecnologías cuánticas ya anticipan.

Esta evolución sinérgica de las tecnologías plantea serios **problemas éticos** en su uso para los que no existe un marco legislativo apropiado y consensuado a los que distintos actores políticos e institucionales relevantes de la sociedad, entre ellos, pero no solo, las Fuerzas Armadas, deben dar respuesta. Además, es probable que se genere una asimetría sobre la base de que los marcos éticos de referencia empleados sean diferentes entre países enfrentados.

2.2 Relevancia geopolítica de la IA

Un factor adicional al meramente tecnológico, que confiere a la IA una relevancia especial en relación con la defensa y, en menor medida, con la seguridad es la **dimensión geopolítica adquirida** por la misma. Dimensión enraizada en la creciente confrontación tecnológica entre grandes potencias.

Actualmente, la **batalla entre grandes potencias por el dominio de las tecnologías emergentes**, de la que la IA se ha convertido en una tecnología habilitadora fundamental, se basa en un doble juego de intereses geopolíticos:

1. **acelerar el uso de la tecnología de IA** para el desarrollo de sistemas más avanzados que logren una mejora de competitividad y, con ella, una supremacía en los mercados internacionales de productos y servicios tecnológicos, incluyendo el control de los componentes y las rutas comerciales necesarias para ello;
2. **impedir que las potencias contrincantes tengan acceso a tecnologías de IA avanzadas** que puedan usarse para debilitar la posición propia, ya sea en mercados civiles como de superioridad militar, mediante el establecimiento de restricciones y sanciones de exportación de componentes, de sistemas, o de las herramientas (de diseño o de fabricación) necesarias para el acceso o desarrollo de sistemas basados en IA, impulsadas por decisiones unilaterales o multilaterales.

Ambos elementos se combinan y ejemplifican en la **confrontación tecnológica entre Estados Unidos y China**, exacerbada en los últimos cinco años en el ámbito de la tecnología de los semiconductores y de la inteligencia artificial, fuertemente dependiente del uso de circuitos integrados específicos como se analizará en el capítulo 3.

La **dimensión geopolítica de la IA ha adquirido tintes globales** con impactos relevantes derivados de ella en terceros países generadores de conocimiento o convertidos en actores clave de la cadena de valor de la IA como son los casos de la UE, Reino Unido, Taiwán, Japón, Corea del Sur, India, Israel, Canadá, Australia, Rusia, y otros; y, por supuesto, también impacta en todos los países del mundo, usuarios en mayor o menor medida de sistemas basados en IA.

La UE, anclada al bloque occidental y, en el marco defensivo muy dependiente hasta ahora de la OTAN, liderada por Estados Unidos, a la que pertenecen la mayor parte de sus Estados miembros (23 de 27), se ve **constreñida en un proceso de globalización** en el que ha dejado de ser líder de muchas áreas tecnológicas.

La figura 2.3, adaptada del informe presentado en septiembre de 2024 por Mario Draghi sobre la competitividad europea en base a análisis de patentes es revelador. En el **eje vertical** se posicionan diversas tecnologías en función del “índice de complejidad tecnológica” (tecnologías valoradas desde 0, la menos compleja, a 100, la más compleja), y en el **eje horizontal** la “densidad de relación” que representa la facilidad con la que un país puede construir una ventaja comparativa en una tecnología determinada (dependiendo de qué estrecha es la relación con otras tecnologías en las que el país en cuestión ya es fuerte). El *tamaño de las burbujas* muestra el grado en el que cada país ya se ha especializado en una

tecnología, utilizando una medida de ventaja comparativa revelada que refleja su ventaja competitiva en ese campo en base a patentes.

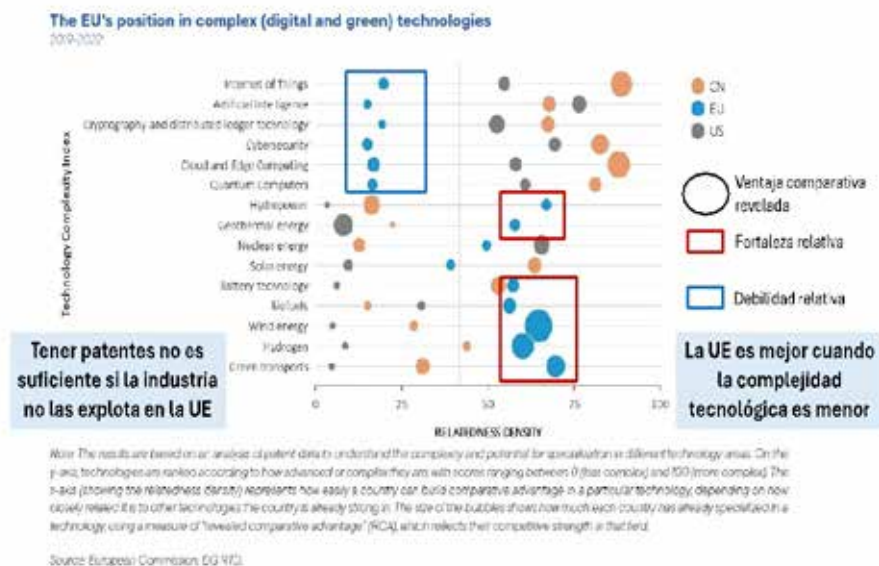


Figura 2.3 Situación comparada de la UE en diversas áreas tecnológicas digitales y verdes en base a patentes. Fuente: adaptada de Draghi (2024)

El análisis de esta figura presenta una posición preocupante de la UE dada su acusada debilidad relativa en tecnologías como la internet de las cosas, la **inteligencia artificial**, la criptografía y cadenas de bloques, la ciberseguridad, la computación en la nube y en el borde, y los computadores cuánticos. Además, es significativo que **la UE se comporte mejor en áreas en las que la complejidad tecnológica es menor** como ocurre con las relacionadas con las energías alternativas. En resumen, refleja una situación que explica la pérdida de competitividad global de la UE.

No es extraño que esta situación, conocida desde hace años, haya motivado que **la UE haya decidido incrementar su nivel de soberanía tecnológica** como parte de su estrategia política a largo plazo de lograr una **mayor autonomía estratégica** en muchos ámbitos, entre ellos, el de la defensa y la seguridad.

En este contexto, la IA juega un papel fundamental dado su carácter **dual y habilitador** como elemento esencial para su **integración** junto con la microelectrónica y la nanotecnología, **en múltiples sistemas complejos** como pueden ser los satélites militares, las plataformas de decisión, o los sistemas de armas autónomos.

Desde la perspectiva del GT, **la IA se ha convertido en un factor básico en la búsqueda de la supremacía militar** con el desarrollo de aplicaciones específicas que pueden marcar la

diferencia entre ganar o perder en un conflicto militar. Por estos motivos, la adopción de la IA en defensa se ha considerado como una **prioridad** en Estados Unidos, Rusia, China, la UE y otras potencias militares con incrementos significativos de los presupuestos asignados al desarrollo y adquisición de sistemas de defensa potenciados por el uso de la IA.

En el caso de la UE esta relevancia se pone de manifiesto en los diferentes informes solicitados por la presidenta de la Comisión Europea tras las elecciones al Parlamento Europeo de junio de 2024, y expresamente en el denominado *informe Draghi*. Algunas de sus ideas han tomado cuerpo con la publicación en marzo de 2025 del denominado **“Libro Blanco sobre el futuro de la defensa europea”**.

2.3 Soberanía tecnológica europea en el sector de la defensa

2.3.1 Necesidad de conseguir la máxima autonomía estratégica

No parece necesario insistir en que **nos encontramos ante una crisis del orden global** creado tras la Segunda Guerra Mundial y mantenido durante las décadas de la Guerra Fría sin que ese “nuevo orden” esté bien definido ni asentado.

La **confrontación entre bloques ideológicos** liderado por Estados Unidos en el contexto de la OTAN y la Unión Soviética con el Pacto de Varsovia se sustentó durante décadas en el empleo de la tecnología en sistemas de armas avanzados, superioridad manifestada en múltiples dominios, compatible con una situación de relativa paz apoyada por el paraguas de la **disuasión nuclear** para evitar una confrontación directa entre las dos grandes potencias hegemónicas.

Esta situación de relativa estabilidad en la “guerra fría”, no obstante, no impidió el **estallido de múltiples conflictos militares** hasta el primer cuarto del siglo XXI con intervención directa o indirecta de las grandes potencias y en las que el uso de sistemas tecnológicos avanzados potenciados por la IA se ha convertido, paulatinamente, en un factor crítico de superioridad relativa.

En las últimas dos décadas, el **desarrollo tecnológico**, impulsado por las tecnologías de la información y las comunicaciones (TIC), corrió paralelo ante un proceso globalizador impulsado por mercados abiertos de productos en cadenas de provisión global y, en menor medida, de servicios digitales que alentaron un desarrollo económico continuado en los países que configuran el “occidente” al que, desde finales del siglo XX, se unen otros países de Asia y, especialmente, China.

Desde la perspectiva de la UE, **la soberanía tecnológica emerge como un elemento habilitador de la autonomía estratégica**, definida por el Servicio de estudios del Parlamento

Europeo como la “Capacidad de actuar de forma autónoma, de confiar en los propios recursos en ámbitos estratégicos clave y de cooperar con los socios cuando sea necesario”.

En la figura 2.4 se representa esquemáticamente este papel habilitador de la soberanía tecnológica basado en la capacidad de asegurar el suministro de productos críticos (como ejemplifica el caso del acceso a las tierras raras), la capacidad de fabricación de componentes y sistemas, y el acceso al conocimiento. Desde el punto de vista tecnológico, la tecnología digital toma un protagonismo creciente en todos ellos.

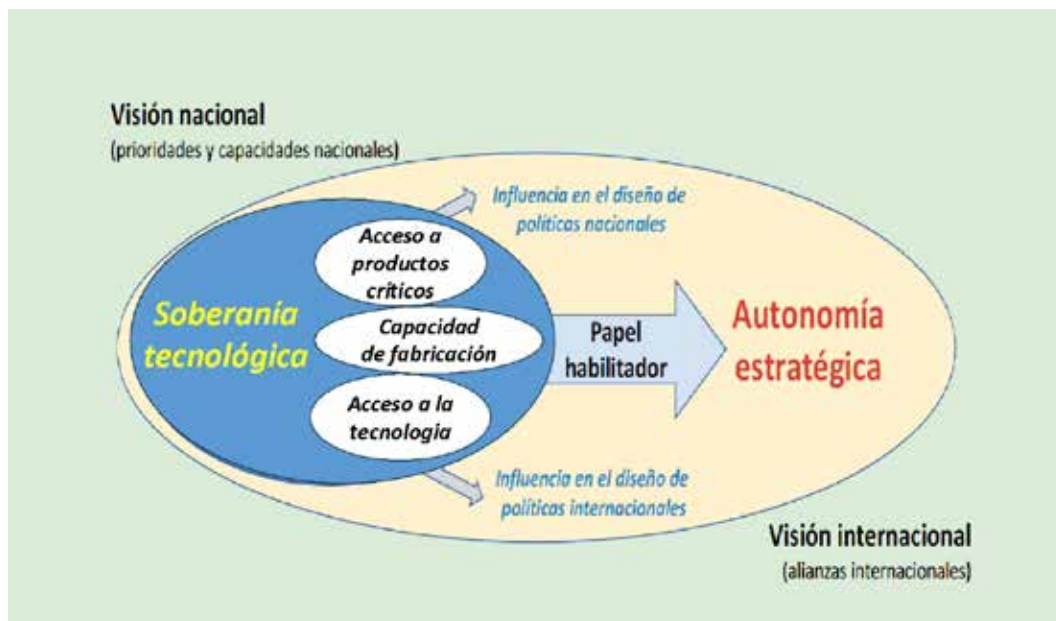


Figura 2.4 Relación entre autonomía estratégica y soberanía tecnológica

Fuente: León (2024)

La UE, en función de la posición de fortaleza tecnológica que posea en un momento determinado en algunas tecnologías clave, ha elaborado políticas públicas específicas en el contexto nacional de sus Estados miembros, el comunitario y el internacional con el objetivo de **potenciar su soberanía tecnológica y que permitan reducir la distancia existente con los países líderes**.

Sin embargo, no es posible para la UE disponer de una soberanía tecnológica plena en IA. **No es posible ni deseable**, sobre todo si se quiere profundizar la acción de la UE en un marco de relaciones multilaterales en los que la IA estará integrada en múltiples productos manufacturados en los que se basa la capacidad exportadora de la Unión. Sin acceso a componentes específicos de IA que Europa no fabrica (como son las unidades gráficas de procesamiento, GPUs por sus siglas en inglés), o con restricciones de los proveedores para su integración y exportación a terceros países, **la UE tiene una limitada soberanía tecnológica en IA**.

Esta débil posición de partida se refleja también en los mercados militares en los que la **dependencia europea** combinada con la existente en semiconductores y en la provisión de servicios basados en plataformas digitales para la toma de decisiones plantea un reto urgente al que debe hacer frente.

2.3.2 Impulso civil-militar ligado al control de la tecnología

No es sencillo separar el ámbito civil del de la defensa en múltiples aplicaciones tecnológicas en las que las características duales surgen como factores clave. De hecho, esta situación sucede en el caso de la IA con el uso de modelos grandes de lenguaje (LLM), de chips de IA, de herramientas para la generación de contenido multimedia o de datos sintéticos que, aunque desarrollados inicialmente para mercados civiles, son crecientemente empleados en el sector de la defensa.

Una consecuencia directa de ello es la influencia que ha tenido para los gobiernos en la definición de las **estrategias de acceso impuestas a otros países para el uso y control de tecnologías como la IA en mercados civiles**. El caso de China y el de Estados Unidos muestran la tendencia en estrechar la relación entre el ámbito civil y el militar con diferentes enfoques.

En Estados Unidos, el objetivo de la **integración civil militar** es el de incrementar la cooperación entre el gobierno y las empresas en investigación y desarrollo (I+D), fabricación y operaciones de mantenimiento, en base a las grandes licitaciones en contratos de defensa para sistemas de armas o plataformas, o de las agencias de investigación para desarrollos tecnológicos más disruptivos como **DARPA** (Agencia de investigación en Proyectos de I+D en defensa avanzados de defensa) en la que también se busca la participación de universidades y centros de investigación. Adicionalmente, se cuenta con una **red de laboratorios nacionales** financiados directamente por el presupuesto federal de Estados Unidos que desarrollan proyectos con un alto grado de confidencialidad.

En el caso de China, se ha producido una transición desde el concepto de “*integración civil- militar*” (*junmin jiehe*, 军民结合) a la “*fusión civil-militar*” (*junmin ronghe*, 军民融合) con la creación de la *Comisión Central para el Desarrollo de la Fusión Civil-Militar (MCF)* en enero de 2017 que ha financiado proyectos sobre neurociencias de aplicación militar, sistemas biomiméticos avanzados, mejora del rendimiento humano y biotecnología⁰⁸. En China, a diferencia de Estados Unidos en el que el sector civil tiene un innegable protagonismo, se trata de un plan orientado y dirigido por el gobierno (DoD, 2024).

Actualmente, el sector de Defensa de China sigue estando fuertemente dominado por sus empresas estatales. Se han implantado **comités del Partido Comunista de China (PCCh) en más de 35 gigantes tecnológicos chinos** para asegurarse de que los objetivos de la empresa no se desvíen de los del PCCh. Las ramas militares, como la *Fuerza de Apoyo Estratégico*

08 Science and Technology Military-Civil Fusion Special Projects Plan (科技军民融合发展专项规划)

del EPL (PLASSF), han firmado acuerdos con universidades y empresas de desarrollo de software para aumentar su integración fuera del ejército (García-Cantalapiedra, 2022).

Según la agencia EFE, este proceso continúa actualmente⁰⁹. Durante la reunión anual de la *Asamblea Popular Nacional* y la *Conferencia Consultiva Política del Pueblo Chino (CCPPCh)* en marzo de 2025, delegados del Ejército Popular de Liberación (EPL) y la Policía Armada enfatizaron la **necesidad de intensificar la colaboración entre el ámbito militar y los gobiernos locales** para optimizar el uso de terrenos, infraestructura, tecnología e industria en la construcción de defensa, así como optimizar los procesos de certificación y adquisición para **facilitar la incorporación de tecnologías civiles en el sector de defensa**.

La estrategia nacional china se centra en **tecnologías civiles y militares específicas**, incluida la IA; información cuántica; neurociencias; biotecnología; medicina clínica; tecnología del espacio, mar y tierra profundo; y circuitos integrados, en fotónica, nanoelectrónica, comunicaciones de red, robótica y nuevos sistemas energéticos.

Esta estrategia no se limita al interior de China, sino que tiene una vertiente de **presencia internacional**¹⁰. La presencia global se fortalece por la *Ley de Inteligencia Nacional de China* (2017) que exige la cooperación organizacional con los esfuerzos de inteligencia del Estado, y que ha alimentado los recelos en países occidentales sobre posibles “puertas traseras” que permitirían obtener información de los usuarios o el lanzamiento de ciberataques (López-Miralles, 2025).

Para Estados Unidos, el **despliegue de infraestructura 5G** en varias naciones pertenecientes a la OTAN procedente de proveedores chinos complica las relaciones de intercambio de inteligencia, por lo que han presionado a sus aliados para disuadirles de adoptar tecnologías chinas, ofreciendo incentivos y marcos para telecomunicaciones seguras como alternativas. No es posible ignorar que, detrás de estas actuaciones, se juega el dominio de los mercados internacionales.

Por su lado, China está integrando activamente la IA en su estrategia militar para transformar su ejército en una “*fuerza militar de clase mundial*” a mediados de siglo. El enfoque empleado se ha centrado en aprovechar la IA como un habilitador crítico de la **guerra “inteligente”**.

La creación del *Instituto de Investigación en Innovación en Ciencia y Tecnología de Defensa Nacional* de la Academia de Ciencias Militares (AMS) y su *Centro de Investigación en Inteligencia Artificial* subraya el compromiso del gobierno chino para fomentar la colaboración

09 Para más detalles puede consultarse: <https://www.swissinfo.ch/spa/el-ej%C3%A9rcito-chino-pide-m%C3%A1s-recursos-civiles-para-su-modernizaci%C3%B3n-militar/88987427>

10 Un ejemplo es el del 5G en el que las empresas chinas, fuertemente subsidiadas por el Estado, han establecido contratos para construir infraestructura 5G en más de 30 países.

interdisciplinar y la investigación en áreas como la robótica, los sistemas inteligentes y la ciencia cognitiva (un ejemplo de estos avances en el ámbito de la robótica inteligente aplicada a la defensa se ve en la figura 2.5).



Figura 2.5 Perro robótico de combate durante la 9ª Exposición de Tecnología Militar Inteligente de China (Pekín). Fuente: <https://thepoliticalroom.com/blog/el-5-g-en-la-estrategia-militar-de-china>

El Departamento de Defensa de Estados Unidos se ha hecho eco de estos avances hacia la “*inteligentización de la guerra*” desde la perspectiva de China en el informe presentado al Congreso en diciembre de 2024 (DoD, 2024). No se trata únicamente de armas. Un componente clave de esta transformación es el uso de la IA (人工智能) para la guerra cognitiva (认知战)¹¹, una estrategia que tiene como objetivo dar forma a las condiciones del campo de batalla y manipular las percepciones de los adversarios mucho antes de que comience el conflicto cinético. No es fácil evaluar hasta qué punto el sistema de control de la información utilizado por el gobierno chino influirá en la capacidad para el entrenamiento de sus sistemas de IA (Vaughn, 2025).

En todo caso, las diversas **restricciones de Estados Unidos a la exportación de alta tecnología de uso dual a China** (como son los semiconductores) pueden ralentizar, pero no detener, el desarrollo de la IA militar que podría cambiar el equilibrio de poder global. A medida que se intensifica la competencia entre Estados Unidos y China, existe el riesgo de

11 Para más detalles puede consultarse: <https://www.oxan.com/insights/china-will-continue-to-advance-its-military-ai/>

que proliferen las armas habilitadas por la IA sin que exista un enfoque regulatorio común ni un consenso en su uso.

2.3.3 Aceleración de los acontecimientos

La elaboración del presente documento ha coincidido en el tiempo con la **emergencia de acontecimientos relevantes para la defensa europea** como se indica en la figura 2.6. Los acontecimientos identificados en la parte superior de la figura son los derivados de la nueva administración de Estados Unidos y los de la parte inferior las “respuestas” más relevantes generadas por la UE en el primer semestre de 2025.



Figura 2.6 Factores relevantes desde 2024.
Fuente: León (2025)

En relación con los primeros, y que potencialmente afectan al uso de la IA en defensa, debe destacarse la emergencia, en muy pocos meses, de los siguientes eventos:

- Desencadenamiento de una **guerra arancelaria** promovida por Estados Unidos, y respondida de forma cruzada por otros países, incluida la UE, sobre multitud de productos tanto materias primas como productos tecnológicos, generando incertidumbres, limitando y encareciendo el comercio mundial.
- Posición contraria de Estados Unidos a la regulación digital europea y, expresamente, al **Reglamento de IA** que impone condiciones a las empresas americanas en su operación en la UE que han desembocado en la aplicación de diversas multas.
- **Cambio de actitud unilateral de Estados Unidos ante el apoyo a Ucrania** sin contar con la UE que, desde la perspectiva tecnológica, ha conducido a amenazas de impedir el uso de la constelación satelital *Starlink* o el envío de imágenes satelitales procesadas de *Maxar*, esenciales para alimentar la inteligencia del ejército ucraniano.
- Búsqueda de una **solución al conflicto en Gaza sin contar con la UE**, pero dotando a Israel de armamento sofisticado o acelerando el desarrollo de otros con posibles incrementos de la distancia en el posicionamiento ya existente con la UE.

- Preparación y discusión previa al **Consejo Atlántico** (Cumbre de la OTAN) en junio de 2025 en La Haya que, entre otras medidas, ha aprobado el compromiso de gasto en defensa con respecto al PIB de los países miembro de la Alianza hasta 2032, en el 5% de los que el 1,5% incluye los aspectos más generales de seguridad.

La **respuesta de la UE** se ha basado en un amplio debate y la adopción de diversas medidas como las indicadas en la parte inferior de la figura 2.6 que se detallan seguidamente:

1. **Brújula estratégica por la competitividad.** En enero de 2025 la Comisión Europea presentó un documento de marco para la mejora de la competitividad con una nueva hoja de ruta que permita restaurar el dinamismo de Europa e impulsar el crecimiento económico.
2. **Paquete “ómnibus” de simplificación.** En febrero de 2025 la Comisión Europea presentó un paquete de medidas que busca reducir la carga administrativa de las empresas de la UE, garantizando que puedan seguir siendo competitivas sin comprometer sus obligaciones en materia de sostenibilidad.
3. **Replanteamiento del presupuesto comunitario.** El 11 de febrero de 2025 la Comisión Europea presentó la comunicación titulada *“El camino hacia el próximo marco financiero plurianual”* con el objetivo de arrancar el debate para transformar el presupuesto comunitario a partir de 2028.
4. **Medidas hacia el rearme de la UE.** El 4 de marzo de 2025 la presidenta de la Comisión Europea anuncia el “Plan de Rearme Europeo” centrado en utilizar todas las palancas financieras disponibles, con el fin de apoyar a que los Estados miembros aumenten rápida y significativamente los gastos en capacidades de defensa.
5. **Libro Blanco sobre el futuro de la defensa europea / Preparación 2030** ¹² Finalmente, el 19 de marzo de 2025, la Comisión presenta el “Libro Blanco” con el que se inicia un proceso de debate en profundidad.

En el **Consejo Europeo** celebrado el 6 de marzo de 2025 focalizado en la defensa ya se acordó que **Europa debía ser más soberana y responsable de su propia defensa**. Consecuentemente, se pretende estar mejor equipada para actuar y hacer frente de manera autónoma a los retos y amenazas inmediatos y futuros con un enfoque de 360 grados. Concretamente: *“la Unión reforzará su preparación general en materia de defensa, reducirá sus dependencias estratégicas, abordará sus carencias en materia de capacidades esenciales y afianzará en consecuencia la base tecnológica e industrial de la defensa europea en toda la Unión.”*

Desde el punto de vista tecnológico, el Consejo identificó un **conjunto de prioridades en sistemas tecnológicos para la defensa** en las que deben concentrarse las inversiones adicionales:

¹² https://defence-industry-space.ec.europa.eu/eu-defence-industry/white-paper-future-european-defence-rearming-europe_en

- ─ la defensa aérea y antimisiles;
- ─ los sistemas de artillería, incluidas las capacidades de ataque de precisión en profundidad;
- ─ los misiles y la munición;
- ─ los drones y los sistemas antidrones;
- ─ los elementos de apoyo estratégicos, también en relación con el espacio y con la protección de las infraestructuras críticas;
- ─ la movilidad militar;
- ─ el ámbito cibernético;
- ─ la inteligencia artificial;
- ─ y la guerra electrónica.

Estos elementos de debilidad europea se han incorporado al **Libro Blanco sobre el futuro de la defensa europea**. En la presentación del Libro Blanco, la presidenta de la Comisión Europea decía: *“La era del dividendo de la paz hace mucho que acabó. La arquitectura de seguridad con la que contábamos ya no puede darse por sentada. Europa está dispuesta a estar a la altura de las circunstancias. Debemos invertir en defensa, reforzar nuestras capacidades y adoptar una actitud activa en materia de seguridad. Estamos tomando medidas firmes al presentar una hoja de ruta de “Preparación 2030”, con un aumento del gasto en defensa e importantes inversiones en las capacidades industriales europeas de defensa. Debemos comprar más producción europea, porque eso significa reforzar la base industrial y tecnológica de la defensa europea, y también estimular la innovación, así como crear un mercado de equipos de defensa a escala de la UE”*.

De la primera parte del Libro Blanco pueden extraerse cuatro frases que muestran la situación actual:

- ─ *“Europa no puede dar por hecho la garantía de seguridad de Estados Unidos y debe incrementar su contribución para preservar la fortaleza de la OTAN”*.
- ─ *“Los Estados miembros de la UE han gastado menos en su defensa que Rusia, China y Estados Unidos”*
- ─ *“Un simple aumento del gasto, la producción y las adquisiciones nacionales de defensa de los Estados miembros no resolverá por sí solo el problema, ya que intensificaría la ya aguda fragmentación de la defensa europea a lo largo de las fronteras nacionales”*
- ─ *“El aumento del gasto en defensa debe ir acompañado de una consolidación sustancial de la base industrial europea de defensa”*.

Será necesario conocer el recorrido real de estas acciones propuestas por la UE en los próximos meses, y en el supuesto de que se aprueben y pongan en marcha, analizar su efectividad. Un paso muy relevante ha sido la aprobación por el Consejo de la UE en mayo de 2025 del Reglamento sobre el Instrumento de **Acción por la Seguridad de Europa (SAFE)** previsto en el Libro Blanco¹³.

13 Reglamento (UE) 2025/1106 del Consejo, de 27 de mayo de 2025, por el que se crea el instrumento «Acción por la Seguridad de Europa (SAFE) mediante el Refuerzo de la Industria Europea de Defensa. <https://www.boe.es/buscar/doc.php?id=DOUE-L-2025-80804>

Su puesta en marcha supondrá que la Comisión recaudará hasta **150.000 millones de euros** en los mercados de capitales, proporcionando *“palancas financieras a los Estados miembros de la UE para aumentar las inversiones en ámbitos clave de la defensa, como la defensa antimisiles, los drones o los elementos de apoyo estratégicos”*.

Concretamente, de acuerdo con el Artículo 1 del Reglamento, los ámbitos en los que los créditos (no se trata de subvenciones) de SAFE pueden ser aplicados por los países que los soliciten¹⁴, muchos de ellos relacionados directa e indirectamente con la IA, son:

a) categoría 1: municiones y misiles; sistemas de artillería, incluidas las capacidades de ataque de precisión en profundidad; capacidades de combate en tierra y sus sistemas de apoyo, incluidos los equipos para soldados y las armas de infantería; drones pequeños (clase 1 de la OTAN) y sistemas antidrones conexos; protección de infraestructuras críticas; ciberdefensa; y movilidad militar, incluida la contra movilidad;

b) categoría 2: sistemas de defensa aérea y antimisiles; capacidades marítimas superficiales y submarinas; drones distintos de los pequeños (clases 2 y 3 de la OTAN) y sistemas antidrones conexos; elementos de apoyo estratégicos como el transporte aéreo estratégico, el repostaje en vuelo y los sistemas C4 ISTAR, entre otros, así como los activos y servicios espaciales; protección de activos espaciales; inteligencia artificial y guerra electrónica.

El objetivo pretendido con SAFE no es solo proporcionar el acceso a recursos financieros en buenas condiciones, sino también **fortalecer el mercado europeo de la defensa** por los que, de acuerdo con el Artículo 4, *“las actividades, gastos y medidas se referirán a productos de defensa u otros productos con fines de defensa obtenidos por medio de adquisiciones en común”*. Para ello, *“Los Estados miembros que deseen recibir ayuda financiera en el marco del Instrumento SAFE enviarán a tal efecto una solicitud a la Comisión a más tardar el 30 de noviembre de 2025. La solicitud irá acompañada de un plan de inversión de la industria europea de defensa”*.

El objetivo de fortalecimiento de la industria de defensa se cuantifica en el Reglamento SAFE incluyendo la condición de que *“los contratos de adquisición en común deben contener el requisito de que el coste de los componentes con origen fuera de la Unión, de los Estados AELC del EEE y de Ucrania no sea superior al 35 % del coste estimado de los componentes del producto final”*. Obsérvese la inclusión de Ucrania en este contexto.

¹⁴ La decisión depende criterios económicos en función del coste de acceder de forma nacional al mercado de capitales comparado con el coste de los créditos del instrumento SAFE, y los criterios políticos de aceptación o no de las condiciones establecidas en el Reglamento de SAFE. En este sentido el gobierno alemán ha anunciado que no recurrirá a ellos.

Capítulo 3

CAPÍTULO 3.

DIMENSIÓN TECNOLÓGICA DE LA IA COMO TECNOLOGÍA DUAL

3.1 Situación de la tecnología de la IA

3.1.1 Máquinas con capacidades cognitivas

Erróneamente se piensa que muchos de los conceptos de inteligencia artificial son relativamente modernos. ¡Nada más lejos de la realidad! En el siglo XIX, los inventores británicos *Charles Babbage* y *Ada Byron*, y en el siglo XX *Alan Turing* y el español *Leonardo Torres Quevedo*, ya diseñaron **artefactos mecánicos y eléctricos para realizar actividades cognitivas**. Desde mediados del siglo XX han aparecido máquinas y dispositivos digitales que incorporan la electrónica, los semiconductores y las tecnologías de la información y comunicaciones para ayudar en el procesado de esa información.

Comencemos por los **orígenes de la inteligencia artificial**. Si bien fue Alan Turing (1950) quien planteó en la siguiente pregunta: «¿Pueden pensar las máquinas?», fue mucho más recientemente, en agosto de 1955, cuando un grupo de investigadores propuso realizar un estudio sobre inteligencia artificial (McCarthy *et al*, 1955). La conferencia de Dartmouth fue el evento fundacional de este campo. Los padres de esta ciencia plantearon demostrar la siguiente conjetura: *«Cualquier aspecto del aprendizaje o cualquier otra característica de la inteligencia puede, en principio, estar tan precisamente descrita que se puede construir una máquina para simularla. Se intentará descubrir cómo hacer que las máquinas utilicen el lenguaje, formen abstracciones y conceptos, resuelvan tipos de problemas hasta ahora reservados a los humanos y se mejoren a sí mismas»* (McCarthy *et al.*, 1955). En definitiva, se trataba de introducir en dispositivos físicos **sistemas informáticos con capacidades cognitivas para que puedan pensar como humanos**.

La Comisión Europea (2019) ha definido los sistemas de inteligencia artificial en el documento de **guías éticas para una inteligencia artificial fiable**, como *«sistemas de software (y en ocasiones hardware) diseñados por humanos que, ante un objetivo complejo, actúan en el mundo físico o digital percibiendo su entorno a través de la adquisición e interpretación de datos estructurados, semiestructurados o nada estructurados, razonando con el conocimiento, procesando la información derivada de estos datos y decidiendo las mejores acciones a realizar para alcanzar el objetivo»*.

Los sistemas de IA usan modelos simbólicos para razonar, y modelos numéricos para aprender y adaptar su comportamiento analizando cómo se ve afectado el entorno por sus decisiones previas. De esta forma la IA propone imitar, emular o mimetizar el comportamiento de los seres humanos que, como se muestra en la figura 3.1, mediante los senti-

dos, perciben el entorno y adquieren datos, razonan con el conocimiento aprendido para inferir nuevos datos y conocimiento, ayudan en la toma de decisiones en el mundo físico o en el virtual para alcanzar el objetivo o resolver una tarea, y aprenden al analizar cómo el entorno se ve afectado por sus decisiones previas. Además, la tecnología de IA permite reconocer imágenes, realizar recomendaciones, predicciones y simulaciones, trabajar con el lenguaje al entender órdenes habladas, analizar textos escritos, generar nuevos textos, traducir y responder a preguntas, entre otras.

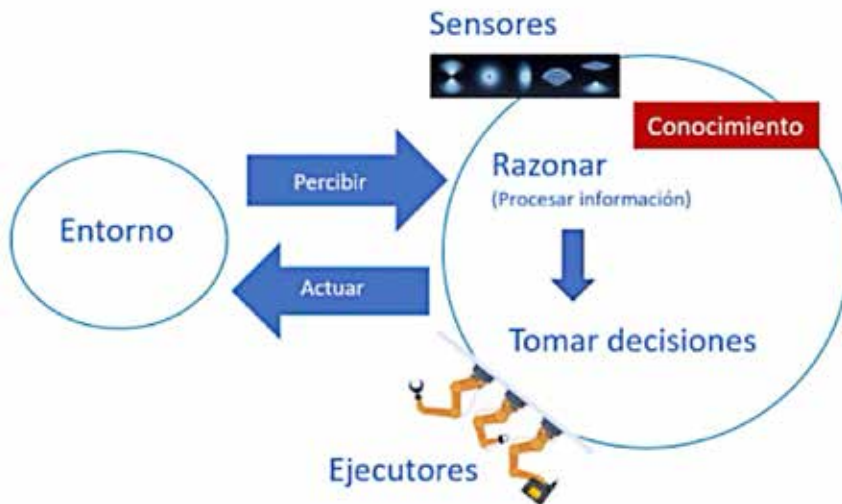


Figura 3.1 Percibir, razonar, decidir y actuar

Fuente: Adaptada de https://cs.brynmawr.edu/Courses/cs372/spring2012/slides/02_IntelligentAgents.pdf

3.1.2 Tipos de inteligencias artificiales

La inteligencia artificial surge como una disciplina científica de la informática, compartiendo métodos y técnicas con otras ciencias, como las matemáticas, la estadística, la psicología, la lingüística, la filosofía y la economía, entre otras. Actualmente se utiliza en multitud de aplicaciones en sectores como la ingeniería, la arquitectura, las ciencias de la salud, las finanzas, las humanidades digitales, el descubrimiento científico, entre otros.

En función de la complejidad de la tarea que la inteligencia artificial resuelve, la literatura distingue **tres tipos de inteligencias artificiales**. En nuestros días existen **muchas inteligencias artificiales específicas**, también llamadas especializadas, estrechas o débiles, que resuelven actividades concretas de forma muy satisfactoria. Así, una inteligencia artificial especializada y autónoma (a la que recientemente se le ha rebautizado con el nombre de «agente») puede crecer a medida que interactúa con otras inteligencias artificiales también especializadas; de esta forma se aproxima, mediante un proceso de

agregación, a una inteligencia artificial que resuelve más tareas y de mayor complejidad, acercándose así a la **inteligencia artificial general o fuerte** (en inglés conocida por el acrónimo AGI), que es aquella que puede imitar por completo todas las capacidades relacionadas con la inteligencia humana, como la resolución de tareas complicadas y heterogéneas, la planificación, el aprendizaje, el razonamiento o la capacidad de abstraer y generalizar.

En los últimos años ha surgido el término **inteligencia artificial generativa** (en inglés, *generative artificial intelligence GAI*). Se refiere a una **tecnología** que es capaz de generar textos, imágenes, videos, programas de ordenador, entre otros, y que pueden ser utilizadas para realizar tareas sencillas o complejas. Las técnicas de inteligencia artificial generativa se utilizan para construir agentes que realizan tareas sencillas con cierta autonomía y también sistemas multiagentes que de forma coordinada resuelven tareas de mayor dificultad.

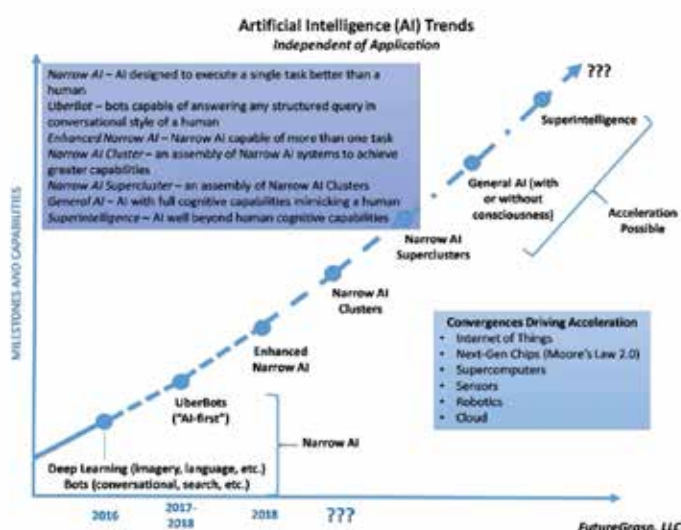


Figura 3.2 Kardashev Scale Analogy: Long-Term Thinking about Artificial Intelligence

Fuente: FutureGrasp, LLC. https://irp-cdn.multiscreensite.com/9297f8c7/files/uploaded/The%20Kardashev%20Scale-An%20AI%20Analogy_FINAL.pdf

3.1.3 De los datos a la toma de decisiones

3.1.3.1 La pirámide del conocimiento

El siglo XXI ha traído novedosas infraestructuras con importantes avances en los procesadores, en la capacidad de comunicación y almacenamiento de grandes volúmenes de datos, y en multitud de máquinas, dispositivos, aplicaciones y seres vivos interconectados en un

ecosistema multidominio. **Los datos multimedia generados en un mundo digitalizado han originado el tsunami de la inteligencia artificial.**

En esta revolución, **la inteligencia artificial está acompañada por otras tecnologías habilitadoras**, como la Web y la Web 2.0, la Internet de las cosas, el almacenamiento masivo de datos y la computación en la nube; las cadenas de bloques, tan empleadas en los ámbitos económico y financiero; y el metaverso, que nos llevará a una realidad híbrida, entre lo físico y lo virtual, y en el que disfrutaremos de la realidad virtual y de la realidad aumentada.

Al mismo tiempo, **la integración de la IA con otras tecnologías** como la computación cuántica, la computación neuromórfica, la neurotecnología o los chips implantados en humanos para incrementar sus capacidades físicas, cognitivas y de comunicación con otros dispositivos están contribuyendo también a esta revolución tecnológica. Todo ello permite incorporar tecnologías de inteligencia artificial para ayudar y asistir a las personas en muchas industrias y sectores de la actividad económica, en las administraciones públicas, en la investigación y en las actividades cotidianas que realizamos en el tiempo de ocio y en el hogar, y, por supuesto, en el sector de la defensa.

La **toma de decisiones en tiempo real** requiere de un intercambio de datos, y también de una interpretación consensuada de los datos y de los metadatos que se intercambian. La heterogeneidad en los protocolos de comunicación, en la sintaxis de los datos y en la semántica de los modelos puede originar problemas de interoperabilidad a la hora de intercambiar y de compartir datos. Todo ello sin olvidar otros aspectos importantes relacionados con la gobernanza, las duplicidades, las inconsistencias, el grado de certeza, la granularidad con la que está descrito el dato o su idioma. A ello se suman otras dimensiones no técnicas como son los aspectos regulatorios relacionados con el cumplimiento de las normas, la propiedad intelectual y los derechos de acceso, y los marcos contractuales entre proveedores y clientes.

La **pirámide de conocimiento** asiste en la cadena de valor que transforma el dato en conocimiento hacia la toma de decisiones. La pirámide del conocimiento (Borrajó *et al.*, 1993) es un modelo que se utiliza en inteligencia artificial para entender cómo se adquiere, organiza, representa y procesa la información de forma jerárquica, desde los niveles más básicos a los más complejos. Se estructura en cuatro niveles: datos, información, conocimiento y sabiduría (ver figura 3.3).

Cada nivel de la pirámide representa un tipo de conocimiento que se va construyendo sobre los anteriores para llegar desde el dato a la toma de decisiones en el nivel superior. El ejemplo de la figura 3.3 muestra cómo **los datos se transforman en conocimiento útil para la toma de decisiones.**

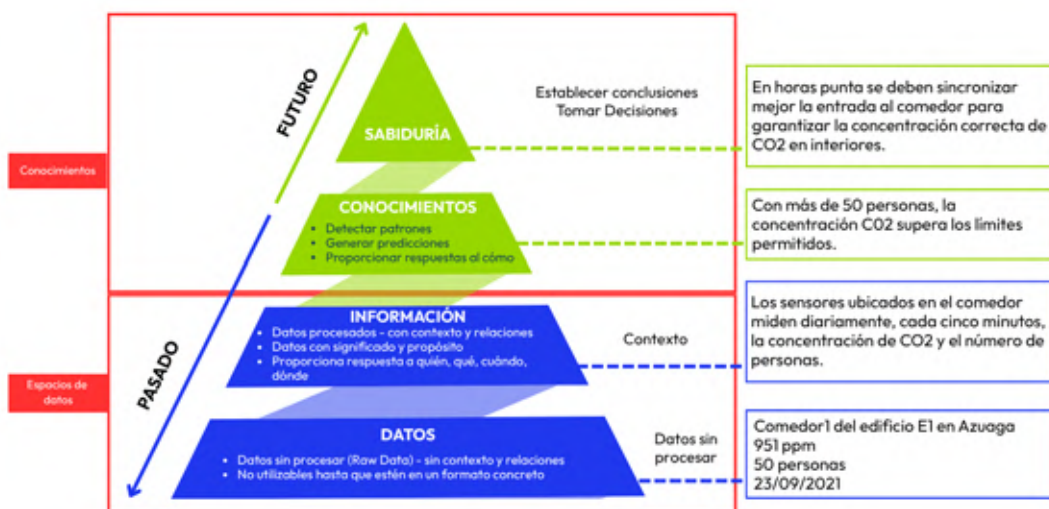


Figura 3.3 Pirámide de conocimiento

Fuente: Elaboración propia

El primer nivel de la pirámide son los **datos**. Los datos son los hechos aislados, sin contexto o interpretación. Además de los números, las palabras, observaciones o un registro oral, también son datos un documento, una imagen, una ruta, una huella dactilar, un iris, una onda de voz, un movimiento, una señal cerebral, un comentario en redes sociales, es decir, cualquier cosa que esté digitalizada. Los datos son fundamentales para que los modelos aprendan, razonen y tomen decisiones.

El segundo nivel de la pirámide es la **información**. En cualquier escenario, los datos han de ir acompañados de información adicional que recibe el nombre de **metadatos**. Los metadatos proporcionan el contexto que permite comprender mejor los datos; los metadatos aportan significado al dato y proporcionan información relevante sobre diferentes características que son útiles para la toma de decisiones, entre otras:

- **Autoría:** Especifica quién creó, recopiló, modificó e incluso borró el dato, si procede del enemigo o de fuentes aliadas, etc.
- **Formato:** Detalla el tipo de archivo o estructura del dato.
- **Tamaño:** Incluye la cantidad de espacio que ocupa el dato.
- **Tiempo:** Indica cuándo se obtuvo el dato.
- **Versionado:** Muestra los cambios o actualizaciones en el dato.
- **Procedencia:** Especifica el origen del dato, que puede ser un sensor, un dispositivo, una aplicación, una encuesta, o una persona.
- **Finalidad:** Describe el proceso que ha generado el dato.
- **Duración:** Señala la periodicidad de la medición.
- **Geolocalización:** Enmarca las coordenadas de la ubicación.

- ─ Idioma: Determina el idioma en el que está registrado el dato.
- ─ Licencias: Define las licencias de uso.
- ─ Privacidad: Precisa la protección de los datos personales.
- ─ Accesibilidad: Delimita quién puede acceder al dato y en qué condiciones.
- ─ Clasificación o nivel de seguridad: Acota las personas, aplicaciones, dispositivos, etc., que acceden a información clasificada en función de su nivel de seguridad.
- ─ Estado: Define si el dato es preliminar, está en observación, validado, en desuso, etc.

Organizaciones de normalización como el Consorcio de la *World Wide Web*, o el *European Telecommunications Standards Institute (ETSI)* están proporcionando **vocabularios consensuados para metadatar los datos** que proceden de proveedores de diferentes sectores en la Internet de las Cosas o en los datos generados por aplicaciones. Un metadatado rico ayuda siempre a mejorar la comprensión, trazabilidad y confiabilidad de los datos.

El tercer nivel de la pirámide es el nivel de **conocimientos**. En este nivel los datos y los metadatos se analizan para extraer patrones y tendencias, generar predicciones e intentar dar respuestas a hechos o experiencias previas. Tiene como finalidad interpretar, estructurar y organizar lo ocurrido para facilitar la resolución de un problema; en otras palabras, permite adaptarse a nuevas situaciones basándose en el aprendizaje previo. El análisis estadístico, la minería de datos, el aprendizaje automático, el cuadro de mandos, entre otras, son técnicas de análisis y procesamiento de la información que se utilizan en este nivel. Además, otras técnicas como las heurísticas, las taxonomías, las ontologías y los mapas conceptuales permiten crear modelos conceptuales o abstracciones para compartir conocimientos y datos dentro de una organización y entre organizaciones.

En este nivel, la simulación permite probar escenarios, bien en entornos virtuales o físicos, para acelerar la transferencia del conocimiento. En secciones posteriores se describe las técnicas de inteligencia artificial que permiten construir, razonar y aprender modelos computacionales.

El cuarto nivel en la pirámide es la **sabiduría**. En este nivel se utiliza el conocimiento para tomar decisiones o establecer conclusiones, siempre teniendo en cuenta el impacto económico, social, medioambiental, ético y legal de las decisiones. La toma de decisión origina una actuación sobre el entorno físico o virtual, lo cual nos lleva a la base de la pirámide de la Figura 3.3, pues el sistema vuelve a adquirir nuevos datos y metadatos representativos que son utilizados para, si procede, ajustar los modelos ya construidos en el nivel de conocimientos, y así mejorar con el paso del tiempo; de esta forma, el sistema puede generalizar mejor y aprende cómo el entorno se ve afectado por sus decisiones previas.

3.1.3.2 La cadena de valor del dato

Para que el sistema aprenda, razone o tome decisiones correctas de acuerdo con el marco regulatorio que en cada caso proceda es necesario analizar los procesos iterativos que

conforman la **cadena de valor** que permite llegar de los datos a la toma de decisiones (ver figura 3.4).

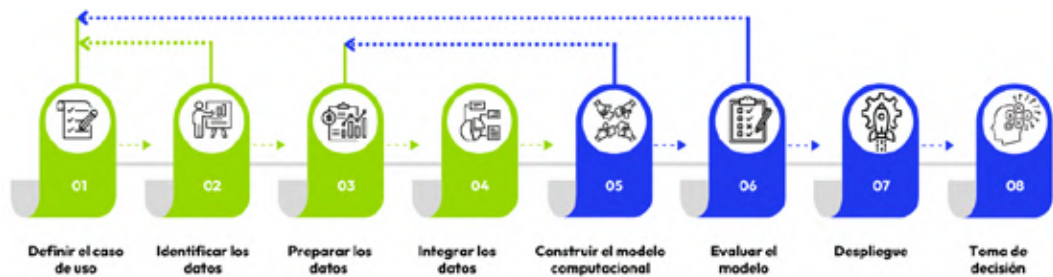


Figura 3.4 Cadena de valor del dato. Fuente: Elaboración propia

- 1. Definir con precisión el caso de uso y su alcance.** Es un proceso iterativo e incremental en el que se presta especial atención a comprender las capacidades cognitivas y las tareas que realizará el sistema. Por ejemplo, si se va a utilizar en la provisión de servicios digitales relacionados con la logística, o si el caso de uso será de predicción de operaciones de mantenimiento, o relacionado con la automatización de procesos que no requieren la intervención humana, o relacionado con el intercambio de datos en un contexto bilateral, multilateral o plurilateral.
- 2. Identificar la procedencia de los datos y metadatos** necesarios para implementar el caso de uso. Los datos y metadatos son fundamentales para que los modelos aprendan, razonen y tomen decisiones. Cuantos más diversos y de mayor calidad sean, mejor será el rendimiento del modelo. Ambos proceden de bases de datos, sensores, APIs, encuestas, tablas, documentos, imágenes, voz, páginas Web, etc.).
- 3. Preparar datos de calidad** es fundamental para obtener un sistema con inteligencia artificial preciso y confiable. Si los datos y metadatos no tienen la suficiente calidad los recursos humanos y materiales empleados en construir el modelo de inteligencia artificial serán infructuosos. Entre otros, los aspectos a comprobar son:
 - ─ Datos que pueden llevar a modelos poco precisos.
 - ─ Sesgos conscientes o inconscientes (relacionados con el sexo, la edad, etc.) que originan discriminación.
 - ─ Datos incorrectos procedentes de personas o de dispositivos. Por ejemplo, la medida de un sensor o de un dispositivo que no esté calibrado.

- ─ Valores numéricos, fechas, horas y unidades de medida diferentes que van a requerir de un proceso de normalización.
- ─ Datos procedentes de bulos o noticias falsas.
- ─ Datos duplicados, obsoletos, caducos, desusados o desactualizados, entre otros.

Adicionalmente, pueden surgir **problemas de naturaleza legal** cuando:

- ─ Se vulnera la privacidad al recopilar y utilizar datos personales sin permiso o datos sensibles como son los datos personales sobre la salud, biometría, financieros, religiosos, de orientación sexual, antecedentes penales, entre otros.
- ─ Los datos personales no han sido correctamente anonimizados.
- ─ Se recolectan datos de sitios web sin permiso.
- ─ Cuando se utilizan datos que fueron recopilados con un determinado fin para otros fines que no fueron autorizados.
- ─ Se utilizan datos o materiales para entrenar modelos sin autorización de sus creadores.
- ─ Se producen brechas en datos clasificados (no necesariamente de defensa) y acceden al dato personas o sistemas no autorizados.

4. Integración de datos y metadatos heterogéneos que están en diferentes formatos, idiomas, nivel de detalle, o contexto y se encuentran almacenados en infraestructuras distribuidas en organizaciones públicas y privadas. En esta etapa se aborda la interoperabilidad de los protocolos, la semántica del dato, las reglas de gestión, los mecanismos de seguridad, entre otros, para asegurar la interoperabilidad, compartición y el intercambio de datos entre actores.

En la estrategia de datos de la Comisión Europea (2020) se busca desarrollar un mercado único europeo de datos, procedan de fuentes públicas o privadas, que garantice la protección de datos personales, los derechos fundamentales, la seguridad, ciberseguridad y protección de consumidores, así como la legislación de sectores específicos. Su estrategia se basa en cuatro pilares: (1) crear un marco de gobernanza intersectorial para el acceso y uso de los datos, (2) una inversión de dos mil millones de euros para desarrollar infraestructuras, herramientas y arquitecturas de gobernanza; (3) el refuerzo de los derechos que tienen las personas sobre los datos que generan, y (4) la identificación de sectores estratégicos en Europa.

Para **incrementar la soberanía tecnológica en espacios de datos** la Unión Europea ya trabaja en definir una gobernanza participativa, y en el desarrollo de **infraestructuras federadas** y tecnologías que habiliten las normas de acceso a los datos y su uso por

parte de todos los actores bajo los principios FAIR¹⁵. La finalidad de estos principios es que las aplicaciones informáticas reutilicen y compartan los conjuntos de datos directamente, sin necesidad de la intervención humana. Para ello, los datos han de estar organizados y descritos de manera estandarizada, en formatos digitales, de forma clara y sin ambigüedad.

Los **espacios de datos** permiten a los proveedores mantener el control sobre sus datos, definir condiciones de uso y beneficiarse de la colaboración al impulsar nuevas oportunidades de negocio. Los sectores identificados son: la salud, la industria y logística, la agricultura, las finanzas, la movilidad, el turismo, el pacto verde, la energía, el sector público, el talento, los medios, la cultura, el lenguaje, y la investigación y la innovación.

Esta necesidad de compartición de datos también aparece en el ámbito de la defensa en el que existe una complejidad adicional por estar los datos clasificados y por la necesidad de identificar las circunstancias que habilitan el acceso bajo ciertos permisos. Por ello, el uso de datos sintéticos se ha generalizado en aquellos escenarios civiles y militares en los que no existen datos suficientes.

5. **Construir modelos computacionales** como reglas, ontologías, grafos de conocimientos, modelos estadísticos o grandes modelos generativos. Esta etapa puede requerir de nuevos datos que han de prepararse e integrarse. Las secciones siguientes presentan técnicas para construir modelos computacionales.
6. **Evaluar los modelos computacionales** para determinar su consistencia con los datos en el caso de uso. Si las métricas que se obtienen de la evaluación del modelo no reflejan o se desvían de la realidad, el problema puede estar en que los datos seleccionados no han sido los correctos, son insuficientes, están desactualizados o están sesgados. Si esto ocurre, hay que volver al principio del proceso para corregir lo que proceda. Antes de pasar al despliegue es importante verificar si el sistema da respuesta al caso de uso.
7. **Desplegar el modelo computacional** en la nube, local o en el borde una vez se haya comprobado que el sistema da respuesta al caso de uso con calidad y eficiencia.
8. **Toma de decisión.** Consiste en tener operativo el sistema de forma continua para que se alimente con nuevos datos y ayude en la toma de decisión, en la analítica, en la predicción, en la simulación, en la recomendación, etc.

¹⁵ El acrónimo FAIR procede del inglés *findable, accessible, interoperable and reusable* y se utiliza para calificar a los datos que habrían de satisfacer cuatro propiedades: ser fácilmente localizables en dispositivos, ser universalmente accesibles, estar operativos en diferentes contextos y con diferentes propósitos (Wilkinson *et al.*, 2016).

3.1.4 Modelos computacionales en inteligencia artificial

Para entender la evolución y el impacto económico, social, medioambiental, ético y legal de la inteligencia artificial conviene recordar que su evolución está ligada a los avances del hardware, al volumen de los datos, y a los modelos y algoritmos que representan el conocimiento y habilitan el razonamiento y el aprendizaje de modelos numéricos a partir de grandes cantidades de datos utilizando técnicas estadísticas y redes de neuronas artificiales. La figura 3.5 muestra las ramas de la inteligencia artificial: la **inteligencia artificial simbólica**, la **inteligencia artificial subsimbólica** y la **inteligencia artificial generativa**.

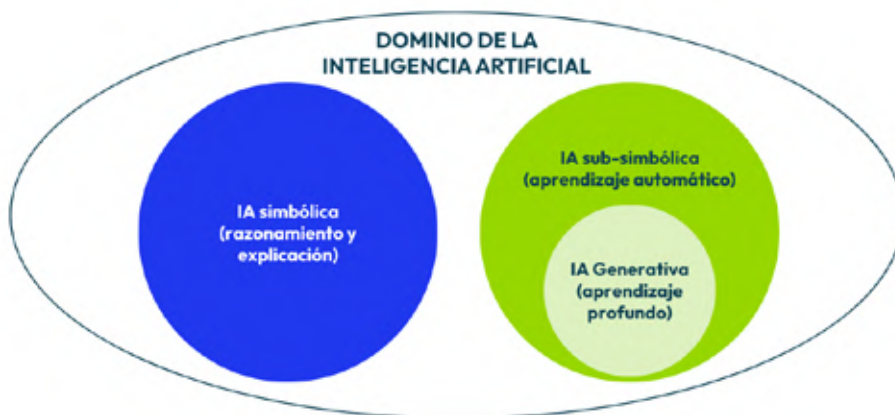


Figura 3.5 Ramas de la inteligencia artificial
Fuente: Gómez-Pérez (2024)

Aprender y razonar son los dos grandes pilares de la IA, tal como se indica en la figura 3.6 ligados a los tipos de IA indicados en la figura 3.5.

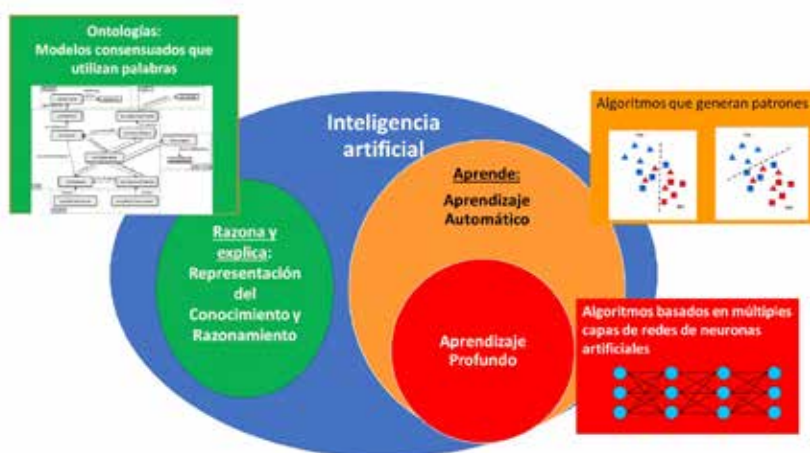


Figura 3.6 Técnicas para aprender y razonar
Fuente: Gómez-Pérez (2024)

Para que un sistema de inteligencia artificial aprenda, razone, decida y explique necesita **modelos computacionales**. Los modelos computacionales son abstracciones del mundo físico o virtual y en ellos se encuentra el conocimiento de dominio que necesitan los sistemas de IA para razonar, decidir, explicar y adaptar su comportamiento.

Los **modelos simbólicos**, que se corresponde con la rama de la IA que trata la representación del conocimiento y el razonamiento, se fundamentan en el álgebra de Boole (1854) y en las leyes de la lógica y por este motivo habilitan el razonamiento y la explicabilidad. Otros tipos de modelos, principalmente **modelos numéricos**, se construyen con algoritmos muy sofisticados que utilizan técnicas estadísticas muy avanzadas. También están los **modelos conexionistas** que se construyen con nuevas arquitecturas de redes de neuronas artificiales profundas que contienen múltiples capas y que aprenden representaciones o patrones muy complejos con miles de millones de parámetros a partir de grandes conjuntos de datos. Estos modelos mejoran el rendimiento humano¹⁶.

A continuación, se introduce brevemente el tema de las técnicas de inteligencia artificial que permiten construir modelos computacionales.

3.1.5 Representación del conocimiento y razonamiento

La representación del conocimiento y el razonamiento tuvo su auge durante todo el siglo XX en el desarrollo de **sistemas expertos**. En aquellos años, los investigadores se afanaron en el diseño de algoritmos y modelos computacionales que pudieran ejecutarse en infraestructuras muy limitadas y con pocos datos.

Para construir estos modelos computacionales, los ingenieros de conocimiento realizan entrevistas con expertos de dominios y también adquieren el conocimiento a partir de documentos especializados utilizando para ello técnicas de procesamiento del lenguaje natural que extraen los conceptos y relaciones más relevantes. Estas técnicas emplean **símbolos alfanuméricos**, es decir, palabras y reglas lógicas para representar, respectivamente, los datos y los conocimientos que los humanos tienen acerca de un dominio.

Los algoritmos que realizan el razonamiento emplean las reglas de la lógica para limitar las opciones de búsqueda y reducir la explosión combinatoria del espacio de búsqueda, así como para deducir nuevos datos y conocimiento a partir de los datos preexistentes utilizando métodos de inferencia generalmente deductivos. Por este motivo, las técnicas de la IA simbólica (Smith, 1982) facilitan la explicabilidad, lo que significa que pueden explicar sus decisiones, a diferencia de los modelos basados en redes de neuronas profundas. Las

¹⁶ Este documento no pretende realizar un recorrido histórico sobre la inteligencia artificial. Estos temas ya han sido ampliamente tratados en los discursos Inteligencia artificial y lengua española y en Ingeniería Ontológica (Gómez-Pérez, 2023 y 2024).

técnicas de representación del conocimiento más utilizadas son: la lógica, las reglas o heurísticas, las taxonomías, las ontologías y los grafos de conocimientos.

Modelos computacionales basados en reglas. Las **heurísticas** son estrategias o reglas basadas en la experiencia que sugieren cómo abordar un determinado problema (Buchanan y Feigenbaum, 1978; Shortliffe, 1976). Las heurísticas también se han utilizado en el desarrollo de sistemas expertos al representar el conocimiento utilizando estructuras del tipo «si... entonces...»; es decir, si se cumplen unas condiciones entonces el motor de inferencias ejecuta unas acciones y, de esta forma, deduce nuevos datos a partir de los preexistentes. El razonamiento deductivo procesa símbolos y tiene su fundamento en el concepto aristotélico de silogismo¹⁷. A partir de unos símbolos iniciales (que representan los hechos de partida), el sistema genera nuevos símbolos (que representan los hechos de la conclusión). Por ejemplo, a partir de la secuencia de símbolos «manzana(a)», mediante la regla «manzana(X) → fruta(X)», se obtiene la secuencia «fruta(a)».

Modelos computacionales basados en taxonomías. Las taxonomías son sistemas de clasificación jerárquicos que organizan los conceptos de un dominio en categorías o grupos según sus características comunes. Los conceptos se conectan con otros conceptos mediante relaciones de clasificación que permiten construir taxonomías en las que se manifiestan la hiponimia y la hiperonimia. Por ejemplo, el concepto «fragata 110» es más específico que el concepto «fragata», y éste más específico que el concepto «buque». Los conceptos también se relacionan mediante relaciones meronímicas o de agregación, que permiten representar las relaciones de «parte de» o «composición». Por ejemplo, un «árbol» está formado por las «raíces», el «tronco» y muchas «ramas».

Las **ontologías**. Son modelos computacionales consensuados y formales, pues están basados en lógica (Gómez-Pérez *et al.*, 2004). Además de incluir la taxonomía de conceptos de un dominio específico, la ontología incluye propiedades o atributos de cada concepto, relaciones o conexiones con otros conceptos, restricciones de los conceptos, reglas de inferencia y axiomas que se pueden entender como aserciones que suelen utilizarse para verificar la consistencia de la ontología, para realizar razonamiento temporal y deducciones, entre otros. De esta forma, las ontologías proporcionan definiciones (o significados) consensuadas que pueden ser reutilizadas y compartidas en y por numerosas aplicaciones y dominios. Se facilita así la integración de datos heterogéneos procedentes de diferentes sensores y sistemas a la vez que habilita la interoperabilidad o diálogo máquina-máquina, sin intervención humana, al proporcionar vocabularios consensuados en lenguajes formales¹⁸.

¹⁷ El silogismo es un método de razonamiento que consta de tres partes: dos premisas y una conclusión. Las reglas del silogismo describen las pautas del razonamiento humano y, al seguirlas paso a paso, posibilitan la deducción de conclusiones racionales a partir de las premisas iniciales.

¹⁸ Para una revisión detallada de estos conceptos se recomienda el libro *Ingeniería Ontológica* (Gómez-Pérez, 2024).

El consorcio de la *World Wide Web* proporciona ontologías ampliamente consensuadas por numerosas instituciones.

Los **grafos de conocimientos** son modelos computacionales que almacenan datos e información en forma de grafo. Los nodos del grafo representan los conceptos y las entidades (que son los datos junto a sus metadatos) y las aristas las relaciones entre conceptos, entre datos, de los datos con sus metadatos, y de los datos con los conceptos. Las ontologías se pueden utilizar para describir y conectar los conceptos del grafo de conocimiento de múltiples formas y así proporcionar semántica a los datos y metadatos del grafo. Los grafos de conocimientos se utilizan para conectar datos de distintas fuentes facilitando la agregación de información, la detección de inconsistencias, la búsqueda de la información, y habilitando también el razonamiento.

3.1.6 Aprendizaje automático y profundo

La IA que aprende a partir de grandes cantidades de datos se la conoce como IA subsimbólica o aprendizaje automático. **Los sistemas de aprendizaje automático se entrenan con datos para que puedan predecir nuevo conocimiento.** Los algoritmos de aprendizaje automático construyen modelos computacionales y estos modelos se utilizan para hacer predicciones, diagnósticos, resolver problemas de clasificación, encontrar similitudes y patrones en los datos, reconocer imágenes, procesar la voz y el lenguaje natural, controlar robots autónomos, entre otros; en otras palabras, el aprendizaje automático capacita a las máquinas para enseñarse a sí mismas y aprender sin ser programadas por un humano.

Una primera división de la IA subsimbólica considera **dos grandes grupos de técnicas**: las **estadísticas**, que generan patrones utilizando modelos probabilísticos a las que habitualmente se les llama “**aprendizaje automático clásico**”, y otras técnicas que intentan reproducir el proceso biológico del aprendizaje con algoritmos basados en **modelos computacionales bioinspirados en la estructura y el funcionamiento del cerebro**, como es el caso de las redes de neuronas artificiales con múltiples capas de procesamiento – el “**aprendizaje profundo**”.

Según el tipo de problemas que se abordan y la disponibilidad o no de datos etiquetados que puedan ser utilizados en el aprendizaje, las técnicas de aprendizaje automático se agrupan, de manera general, en las de **aprendizaje supervisado** (en las que hay datos etiquetados) y **aprendizaje no supervisado** (en las que no hay datos etiquetados). Asimismo, hay casos en los que es interesante que los modelos se vayan modificando de manera más frecuente -durante su funcionamiento, a partir del análisis de su estado y de las posibles acciones a realizar, hablando en este caso de técnicas de **aprendizaje por refuerzo**.

A lo largo de la historia de la IA, las técnicas de aprendizaje supervisado son las que han recibido mayor atención; y en su aplicación práctica en el ámbito de las empresas, industrial

y de Defensa, son también las técnicas dominantes, por lo que dedicaremos esta sección a explicarlas.

3.1.6.1 El ciclo de vida del aprendizaje supervisado

Los sistemas basados en aprendizaje automático y profundo son sistemas entrada-salida. Una vez desarrollados y puestos en marcha, se le ofrecen unos datos de entrada que pueden ser de formato textual, numérico, imágenes, audio, etc. (el formato que reconozca el sistema), y el sistema produce un resultado que corresponderá a una posible clasificación, o a una previsión del siguiente dato en el futuro (predicción).

Normalmente la información que se ofrece al sistema está compuesta por **varias medidas o características** del fenómeno que se pretende estudiar (una imagen de una pieza en una línea de fabricación a partir de la cual se obtienen las medidas 3D de la pieza; un conjunto de datos sobre la evolución de un paciente; valores de cotización en bolsa de varias acciones de interés); y **el sistema devuelve como resultado uno o varios valores en formato numérico** (la probabilidad de supervivencia de un paciente a los 5 años; los valores previstos para las acciones en el próximo mes), o **categorías** (pieza de alta calidad, pieza aceptable, pieza defectuosa).

Basándose en los resultados se definen y llevan a cabo acciones de control, algunas veces por parte de seres humanos (recomendación de cuidados médicos especiales para los pacientes), o por parte de elementos técnicos (casi siempre software, pero algunas veces hardware) como robots de bolsa que dan órdenes de compra/venta, o elementos de la cadena de fabricación que clasifican las piezas en varias líneas de acuerdo con su nivel de calidad. Esta segunda parte corresponde a lo que tradicionalmente se llama ingeniería de control y, recientemente, recibe el nombre de **agentes**.

La aplicación para la que se construye el sistema determina que el esfuerzo de desarrollo se oriente hacia el desarrollo informático asociado a un sistema de información, o si va a funcionar controlando un sistema físico, por ejemplo para dotarle de autonomía como sería el caso de un sistema de guiado autónomo de un dron, es necesario construir o conectar el sistema de aprendizaje con los sensores de los que va a tomar los datos de entrada, desplegarlo en procesadores especializados como son los embarcados, y conectar la salida con el sistema de operaciones de vuelo. De ser así, hablaríamos de **ingeniería de sistemas**, que son los casos más importantes de la aplicación de la IA en Defensa.

La parte del sistema que convierte las entradas en salidas es el modelo de aprendizaje, que se construye utilizando algoritmos existentes y ya implementados en forma de bibliotecas a las que, en vez de añadir a mano el código para calcular el siguiente valor de una serie temporal (p.ej. para determinar si la pieza es válida o no, o para obtener las medidas de ésta a partir de una imagen), o se crea un modelo de aprendizaje que contiene inter-

namente las operaciones y criterios de selección representadas de forma numérica (en forma de matrices de muchas dimensiones); y es el algoritmo el que va seleccionando los umbrales de decisión, los pesos de las relaciones entre elementos, rellenando las matrices y ajustando estos valores (que pueden ser millones de ellos). Este proceso se denomina **entrenamiento** y es específico de los sistemas de aprendizaje supervisado.

Así pues, **siempre existe un elemento software que es necesario desarrollar para construir un sistema basado en aprendizaje**, por lo que es imprescindible hacer referencia a la ingeniería del software. Basada en los enfoques clásicos de ingeniería, divide las actividades de construcción en grandes bloques de análisis de requisitos, diseño de la solución, implementación, validación y mantenimiento.

Los **métodos ágiles y SCRUM** son los enfoques modernos adaptados al ámbito industrial; se basan en que el producto va mostrando su utilidad de forma temprana y se va refinando gradualmente con la incorporación de nuevas funcionalidades en ciclos rápidos de desarrollo (sprints)¹⁹.

Aunque también existen en la literatura **modelos de procesos de desarrollo de sistemas basados en datos**, como KDD o CRISP-DM, se podría decir que la construcción de estos sistemas ha sido más guiada por los conocimientos prácticos del equipo de desarrollo (en una suerte de “artesanía” de sistemas) que por los procesos de desarrollo académicos. En los últimos años con la popularización de la ciencia de datos, la disponibilidad de conjuntos de datos (*datasets*) y de capacidad de cálculo para procesarlos, la práctica industrial ha ido incorporando los procesos de desarrollo basados en datos con los modernos de desarrollo de software general, apareciendo variantes como SCRUM-CRISP que facilitan la realización de estos sistemas con un enfoque de ingeniería del software.

Realmente, los sistemas de aprendizaje tienen una peculiaridad importante que es obligado tener en cuenta para asegurar el éxito de su desarrollo: la principal es que **el diseño del sistema incluye un proceso de entrenamiento del modelo**. Para entrenar el modelo es necesario disponer de datos de los mismos elementos sobre los que se van a tomar medidas cuando el sistema completo esté en funcionamiento, de los mismos sensores y formatos; y dada la base estadística de los modelos, cuantos más datos, de mejor calidad y más variados sean posiblemente se obtengan mejores resultados. También, como los algoritmos de generación de modelos van refinando los valores internos a base de iteraciones de lectura de los *dataset*, cuantas más iteraciones se hagan mejor calidad se obtendrá. Pero dada la naturaleza combinatoria compleja de los modelos, no es posible conocer la calidad de los resultados hasta que no se construyen los modelos y se prueban (con más

19 SCRUM: Scrum es un marco de trabajo ágil que ayuda a los equipos a organizar y gestionar su trabajo de manera iterativa e incremental, entregando valor en cada ciclo de desarrollo, llamado “sprint”.

datos, normalmente una parte del *dataset* original que se ha reservado para este efecto y no se ha usado en el entrenamiento).

Las **fuentes de datos** (*dataset* en inglés) son un elemento central en la construcción de los sistemas de aprendizaje supervisado; lo que el modelo aprenda durante su fase de entrenamiento está únicamente basado en lo que vea ahí. Si no se le presentan casos con una determinada característica, el modelo no va a tener información para decidir con base en esa característica. Si una característica aparece muy pocas veces en los datos, el modelo no va a poder predecir su aparición con garantías de calidad (la literatura lo denomina como “eventos raros”, Shyalika *et al.*, 2024) y a pesar de contar con técnicas particulares para mejorar la calidad de las predicciones, se reconoce que el grado de acierto es muy bajo.

Las **técnicas de entrenamiento de los modelos de aprendizaje supervisado** tienen, todas, una base común. Se comienza con una propuesta de valores numéricos para cada variable o parámetro del modelo (los pesos de las conexiones entre neuronas, por ejemplo), se toma una muestra de datos etiquetados de las fuentes de datos y se genera un resultado de aplicar el modelo con esos valores iniciales sobre esa muestra de entrada. Este resultado se compara con el resultado que debería de haberse obtenido (esta información está en el *dataset* de entrada en forma de valores de salida esperados para cada entrada, llamados *etiquetas*), y se calcula el error entre lo que se ha obtenido realmente y lo que se esperaba. Si el error es nulo, no es preciso hacer nada más con esta muestra de entrada y podemos pasar a repetir la operación con la siguiente entrada del *dataset*. Si por el contrario hay error, tenemos que cambiar ligeramente los parámetros del modelo buscando reducirlo, y probar de nuevo repitiéndolo hasta que se minimiza el error, antes de pasar a la siguiente muestra.

Cada recorrido completo de entrenamiento usando todos los datos de entrada del *dataset* se llama **época** y, por supuesto, es un proceso tanto más largo cuanto mayor sea el *dataset*, mayor sea el número de parámetros del sistema a entrenar y mayor sea el número de iteraciones de entrenamiento.

Las técnicas de entrenamiento se fueron haciendo más sofisticadas según se proponían algoritmos y métodos más refinados. Llegó un momento durante la segunda mitad de la década de los 80 del siglo XX en que los modelos empezaron a crecer exponencialmente en tamaño y número de parámetros con el aprendizaje profundo. Es el momento en el que se propone el **algoritmo de retropropagación** (Rumelhart, 1986), que permite propagar los cambios necesarios para reducir el error entre un resultado obtenido y uno esperado para una entrada, desde la última capa a la anterior y así sucesivamente hasta la capa de entrada (regla de la cadena), atribuyendo a cada parámetro del modelo la parte que le corresponde en el error final mediante el mecanismo de descenso del gradiente. Aplicado varias veces para cada entrada del *dataset*, y con varias pasadas sobre el *dataset* completo (épocas), los parámetros del modelo van acercándose a los valores ideales sin error, hasta que se estabilizan.

El **sistema va aprendiendo** porque (todos) los pesos de las conexiones entre neuronas, tanto las conexiones hacia adelante (multicapa, CNN, *autoencoders*), como las hacia atrás (recurrentes), van variando cada vez que se le ofrece una muestra del *dataset* y se compara el resultado esperado con el obtenido.

El algoritmo de retropropagación en el entrenamiento ha contribuido a manejar modelos complejos de aprendizaje profundo, pero la explosión del aprendizaje profundo que se ha observado en la segunda década del siglo XXI sólo ha sido posible porque existen ***datasets de entrenamiento suficientemente grandes*** en algunos dominios de actividad (por ejemplo: registros médicos incluyendo bancos de imágenes médicas, volcados de actividad de redes sociales o rastros de navegación en la web, elecciones de consumidores de bienes o servicios); porque se dispone de sistemas software-hardware para almacenar y procesar estos datos masivos (GPUs para entrenamiento de modelos profundos, sistemas como Apache Kafka para el tratamiento de flujos de datos en tiempo real); y por supuesto, porque hay casos de negocio que aseguran la rentabilidad de la inversión necesaria para el desarrollo primero experimental en los laboratorios de investigación de las universidades y luego industrial en las empresas innovadoras.

Animados por un caso de negocio rentable, encontramos que **muchos de estos desarrollos se vieron impulsados por las grandes plataformas de negocio digital que disponían de los datos masivos** (obtenidos de los usuarios), **de la infraestructura** para entrenar modelos (grandes centros de tratamiento de datos con procesadores especializados), y de la **expectativa de retorno de la inversión** al ofrecer servicios basados en sistemas de aprendizaje profundo. La explosión de la IA generativa para proceso de lenguaje natural cumple hoy en día con estas condiciones.

Pero también aparecen nuevos problemas -no solo técnicos- a medida que aumenta el rango de aplicaciones. Un problema tiene que ver con la **obtención y uso del dataset**: ¿Es fiable? ¿Es veraz? ¿Se puede acceder libremente o está protegido por derechos? En todo el mundo hay ya normativa para proteger la privacidad de los usuarios de los servicios digitales, así que recoger, tratar, distribuir, vender sus datos puede no ser posible. También puede ocurrir que los datos recogidos tengan sesgos de diferente tipo y por lo tanto a menos que se neutralicen estos sesgos, se transmitirán a los resultados del sistema. Estas cuestiones que suponen un riesgo para el desarrollo de la IA han dado lugar al campo de análisis denominado Ética de la IA²⁰.

A la hora de **validar un modelo basado en aprendizaje automático** aparecen más dificultades derivadas de la naturaleza no determinista de sus métodos. Bien puede ocurrir que después de un costoso proceso de entrenamiento, los resultados no alcancen los niveles

²⁰ La dimensión ética relacionada con IA en el sector defensa será abordada en el capítulo 6 de este informe.

de calidad necesarios para su puesta en producción. Los modelos de proceso cuentan con vueltas hacia atrás que obligan a repetir parte del proceso de selección de las características de la entrada, a elegir otro algoritmo de modelado, o bien otra combinación de parámetros del algoritmo (hiperparámetros). Por otra parte, la certificación de estos sistemas puede ser complicada en nuestros días, lo que frena su uso en algunos dominios de aplicación.

En cualquier caso, esto implica que la construcción de modelos no solo sea costosa, sino también arriesgada, lo que supone una barrera de entrada para las empresas que tienen que construir aplicaciones basadas en estos sistemas, que, a veces, pueden preferir comprar un modelo preentrenado y adaptarlo a sus necesidades, a desarrollarlo por ellas mismas desde cero.

Esto tiene más implicaciones de las que pudiera parecer. En el caso de su uso en defensa: ¿Sería posible para un ejército comprar un modelo de decisión entrenado en otro país, amigo o neutral, sin poder estar seguro de las condiciones y **dataset con el que se ha entrenado** ¿Es posible asegurar que el modelo no tendrá puertas traseras?

Volviendo a los aspectos puramente técnicos, una vez que se cuenta con los modelos entrenados que han alcanzado los niveles de calidad esperados, viene su fase de implementación y puesta en marcha para dar el servicio para el que se han diseñado. Se llama **inferencia** a la fase en la que el sistema está funcionando: recoge entradas, las pasa a las capas de entrada, se realizan las operaciones matemáticas de ejecución de los modelos y proporciona los resultados. No hay vueltas atrás, no hay iteraciones y **las operaciones son mucho más sencillas** -básicamente las sumas y multiplicaciones de las matrices que se han obtenido como resultado del entrenamiento-.

Se presentan a continuación tres escenarios ampliamente utilizados:

Escenario 1. Si el sistema va a recoger entradas en el mismo centro de proceso de datos y los resultados se van a proporcionar a los usuarios a través de la Web, basta con poner a funcionar los modelos en ordenadores en la misma instalación, posiblemente compartiendo la memoria o el almacenamiento con los ordenadores de entrenamiento. **Los equipos que realizan las inferencias no necesitan tantos recursos como los de entrenamiento**, así que los más potentes se reservan para entrenamiento y los otros se dejan para inferencia.

Escenario 2. Algo diferente ocurre si el sistema va a tener que **funcionar tomando la información de sensores que van recogiendo información del mundo físico**. El primer modelo de despliegue, y que aún se usa, se llama **sensors-to-cloud**; a través de la red los sensores entregan sus datos a los ordenadores de inferencia que están en la nube. De esta forma contamos con los ordenadores del centro de proceso de datos para inferencia; no son tan potentes como los de entrenamiento, pero aun así tienen recursos más que de sobra para la inferencia por muchos sensores que haya conectados. El problema es que todos los datos

viajan a través de la red, lo que puede conllevar riesgos de seguridad de los datos, y una latencia apreciable que impide que los resultados de la inferencia estén disponibles cuando se necesitan -que es cuanto antes en un problema de tiempo real.

Escenario 3. Aquí se está explorando una solución que consiste en **llevar los modelos entrenados a procesadores en el borde de la red, conectados a los sensores que producen los datos de entrada por rápidas redes de acceso**. Con este enfoque se mejora la latencia, pero, por contra, los procesadores disponibles en el borde de la red no tienen la potencia y recursos de los que hay en el centro de proceso de datos. La solución para poder desplegar los modelos en estos procesadores de menores capacidades consiste en **reducir los modelos** (con técnicas como la cuantización, poda, destilación, etc.), a costa de menguar sus niveles de calidad (Rosendo *et al.*, 2022).

Por último, una vez funcionando los modelos, **puede ocurrir que el comportamiento del fenómeno que trata de predecir el sistema de aprendizaje vaya cambiando con el tiempo, dejando obsoleto el modelo obtenido durante la fase de aprendizaje**. Esta deriva de concepto (*drift*) está siendo estudiada desde el punto de vista científico; mientras se llega a conclusiones, la estrategia práctica consiste en ir comprobando, durante su inferencia, si la tasa de aciertos/errores del modelo varía significativamente con el tiempo. Si cae por debajo de cierto umbral, **el modelo debe reentrenarse con un *dataset* actualizado** siguiendo todo el proceso descrito, y redespigarse sobre el mismo entorno de ejecución para seguir siendo útil. Las actividades de gestión de los modelos se engloban bajo una disciplina práctica llamada **MLOps** (operaciones sobre modelos de aprendizaje automático).

3.1.7 La revolución de la inteligencia artificial generativa

En los últimos años hemos asistido al desarrollo de nuevos algoritmos de aprendizaje que han dado lugar a la **inteligencia artificial generativa**. La IA generativa tiene su fundamento en **técnicas de aprendizaje automático basadas en redes de neuronas**.

Antes de entrar en los detalles técnicos y en aras de una rápida comprensión se explica de forma intuitiva cómo aprende un modelo de lenguaje. Durante el aprendizaje, la arquitectura neuronal genera patrones de conexiones entre las «palabras» que suelen aparecer juntas o relacionadas en diferentes partes de una oración. Con esta técnica se empezó a aprender el orden de las «palabras» en problemas de predicción de secuencias de texto. Estos modelos conocen la probabilidad de una secuencia de «palabras» en un lenguaje, pueden predecir las «palabras» que siguen a las que le precede y manejan representaciones numéricas de la información, como valores escalares, vectores o matrices. Por ello, para la creación de un gran modelo de lenguaje, se requiere un gran corpus de textos que permita aprender el vocabulario en él empleado y la relación entre las «palabras» que lo conforman. Las técnicas de aprendizaje profundo aprenden patrones de regularidad, de manera que aquello que es

poco frecuente en el texto se pierde. Con más textos, los patrones estadísticos se calculan mejor y la elección de las palabras en cada contexto será más precisa (Gómez-Pérez, 2023).

Los modelos de lenguaje, en versiones más avanzadas, han dado lugar a los grandes **modelos de lenguaje** (*Large Language Models – LLM*), a los **modelos de difusión** (*Difussion Models*), a los **modelos fundacionales** (*Foundational Models*), a los **pequeños modelos de lenguaje** (*Small Language Models*), a los **modelos cuantificados** (*Quantized Models*) y a los **modelos destilados** (*Distilled models*). A lo largo de esta sección se definirán los conceptos nucleares de estos modelos y las relaciones entre ellos.

3.1.7.1 Construcción de modelos

Para construir un modelo se necesitan extraordinarias cantidades de datos que reciben el nombre de **datos de entrenamiento**, también llamados **corpus**. Estos modelos se han «alimentado» con grandes volúmenes de textos, imágenes, música, vídeos, programas de ordenador, entre otros²¹.

La arquitectura denominada “**Transformers**”²² (Vaswani et al., 2017) ha introducido dos conceptos que servirán para comparar y describir los modelos: los **tokens** y la **atención**. El **token** es la **unidad mínima de significado**. En el lenguaje escrito, la palabra es la unidad mínima, mientras que en una imagen es un píxel. Para las lenguas que utilizan el alfabeto latino, la unidad mínima de descomposición son las palabras y combinaciones de caracteres alfanuméricos separados por espacios o símbolos.

Representar todas las palabras y posibles combinaciones de un idioma o varios supone un problema debido a las dimensiones que se necesitan para que todo el vocabulario sea reconocido por una red de neuronas. Un avance para limitar el número máximo de tokens fue la **tokenización de palabras en subpalabras** (*subtokens*), que divide las palabras en fragmentos en base a las frecuencias de los símbolos más repetidos dentro del corpus, hasta alcanzar el máximo de *tokens* que se haya elegido. Esta solución mejora la flexibilidad del procesamiento del texto, asegurando que palabras desconocidas tengan una representación adecuada²³.

En este contexto, hay que diferenciar entre **el tamaño del vocabulario** que se refiere al número de tokens que reconoce el modelo, y la **longitud de tokens de entrada** que define los tokens que puede procesar al mismo tiempo. Los primeros modelos que se hicieron con

21 Pocas veces se han respetado los derechos de autor de las obras protegidas y no siempre los creadores de los modelos hacen públicas las fuentes utilizadas.

22 Aparecida por primera vez en 2017 en el artículo “*La atención es todo lo que necesitas*” de Google, la arquitectura “transformador” (“Transformer”) está en la base de modelos de lenguaje de vanguardia de OpenAI.

23 La técnica utilizada se llama *Byte-Pair Encoding (BPE)* (Sennrich et al., 2016) que normalmente se usaba para compresión de información.

esta técnica tenían un vocabulario muy reducido de *tokens*. Los modelos actuales pueden superar los 128.000.

Un sistema que genere *tokens* solo a partir de textos en inglés descompondría la expresión en inglés «artificial intelligence» en 3 subtokens: «artificial», «intel», «ligence». El mismo tokenizador, al procesar la expresión en español «inteligencia artificial» podría dividirla en los siguientes subtokens: «intel», «igen», «cia» y «artificial». Una vez obtenidos los tokens, el tokenizador les asigna unos **identificadores numéricos** que son propios. En este ejemplo, [494, 20345, 1356] para la expresión en inglés, y [20345, 17514, 12354, 494] para la expresión en español. Obsérvese que el identificador 494 es para el token «artificial» que aparece en ambas expresiones de ambos idiomas, y que «intelligence» e «inteligencia» tienen dos y tres *subtokens* respectivamente.

Los *tokens* que se generan dependen de los textos que se han utilizado para el entrenamiento y de la representación de idiomas en los textos. Por ello, cada compañía que genera un modelo de lenguaje desde cero tiene su tokenizador y sus identificadores. Los identificadores numéricos se transforman en vectores llamados «embeddings» que «viajan» por los diferentes módulos de la arquitectura del modelo durante el entrenamiento. Las arquitecturas de los modelos actuales son variaciones de la arquitectura *transformer* original.

El tamaño de los modelos de lenguaje se mide por el número de parámetros. Un **parámetro** en redes neuronales es una **variable ajustable del modelo que se aprende durante el entrenamiento para optimizar su rendimiento en una tarea**. En modelos de tipo *Transformer*, los parámetros incluyen los **pesos y sesgos** de las capas neuronales, que determinan cómo se procesan y transforman los datos de entrada. Además, estos modelos también tienen parámetros específicos de sus **mecanismos de atención**, que permiten capturar dependencias contextuales entre palabras. Generalmente, **existe una relación directa entre el número de parámetros con su rendimiento**, cuantos más parámetros se tienen, más posibilidades tiene el modelo de aprender y generalizar.

Los **mecanismos de atención** ya se utilizaban en la traducción de textos, donde era crucial aprender, entre otras tareas, el género del sustantivo. Por ejemplo, en «the moon», el artículo «the» debe traducirse al español como «la» pues se debe prestar atención al sustantivo «luna» que es femenino en español. **El mecanismo de atención en la arquitectura *Transformer* permite que todas las palabras se relacionen entre ellas.** La arquitectura neuronal resultante genera **patrones de conexiones entre las palabras** que suelen aparecer juntas o relacionadas en diferentes partes de una oración.

Estas dos innovaciones unidas, la atención y la tokenización, originan la nueva generación de modelos de procesamiento de lenguaje natural (PLN); los llamados **modelos de lenguaje**. La arquitectura *Transformer* se compone de dos grandes módulos que calculan la atención: el **codificador** (*encoder*) y el **decodificador** (*decoder*). En el codificador se calcula la aten-

ción de toda la secuencia de tokens de entrada, es decir, de todos los tokens con todos los tokens. Sin embargo, el decodificador calcula la atención solo hacia los tokens anteriores, sin poder observar las palabras futuras en la secuencia.

Los investigadores de la empresa *Open AI* solo emplearon el módulo de decodificador para su uso como **modelo de lenguaje**. En este contexto, un modelo de lenguaje estima la probabilidad de que una secuencia de palabras sea “válida”. La validez no se refiere a la validez gramatical, sino a su similitud con los datos utilizados durante el entrenamiento.

En 2018, Open AI publicó el primer modelo de la familia GPT (*Generative Pre-Trained*) con 11 millones de parámetros (Raford *et al.*, 2019, p. 9). Este modelo utilizaba un decodificador como modelo de lenguaje y un corpus en inglés llamado *BookCorpus* (Zhu, 2015).

Una vez entrenado el modelo se podía usar, mediante un **proceso de ajuste fino** (en inglés *fine-tuned*) para mejorar su rendimiento en varias tareas de PLN. **Al realizar un ajuste se parte de unos tokens ya prefijados y con unos parámetros ya inicializados**. El ajuste instruye al modelo para que responda a preguntas, como un ChatGPT. Sin embargo, si lo que se desea es adaptarlo a un dominio concreto, es necesario recopilar un corpus específico sobre la temática. El **corpus de entrenamiento para el ajuste** lo formarían los documentos especializados en el idioma seleccionado, la legislación sobre la materia, un histórico de datos numéricos, un conjunto de preguntas con sus respuestas, unos manuales técnicos, entre otros, que han de prepararse con el formato que el modelo espera. Como ya se ha mencionado, las épocas son el número de iteraciones en las que el nuevo corpus pasa por el algoritmo para realizar pequeños ajustes en los parámetros del modelo, de forma controlada, usando una tasa de aprendizaje para controlar el impacto de los cambios en los parámetros (por ejemplo, permitir actualizaciones inferiores a 0,0001) y para evitar que el modelo olvide lo que ya sabía.

Este nuevo paradigma de usar modelos de lenguaje con ajustes permitía que cualquier tarea de PLN no partiese desde cero, pues el modelo ya tenía información sobre el comportamiento del lenguaje y las relaciones entre sus palabras. El modelo GPT, al utilizar la **atención enmascarada** (solo se fija en el pasado) es adecuado para tareas de generación de texto, razón por las que se les **denomina modelos generativos**.

Ese mismo año, Google propone BERT (Devlin *et al.*, 2019), un modelo de lenguaje que utiliza únicamente el codificador. Para su entrenamiento utilizaron *BookCorpus* y Wikipedia y lo ajustaron para las mismas tareas para las que se entrenó GPT, y así poder compararse y probar su rendimiento. Gracias a su atención completa, estos modelos son eficaces en tareas de extracción o de representación.

En los años sucesivos se han desarrollado modelos de lenguaje con más tokens, con más parámetros, con más datos que contienen datos multimedia (texto, audio, imagen, video)

y textos en varios idiomas, si bien los textos en inglés son mayoritarios. Con la aparición de GPT-3 (Shyam *et al.*, 2020) que contaba con 175 billones americanos de parámetros se empieza a hablar de **Grandes Modelos de Lenguaje** (Large Language Models, LLM). Estos modelos están diseñados para comprender y generar texto en múltiples idiomas. Esto les permite ser eficientes en tareas como la traducción automática, el resumen de textos, la clasificación de texto y el análisis de sentimientos en diferentes lenguas. Ejemplos de modelos que siguieron a GPT-3 fueron Bloom (HuggingFace) (Le Scao *et al.*, 2023) o Flan T5 (Google) (Chung *et al.*, 2024).

En definitiva, estos modelos son **modelos matemáticos que aprenden a imitar o reproducir la distribución de los datos que les proporcionamos y se construyen mediante arquitecturas complejas que mezclan redes de neuronas y mecanismos de atención**. Estos modelos son capaces de generar nuevos contenidos una vez que han sido entrenadas con grandes volúmenes de datos; si se entrenan con textos, los sistemas generarán nuevos textos; o si se entrenan con imágenes, vídeos y música, los sistemas generarán nuevas imágenes, vídeos y música; o si se entrenan con código fuente, los sistemas generarán nuevo código fuente. Muchas empresas están comercializando sus modelos como multimodales y multilingües, lo que significa que pueden procesar texto en diferentes idiomas, imagen, video y sonido al mismo tiempo. A estos modelos se les llama **modelos fundacionales**. Los modelos fundacionales pueden clasificarse según las técnicas y arquitecturas usadas:

1. **Modelos basados en Transformers:** se basan en la arquitectura de codificador, decodificador, o de ambos. Son eficientes para modelar relaciones en secuencias de datos (texto, imágenes, música). Ejemplos de estos modelos son LLaMA (Touvron *et al.*, 2023), RoBERTa (Liu *et al.*, 2019) y Vision Transformers (ViT) (Dosovitskiy *et al.*, 2021).
2. **Modelos de difusión:** la técnica consiste en generar ruido a partir de los datos de entrada para, poco a poco, aprender a reconstruir los datos originales y así aprender patrones. Se emplea en modelos fundacionales que generan imagen y vídeo. Ejemplos de estos modelos son Stable Diffusion (Rombach *et al.*, 2022) o Sora (OpenAI, 2024).
3. **Modelos basados en redes generativas antagónicas (Generative Adversarial Networks, GANs):** se construyen utilizando dos redes de neuronas llamadas generador y discriminador que compiten entre sí para generar datos, normalmente usado en generación de imágenes. Ejemplos de estos modelos son BigGAN (Brock *et al.*, 2019) y GauGAN (Park *et al.*, 2019).

Los modelos fundacionales también se pueden clasificar según las tareas para las que están preparados:

1. **Modelos de Lenguaje Grande** (LLMs – Large Language Models): basándose en la arquitectura *Transformers* están preparados para procesar y generar texto. Ejemplos de estos modelos son los GPT (Radford *et al.*, 2019; Shyam *et al.*, 2020; OpenAI, 2023) LLaMA, Falcon (Penedo *et al.*, 2023) o Mistral (Jiang *et al.*, 2023).
2. **Modelos Multimodales** que trabajan con múltiples tipos de datos como texto, imágenes o audio, etc. Ejemplos de estos modelos son Gemini (Team *et al.*, 2023) y CLIP (Radford *et al.*, 2021).
3. **Modelos de Visión Artificial** o vídeo que funcionan en el reconocimiento y generación de imágenes y vídeos. Ejemplos de estos modelos son ViT, Stable Diffusion y Sora.
4. **Modelos de Audio y Voz** que habilitan el reconocimiento y generación de audio y voz. Como ejemplo representativo se cita a Whisper (Radford *et al.*, 2022).
5. **Modelos de Representación y Embeddings** que generan representaciones de texto en espacios vectoriales. BERT, RoBERTa.
6. **Modelos de Código** que ayudan en la generación y creación de código de programación. Ejemplos de estos modelos son Codex (Chen *et al.*, 2021) o Code LLaMA (Roziere *et al.*, 2023).
7. **Modelos de Biología y Química** que analizan estructuras moleculares como AlphaFold (Jumper *et al.*, 2021).

La gran mayoría de modelos fundacionales son abiertos y se pueden descargar. Actualmente, el mayor repositorio central de modelos fundacionales es HuggingFace²⁴ en el que desarrolladores e investigadores de LLMs de todo el mundo publican y describen sus modelos para que la comunidad pueda usarlos. Además, este repositorio provee de librerías de código para desarrolladores, datos de entrenamiento, computación y la opción de publicar aplicaciones con modelos dentro su infraestructura.

Para el **caso concreto del español**, el primer modelo desarrollado fue BETO en (2019) (Ho *et al.*, 2020) que se basaba en un modelo BERT. Los siguientes fueron los de MarIA en 2022 (Gutiérrez Fandiño *et al.*, 2022), RigoBERTa (Serrano *et al.*, 2022) e IXAes (Agerri y Agirre, 2022) que se basaron en modelos RoBERTa y GPT-2. En los modelos MarIA se utilizó un corpus de más de 600 Gigabytes de la Biblioteca Nacional Española. En estos últimos años ya han aparecido LLMs como como Aguila siguiendo el modelo de FALCON, y Salamandra (González-Agirre *et al.*, 2025) y ALIA²⁵ siguiendo los modelos LLaMA.

²⁴ Disponible en línea: <https://huggingface.co/>

²⁵ <https://alia.gob.es/>

ALIA está diseñado para 35 lenguas de Europa incluyendo las lenguas cooficiales españolas, catalán, gallego, valenciano y vasco. **El modelo ha sido entrenado reduciendo significativamente los textos en inglés a un 39% e incrementando los textos en español a un 16%.** El proyecto ha sido coordinado por el *Centro de Supercomputación de Barcelona*. ALIA cuenta con variantes 2B, 7B y 40B y está publicado con licencia abierta. Para su entrenamiento se han utilizado textos de 35 idiomas europeos y el tokenizador ha generado 6,9 billones de *tokens* nuevos. Esto permite que el modelo segmente mejor las palabras en español. Los parámetros también se han inicializado desde cero. Al ser entrenado con más textos en español, el modelo tendrá menos sesgos lingüísticos.

El entrenamiento y uso de los grandes modelos requiere de poderosas **infraestructuras de computación**. El alto coste económico, unido a la amplificación de sesgos, la presencia de alucinaciones, el coste de adaptación a problemas concretos y al coste energético, han originado alternativas que requieren menor número de recursos computacionales como son los modelos de lenguaje pequeños, la cuantificación de los modelos y la destilación de modelos.

Explicados los grandes modelos de lenguaje, el siguiente paso consiste en definir los **modelos de lenguaje pequeños**, en inglés *Small Language Models (SML)*. Las diferencias se encuentran en: (i) estos modelos se construyen para dominios específicos, (ii) la cantidad de datos utilizados en su entrenamiento es menor y específica para el uso que se pretende; (iii) en el tamaño de los parámetros (por ejemplo, MiSTRAL 7B tiene 7 billones americanos de parámetros); (iv) en utilizar una arquitectura de atención de ventana deslizante que permite un entrenamiento eficiente en un decodificador; y (v) no requieren de grandes infraestructuras computacionales para su entrenamiento.

Adicionalmente, los usuarios pueden ejecutar el modelo en sus máquinas locales y el riesgo de sesgos es menor que en los grandes modelos. En definitiva, **construir un SLM es un camino alternativo al uso de el entrenamiento de los LLMs con ajuste.**

La **cuantificación de los modelos** es un proceso que reduce el número de parámetros para hacerlos más eficiente en términos de memoria y velocidad de ejecución, lo que facilita su despliegue en pequeños dispositivos y reduce el consumo de energía. La cuantificación se puede realizar durante el entrenamiento (*Quantization-Aware Training QAT*) o después del entrenamiento (*Post-Training Quantization – PTQ*). Esta disminución en el número de parámetros puede ocasionar pérdida de precisión en las respuestas, lo cual pueden provocar un reentrenamiento.

La **destilación de los modelos** (*Model distillation*) es una técnica en el que un modelo grande entrena a un modelo más pequeño. El modelo resultante suele tener un leve peor rendimiento, pero a un coste computacional bastante más moderado que los grandes.

Para facilitar la **selección de los modelos**, se han desarrollado numerosos marcos de evaluación continua que ayudan a comparar el buen hacer de los diferentes modelos de lenguaje en la realización de tareas tales como la identificación de entidades nombradas (ej., nombres de personas u organizaciones) o los sistemas de análisis de sentimientos en textos (Tjong Kim Sang y De Meulder, 2003; Pang *et al.*, 2002). Las evaluaciones permiten identificar errores, sesgos o inconsistencias en los resultados y facilitan el progreso al favorecer la comparación de las aportaciones en igualdad de condiciones. Además, evaluar fomenta la creación de estándares y marcos de evaluación (*benchmarks*) que dan pie a la evaluación continua (*benchmarking*) y al desarrollo de tecnologías más avanzadas.

En este contexto, **BIG-bench** (*Beyond the Imitation Game*) (Srivastava *et al.*, 2022) destaca como un *benchmark* innovador al incluir tareas que van más allá de las pruebas tradicionales, evaluando aspectos como la comprensión del mundo real, la capacidad para resolver problemas novedosos y la creatividad en la generación de respuestas. Otro marco de evaluación relevante es **MMLU** (*Massive Multitask Language Understanding*) (Hendrycks *et al.*, 2020), diseñado para evaluar el conocimiento de los modelos en una amplia gama de dominios, incluyendo matemáticas, ciencias, humanidades y otros campos académicos.

3.1.7.2 Ingeniería del Prompt – Uso de los modelos

Los modelos fundacionales grandes pueden usarse en una amplia gama de tareas en diferentes sectores y así ser la base de una amplia variedad de aplicaciones, de gran calado, con gran permeabilidad y transversalidad en numerosos sectores y escenarios.

El usuario interactúa con el modelo realizando una consulta, en inglés “**prompt**”, y la aplicación le proporciona una respuesta. La **ventana de contexto** delimita el número de *tokens* que puede manejar la aplicación en una interacción del usuario. Si la ventana de contexto es grande, el modelo de lenguaje puede procesar entradas más largas e incorporar más información a la salida. En definitiva, la ventana determina la extensión de una conversación que puede llevar a cabo sin olvidar los detalles previos.

Se llama **ingeniería del prompt** a la técnica que permite realizar consultas que guían al modelo de lenguaje hacia una respuesta. Existen multitud de técnicas que han ido apareciendo a lo largo de los años dependiendo del objetivo, además se pueden combinar varias (Sahoo *et al.*, 2024). Las técnicas para realizar un *prompt* son diversas y se utilizan unas u otras según sea el objetivo que se desea alcanzar. Algunas de las más relevantes son:

- Técnicas de prompt para realizar nuevas tareas sin necesidad de entrenamiento.
- **Prompt directo** en el que se le dice que haga una tarea en concreto (Zero Shot Prompting) (Radford *et al.*, 2019).

- **Prompt con ejemplos** de una tarea para que la realice con nuevos datos (Few Shot Prompting) (Brown *et al.*, 2020).
 - Técnicas de prompt para recibir respuestas de formas específicas.
 - **Prompt de rol**, que solicita respuestas desde la perspectiva de una persona con un cometido concreto.
 - **Prompt explicativo**, que solicita las causas o justificaciones de algo.
- Técnicas de prompt para mejorar el razonamiento y la lógica de la respuesta.
- **Prompt de cadena de pensamiento** (Chain of thought) (Wei *et al.*, 2022), en el que se le fuerza al modelo que razone paso a paso para alcanzar la respuesta correcta. Esta técnica mejora la eficiencia del aprendizaje en modelos de lenguaje pequeños.
 - **Self consistency** que se basa en generar múltiples respuestas de tipo cadena de pensamiento y elegir la más frecuente o coherente (Wang *et al.*, 2022).
 - **Árbol de pensamientos** (Tree-of-Thought Prompting) (Yao *et al.*, 2023). Se basa en generar múltiples caminos de razonamiento (ramas) en paralelo y se seleccionan las ramas más prometedoras, similar a cómo los humanos prueban y descartan opciones.
- Técnicas de prompt para reducir las alucinaciones.
- **Retrieval Augmented Generation** (RAG) (Lewis *et al.*, 2020). Se incluyen partes de documentos relevantes para la identificar la respuesta a la pregunta.
 - **ReAct Prompting**. Se fuerza al modelo a realizar tres pasos. Primero razonar paso a paso sobre el problema, luego a actuar realizando consultas sobre fuentes de información para finalmente reflexionar y dar una respuesta (Yao *et al.*, 2023).
 - **Chain-of-Verification** (CoVe). Basada en la cadena de pensamiento, el modelo verifica cada paso de su propio razonamiento antes de proporcionar la respuesta final (Dhuliawala *et al.*, 2023).
- Técnicas de prompt para mejorar la consistencia y la coherencia.
- **Contrastive Chain-of-Thought Prompting** (CcoT). Se generan múltiples cadenas de pensamiento para la misma pregunta, se identifican diferencias entre ellas para detectar inconsistencias y se selecciona la respuesta más lógica y consistente (Chia *et al.*, 2023).

Las **consultas han de estar bien diseñadas y precisas si se quiere que el modelo genere respuestas creíbles**, aunque puede ocurrir que no sean verosímiles. La ausencia de verosimilitud de las respuestas nos lleva al concepto de **alucinación**. Sabemos que los grandes modelos de lenguaje son extremadamente fluidos en sus respuestas y suelen generar textos con una gramática correcta, pero no siempre son veraces, en el sentido de que no siempre garantizan que el texto generado carezca de errores de contenido. Las alucinaciones son invenciones, errores factuales o respuestas incoherentes que genera el sistema.

Para disminuir las alucinaciones, **las técnicas RAG** (Lewis et al., 2020), acrónimo de *Retrieval-Augmented Generation*, **proporcionan al modelo un contexto adicional** que va más allá de para lo que fue entrenado, le habilita a consultar fuentes externas y a usar sus contenidos para fundamentar una respuesta, mejorando así la precisión de lo que finalmente genera.

La preferencia de unas respuestas frente a otras nos conduce al concepto de **sesgo**. Es conocido que los sesgos de sexo y raza son necesarios, en cierta medida, para algunos diagnósticos médicos y para el análisis de la genética humana. Pero el sesgo es inherente a los seres humanos e influye en la toma de decisiones.

Existe un **sesgo inconsciente**, propio de cada uno, que está relacionado con prejuicios, discriminación, racismo, sexo, estereotipos o el nivel educativo, por mencionar solo algunos. Por ello, es imprescindible detectar, en etapas tempranas, los sesgos en los datos que se utilizan en el entrenamiento de los modelos de aprendizaje profundo. Así, si los datos de entrenamiento están sesgados de forma consciente o inconsciente, el algoritmo podría favorecer una respuesta frente a otra, o tomar una decisión potencialmente dañina que perjudicaría a un individuo o a un colectivo. Obsérvese también que un sesgo no es un requisito, una cualidad, una circunstancia o algo que se requiera *a priori* para, por ejemplo, dar un crédito o ser elegible para un puesto de trabajo (Gómez-Pérez, 2023).

3.1.8 Una mirada al futuro: Inteligencia artificial neurosimbólica

En los últimos años ha aparecido el **enfoque neurosimbólico**, que **hibrida las técnicas de IA simbólica y de la IA generativa** mencionadas. Este camino inyecta conocimiento procedente de ontologías y grafos de conocimientos en los grandes modelos de lenguaje ya entrenados para realizar un ajuste fino y mejorar su calidad. La inyección de conocimiento se plantea, por ahora, en la entrada de datos o en el propio modelo (Yao *et al.*, 2022). **Los datos factuales almacenados en grafos de conocimientos se pueden utilizar para entrenar y también validar la veracidad de los textos generados, disminuir las alucinaciones y explicar el origen de las respuestas.** El ajuste fino realizado con grafos de conocimientos ayuda a reducir sesgos y mejora la precisión en dominios específicos.

La incorporación de ontologías y grafos de conocimiento en las aplicaciones que utilizan la técnica de recuperación por generación aumentada permite guiar, y también enriquecer, las consultas que se realizan al sistema. De esta forma, se aumenta o enriquece la consulta, y el modelo de lenguaje genera una respuesta en la que el peso estadístico de la siguiente palabra disminuye.

Por otro lado, la IA generativa facilita algunas fases del proceso de desarrollo de las ontologías y de los grafos de conocimiento ayudando a construir las preguntas de competencia, su construcción automática o aprendizaje, y también para alinearlas (Giglou *et al.*, 2023). Los grandes modelos de lenguaje son un método alternativo a las técnicas de los patrones léxico-sintácticos y de agrupamiento que conviene explorar.

3.1.8.1 Creación de conjuntos de datos sintéticos

El desarrollo de un sistema basado en algoritmos de IA implica la **creación o disponibilidad de un conjunto elevado de datos confiables para entrenar, validar o probar un modelo de red neuronal**. Aunque las herramientas de análisis utilizadas por los operadores de SDA para producir datos del mundo real también aprovechan las técnicas de modelado y simulación, el algoritmo exacto empleado, los parámetros de calibración del modelo y las suposiciones que sirven de base para su construcción se consideran **información clasificada**.

Las **técnicas de generación de datos sintéticos para IA** pueden ser muy variadas, desde el uso de modelos estadísticos tradicionales hasta técnicas avanzadas de aprendizaje profundo con consecuencias éticas sobre el uso de estos datos para la toma de decisiones (Hao *et al.*, 2024). Concretamente, los LLM han surgido como un enfoque revolucionario para generar conjuntos de datos sintéticos. En todo caso, seguirán produciéndose avances en el uso de la IA en los próximos años que reducirán los problemas de la generación de datos sintéticos. Entre ellos:

- **Adopción de modelos generativos más avanzados** como las redes generativas antagónicas (GAN) o los autocodificadores variacionales (VAE). Estos modelos poseen capacidades de aprendizaje más sólidas, lo que permite un modelado más preciso de la compleja distribución de datos del mundo real.
- **Integración de la experiencia específica del dominio para mejorar el realismo de los datos sintéticos**. La integración de conocimientos específicos de dominio, como gráficos por computadora, física y ciencia cognitiva, puede contribuir a mejorar el realismo de los datos sintéticos.

3.2 Hardware/Chips para IA aplicada a la defensa

Desde la invención del transistor en los *Bell Labs* en 1947, la aparición del circuito integrado²⁶ en la década de los 50 del siglo pasado y la invención de los microprocesadores por *Federico Faggin* en Intel (ca 1970), la **microelectrónica -la rama de la electrónica que se ocupa de los circuitos y componentes electrónicos miniaturizados a escala micrométrica (μm) y nanométrica (nm)**, es una tecnología habilitadora clave que ha posibilitado el avance de otras tecnologías que han transformado la economía y la sociedad.

Actualmente, se encuentra en la base de todos los procesos de digitalización y automatización industriales clave, como las telecomunicaciones, el control industrial, la automoción/movilidad, la monitorización de infraestructuras, la ciberseguridad, la aeronáutica, el sector espacial, la energía,

²⁶ El circuito integrado (la interconexión monolítica de dispositivos activos -transistores), fue inventado por J. Kilby (premio Nobel de Física 2000) en Texas Instrumens y B. Noyce en Fairchild.

la defensa y la seguridad, contribuyendo de forma notable a un incremento de la productividad y, en consecuencia, si la cantidad de trabajo se mantiene constante, a un crecimiento de su PIB.

El objetivo de esta sección es analizar las tecnologías actuales y las proyecciones futuras en el diseño y fabricación de **chips para la IA aplicada a la Defensa**. Tras una panorámica general de las tecnologías de semiconductores, se abordan las características específicas de los semiconductores adaptados a las necesidades de la Defensa con foco en los requisitos de los chips para la IA.

3.2.1 Evolución de las tecnologías de semiconductores

Gordon Moore, cofundador de la empresa Intel, predijo en 1965 que el número de transistores en un chip se duplicaría aproximadamente cada dos años. Esta predicción se conoce como “*ley de Moore*”. Aunque en varias ocasiones se ha anunciado la muerte de la ley de Moore, las empresas de diseño y fabricación de chips la mantienen viva con grandes esfuerzos de innovación. La figura 3.7 muestra las innovaciones de la empresa *Intel* (Kelleher, 2022) que mantiene la ley de Moore con innovaciones como la tecnología de puerta metálica de alta k, los transistores 3D tri-gate o el silicio tensado.

Durante los primeros 40 años, las mejoras provinieron principalmente de las innovaciones en el proceso tecnológico. En el futuro, vendrán de las innovaciones tanto en el proceso como en el encapsulado y el diseño de dispositivos y arquitectura. Intel y otros fabricantes consideran que los procesos tecnológicos seguirán ofreciendo mejoras en densidad, mientras que las tecnologías de apilamiento 2.5D y 3D permitirán aumentar la cantidad de transistores por dispositivo. Se espera integrar aproximadamente 1.000 de transistores en un solo dispositivo para 2030.

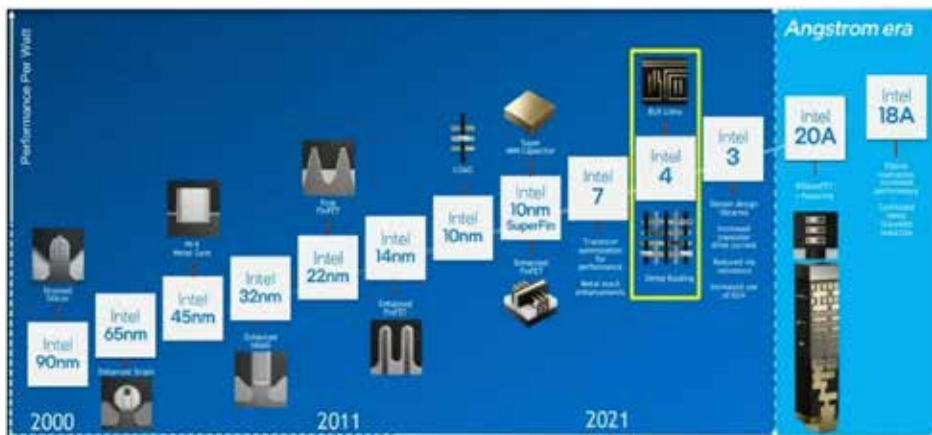


Figura 3.7 Innovaciones de Intel: “Prestaciones por watio” frente a tiempo
Fuente: Kelleher (2022)

El concepto básico para medir el grado de avance de la microelectrónica es el **nodo tecnológico**, que se refiere al **tamaño mínimo de las características de un chip fabricado mediante un proceso específico**, y generalmente se expresa en nanómetros. El término apareció asociado al

tamaño de una celda de memoria en un chip *DRAM* (memoria dinámica de acceso aleatorio); en realidad se refiere a la mitad de la distancia entre dos elementos repetidos como los contactos entre los que se coloca una celda de memoria; también se llama medio paso o semiperíodo de interconexión (half pitch). Este parámetro define aspectos clave como la frecuencia de operación, densidad por mm², rendimiento de la oblea y el consumo energético. No se trata de una medida física exacta, pero se utiliza para distinguir diferentes generaciones de chips.

Así pues, **la reducción de las dimensiones del nodo tecnológico no es simplemente una reducción de dimensiones, sino que requiere de innovación en materiales, procesos y dispositivos**. A medida que se reduce el tamaño, aparecen problemas relacionados con las corrientes de fuga y la disipación de energía. Esto provocó, por ejemplo, que a partir de 22 nm, se abandonara la tecnología planar tradicional y se introdujeran los dispositivos **3D FinFET** (transistores de efecto de campo Fin), y luego, a partir de 7nm los dispositivos **FET GAA** (Gate-All-Around). En la figura 3.8 (izquierda) se aprecia que a medida que se reduce el nodo, aumenta la eficiencia y velocidad de proceso. En el caso de la eficiencia del transistor, la del nodo de 50 nm es 50 veces la del nodo de 90 nm.

La reducción de dimensiones de los dispositivos permite integrar muchos más dispositivos (circuitos más complejos, verdaderos sistemas) en la misma área por lo que según disminuye el tamaño del nodo, aumenta el coste de diseño del chip -no linealmente. Al mismo tiempo, para una misma oblea de 300 mm a medida que se escala hacia abajo (para la misma complejidad de circuito) se obtienen menores precios unitarios (más chips por oblea).

Sin embargo, los costes de fabricación de los prototipos son más elevados pues la amortización de equipos y el coste de las máscaras (procesos más complejos y dimensiones más pequeñas) son mayores. En la figura 3.8 (derecha) puede apreciarse el aumento del coste del diseño del chip (ingeniería de diseño más fabricación, encapsulado y prueba de prototipos).

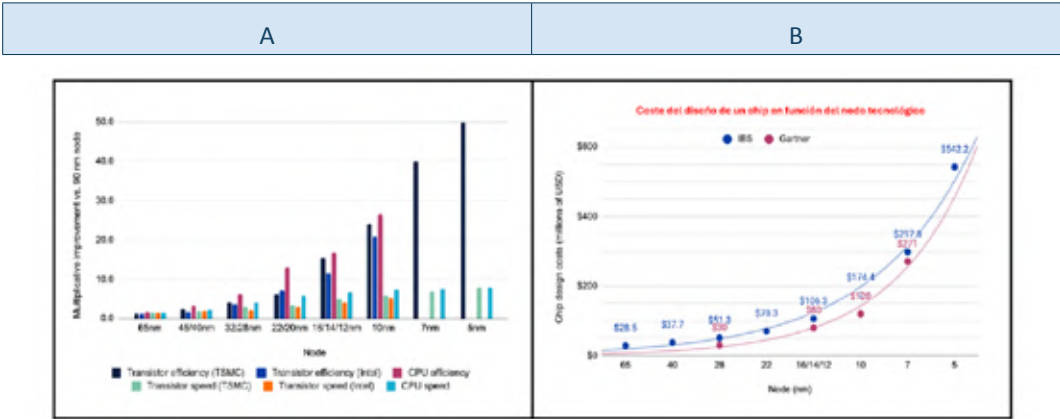


Figura 3.8 (izq.) Eficiencia y velocidad en comparación con nodo de 90 nm; (der.) Coste de diseño de un chip en función del nodo tecnológico Fuente: Khan y Mann (2020)

Respecto al futuro, la Hoja de Ruta Internacional para Dispositivos y Sistemas (IRDS) de la IEEE Rebooting Computing Initiative, define las tendencias clave en tecnología de semi-conductores (véase la figura 3.9). Lo hace mediante tres enfoques complementarios: **More Moore** impulsa el escalado convencional, **More than Moore** integra nuevas funcionalidades y **Beyond CMOS** investiga futuros sustitutos de las tecnologías informáticas tradicionales.

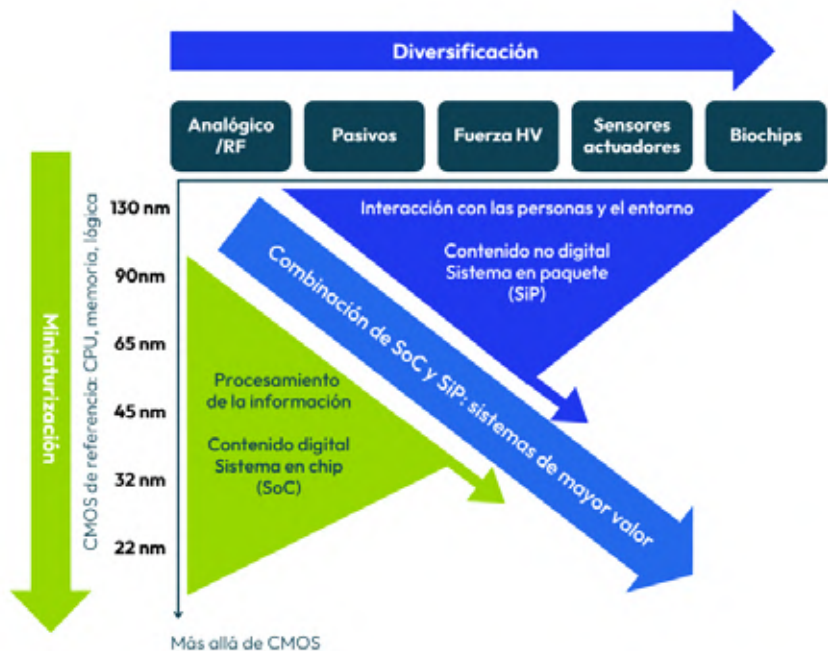


Figura 3.9 Hoja de ruta de los sistemas integrados Fuente: IRDS (2023)

More Moore: La reducción de dimensiones se ve cada vez más dificultada por los retos de rendimiento como el excesivo consumo de energía y el limitado ancho de banda de interconexión, lo que es aún más complejo ante requisitos de interacción fluida entre big data y flujos de datos instantáneos. Esto requiere dispositivos de alto rendimiento y consumo ultra bajo con función de “siempre activo”, que puedan generar datos en tiempo real. Esta necesidad se ha visto acelerada con el **aumento de las cargas de trabajo de IA**.

La IRDS establece los requisitos físicos, eléctricos y de fiabilidad para las tecnologías de lógica y memoria con el fin de mantener el escalado de potencia, rendimiento, área y coste, con un horizonte temporal de 15 años para la fabricación convencional/de alto volumen. Es probable que el finFET se mantenga hasta 2025. En 2022 se inició la transición a **dispositivos** Gate-All-Around **GAA laterales** debido a las limitaciones de rendimiento de finFET, y se prevé que el FET complementario (CFET) será la evolución posterior de los GAA laterales en formato 3D. También propone usar litografía ultravioleta extrema.

More than Moore se refiere a la incorporación en los dispositivos que no necesariamente escalan según la ley de Moore, pero que **aportan valor añadido**, por ejemplo, funcionalidades no digitales (analógicas, comunicación por RF y ondas milimétricas 5G/6G, fotónica integrada para comunicaciones ópticas, sistemas microelectromecánicos MEMS, control de potencia, componentes pasivos, sensores, etc.), que pasan del nivel de sistema al de encapsulado (SiP) o al chip (SoC). La integración con el software también debe de considerarse en cuanto al rendimiento (codiseño HW/Sw).

Beyond CMOS: a medida que el escalado dimensional de los CMOS se acerca a **límites físicos fundamentales**, es necesario explorar **nuevos dispositivos de procesamiento de información y microarquitecturas**, mediante la combinación de materiales, dispositivos y arquitecturas emergentes, como la computación cuántica, neuromórfica, espintrónica y materiales 2D como el grafeno.

Una vez fabricados los chips, debemos ensamblarlos y empaquetarlos. En la actualidad, los enfoques principales son **System on Chip (SoC)** y **System in Package (SiP)**. Como conceptos relacionados aparecen **chiplet** e **integración heterogénea**.

Un **SoC** integra múltiples componentes funcionales (CPU, GPU, memoria, interfaces, etc.) en un **solo chip de silicio**, como un circuito integrado monolítico. Es una solución muy compacta, con alto rendimiento, bajo consumo y comunicación de alta velocidad entre sus componentes por las cortas interconexiones. Se basa en procesos avanzados de fabricación CMOS, y se optimiza para aplicaciones específicas, como smartphones o dispositivos IoT. Todos los bloques deben diseñarse y fabricarse con el mismo nodo tecnológico, lo que aumenta la complejidad y coste y reduce su flexibilidad.

Un **SiP** agrupa varios chips individuales (a veces de diferentes nodos o tecnologías -CMOS, RF, MEMS, fotónica) en un único encapsulado (como una pequeña placa base encapsulada). Los componentes no están en un solo troquel, sino en varios, que se comunican dentro del paquete. Se usa en dispositivos 5G, automoción, aceleradores de IA o IoT. Permite un diseño modular y flexibilidad para integrar diversas funcionalidades y el uso de técnicas avanzadas de encapsulado (integración 2.5D/3D).

Un **chiplet** es un circuito integrado monolítico especializado, diseñado para combinarse con otros dentro de un único encapsulado y formar un sistema completo. En lugar de diseñar un chip monolítico, se fabrican chiplets más pequeños por separado y se integran en un SiP (Evanson, 2025). Los chiplets están diseñados específicamente para ser **modulares, reutilizables y conectables entre sí** con interfaces estandarizadas de alta velocidad (como UCIe). Se encuentra en la computación de alto rendimiento, aceleradores de IA y procesadores avanzados (p. ej., AMD, Intel, NVIDIA).

La **integración heterogénea** es un concepto más amplio que engloba a los otros. Se refiere a la capacidad de **combinar diferentes tipos de tecnologías (procesos, materiales, funcionalidades)** en un único sistema empaquetado o interconectado. Puede incluir lógica avanzada, memoria, sensores, componentes RF, etc., integrados a través de tecnologías de interconexión como 2.5D o 3D. Su objetivo es superar las limitaciones del escalado tradicional proporcionando una funcionalidad avanzada que no se puede lograr con un solo circuito integrado. Puede incluir diferentes materiales (p. ej., silicio, GaN, InP, grafeno). Se encuentra en aplicaciones como 5G, IA, automoción, defensa, aeroespacial y dispositivos médicos.

La tabla 3.1 expone una comparativa que permite una mejor comprensión de lo desarrollado:

Característica	SoC (System on Chip)	SiP (System in Package)	Chiplet	Integración Heterogénea
Definición	Todos los componentes en un solo chip	Varios chips en un único encapsulado	Bloques funcionales modulares interconectables	Integración de distintos chips/ funciones/ tecnologías
Tipo de integración	Monolítica	Multi-chip (dentro del mismo paquete)	Modular (predefinida para ensamblaje flexible)	2.5D, 3D, SiP, chiplets, y más
Tecnologías involucradas	Un único nodo/ fabricación	Diferentes tecnologías posibles	Diferentes nodos y foundries posibles	Totalmente diversa: lógica, memoria, RF...
Flexibilidad de diseño	Baja (todo en el mismo chip)	Media	Alta	Muy alta
Reutilización de componentes	Limitada	Limitada	Alta (bloques reutilizables)	Alta
Interconexión	Interna al chip	Cables, microbumps o interposers	Interfaces de alta velocidad (ej. UCIe)	TSV, interposers, interfaces estandarizadas
Ventajas principales	Alto rendimiento, bajo consumo, tamaño reducido	Integración rápida de funciones mixtas	Modularidad, escalabilidad, menor coste de diseño	Máxima eficiencia funcional, flexibilidad y escalabilidad
Limitaciones	Coste y complejidad aumentan con nodos avanzados	Menor densidad y rendimiento comparado con SoC	Requiere estándares y ecosistema maduro	Complejidad tecnológica y de ensamblaje

Tabla 3.1 Comparativa de tendencias clave en tecnología de semiconductores

Fuente: elaboración propia

3.2.2 Chips para aplicaciones en Defensa

Desde el punto de vista económico es muy difícil rentabilizar la inversión del diseño o la fabricación de los chips, a no ser que las tiradas (volumenes de chips idénticos fabricados) sean masivas. Por ese y otros motivos, con frecuencia se habla del **uso dual de los semiconductores**, que se refiere a su capacidad de ser utilizados tanto en aplicaciones **civiles** como **militares**. Esta característica por una parte facilita la inversión y aumenta las tiradas, pero por otra, los convierte en una tecnología estratégica y, a menudo, objeto de regulaciones gubernamentales y restricciones comerciales.

Ejemplos de uso dual son los chips usados en las antenas 5G o los radares de automóviles, que también se pueden integrar en **sistemas de radar militar** o en **equipos de guerra electrónica**; los procesadores de alto rendimiento como los de AMD o Intel se usan en **centros de datos** para el entrenamiento de IA y también en **simulaciones militares** o **criptografía avanzada**; un chip de IA usado en un **smartphone** puede ser el mismo que se emplea en sistemas de **reconocimiento de imágenes** en drones militares²⁷.

Los **requisitos que deben cumplir los chips para su uso en Defensa** son más exigentes que los de uso civil, lo cual encarece su costo y hace más complejo su diseño, proceso de fabricación, prueba, encapsulado y certificación. En efecto, deben diseñarse para ofrecer una durabilidad, seguridad y fiabilidad extremas en entornos hostiles, con dificultades de recambio y mantenimiento, estableciéndose un conjunto de especificaciones que estos chips deberán cumplir para ser certificados en grado militar. Suelen utilizar tecnología más antigua y probada en lugar de nodos de última generación. Entre sus características se destaca:

- **Rango de temperatura y tolerancia ambiental:** la *temperatura de operación* puede variar entre -55 °C y +125 °C (a veces hasta + 200 °C), mientras que los de uso civil suelen funcionar entre 0 y 70° C. Deben ser resistentes a golpes y vibraciones en condiciones extremas. Deben de estar protegidos contra la humedad y la corrosión de la niebla salina.
- **Confiabilidad y Longevidad:** tasa de fallos muy baja en sistemas de misión crítica. Su vida útil debe ser de 15 a 30 años.
- **Seguridad y Anti-manipulación:** deben contar con sistemas de arranque seguro, mecanismos de autodestrucción y de cifrado en hardware. Deben de contar con *protección electromagnética (EMI/EMC)*. Su *cadena de suministro debe ser segura* con seguimiento estricto, a menudo integrado en fábricas seguras.
- **Endurecimiento por Radiación (rad-hard):** diseñados para soportar rayos gamma, rayos cósmicos y bombardeo de neutrones. Tolerancia a la dosis ionizante total de entre 100 Krad y 1Mrad.
- **Proceso de fabricación y materiales:** los nodos tecnológicos son mayores que los de los chips comerciales por robustez (90 nm, 120 nm, 180 nm). Los nodos muy pequeños (5 nm) son muy sensibles a la radiación por lo que no cumplen los requisitos anteriores. El material

27 El SoC SAF85xx de NXP Semiconductor es de claro uso dual; se trata de un radar para automoción altamente integrado que opera en la banda de 76 a 81 GHz. Su empleo se extiende cada vez más, no solo por la utilización de Sistemas Avanzados de Asistencia al Conductor (ADAS) en los vehículos actuales o el sistema de frenado de emergencia autónomo, sino también con el advenimiento de los vehículos autónomos. Estos sistemas también se pueden aplicar a los vehículos militares, que además de cumplir la norma de Calidad en Automoción AEC-Q100, tendrán que adaptarse para cumplir otras normas (por ejemplo, MIL-STD).

del sustrato puede ser: SOI²⁸, carburo de silicio (SiC), nitruro de galio (GaN), que soportan mejor la radiación y las temperaturas altas que el silicio convencional. El *encapsulado debe ser* cerámico, sellado con metal para encapsular los chips y protegerlos de interferencias electromagnéticas (EMI) y ataques de hardware.

- **Coste y disponibilidad:** cuestan entre 10 y 100 veces más que los chips comerciales equivalentes. Tienen un volumen bajo de producción, organizándose por pedidos personalizados a fábricas clasificadas. Finalmente, su *disponibilidad* es restringida, controlada por los gobiernos.

3.2.2.1 Sustratos para la fabricación de chips para la Defensa

Los **sustratos** son los materiales semiconductores sobre los que se fabrican los elementos activos, que, una vez interconectados, forman los denominados **sistemas integrados**. Se distinguen dos grandes grupos: los **semiconductores simples**, como el silicio y el germanio; y los **semiconductores compuestos**, prioritariamente los del grupo III-V.

El **silicio** es un elemento muy abundante en la naturaleza lo que garantiza un suministro relativamente estable en el futuro cercano; resulta un elemento clave en la fabricación de chips semiconductores. Su banda prohibida es de aproximadamente 1.1 eV, funciona bien a temperatura ambiente y la movilidad de sus electrones es moderada (alrededor de 1400 cm²/V.s). En la figura 3.10 se puede ver un lingote de silicio purificado antes de cortar para obtener obleas.

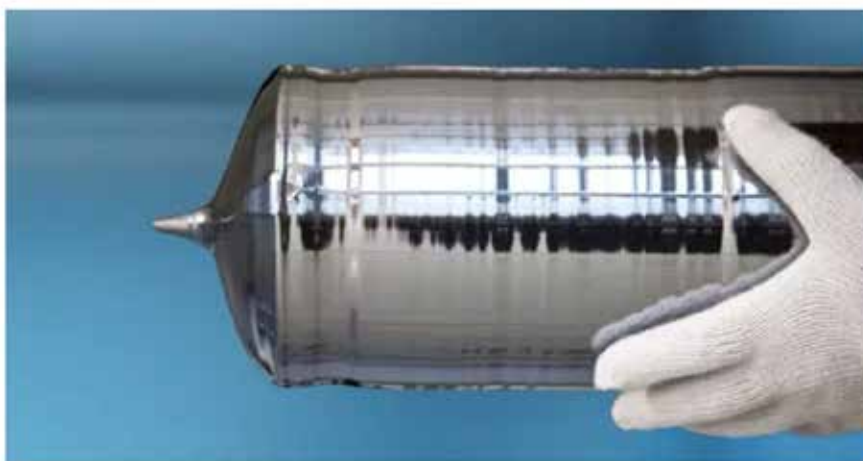


Figura 3.10 Barra de silicio formada a partir de un cristal de silicio por el método de Czochvalski. Las obleas se obtienen cortando la barra en rodajas con sierras especiales. Fuente: Waferpro²⁹

²⁸ SOI Silicon On Insulator: Es una estructura semiconductor que consta de una capa de silicio monocristalino separada del sustrato principal por una fina capa de aislante.

²⁹ Waferpro (2024). Silicon Ingots: The Building Blocks of Modern Electronics. Disponible en línea: <https://waferpro.com/silicon-ingots-the-building-blocks-of-modern-electronics/?srsltid=AfmBOop1vrL5MMOKUoJq>

Los **semiconductores III-V** se crean mediante la combinación de elementos del grupo III de la tabla periódica (como el *galio*, el *aluminio* y el *indio*) con elementos del grupo V (incluido el *fósforo*, el *arsénico* y el *nitrógeno*), lo que da como resultado la generación de una estructura de red cristalina con características electrónicas excepcionales.

Su banda prohibida es mayor que la del silicio, lo que proporciona una **conversión altamente eficiente de energía de fotones a electrones y permite manejar tensiones mayores**; esto hace que los semiconductores III-V sean muy adecuados para aplicaciones optoelectrónicas. La movilidad de electrones es mayor (2000 cm²/V.s aproximadamente), y su temperatura de funcionamiento es adecuada para altas temperaturas y alta potencia; tienen una eficiencia mayor que el silicio.

En 2006, se empezaron a fabricar transistores **FET** (*Field Effect Tunnel*) de **nitruro de galio** (*GaN*), mediante el crecimiento de una fina capa de GaN sobre una oblea de silicio estándar mediante deposición química en fase de vapor de metal orgánico. Este proceso permitió que los transistores de nitruro de galio se pudieran producir en las mismas fábricas y con casi los mismos procesos que los de silicio, lo que redujo sus costes de fabricación y la barrera para la adopción de transistores más pequeños con un rendimiento mejorado.

El GaN se utiliza desde hace unos años en chips para Defensa por sus propiedades de alta movilidad de electrones y velocidad de saturación que posibilitan el desarrollo de dispositivos de alta frecuencia (como los necesarios para comunicaciones de alta frecuencia, navegación eficiente y control de tráfico aéreo en tiempo real, bloqueadores de señal y radios terrestres).

El ancho de su banda prohibida -tres veces mayor que el silicio- hace que aguante altos voltajes sin comprometer el rendimiento en aplicaciones de alta potencia (como los sistemas de radar de matriz de barrido electrónico activo y guerra electrónica). Igualmente, **disipan el calor de forma eficaz** lo que mejora la fiabilidad del dispositivo y reduce la necesidad de sistemas de refrigeración complejos. Por su alta densidad de potencia, los **componentes basados en GaN pueden ofrecer salidas de alta potencia mientras ocupan espacios físicos más pequeños** (necesario en equipos que se despliegan en campaña). **Los chips fabricados con GaN cobran una relevancia especial cuando se trata de sistemas de ondas milimétricas**³⁰, cada vez más usadas en Defensa.

U9rLjpjOOQVMiQieLyhoEj6e0a_dggw6gHL

30 Las ondas milimétricas (MMW) se refieren a ondas electromagnéticas con frecuencias entre 30 GHz y 300 GHz y longitudes de onda que van desde 1 mm a 10 mm. Estas ondas se ubican entre las frecuencias de microondas e infrarrojas en el espectro electromagnético.

La figura 3.11 muestra las ventajas de estos circuitos sobre otras tecnologías en cuanto a **frecuencia de operación** y **potencia** que son capaces de manejar.

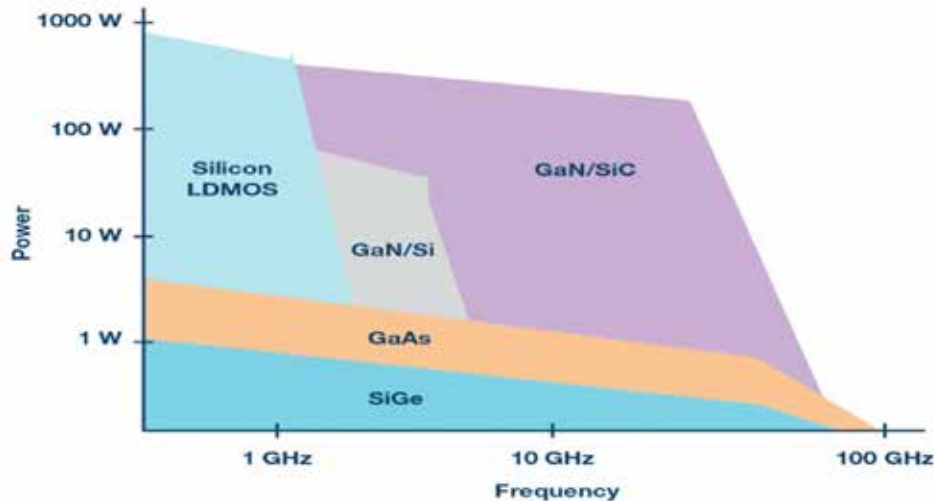


Figura 3.11 Comparación de potencia y frecuencia de diferentes materiales semiconductores en el rango de microondas, que incluye a las ondas milimétricas. Analog Devices
Fuente: Fogarty (2019)

3.2.3 Tipos de chips para la Defensa

Sensores

Uno de los puntos fundamentales para los sistemas de IA de computación en el borde es el suministro de datos, tanto para entrenamiento como para inferencia. El suministro de datos para inferencia en computación en el borde, por ejemplo, para un vehículo autónomo, o para un sistema de guiado de misiles, debe ser obtenido en tiempo real. **Los sistemas de sensores son los encargados de la captura de datos**, muchas veces en tiempo real.

Procesadores de hardware abierto (RISC-V)

La mayoría de los chips que se usan en defensa tienen diseños propietarios y están sujetos a restricciones de uso; por este motivo sólo se pueden conseguir de proveedores oficiales certificados que eligen a quién proporcionárselos. Unas secciones más adelante se explicará la cadena de valor de los chips, en donde veremos que la fase de diseño de los chips no tiene por qué estar acoplada con la de fabricación.

En este contexto, la arquitectura **RISC-V** (Ver figura 3.12) soporta un **conjunto de instrucciones (ISA) abierta y modular**, y ha ganado interés en aplicaciones de defensa por su flexibilidad y ausencia de restricciones de propiedad intelectual. Sin embargo, su uso en entornos militares

tiene ventajas e inconvenientes, que describimos a continuación comparándola con sus alternativas comerciales de Intel, AMD o ARM. Entre las ventajas principales se pueden mencionar:

- **Soberanía tecnológica y reducción de dependencia de terceros.** Cualquier empresa o institución puede acceder a la arquitectura, que es abierta y personalizarla para desarrollar sus procesadores adaptados³¹.
- **Seguridad y personalización:** en el diseño se pueden incluir medidas de seguridad específicas como criptografía avanzada y protección contra ataques de hardware.
- **Diseño** permite aplicar optimizaciones de consumo energético, que resultan claves para drones, satélites militares y dispositivos portátiles para soldados.
- **Escalabilidad y modularidad:** partiendo de la arquitectura base se pueden hacer adaptaciones para cubrir un gran rango de procesadores, desde los de bajo consumo para equipos de campo hasta los de alto rendimiento para supercomputación.
- **Reducción de costes:** los de diseño se reducen mucho, manteniéndose los de fabricación.

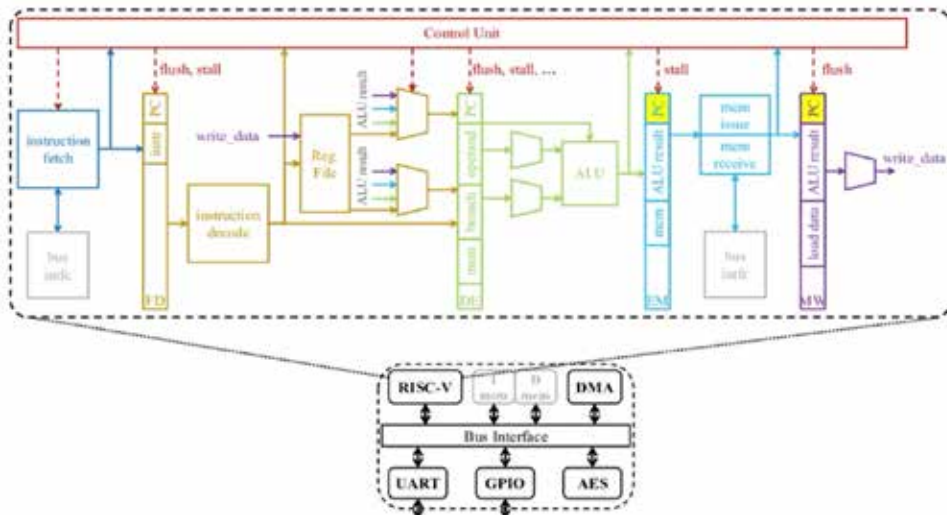


Figura 3.12 Diagrama simplificado arquitectura RISC-V
Fuente: Kiaei y Schaumont (2022).

Las ventajas son innegables, igual que los inconvenientes que presenta y por lo que **su grado de adopción es aún bajo**: el ecosistema de software y herramientas de desarrollo está inmaduro y mucho menos probado que en las alternativas comerciales; el rendimiento de las versiones comerciales de RISC-V no está al mismo nivel que el de sus competidores comerciales; **los chips RISC-V no han alcanzado las certificaciones de seguridad y fiabilidad que se requieren en el ámbito de la Defensa.**

31 Este es el caso de China y Rusia, con lo que tratan de evitar las restricciones de importación que tienen impuestas para el uso de productos de Intel, AMD o ARM.

Además, la fuerte inversión de China en este chip y el hecho de que las empresas líderes en su desarrollo sean chinas (p.ej. Alibaba, SiFive) ha suscitado preocupaciones en países occidentales sobre su desarrollo con posibles puertas traseras o espionaje; Estados Unidos está considerando imponer restricciones al acceso de China a esta tecnología, lo que podría afectar su adopción global.

3.2.3.1 Principales usos de los chips para Defensa

Los semiconductores desempeñan un papel crucial en diversas aplicaciones militares. Su pequeño tamaño, bajo consumo de energía y alta confiabilidad los hacen ideales para tecnologías militares que requieren compacidad, eficiencia y durabilidad.

Una aplicación de creciente interés son las **tecnologías de cifrado** que garantizan la comunicación segura y protegen la información militar confidencial del acceso no autorizado. En particular, se prevé un uso creciente en los sistemas basados en ondas milimétricas, por sus capacidades de detección precisa de objetivos (debido a su alta resolución), la congestión reducida y baja interferencia en comparación con frecuencias más bajas, la dificultad de detectarlas con sistemas de radar convencionales (lo que aporta capacidades de sigilo o secreto) y su capacidad de penetración de algunos materiales como la niebla, la lluvia y ropa.

Las aplicaciones principales son: 1) **Sistemas de guía de misiles**; 2) **Sistemas de Radar**; 3) **Imágenes y vigilancia**; 4) **Comunicaciones militares seguras** (los enlaces de ondas milimétricas proporcionan un gran ancho de banda seguro (por ejemplo, la comunicación en banda W 75-110GHz); 5) **Armas de energía dirigida** (las ondas milimétricas de alta potencia se pueden utilizar como armas para desactivar los dispositivos electrónicos enemigos).

Las limitaciones más importantes para su uso están relacionadas con la absorción atmosférica, su penetración limitada, y el alto coste de fabricación de los equipos.

3.2.4 Tipos de chips para su uso en IA

Los algoritmos de IA necesitan una potencia de cálculo importante, lo que implica la utilización de arquitecturas paralelas en las que se puedan realizar muchas operaciones aritméticas, como multiplicaciones y acumulaciones simultáneamente. Esto **sólo ha sido posible cuando los nodos tecnológicos han bajado de los 40 nm y la frecuencia de funcionamiento ha superado 1 GHz**. Esto ha inducido un aumento del consumo y la necesidad de disipación de calor, que es uno de los problemas actuales de los chips IA.

Se entiende por chips de IA los procesadores de datos de alta eficiencia y velocidad, adecuados para el entrenamiento o la inferencia de modelos IA. Son capaces de manejar operaciones con matrices multidimensionales (denominadas tensores) a gran escala mediante

el uso de computación paralela (Li, 2023), ya que los modelos de IA (redes neuronales, aprendizaje profundo y transformadores) se suelen representar con tensores y las operaciones se realizan sobre los tensores. Los chips de IA responsables de ejecutar las tareas de IA utilizan una arquitectura SIMD³², que realizan las mismas operaciones sobre múltiples puntos de datos simultáneamente, acelerando de forma significativa la velocidad de cómputo.

Estos chips se han optimizado para satisfacer las necesidades de cómputo de los algoritmos IA, habilitando un procesamiento más rápido y eficiente desde el punto de vista de consumo de energía que los procesadores tradicionales de propósito general (CPUs). A su vez, el uso de la IA en la construcción de las herramientas EDA para el diseño de los chips permite mejorar el rendimiento, la potencia, área, coste y “time to market”. Este ciclo virtuoso IA-tecnología de semiconductores se ha arraigado, impulsando nuevas arquitecturas, reduciendo los ciclos de desarrollo de dos años a uno, y aumentando considerablemente la productividad del diseño, uno de los factores de coste más elevados para obtener un chip IA.

Según su construcción los chips para IA pueden clasificarse en **Unidades de Procesamiento Gráfico** (*Graphic Processing Units -GPU-*); **Arreglos Programables en campo** (*Field Programmable Gate Arrays -FPGA-*); y **Circuitos Integrados de Aplicación Específica** (*Application Specific Integrated Circuits -ASIC-*) que incluyen a los aceleradores que la de IA, a los circuitos neuromórficos, Artificial Intelligence Memory in Computing (AIMC). Se tratarán aparte los aceleradores de IA.

Los ASICs son ya el mayor componente de la computación en IA debido a sus altas capacidades de procesamiento paralelo. Dan muy buenos resultados para ejecutar aplicaciones IA específicas, porque se diseñan para optimizar su rendimiento y eficiencia energética al ejecutar estas aplicaciones IA específicas, pero tienen menos flexibilidad de las GPUs y FPGAs (Pang, 2022). En la figura 3.13 pueden verse estas relaciones entre los diferentes tipos de chips de IA.

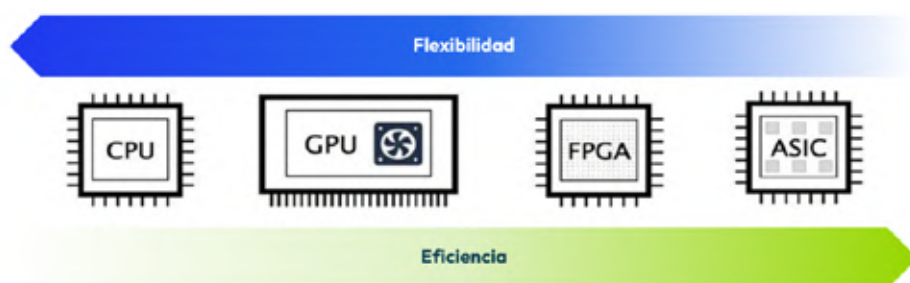


Figura 3.13 Clasificación general de los chips IA según su construcción. De izquierda a derecha aumentan su eficiencia energética; de derecha a izquierda aumentan su flexibilidad
Fuente: Li (2023)

32 SIMD (*Single Instruction Multiple Data*): Las instrucciones SIMD, o instrucciones vectoriales, son un tipo especial de instrucciones de procesador que pueden funcionar con varios elementos de datos (vectores) al mismo tiempo. Por ejemplo, en lugar de agregar dos números a la vez, una instrucción SIMD puede agregar cuatro u ocho números a la vez. Esto ahorra tiempo y recursos, ya que el procesador ejecuta menos instrucciones con menos registros.

La capacidad necesaria para entrenar un modelo depende del tamaño del modelo, el tamaño del dataset y la calidad esperada del modelo entrenado. **La nube es un lugar ideal para el entrenamiento** porque proporciona acceso a grandes datasets de múltiples servidores. Además, la nube puede reducir los gastos porque permite que GPU y otro hardware costoso entrenen múltiples modelos.

La segunda fase es la de **inferencia** en la cual se pone a funcionar el modelo para que cuando se le ofrezcan entradas, proporcione salidas. En la mayoría de los casos de uso en defensa esta respuesta debe darse sobre los datos que se obtienen de los sensores, y hacerlo en tiempo real porque una demora en la obtención de la predicción o análisis puede significar la diferencia entre la vida y la muerte. Para reducir esta demora o latencia, los modelos se despliegan en procesadores cercanos a los sensores.

Por ejemplo, un automóvil autónomo no tiene tiempo de enviar imágenes a la nube para su procesamiento una vez que detecta un objeto en la carretera, ni las aplicaciones médicas que evalúan a pacientes críticos tienen margen de maniobra para interpretar los escáneres cerebrales después de una hemorragia, **ni las aplicaciones militares que detectan un misil que se dirige a su objetivo y debe actuarse con el escudo antimisiles antes de que impacte**. Y eso hace que la computación en el borde, o dentro del dispositivo, sea la mejor opción para la inferencia (Batra *et al.*, 2018).

La tabla 3.2 muestra una comparación de las prestaciones que los cuatro grandes tipos de chips para IA ofrecen en la fase de entrenamiento y de inferencia.

	Training		Inference		Generality ⁸⁸	Inference accuracy ⁸⁹
	Efficiency	Speed	Efficiency	Speed		
CPU	1x baseline				Very High	~98-99.7%
GPU	~10-100x	~10-1,000x	~1-10x	~1-100x	High	~98-99.7%
FPGA	-	-	~10-100x	~10-100x	Medium	~95-99%
ASIC	~100-1,000x	~10-1,000x	~100-1,000x	~10-1,000x	Low	~90-98%

Tabla 3.2 Comparación de prestaciones entre los grandes tipos de chips para IA.
Fuente: Khan y Mann (2020)

3.2.4.1 De las CPUs (arquitecturas Von Neuman) a las GPUs

Los primeros sistemas que pueden considerarse dentro de lo que se denomina IA, llamados sistemas expertos, se implementaban sobre chips que se basaban en una CPU que es la arquitectura Von Neuman por antonomasia. Una CPU Von Neuman se basa en una memoria donde se comparten los datos y las instrucciones, con una unidad de control (donde están el contador de programa y el decodificador de instrucciones), registros y una ALU (Unidad Aritmético-Lógica).

La GPU realmente es un procesador de imágenes y muestra la información que se va a visualizar, proporciona señales de escaneo a la pantalla y la controla. Es un componente esencial que conecta la pantalla y la placa base del ordenador. Comparada con una CPU tradicional, la GPU tienen una arquitectura con mucho más paralelismo y es más eficiente en el procesamiento de datos gráficos y algoritmos complejos³³ (ver figura 3.14).

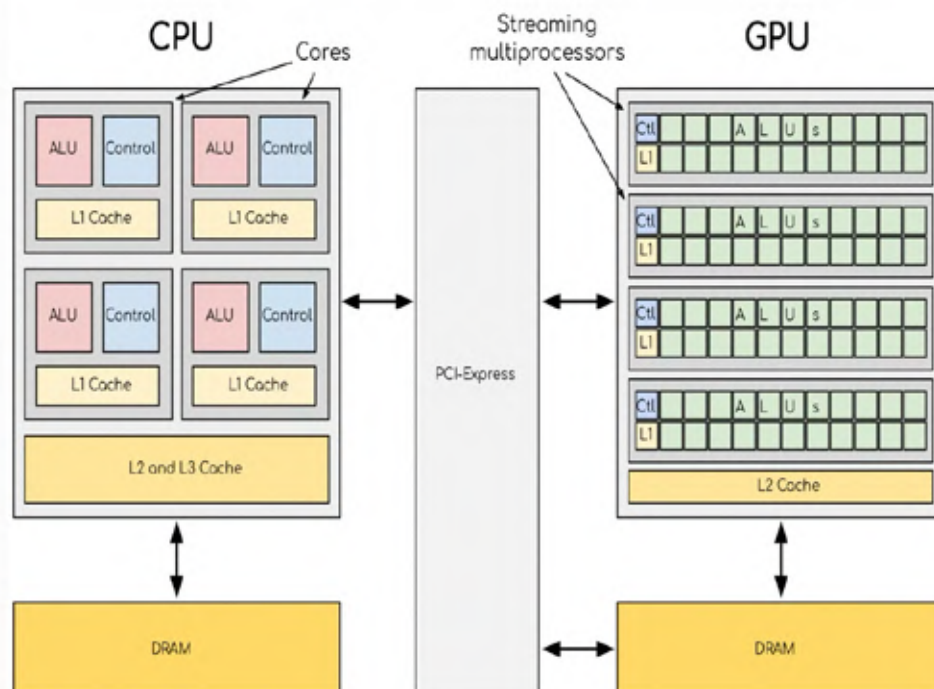


Figura 3.14 Comparación entre una arquitectura CPU y una arquitectura GPU (paralelismo)

Fuente: EuroCC National Competence Centre Sweden³⁴

La velocidad de ejecución de los programas sobre una GPU es frecuentemente centenas o millares de veces mayor que sobre CPUs de núcleo único. Las GPUs tienen una gran versatilidad, alta velocidad y eficiencia, y está especialmente indicadas para aprendizaje profundo (*deep Learning*). La intención original del diseño de las GPUs era hacer frente a la necesidad de la computación paralela a gran escala en el procesamiento de imágenes. Es esta facilidad la que se usa en la fase de entrenamiento de los modelos IA. Por otra parte, su estructura hardware no se puede configurar de forma flexible, ya que es fija; y la ejecución de un algoritmo es menos eficiente en una GPU que en una FPGA, por ejemplo.

³³ La diferencia en estructura entre GPU y CPU consiste en que la mayor parte del área de una CPU es el controlador y los registros, mientras que en la GPU tiene mucha más área dedicada a ALUs para el procesamiento paralelo a través de instrucciones SIMD (Single Instruction Multiple Data) para ejecutar el procesamiento sobre múltiples datos de forma simultánea. (Li Gu y Jiang, 2019).

³⁴ Para más detalles puede consultarse <https://enccs.github.io/gpu-programming/2-gpu-ecosystem/>

3.2.4.2 GPUs: Tipos, Prestaciones. NVIDIA H100 Tensor Core

Las GPUs son el tipo de chip IA predominante en los centros de datos IA en la nube, aunque se van usando cada vez más las combinaciones de CPU con Aceleradores de IA (chips con arquitecturas especializadas ASICs).

En la década de 2000 ya era evidente que las GPU eran ideales para tareas intensivas en cálculo tensorial. Sin embargo, la empresa *Nvidia* apostó por una expansión significativa del mercado del aprendizaje profundo y agregó una característica adicional a su arquitectura *Volta* para destacar en este campo. Comercializados como núcleos tensoriales, estos eran bancos de unidades lógicas FP16, que operaban juntas como una gran matriz, pero con capacidades muy limitadas. De hecho, eran tan limitados que solo realizaban una función: multiplicar dos matrices FP16 4x4 y luego agregar otra matriz FP16 o FP32 4x4 al resultado (un proceso conocido como operación GEMM³⁵). El resto es esencialmente un chip SIMD (Single Instruction Multiple Data) masivamente paralelo, respaldado por un sistema de memoria/caché robusto e intrincado (véase figura 3.15).

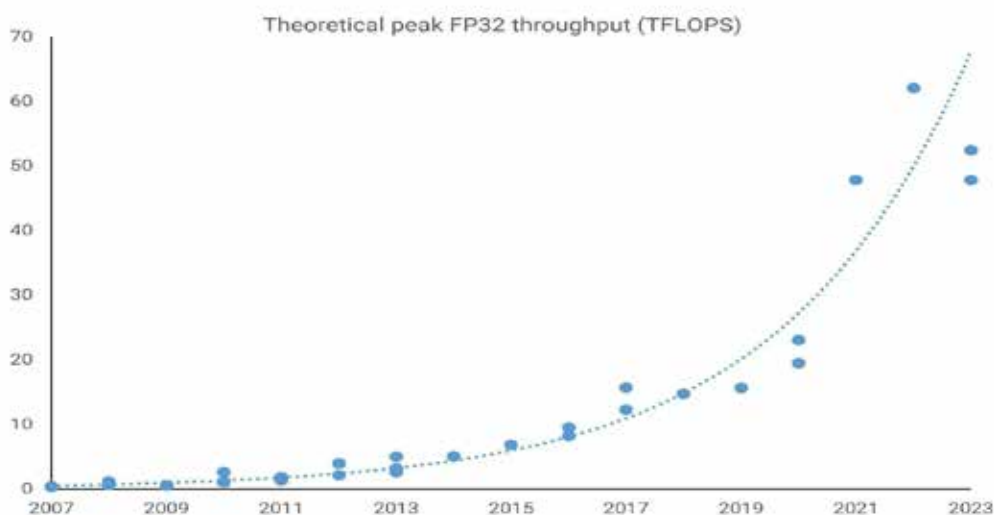


Figura 3.15 Evolución en el tiempo del “Rendimiento máximo teórico en FP32” en TFLOPs³⁶
Fuente: Evanson (2024)

35 La operación GEMM (General Matrix Multiplication) es un proceso fundamental en Modelos de IA como GPT y es una de las operaciones más intensivas en cómputo utilizadas en redes neuronales. GEMM realiza la operación matricial: $C = \alpha \cdot A \cdot B + \beta \cdot C$, donde A y B son matrices de entrada, C es la matriz de salida (puede ser inicializada con valores previos), α y β son escalares que controlan la contribución de cada término. Esto permite una multiplicación de matrices más flexible y eficiente en hardware optimizado.

36 TFLOP (Tera Floating Point Operations Per Second) es una unidad de medida del rendimiento computacional, especialmente usada en IA, videojuegos y supercomputación. TFLOP = 1 billón de operaciones en punto flotante

Las GPUs más extendidas hoy en día son las de Nvidia. En la mayoría de los centros de datos en la nube se encuentran el H100 y el H200. En 2025 se empieza a instalar el B200, que mejora sustancialmente el rendimiento del H100³⁷ (ofrece 3 veces el rendimiento de entrenamiento y 15 veces el rendimiento de inferencia que los sistemas de la generación anterior).

Según Smith (2024): *“El dominio de la IA de Nvidia, como la explosión del aprendizaje automático en sí, es un giro reciente de los acontecimientos. Pero tiene sus raíces en el esfuerzo de décadas de la compañía para establecer las GPU como hardware de computación general que es útil para muchas tareas además de la representación de gráficos. Ese esfuerzo abarca no solo la arquitectura de GPU de la empresa, que evolucionó para incluir ‘núcleos tensores’ expertos en acelerar las cargas de trabajo de IA, sino también, fundamentalmente, su plataforma de software, llamada **CUDA** (Compute Unified Device Architecture), para ayudar a los desarrolladores a aprovechar el hardware”.*

Es esencial la existencia de herramientas software eficientes que permitan a los desarrolladores aprovechar al máximo los recursos hardware que se les ofrecen. Lanzada en 2006, **CUDA** ayuda a los desarrolladores a utilizar los numerosos núcleos de una GPU de Nvidia. Eso ha demostrado ser esencial para acelerar las tareas de cómputo altamente paralelizadas, incluida la IA generativa moderna. El éxito de Nvidia en la creación del ecosistema CUDA hace que su hardware sea el camino de menor resistencia para el desarrollo de IA.

La **GPU NVIDIA H100 Tensor Core** basada en la arquitectura de GPU NVIDIA Hopper, (véase figura 3.16) ofrece un alto rendimiento para las plataformas de centros de datos, y es capaz de adaptarse a diversas cargas de trabajo, desde cargas de trabajo de pequeñas empresas, hasta la exaescala y modelos de IA de billones de parámetros. Implementado mediante el proceso 4N de TSMC personalizado para NVIDIA con 80 mil millones de transistores y que incluye numerosos avances arquitectónicos, H100 fue el chip más avanzado del mundo jamás construido hasta el año 2024.

por segundo. El cálculo aproximado es TFLOPS = núcleos X Frecuencia (GHZ) x Instrucciones FLOP por ciclo.

37 NVIDIA DGX™ B200 es una plataforma de IA unificada para procesos de desarrollo a implementación para empresas de cualquier tamaño en cualquier etapa de su viaje de IA. Equipada con ocho GPU NVIDIA Blackwell interconectadas <https://www.nvidia.com/es-es/data-center/dgx-b200/>



Figura 3.16 GPU Nvidia H100. Fuente: NVIDIA

Su sucesora es la **NVIDIA H200**, y se basa en la arquitectura de NVIDIA Hopper. Es la primera GPU que ofrece 141 gigabytes (GB) de memoria HBM3e a 4,8 Terabytes por segundo (TB/s), lo que supone casi el doble de capacidad que la H100 con 1,4 veces más ancho de banda de memoria. La H200 cuenta con una memoria más grande y rápida que acelera la IA generativa y los LLM, a la vez que hace avanzar la computación científica para cargas de trabajo de HPC con una mejor eficiencia energética y un menor coste total de propiedad.

También de la empresa NVIDIA, la **GPU Blackwell** tiene más de 2,5 veces la cantidad de transistores en las GPU NVIDIA Hopper, y usa el proceso 4NP de TSMC diseñado para NVIDIA, para lograr alcanzar los 20 petaFLOP. Esta arquitectura fusiona dos matrices en una única GPU unificada. Cada una de las dos matrices es la matriz más grande posible dentro de los límites del tamaño de la retícula, tan grande como se puede construir actualmente. Los dos chips están conectados y unificados con una única interfaz de alto ancho de banda (NV-HBI) de chip a chip de NVIDIA de 10 terabytes por segundo (TB/s), lo que proporciona una GPU unificada y totalmente coherente. Sigue aprovechando y beneficiándose del ecosistema de herramientas de desarrollo de NVIDIA, bibliotecas CUDA-X, más de cuatro millones de desarrolladores y más de 3000 aplicaciones que escalan el rendimiento en miles de nodos.

Recientemente se ha presentado el nuevo Transformer Engine de segunda generación, que usa la tecnología Blackwell Tensor Core personalizada combinada con las innovaciones de TensorRT-LLM y Nemo Framework para acelerar la inferencia y el entrenamiento para los modelos LLM y Mixture-of-Experts (MoE).

El segundo gran fabricante de GPUs -a distancia-, AMD ha luchado contra Nvidia en el campo de los chips gráficos durante casi dos décadas, sin alcanzar su nivel de ventas. Aun así, el hardware de AMD tiene sus puntos fuertes. La amplia cartera de GPU de la empresa se extiende desde gráficos integrados para portátiles hasta GPU para centros de datos enfocados en IA con más de 150 mil millones de transistores. La empresa también fue una de las primeras en apoyar y adoptar la memoria de gran ancho de banda (HBM), un tipo de memoria que ahora es esencial para las GPU más avanzadas del mundo.

La GPU discreta **AMD Instinct MI325X** (Ver Figura 3.17) ofrece un buen rendimiento en un amplio conjunto de tipos de datos necesarios para el software de IA, incluidos FP16, BF16, FP8 e INT8 utilizados tanto en inferencia como en entrenamiento de alta precisión. Una memoria HBM3E líder en la industria de **256 GB** MI325-001^a y **un ancho de banda de 6 TB/s** permiten que un solo acelerador contenga y procese un **modelo de 1 billón de parámetros**, al tiempo que reduce el costo total de propiedad para modelos de selectos “Large-Language”. La compatibilidad con mecanismos de matrices dispersas³⁸ economiza el uso de memoria y aumenta el rendimiento.

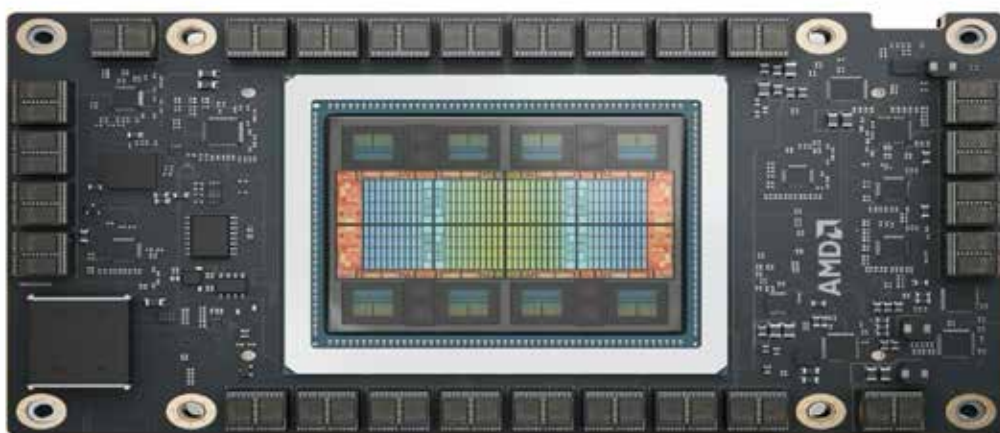


Figura 3.17 GPU Instinct MI325X AI Accelerator. Fuente: AMD

3.2.4.3 FPGAs: Xilinx VITIS de AMD

Una FPGA es un circuito hardware con puertas lógicas reconfigurables. Por tanto, se puede montar cualquier circuito lógico sobre el conjunto de puertas con lo que es posible un circuito personalizado sobre el chip ya fabricado, no solo durante la fase de diseño o fabricación, sobrescribiendo su configuración.

³⁸ “Matrices dispersas” se refiere a la proporción de elementos cero o muy cercanos a cero en una matriz. Se usa en redes neuronales, procesamiento de datos y optimización para reducir la carga computacional.

El proceso de diseño lógico y simulación es muy similar a un ASIC, pero en lugar de mandar el diseño a la fábrica (*foundry*), se mapea sobre el circuito físico. Así, es posible crear desde puertas lógicas simples de una sola función hasta procesadores de múltiples núcleos. Por ejemplo, se puede configurar una FPGA con miles de unidades de memoria en un modelo de computación masivamente paralela como las GPU.

La reconfigurabilidad, el bajo consumo y su latencia reducida hacen que los FPGA se destaquen en las tareas de inferencia, sobre todo en tiempo real. El chip FPGA puede rediseñarse para implementar mejor los diferentes requisitos cambiantes de las redes neuronales profundas (Li, Zhang y Wang, 2020). Su programación (con lenguajes de descripción de hardware) requiere una experiencia que no existe por ahora para la IA, hay muy pocas bibliotecas de aprendizaje profundo que admitan FPGA sin modificaciones (LeFlow es un intento de adaptar TensorFlow); y la inversión necesaria en coste de FPGA, implementación y programación, son factores que han frenado su uso en este ámbito.

Los FPGA sirven como un compromiso entre estos dos extremos de flexibilidad y rendimiento que representan los procesadores de propósito general y los ASICs. Brindan los beneficios de rendimiento de los circuitos integrados, con la flexibilidad reconfigurable de los GPP. En un nivel bajo, los FPGA pueden implementar lógica secuencial mediante el uso de flip-flops y lógica combinacional a través del uso de tablas de búsqueda. Los FPGA modernos también contienen componentes reforzados para funciones de uso común, como núcleos de procesador completos, núcleos de comunicación, núcleos aritméticos y RAM de bloque (BRAM). Además, las tendencias actuales de FPGA tienden hacia un enfoque de diseño de sistema en chip (SoC), donde los coprocesadores ARM y los FPGA se encuentran comúnmente en la misma estructura.

Los FPGA modernos también admiten la reconfiguración dinámica parcial, donde parte del FPGA se puede reprogramar mientras se utiliza otra parte del FPGA. Esto puede tener implicaciones para los grandes modelos de aprendizaje profundo, donde las capas individuales se pueden reconfigurar en el FPGA sin interrumpir el cálculo en curso en otras capas. Esto permitiría adaptar modelos que pueden ser demasiado grandes para caber en un solo FPGA y también aliviaría las costosas lecturas de memoria global al mantener los resultados intermedios en la memoria local.

Las principales FPGAs del mercado son AMD (Xilinx) e Intel (Altera). Xilinx y Altera han dominado más del 85 % del mercado de FPGAs durante tres décadas hasta que fueron adquiridas por los principales fabricantes de procesadores.

Conscientes de la necesidad de proporcionar herramientas de desarrollo, los fabricantes de FPGA ofrecen entornos como Xilinx Vitis-AI (Van Maarseveen, Julio 2023). La figura 3.18 ilustra el flujo de trabajo propuesto por (Khaki y Choi, 2025) para implementar modelos CNN preentrenados, específicamente VGG16 y VGG19, en FPGA utilizando estas herramientas.

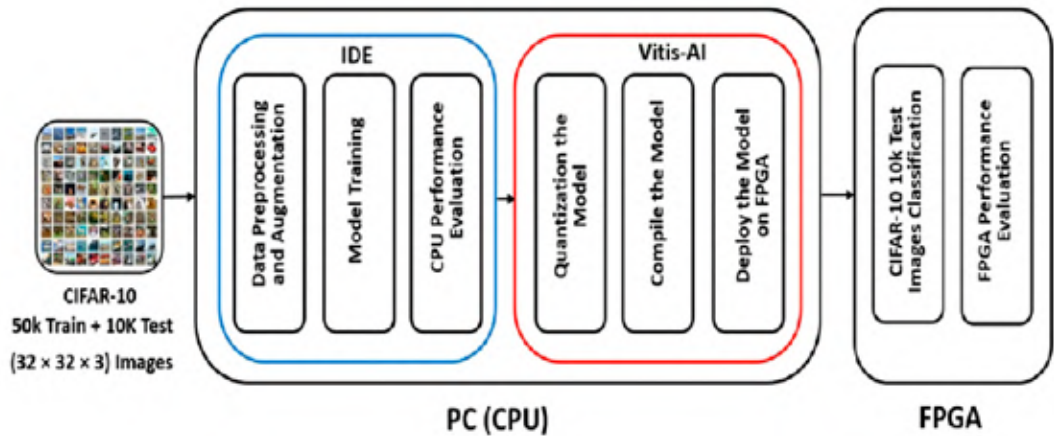


Figura 3.18 Flujo de diseño para implementar modelos sobre FPGA con Xilinx-Vitis IA
Fuente: Khaki y Choi (2025)

Las FPGA se utilizan para soportar aplicaciones de IA en la nube, en el centro de datos y en el borde. La FPGA AMD Versal AI Edge se ha utilizado para inteligencia de señales en tiempo real, procesamiento de radar y sonar, interferencia y suplantación de identidad electrónica, y sistemas antidrones.

3.2.5 ASICs y aceleradores IA

Un ASIC es, en general, un chip optimizado y personalizado para una aplicación específica. Los ASICs pueden optimizarse para tareas de IA específicas, alcanzando mejores prestaciones y eficiencia energética comparados con la GPUs y CPU; suelen optimizarse a nivel de hardware, procurando que ocupen la mínima área de silicio, el menor consumo de energía posible, altas prestaciones y mínimo coste. Tanto los ASICs como las FPGAs implican ciclos de diseño largos y costosos, pero los ASICs pueden resultar en mejores precios al tener un hardware optimizado, a costa de perder flexibilidad para implementar cambios.

Están especializados para desplegar y ejecutar modelos de aprendizaje automático entrenados, habilitando las predicciones en tiempo real y toma de decisiones en varias aplicaciones. Esto es, procesan eficientemente los datos de entrada a través de los modelos IA para generar predicciones rápidas y fiables: son adecuados para inferencias.

Un paradigma de computación prometedor, dentro de los ASIC, es la **computación analógica en memoria (AIMC)**, que elimina la necesidad de un movimiento constante de datos al ubicar el almacenamiento y el procesamiento en un mismo lugar, lo que **reduce significativamente el consumo de energía y acelera los cálculos**. Aprovechando las tecnologías de memoria no volátil programable, como la memoria de acceso aleatorio resistiva (RRAM), la memoria

de cambio de fase (PCM) y la memoria flash, la AIMC permite un almacenamiento de alta densidad y ejecuta operaciones de acumulación múltiple (MAC) directamente dentro de las celdas de memoria, siguiendo la ley de Ohm y la ley de Kirchhoff. (Li *et al.*, 2024).

Al integrar los dispositivos emergentes en matrices de barras cruzadas resistivas (RCA), se puede ejecutar la multiplicación de matriz-vector aproximada (MVM) en el dominio analógico -este es el cálculo dominante en muchas aplicaciones IA. Esto es prometedor porque **el cálculo es significativamente más eficiente energéticamente que en el dominio digital**. El movimiento de datos también se reduce sustancialmente al almacenar la matriz en la memoria y realizar el cálculo in situ.

Sin embargo, el principal desafío de aprovechar la computación analógica en memoria es que la precisión computacional puede degradarse por varias fuentes de errores y variaciones. Esto incluye errores de escritura del dispositivo, parásitos de matriz distintos de cero, rendimiento limitado del dispositivo, deriva de resistencia, variaciones de temperatura, ruido aleatorio y aguante limitado del dispositivo (Channamadhavuni *et al.*, 2021).

Mientras que empresas con décadas de antigüedad como AMD e Intel buscan utilizar sus propias GPU para competir con Nvidia, algunas empresas emergentes tratan de diferenciarse desarrollando aceleradores IA: chips que mejoran drásticamente la eficiencia del entrenamiento y la inferencia de la IA generativa (Smith, 2024).

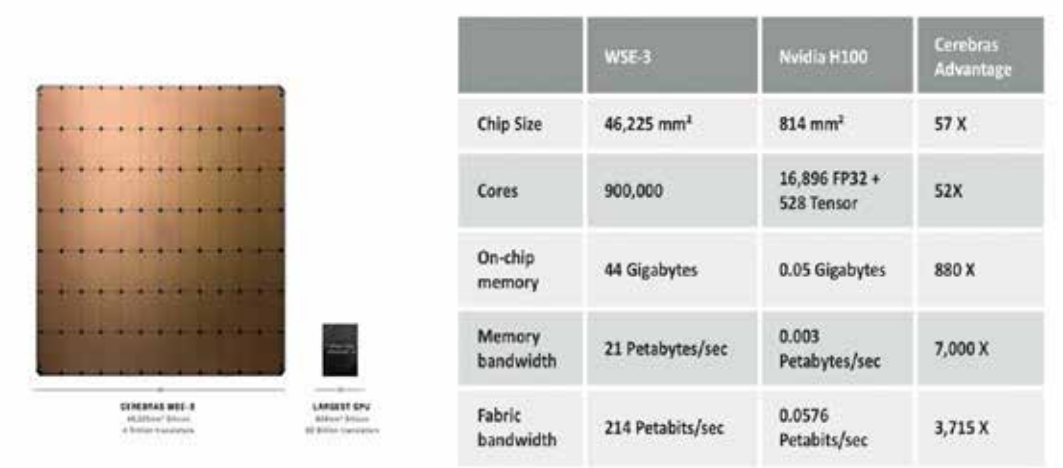


Figura 3.19. Cerebras WS-3. Integración a escala de oblea. Fuente: Cerebras

Por otra parte, **la integración a nivel de oblea plantea problemas como la alta complejidad de la fabricación** (necesita litografía avanzada y es difícil garantizar la calidad uniforme de una oblea grande), el **bajo rendimiento** (grandes tasas de rechazo, un solo defecto arruina

39 <https://www.cerebras.ai/chip>

una oblea completa), la **difficultad de enfriar la oblea completa**, su **escalabilidad limitada** y los **costes de fabricación elevados**.

SambaNova, fundada en 2017, es otra empresa de diseño de chips que aborda el entrenamiento de IA con una arquitectura de chip poco convencional. Su producto estrella, el SN40L “Cerulean”, se basa en una “arquitectura de flujo de datos reconfigurable” compuesta por mosaicos de memoria y procesadores. Los enlaces entre estos mosaicos se pueden alterar sobre la marcha para facilitar el movimiento rápido de datos para grandes redes neuronales. En este sentido, puede afirmarse que SN40L comparte, en parte, una filosofía de diseño parecida a las FPGAs (reconfigurabilidad), pero con mucha más eficiencia que éstas en el entrenamiento de los modelos IA.

También ofrece una pila de software adaptada al SN40L; SambaFlow permite analizar modelos de IA y ayudar a reconfigurar el SN40L para acelerar el rendimiento. Podría ser útil para entrenar grandes modelos de lenguaje. No es aún una empresa consolidada, pero tiene ya clientes como Analog Devices (Smith, 2024).

El chip SN40L se implementa en un chip de 5 nm de TSMC con tres niveles de memoria (520 MB en el chip, 64 GB memoria de alta velocidad y 1.5TB de capacidad máxima), 1040 unidades de cómputo y memoria con sus conmutadores en malla sobre el mosaico. Contiene 102000 millones de transistores y alcanza 638 TFLOPS (bf16). Según indica la empresa, es útil tanto para entrenamiento como para inferencia de modelos de IA generativa.

Google también fabrica sus propios ASICs -las unidades de procesamiento tensorial TPUs, específicas para entrenar grandes modelos IA basados en Transformers o CNN, definidos con entornos de programación como TensorFlow, Pytorch o JAX. Un chip TPU contiene uno o más TensorCores, y cada uno de ellos consta de una o más unidades de multiplicación de matrices (MXUs), una unidad vectorial y una unidad escalar. A su vez, una MXU se compone de acumuladores multiplicadores de 256 x 256 (TPU v6e) en un array sistólico, capaz de realizar 16,000 operaciones de multiplicación y acumulación por ciclo. Todas las multiplicaciones toman entradas de bfloat16, pero todas las acumulaciones se realizan en formato de número FP32. La unidad vectorial se usa para el procesamiento general, como las activaciones y la operación softmax. Por último, la unidad escalar se usa para el flujo de control, el cálculo de direcciones de memoria y otras operaciones de mantenimiento.

Sus especificaciones son realmente interesantes (v6e): proceso máximo por chip (bf16) 918 TFLOPS y 1836 TOPS para INT8; capacidad HBM por chip de 32 GB; ancho de banda HBM por chip de 1640 GBps; 1536 GiB de DRAM por host con 8 chips en cada uno. A nivel de agregación, son 256 chips por pod, con un procesamiento máximo (BF16) de 234.9 PFLOP con un ancho de banda de red del centro de datos por pod de 25.6 Tbps.

La empresa china *Cambrian* también tiene su propia arquitectura de chips IA, con su chip más avanzado Siyuan 370 y que se presenta como una tarjeta aceleradora MLU370-S4/S8. Según indican, el consumo de energía de la tarjeta es de solo 75 W, lo que puede proporcionar 3 veces la capacidad de decodificación y 1,5 veces la capacidad de codificación en comparación con las GPU del mismo tamaño, y por su eficiencia y compacidad las hace adecuadas para su uso en servidores con alta densidad. Sus características más notables son: su proceso de fabricación de 7nm por TSMC; la tecnología chiplet que permite integrar componentes de forma escalable; el número de transistores integrados que llega a 39000 millones; y su potencia de cómputo de hasta 256 TOPS en precisión INT8. Es el primer chip de IA en la nube en China que soporta memoria **LPDDR5**, triplicando el ancho de banda de memoria en comparación con la generación anterior y mejorando la eficiencia de acceso en un 50% respecto a GDDR6.

3.2.6 Uso avanzado de chips para IA en Defensa

De lo explicado hasta el momento se entiende que los chips dedicados (ASICs) son más eficientes que las GPUs, quedando las GPUs para entrenamiento con ingentes cantidades de datos. **Se estima que para 2030 la solución más extendida será “CPU+ acelerador IA”** (Burkacky *et al.*, 2024), es decir, una arquitectura de chip especializada (ASIC) y FPGA (si se desea más flexibilidad, a costa de más consumo de energía) con rendimiento óptimo para tareas de IA específicas.

A continuación, se describen ejemplos concretos de desarrollos de sistemas específicos de defensa en los que se han usado los tipos de chips descritos anteriormente⁴⁰.

3.2.6.1 Aplicaciones de chips IA para Defensa

Chips para guiado de misiles hipersónicos

Un misil hipersónico sigue una trayectoria de órbita baja con la intención de avanzar más en su trayecto que un misil balístico, que puede ser detectado antes por los radares del objetivo. La IA está transformando los sistemas de guía de estos misiles al proporcionar capacidades avanzadas para el procesamiento de datos, la toma de decisiones y el ataque a objetivos. Por ejemplo, pueden adaptar sus rutas de vuelo en tiempo real, mejoran el reconocimiento y clasificación de objetivos diferenciando mejor los objetivos reales de los señuelos, y facilitan la realización de maniobras evasivas en rutas previstas de interceptores enemigos. El chip Jetson TX2i GPU de Nvidia se utiliza en el guiado de misiles hipersónicos.

Chips para drones

⁴⁰ Se han seleccionado por su interés; nótese que se mencionan sobre todo aplicaciones de campo de batalla donde la inferencia de modelos IA juega un papel relevante.

Los chips IA para montar en un dron tienen que ser capaces de funcionar en un entorno operativo difícil en cuanto a condiciones variables de humedad, temperatura, presión, fuerza G ascendente/descendente; consumiendo poca energía (la batería del dron debe ser capaz de mantenerlo en vuelo además de alimentar al resto de sistemas); e integrados con los sensores y actuadores propios del dron.

El sistema FLYC-300 (Ver figura 3.20) de Neousys se basa en el chip NVIDIA Jetson Orin NX y se ha diseñado específicamente para este uso. Sus dimensiones son reducidas (124mm x 123mm x 30.5mm), pesa menos de 300 gr, proporciona hasta 100 TOPS por su GPU y tiene varias interfaces de cámaras (RGB, infrarrojas, hiperspectrales, lidar, radar, HDR, 3D). UART y CAN integradas para interactuar con el controlador de vuelo, y unidad de comunicación 4G/5G disponible. Admite un paquete de baterías para drones 4S-14S.

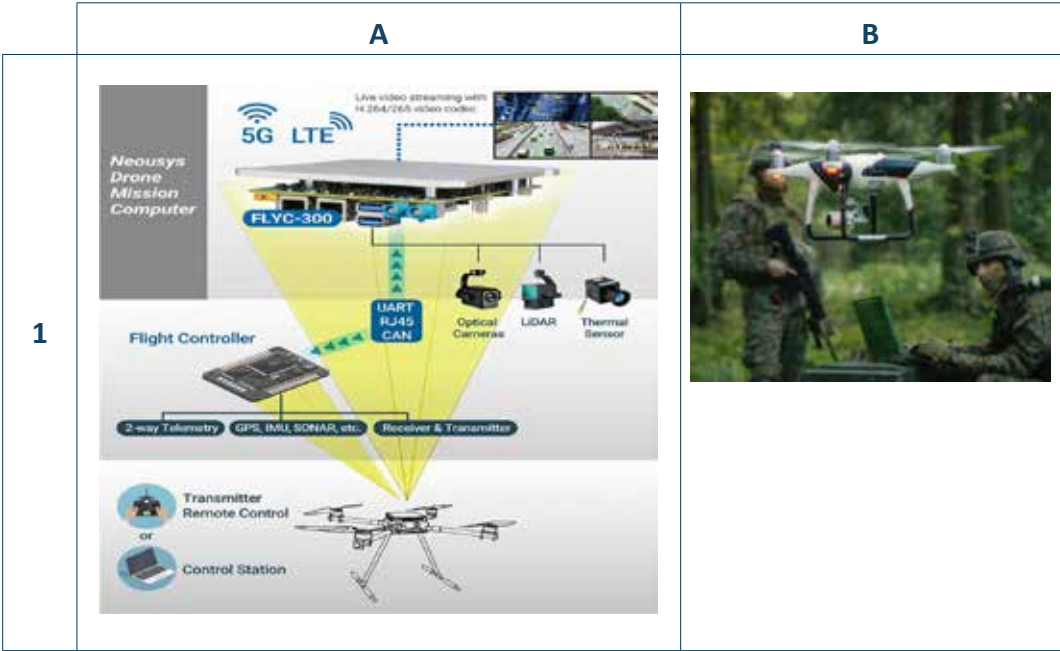


Figura 3.20 FLYC-300 de Neousys. Chip IA en el borde para drones
Fuente: Neousys

El chip Jetson Orin NX está construido en torno a una versión de bajo consumo de energía del SoC NVIDIA Orin, que combina la arquitectura de **GPU NVIDIA Ampere** con capacidad operativa de 64 bits, procesamiento de imágenes y video multifunción avanzado integrado y **aceleradores de aprendizaje profundo (LDA) NVIDIA**. El rendimiento de cómputo de hasta 100 TOP INT8 (dispersos) y 50 TOP INT8 (densos) en Jetson Orin NX de 16 GB y hasta 70 TOP INT8 (S) y 35 TOP INT8 (D) en Jetson Orin NX de 8 GB permite que Jetson Orin NX ejecute múltiples redes neuronales en paralelo y procese datos de múltiples sensores de alta resolución simultáneamente. Con estas capacidades, es posible para el dron analizar datos de tiempo real de sus cámaras para realizar un mapa 3D y compararlo con la infor-

mación topográfica preexistente para optimizar las rutas de vuelo, minimizar los desvíos y apuntar directamente a las áreas de interés.

Chips para ciberseguridad

Algunos gobiernos han establecido programas sobre ciberseguridad en la que se aplica la IA con chips especializados. Algunos de los programas más notables son:

- **DARPA HALO** (aprendizaje jerárquico con adaptación en chip): es un chip neuromórfico de IA para detección de amenazas cibernéticas en tiempo real con consumo ultra bajo. Se utiliza en sistemas de defensa autónomos seguros.
- **Iniciativa de criptografía post-cuántica de la NSA e IBM** utiliza procesadores de IA cuánticos para cifrado de grado militar. Diseñado para resistir futuras amenazas cibernéticas cuánticas.
- **Proyecto MAVEN con NVIDIA para ciberdefensa**, usa GPUs NVIDIA Jetson y el entorno Morpheus para la monitorización de red por inspección profunda de paquetes, para detectar anomalías en tiempo real y bloquear ataques de día cero, malware y amenazas internas.
- **Sistemas militares mejorados con IA de Intel**: se utilizan procesadores Intel TDT Xeon para la detección de malware basada en IA en defensa. Protege las comunicaciones clasificadas y los puntos finales militares.

En la Tabla 3.3 se incluye una comparativa entre iniciativas que usan chips IA para la ciberseguridad. Siendo un campo de trabajo tan amplio en el mundo civil no se profundiza más en este estudio.

Característica	NVIDIA Jetson & Morpheus (IA para ciber defensa militar)	Intel Xeon + TDT (Detección de ciber amenazas mejorada por IA)	AMD EPYC + AI Security (IA cifrada para defensa)	DARPA HALO (IA neuromórfica para seguridad militar)	IBM AI + Quantum Cybersecurity (Cifrado a prueba de futuro)
Caso de uso principal	Detección y defensa contra amenazas cibernéticas impulsadas por IA en redes militares	Detección de amenazas basada en hardware IA en sistemas militares seguros	Cifrado y procesamiento de datos seguro-basados en IA	Procesadores neuromórficos basados en IA para ciberdefensa de consumo ultra bajo	Cifrado cuántico seguro basado en IA e infraestructura de nube segura
Tipo de Hardware	GPUs IA (Jetson Xavier, Orin)	CPUs x86 Aceleración IA (Xeon)	Servidores CPUs Seguro, Optimizado IA	Chips IA Neuromórficos	Chips Híbridos de IA Cuántica.
Fortalezas Clave	Detección de ciberataques en tiempo real, inspección profunda de paquetes, defensa de red	Protege los sistemas seguros contra malware, APT y ciber espionaje	Cifrado y virtualización impulsados por IA para infraestructura de nube de defensa	IA inspirada en el cerebro para detección de anomalías en tiempo real y con consumo ultra bajo	Cifrado pos-cuántico basado en IA para ciberseguridad militar a prueba de futuro

Característica	NVIDIA Jetson & Morpheus (IA para ciber defensa militar)	Intel Xeon + TDT (Detección de ciber amenazas mejorada por IA)	AMD EPYC + AI Security (IA cifrada para defensa)	DARPA HALO (IA neuromórfica para seguridad militar)	IBM AI + Quantum Cybersecurity (Cifrado a prueba de futuro)
Beneficios de Ciber seguridad	Previene ataques de guerra cibernética y amenazas de día cero	Detección a nivel de hardware de amenazas cibernéticas de clase militar	Computación de IA segura y procesamiento de datos cifrados	Monitoreo de red en tiempo real basado en IA con un consumo mínimo de energía	Protege contra amenazas cibernéticas cuánticas de próxima generación
Consumo de energía	Moderado (Optimizado para análisis de seguridad impulsados por IA)	Bajo (Integrado en CPUs seguras)	Moderado (Eficiencia de seguridad de IA de nivel de servidor)	Consumo ultra bajo (Eficiencia neuromórfica)	Alto (Cifrado híbrido de inteligencia artificial y cuántica)
Adecuado para	Agencias de inteligencia militar, redes de defensa, comunicación segura	Ciberseguridad táctica con IA para entornos militares seguros	Sistemas de defensa cifrados basados en IA y protección de datos clasificados	Operaciones cibernéticas mejoradas con IA que requieren un consumo mínimo de energía	Ciberseguridad poscuántica para sistemas criptográficos militares

Fuente: elaboración propia

Chips IA en el borde

A los requisitos militares de equipamientos en el borde se les suma la **necesidad de poder realizar inferencias** (en algunos, muy pocos casos, también entrenamiento) **de forma local, con latencias mínimas y poco acceso a la red** (intermitente o desconectada). Para que sea posible la inferencia en el borde, los modelos deben haber sido **optimizados** para dispositivos con recursos limitados. Por ejemplo, existen modelos reducidos de redes neuronales convolucionales como mobileNet, efficientNet o YOLO (You Look Only Once) que pueden ejecutarse sobre NVIDIA Jetson.

Quizás uno de los mayores desafíos a los que se enfrentan los chips IA en el borde es el del **consumo de energía**. Estos chips no pueden conectarse a fuentes de alimentación de cierta potencia, sino que se suelen alimentar con baterías muy pequeñas (pilas de botón) y además deben tener una duración importante pues no es fácil su recambio por estar situados en ambientes con accesos difíciles. Así pues, estos chips deben operar con un consumo de energía muy reducido.

Para ensayar y conciliar la necesidad de recursos limitados en consumo y las necesidades computacionales de las redes neuronales profundas en el borde, se ha propuesto la utilización de un **chip GAP8, basado en RISC-V como motor de computación en el borde, de ultra bajo consumo**. El GAP8, contiene 8 núcleos de RISC-V. Lo más importante es que GAP8

admite la implementación y aceleración de estas redes. Sin embargo, existen limitaciones en el tamaño de la memoria. Los investigadores proponen un algoritmo de optimización adaptativo al hardware para garantizar el funcionamiento a alta velocidad de las redes neuronales profundas en la IA de borde (Zhenling *et al.*, 2024).

Los resultados experimentales muestran que después de implementar las DNN, el conteo de parámetros y la tasa de poda de operaciones de punto flotante del modelo optimizado con el algoritmo EN-HSPG alcanzan hasta el 98,82 % y el 91,28 % respectivamente, utilizando solo el 54 % de la memoria L2. Además, el tiempo de inferencia del modelo optimizado EN-HSPG es de solo 115,26 ms en GAP8. Por lo tanto, la investigación permite el entrenamiento de redes de aprendizaje profundo complejas en dispositivos de borde con capacidades informáticas limitadas.

Otro ejemplo que muestra el método de diseño de sistemas de consumo de energía ultra bajo de la computación de borde de IA es cada vez más importante es el desarrollado por Meng *et al.* (2023) con un suministro de energía limitado, **los dispositivos de computación de borde de IA no solo necesitan completar el algoritmo de razonamiento de borde de IA en tiempo real, sino que también deben entrar en el estado de “sueño profundo” (Deep sleep State) a tiempo para reducir la pérdida innecesaria de energía.** Basado en el chip de computación de borde de IA Hisilicon hi3559av100, el trabajo estudia los métodos de diseño de sistemas de consumo de energía ultra bajo como reloj, red de suministro de energía y lógica de aplicación, de modo que todo el sistema pueda minimizar la pérdida de energía del sistema y cumplir con los requisitos del sistema de aplicación mientras calcula el algoritmo de IA en tiempo real.

Una revisión del hardware para computación IA en el borde, así como las librerías y el software para cargar los modelos IA específicos, como Tensor Flow, se puede encontrar en (Sipola *et al.*, 2022)

3.2.7 Evolución y tendencias de Chips IA

Tanto la potencia de cómputo de los chips es esencial para la aplicación de la IA en general y en la defensa en particular, como la necesidad de reducir el consumo de energía. Por este motivo, se han estado buscando técnicas mediante el **desarrollo de nuevos algoritmos y arquitecturas hardware más eficientes energéticamente.** Entre los enfoques en un estado incipiente podemos mencionar la **detección neuromórfica**, la **fotónica integrada** y la **microelectrónica para la computación cuántica.**

La **detección neuromórfica** imita las capacidades de procesamiento sensorial del cerebro, en un enfoque basado en el **procesamiento basado en eventos**, lo que reduce el consumo de energía y aumenta la eficiencia en comparación con los sensores tradicionales. El sistema

sensorial biológico procesa estímulos externos, como el tacto físico, la luz, el sonido y los productos químicos, en paralelo con un consumo de energía ultra bajo que es detectado por los receptores, se genera un pico eléctrico y se transmite al sistema nervioso central para decodificarlo.

En los últimos años, inspirándose en este mecanismo, se han explorado los **dispositivos neuromórficos emergentes basados en neuronas sensoriales artificiales** (ASN) que pueden simular los sentidos humanos y convierten de manera eficiente la información ambiental en impulsos eléctricos, con el objetivo de superar las limitaciones de los circuitos convencionales basadas en CMOS. Los dispositivos neuromórficos emergentes generalmente ofrecen alta escalabilidad, bajo consumo de energía y alta velocidad, lo que puede reducir los costes de energía y hardware asociados con la transducción sensorial (Zhong *et al.*, 2025). *Intel Loihi* es un chip neuromórfico basado en neuronas digitales que funciona en modo dirigido por eventos, de bajo consumo muy adecuado para drones de combate y sistemas de defensa antimisiles.

Otro tipo de ASN son las olfativas, que pueden ser de gran utilidad para detectar compuestos orgánicos volátiles y otras sustancias químicas en el aire, y se aplican ampliamente en una variedad de aplicaciones, como la calidad de los alimentos, el monitoreo ambiental y el diagnóstico. Este enfoque de **sensores bioinspirados** pueden utilizarse en el ámbito de la Defensa para imitar la visión de los insectos y la audición de algunos animales; para implementar interfaz cerebro-ordenador y para mejorar la criptografía.

Una de las partes más desafiantes del diseño de un sistema neuromórfico a gran escala es diseñar una **red de comunicación de impulsos escalable**, que sea capaz de mantenerse al día con los requisitos de conectividad masivos que se encuentran en estos sistemas. La Tabla 3.4 resume los diferentes sistemas de comunicación que se encuentran en el hardware neuromórfico. Estos sistemas pueden escalar de manera eficiente a tamaños mayores que los de las computadoras von Neumann, ya que almacenan información con el elemento computacional, lo que elimina el cuello de botella de von Neumann. Los sistemas neuromórficos pueden escalarse horizontalmente con un acoplamiento flexible de placas (Young *et al.*, 2019).

Chip neuromórfico	Conexionado	Máximo ancho de banda de la comunicación	Conexión con el host	Tipo de paquete y tamaño	Pérdida de paquetes	Tiempo de simulación
Human brain	Conexiones de larga distancia entre clústeres	No disponible		Pulsos eléctricos Hendidura (cleft) sináptica	Si	Tiempo real
Neurogrid	Árboles de encañamiento multibcast	Transmisor: 43.4 Mspike/s Receptor: 62.5 Mspike/s Router: 1,17 Gpalabras/s	USB via FX2	Paquetes de longitud variable con identificador cola (tailword). Secuencia de palabras de 12 bits (ruta y dirección)	No	Tiempo real
Spinnaker	Mesh triangular 2D envuelto en forma toroidal	5 billones paquetes/s Cada nodo puede enviar a un máximo de 7.4 Gbit/s	Ethernet 100 Mbps o 10Gbps	Cabecera de 8 bits Contenido de 32 bits Datos (opcionales) de 32 bits	Si (reconfigurable)	Tiempo real
BrainScaleS	L1: intra wafer Rejilla asincrónica L2: inter wafer Árboles jerárquicos	Routing on wafer: 32 Gb/s Routing entre wafers: 2.8 Geventos/s	Ethernet	L1: 6 bits n° de neurona (sin sello temporal) L2: 24 bits (eventos de impulso con sello temporal)	Si. Pueden perderse paquetes si llegan al mismo tiempo o hay congestión de red	10 ³ x a 10 ⁵ x
TrueNorth	Crossbar sináptica dentro del core Rejilla asincrónica entre cores y chips	160 millones de impulsos/segundo (5.44 Gbit/s)	AXI bus a SoC PCI 2.0 (un carril)	0 bits para dx y 9 bits para dy 4 bits tick de entrega 8 bits para índice de axón 2 bits de corrección/depuración	Si. Señal de error global cuando se pierde un paquete	Más rápido que tiempo real (1x a 21x) Sync cada más para el siguiente paso
Loihi	Asincrónico NoC en una red mesh 2D. NoC se extiende en 4 direcciones para otros chips	3.4t Geventos/s de ancho de banda de impulso cross-section por fichero.	Ethernet USB	Escritura. Petición de lectura. Respuesta de lectura Mensaje de impulso Mensaje de barrera	No. Utiliza barrera asincrónica en un tiempo de ciclo de reloj de longitud variable	Tiempo de ciclo variable en función de la carga (más rápido que tiempo real)
Darwin	Las conexiones y pesos se almacenan en chip DRAM externo. Se usa la topología y retardos para actualizar los pesos.	No especificado	UART a USB	Longitud fija de cada paquete con el identificador de la neurona fuente. Sello temporal de cuando se generó el paquete	No. El tiempo progresa una vez se han enviado todos los paquetes del paso anterior	Reloj de 70 MHz
Dynap-SEL	Esquema de direccionamiento mixto con etiquetas (1º punto a punto jerárquico en chip y 2º con difusión 2D)	Tiempo de difusión 27 ns Latencia entre chips 15,4 ns Entrada: 30 M eventos/s Salida: 21 M eventos/s	Via FPGA	Etiqueta de 10 bits Cabecera de 6 bits (con dx, dy) Destino de 4 bits	No	Tiempo real

Tabla 3.4 Comparación de chips neuromórficos. Fuente: Young et al. (2019)

Es bien sabido que uno de los problemas en los centros de datos de IA es el excesivo consumo de energía⁴¹. Uno de los factores que influyen, además del movimiento de datos procesador/memorias son las interconexiones electrónicas entre chips y equipos. La fotónica que utiliza fotones (luz) en lugar de electrones para la transmisión de la información, puede ser parte de la solución. A diferencia de los electrones, los fotones proporcionan diversas dimensiones para controlar, como la longitud de onda, la polarización y el modo espacial.

Estas ventajas de las propiedades fotónicas permiten un procesamiento de datos más rápido, un **menor consumo de energía** y un **paralelismo inherente** en todos los niveles de los circuitos fotónicos integrados, lo que la posiciona como una solución transformadora para la IA. Los modelos informáticos no digitales, en particular los que se posibilitan mediante la fotónica, prometen soluciones a desafíos como la baja latencia, el alto ancho de banda y las bajas energías, lo que da lugar a un campo de **fotónica neuromórfica** en la intersección de la fotónica y el marco de la ingeniería neuronal (Gupta y Jolly, 2024)

41 Esta problemática ha abierto líneas de investigación orientadas a dimensionar la **huella hídrica de la IA**. Un estudio del grupo de investigación Hidrogeología y Medio Ambiente en la Facultad de Ciencias Geológicas de la UCM señala lo siguiente: “Se estima que el entrenamiento de un modelo de lenguaje, como el archiconocido ChatGPT, consume millones de litros de agua en concepto de refrigeración. De la misma manera, por cada veintena de respuestas que esta aplicación proporciona a cualquier usuario, se consume un litro de agua”. Evidentemente este es un asunto que merece gran atención tanto de las Administraciones Públicas como de las empresas. Para más detalles puede consultarse: ¿Cuánta agua consume la inteligencia artificial? Disponible en línea: <https://www.madrimasd.org/notiweb>

Las **redes fotónicas neuronales (NPN)** son arquitecturas de IA que utilizan luz (**fotones**) en **lugar de electrones** para realizar cálculos de redes neuronales. Aprovechan componentes ópticos como láseres, guías de ondas y circuitos fotónicos para acelerar las tareas de aprendizaje profundo con una velocidad y una eficiencia energética ultra altas. Además, son inmunes a las interferencias electromagnéticas y son más escalables que las interconexiones eléctricas.

Por el momento presentan problemas en cuanto a fabricación, limitaciones para integrar elementos de memoria, y dificultad de resolver la interfaz fotónica-electrónica en el desarrollo de sistemas IA. Una solución intermedia es la **fotónica de silicio**, que integra circuitos fotónicos (basados en luz) con circuitos electrónicos de silicio tradicionales para mejorar el procesamiento de IA neuromórfica. Al combinar la velocidad y la eficiencia energética de los fotones con la versatilidad computacional de los chips de silicio, este enfoque híbrido puede revolucionar las aplicaciones de IA en defensa, ciberseguridad e inteligencia en tiempo real.

La red neuronal fotónica con elementos ópticos configurables reside en una matriz de circuito integrado fotónico (PIC) de silicio. Algunos elementos se pueden configurar de forma analógica y no volátil mediante materiales de cambio de fase (PCM). Las líneas blancas representan el enrutamiento de la guía de ondas (ver figura 3.21).

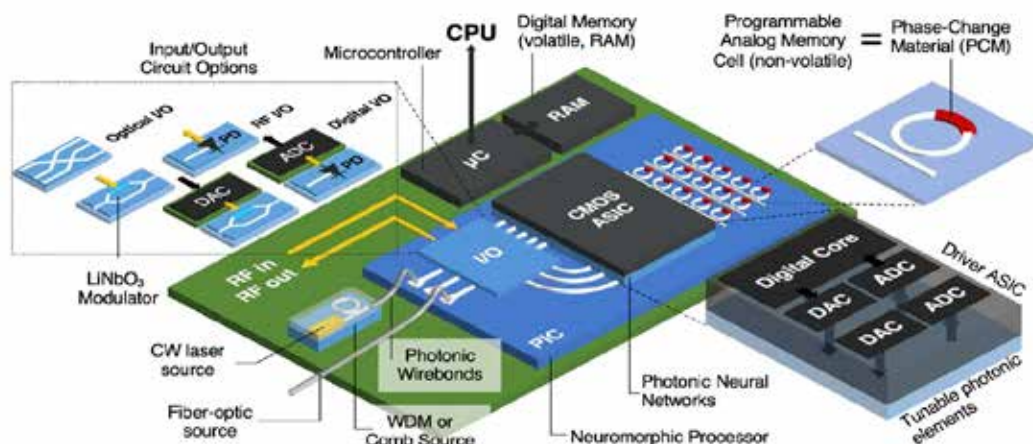


Figura 3.21 Arquitectura de procesador fotónico neuromórfico. Fuente: Shastri *et al.* (2021)

Un reto clave es hacer llegar la energía óptica a la matriz de silicio. La energía óptica puede ser proporcionada por una matriz ópticamente activa, es decir, capaz de generar luz, o, alternativamente, una interfaz de fibra externa. Para la E/S de señal (recuadro superior

izquierdo), las conversiones eléctricas a ópticas y viceversa se realizan mediante moduladores fotónicos de silicio (estructuras hexagonales) y fotodetectores (triángulos con cruces). Esto significa que todas las E/S a nivel de paquete pueden ser eléctricas u ópticas, digitales o analógicas, según la aplicación del usuario.

El otro desafío clave es controlar la red neuronal fotónica. Los recuadros negros representan matrices CMOS que satisfacen varias funciones de control, interfaz y programación. La interfaz de programación digital consta de un microcontrolador (μC) con memoria digital (RAM) co-ubicada, ambos componentes estándar (Shastri *et al.*, 2021).

3.2.8 Proyectos de financiación pública de chips IA para Defensa

Un conjunto de agencias públicas de gestión de fondos de investigación y desarrollo en EEUU y Europa han financiado diversos proyectos para el diseño y desarrollo de nuevos chips semiconductores.

En Estados Unidos, DARPA (*Defense Advanced Research Projects Agency*) gestiona el **Programa CHIPS** (*Common Heterogeneous Integration and IP Reuse Strategies*), que busca **crear un ecosistema de bloques IP (propiedad intelectual) modulares y reutilizables**, que puedan integrarse en sistemas utilizando tecnologías de integración existentes y emergentes, facilitando diseños de circuitos integrados más flexibles y reduciendo los costes y tiempos de desarrollo.

También DARPA en sus programas militares cuenta con el **Programa IDEA** (*Intelligent Electronic Assets*), que trata de desarrollar un **compilador de hardware de propósito general** que permita la traducción automática, sin intervención humana, de código fuente o esquemas a diseños físicos de circuitos integrados en menos de 24 horas. Esto busca acelerar el desarrollo de sistemas electrónicos de próxima generación y reducir la dependencia de grandes equipos de diseño especializados.

El programa **DARPA.MIL SAHARA** (*Structured Array Hardware for Automatically Realized Applications*) tiene como objetivo ampliar el acceso a capacidades de fabricación en Estados Unidos para abordar los desafíos en el desarrollo seguro de chips personalizados para sistemas de defensa. En colaboración con Intel y varias universidades, el programa busca automatizar la conversión de diseños FPGA a ASICs estructurados, mejorando el rendimiento y reduciendo el consumo energético en aplicaciones militares.

La **NASA** (*Administración Nacional de Aeronáutica y del Espacio*) ha desarrollado un método utilizando difracción de rayos X para evaluar la concentración de defectos en la estructura cristalina de obleas semiconductoras. Este enfoque permite determinar la calidad de las obleas de manera no destructiva y en menos tiempo, mejorando la fabricación de chips para aplicaciones aeronáuticas.

La **Comisión Europea y Agencias Europeas**, mediante el Fondo Europeo de Defensa (EDF) y la Agencia Europea de Defensa (EDA) han lanzado convocatorias para proyectos de investigación y desarrollo en microelectrónica y semiconductores, buscando fortalecer la autonomía tecnológica europea en sectores clave como la defensa y el espacio. Las fuentes consultadas no detallan proyectos específicos. También en Europa, la **ESA** (Agencia Espacial Europea) financia proyectos orientados al desarrollo de componentes semiconductores capaces de operar en entornos espaciales extremos, incluyendo la resistencia a la radiación y temperaturas extremas. Estos proyectos son fundamentales para garantizar la fiabilidad de los sistemas electrónicos en misiones espaciales.

3.2.9 Conclusiones sobre chips IA

Del estudio de los chips para IA en defensa se concluye que existen importantes desafíos que se deben afrontar:

1. Los sistemas de IA, cada vez más, se van desplazando hacia el borde (*edge*), donde los sensores recogen datos en tiempo real y los sistemas deben tomar decisiones críticas, realizando las **inferencias en el propio hardware en el borde**, en tiempos muy breves. Esto exige una **gran capacidad de cómputo y alta eficiencia energética**. Los chips conocidos como “aceleradores de IA” (ASICs), se utilizan cada vez más para tareas de inferencia específicas.
2. El desafío del **consumo energético** de los chips IA, tanto en la nube (GPUs), como en el borde es un tema capital al que se dedica mucho esfuerzo y que está produciendo avances como los **chips neuromórficos** (redes neuronales de impulsos), o los **chips AiMC** (analog in memory computing) que evitan el trasiego de datos entre procesador y memoria, y ahorran gran cantidad de energía. La fotónica integrada también puede jugar un papel para conseguir hardware IA más eficiente.
3. El desarrollo de **sensores del tipo de neuronas sensoriales artificiales** es de gran interés en el mundo de la **seguridad**.
4. En los sistemas militares para la detección de objetivos, van a ser de mucho interés los **sistemas de encapsulado de integración heterogénea** para interconectar de forma eficiente MEMs, sensores, antenas, receptores/emisores para radar en chips de GaN y procesadores de IA, tanto para **entrenamiento como para inferencia en un único encapsulado**. También los **chipelets en SiP** son de interés para **acortar tiempos de diseño** mediante su reutilización.
5. **Los chips IA tienen un gran valor industrial y una importante posición estratégica.**
6. Sin chips de IA en el borde no hay posibilidad de aplicar los algoritmos de IA para las aplicaciones de Defensa en tiempo real, por tanto, hay que asegurar el **suministro** y, mucho más deseable, tener **capacidad de diseño y producción**.
7. **Europa no tiene FPGAs**, una de las soluciones para chips IA que equilibran flexibilidad y eficiencia energética y que no requieren largos tiempos de diseño.

Capítulo 4

CAPÍTULO 4.

DIMENSIÓN SOCIOECONÓMICA DE LA IA EN EL SECTOR DE LA DEFENSA

La **inteligencia artificial** se ha consolidado como un pilar esencial tanto en la economía como en la sociedad, transformándose en un **elemento clave en la geopolítica actual**, de acuerdo con múltiples informes (IEEE, 2024).

Desde una perspectiva económica, **la inversión en IA en el sector de la defensa estimula la creación de empleos altamente cualificados** en sectores clave como la ingeniería de software, la robótica y la analítica de datos. Además, **impulsa la competitividad de empresas** en el mercado global, promoviendo la exportación de soluciones avanzadas en seguridad y tecnología de doble uso civil y militar. A nivel industrial, la **automatización inteligente** optimiza la producción, el mantenimiento y la logística, reduciendo costos y aumentando la eficiencia operativa. Los **ecosistemas de innovación en IA** fomentan la colaboración entre gobiernos, startups y grandes corporaciones, acelerando la transferencia tecnológica y el desarrollo de capacidades estratégicas.

En el caso de la UE, el **uso de la IA en el sector de la defensa** no solo transforma la seguridad y la estrategia militar, sino que también **impulsa el desarrollo económico, tecnológico e industrial**. La integración de la IA en sistemas de defensa fortalece un **ecosistema de innovación** donde convergen industrias tecnológicas, aeroespaciales y de ciberseguridad, fortaleciendo la soberanía tecnológica y reduciendo la dependencia de proveedores externos.

4.1 Estructura del mercado internacional de la IA en defensa

La adopción de la IA en sistemas de defensa y seguridad ha generado una **reconfiguración del poder a nivel mundial**, ya que numerosos países la integran en sus estrategias militares, reconociéndola como un eje estratégico para mantener o alcanzar la predominancia global. Este contexto impulsa el desarrollo industrial, donde actores tecnológicos y empresas especializadas en defensa compiten por liderar la innovación y asegurar su posición en un mercado cada vez más relevante y decisivo en el escenario internacional.

El **impacto socioeconómico significativo de la IA** está influido directamente por tres componentes clave: **software, hardware y servicios**. El desarrollo del **software** estimula la creación de empleo especializado en áreas como análisis de datos y programación avanzada, mientras que la fabricación de componentes **hardware** impulsa el desarrollo de industrias tecnológicas y aumenta la demanda de componentes de alta tecnología, beneficiando a economías locales e internacionales. Por otro lado, los **servicios** asociados generan nuevas oportunidades económicas en consultoría estratégica, formación y mantenimiento técnico,

fortaleciendo así el mercado laboral y promoviendo una mayor inversión en innovación tecnológica.

En el **mercado de defensa en 2023**, el software constituye el núcleo de las capacidades de inteligencia artificial, abarcando algoritmos avanzados de aprendizaje automático para análisis predictivo, toma de decisiones autónoma, visión artificial para vigilancia y reconocimiento de objetivos, procesamiento de lenguaje natural para análisis de comunicaciones y herramientas de ciberseguridad diseñadas para defender proactivamente frente a amenazas emergentes.

Sin pretender ser exhaustivos, **ejemplos destacados del uso de la IA en defensa** incluyen el uso de algoritmos de aprendizaje automático para analizar rápidamente imágenes de drones e identificar objetivos. Las capacidades autónomas también están presentes en municiones inteligentes, que identifican, rastrean y atacan objetivos por sí mismas; plataformas ISR (Inteligencia, Vigilancia y Reconocimiento) de las Fuerzas Aéreas aplican procesamiento de lenguaje natural para analizar comunicaciones interceptadas; herramientas de ciberseguridad detectan y neutralizan autónomamente amenazas cibernéticas. Asimismo, el uso de la inteligencia artificial se ha extendido profusamente en sistemas autónomos aéreos (drones), terrestres o marítimos, equipados con sensores avanzados y capacidad de análisis automático de datos para vigilancia e inteligencia.

La puesta en marcha de nuevas **plataformas militares complejas** como los proyectos de desarrollo de aviones de combate de nueva generación **integran IA para sistemas adaptativos y operaciones autónomas**. Actualmente, operan en Ucrania drones con capacidad de adquisición automática de objetivos y operaciones de vuelo autónomas. En el dominio terrestre y marítimo se encuentran vehículos no tripulados que navegan y reconocen objetivos mediante algoritmos avanzados de procesamiento de imágenes. Asimismo, algoritmos de IA alimentan simuladores tácticos y estratégicos. En estos casos, **el componente software es clave y representa el 50% del mercado** (Technavio, 2023)⁴².

Los **servicios en soluciones de defensa con IA** principalmente abarcan la integración de sistemas, asegurando la incorporación fluida del software y hardware avanzado en infraestructuras existentes. Una fuente de negocio que ha adquirido relevancia es la **integración de IA en plataformas heredadas** (*“legacy systems”*) por ejemplo, incorporando nuevas funcionalidades como son el análisis avanzado de datos y la mejora (*“upgrade”*) de capacidades autónomas, como ocurre en los sistemas de mando y control. Hoy día, los **servicios de IA generativa y analítica de datos** ya representan un importante volumen de negocio.

Como resultado, diversas empresas asesoran estratégicamente sobre la implementación tecnológica y el cumplimiento regulatorio; otras empresas ofrecen servicios integrales de

42 <https://www.technavio.com/report/artificial-intelligence-ai-in-military-industry-market-analysis>

integración y formación en sistemas mejorados con IA. Además, **colaboraciones en I+D entre actores públicos y privados** como las que se producen en el contexto de numerosos proyectos enfocados en IA de la agencia *DARPA* en Estados Unidos, y en agencias de I+D en defensa similares en Europa, Rusia, China y Turquía continúan impulsando la innovación y el fortalecimiento continuo ante desafíos de defensa en continua evolución.

Las cifras presentadas en este capítulo preceden a los cambios gubernamentales ocurridos en 2025 en Estados Unidos, la UE y otros países, y a reconfiguraciones de conflictos como el de Ucrania por lo que las cifras relativas al uso de la IA cambiarán significativamente en años venideros. Tampoco se contabilizan los impactos de las nuevas políticas europeas de inversión en defensa anunciadas en marzo de 2025 y los compromisos alcanzados en la cumbre de la OTAN de junio de 2025. En este contexto, **los principales eventos geopolíticos de 2025 traerán como consecuencia el incremento de gastos en defensa, reforzando el rol de la IA.**

En *Estados Unidos*, el lanzamiento de programas como el desarrollo del avión *Next-Generation Air Dominance (NGAD)* cuyo estudio preliminar fue adjudicado a *Boeing* en marzo de 2025 abren las puertas a la adopción de múltiples innovaciones disruptivas. El proyecto, si los planes se cumplen, conducirá al desarrollo del **F-47, el primer avión de combate de sexta generación del mundo**⁴³.

Con todo ello, **el mercado de IA en el ámbito militar está experimentando un crecimiento notable.** Su crecimiento ya es histórico: creció a una sólida tasa de crecimiento compuesta anual (CAGR) del 16,72 % desde 2019, alcanzando los 9.671 millones de dólares en 2024 (*The Business Research Company*, 2025)⁴⁴. Esta firma de consultoría estima que el mercado de IA en el ámbito militar experimente un crecimiento acelerado en los próximos años, proyectando que alcance un valor de **19.740 millones de dólares en 2029**, con una CAGR del 15,1 %.

Otro estudio conducido por *MarketsAndMarkets* (2023)⁴⁵ considera un crecimiento mucho más acentuado partiendo de 9.200 millones de dólares para 2023, en línea con los 8.450 millones de *The Business Research Company* (2025).

En el caso de *Precedence Research* (2024)⁴⁶, la firma estima que el tamaño del mercado global de IA en el ámbito militar sería de 9.560 millones de dólares en 2024, y con estimaciones de crecer hasta los 10.790 millones en 2025. Sin embargo, comparativamente

43 <https://www.af.mil/News/Article-Display/Article/4131345/air-force-awards-contract-for-next-generation-air-dominance-ngad-platform-f-47/>

44 <https://blog.marketresearch.com/why-the-artificial-intelligence-in-military-market-is-set-to-skyrocket-to-61-billion-by-2034>

45 <https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-military-market-41793495.html>

46 <https://www.precedenceresearch.com/artificial-intelligence-in-military-market>

a otros análisis, son más conservadores en las proyecciones, apuntando que se **alcance unos 32.170 millones de dólares para 2034**, registrando una tasa de crecimiento CAGR del 12,9% entre 2024 y 2034.

El crecimiento durante el período de pronóstico, que culmina en 2028, se atribuye a tensiones geopolíticas, aumento en la I+D, expansión del sector militar y de defensa, mayor apoyo gubernamental y el incremento de la automatización industrial (*The Business Research Company*, 2025b)⁴⁷.

Este crecimiento está impulsado por la **mayor adopción de vehículos aéreos no tripulados (UAVs), programas de modernización militar y un aumento en los presupuestos de defensa a nivel mundial**. Más concretamente, entre las principales tendencias tecnológicas esperadas en este período se incluyen alianzas estratégicas en la industria, colaboración entre humanos y máquinas, tecnologías de doble uso, guerra electrónica cognitiva y el desarrollo de tecnología de “enjambres” (*swarms*).

4.1.1 Segmentación

El mercado de IA en defensa se puede segmentar en **varias categorías** según su oferta: tecnología, plataforma, tipo de instalación y aplicación (*Grand View Research*, 2025)⁴⁸.

Por tipo de **oferta**, el mercado se divide en **hardware, software y servicios**, como ya se ha expuesto previamente. Cada una de estas tres categorías desempeña un papel clave en la implementación y desarrollo de soluciones de inteligencia artificial en el ámbito militar. La cuota para el negocio de software representa 50% del mercado en 2022 de acuerdo con un estudio de Technavio (2023)⁴⁹.

Se atribuye a la expansión del segmento software la **importancia del software de IA en la creación de la infraestructura de tecnologías de la información (TI) y en la prevención de brechas de seguridad**. También se proyecta que el segmento de hardware registre un crecimiento robusto y sostenido en sus ingresos hasta el 2030 (*Grand View Research*, 2025). Este comportamiento se atribuye al uso cada vez más intensivo de tecnologías de inteligencia artificial (IA) en procesos complejos, así como al aumento en la demanda de componentes especializados, como procesadores diseñados específicamente para IA y módulos de memoria de alto rendimiento.

En cuanto a la **tecnología**, se incluyen diversas áreas como aprendizaje automático, procesamiento de lenguaje natural, computación consciente del contexto, visión por computadora

47 <https://www.thebusinessresearchcompany.com/report/artificial-intelligence-in-military-global-market-report>

48 <https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-military-market-report>

49 <https://www.technavio.com/report/artificial-intelligence-ai-in-military-industry-market-analysis>

y agentes virtuales inteligentes (*Intelligent Virtual Agents, IVA*), además de otras tecnologías relacionadas. *Grand View Research* (2025) predijo que **el segmento del aprendizaje automático representaría la mayor cuota de ingresos en 2024**, impulsado por su creciente integración en las tecnologías militares.

Los sistemas de **aprendizaje automático** tienen la capacidad única de procesar y analizar eficientemente grandes cantidades de datos, lo que es crucial para la guerra moderna en el que el número de sensores que proporcionan datos en tiempo real está creciendo rápidamente. Además, el **aprendizaje automático desempeña un papel fundamental en la mejora de la autonomía de los sistemas militares, como los innovadores enjambres (“swarms”) de drones**. Esta autonomía no sólo aumenta la eficacia de las operaciones de defensa, sino que también reduce el riesgo para el personal. Se prevé que el segmento de visión por computadora crezca por requisitos de inteligencia, vigilancia y reconocimiento (ISR). Se están desarrollando programas para filtrar una gran cantidad de datos de sensores y alertar a los responsables de inteligencia militar de la presencia de objetos o individuos de importancia estratégica.

Desde el punto de vista de la **plataforma**, el mercado se clasifica en sistemas **terrestres, navales** (superficie y submarinos), **aeronáuticos y espaciales**. Cada una de estas plataformas puede utilizar la IA para mejorar la toma de decisiones, la eficiencia operativa (autonomía) y la seguridad en el campo de batalla, maximizándose los beneficios al combinar plataformas de varias naturalezas.

Grand View Research (2025) prevé que **el segmento terrestre experimente un crecimiento significativo hasta el año 2030**. Este segmento abarca vehículos de combate autónomos, vehículos terrestres no tripulados (UGV) y robots de combate autónomos. Constituye un factor clave el aumento en la demanda de vehículos terrestres no tripulados para la realización de tareas civiles, junto con su capacidad para reducir los riesgos para la vida humana al desplazar a los operadores militares de la línea del frente. Como ya enseña la guerra de Ucrania, la integración de capacidades autónomas en vehículos de combate es fundamental para minimizar bajas en escenarios de conflicto.

En cuanto al **tipo de instalación**, se diferencian dos categorías principales: **nueva adquisición** de soluciones IA y **actualización de sistemas existentes**. Esto permite comprender cómo los ejércitos y organismos de defensa implementan nuevas soluciones de IA o mejoran las ya existentes. Según una previsión de *Grand View Research* (2025), el volumen de negocios con **nuevas adquisiciones** representaría la mayor cuota de ingresos en 2024, que se atribuye al **impulso creciente por parte de los gobiernos para incorporar tecnologías de IA en el sector defensa**, así como al surgimiento de nuevos desarrollos vinculados a la aplicación de la IA en la industria militar. Estas iniciativas estratégicas están acelerando la adopción de soluciones avanzadas y fomentando la modernización de capacidades operativas mediante sistemas inteligentes y autónomos.

Finalmente, **el mercado se segmenta por tipo de aplicación**, incluyendo el procesamiento de información, la simulación y entrenamiento, las plataformas de combate, la monitorización de amenazas y conocimiento situacional, la ciberseguridad y otras aplicaciones. Estas aplicaciones abarcan desde el análisis de datos en tiempo real hasta la protección contra ciberataques, contribuyendo a una mayor capacidad operativa y defensiva. Según el desglose por categorías de *Grand View Research* (2025), la distribución entre Procesamiento de información, Vigilancia y conciencia situacional, identificación de amenazas, plataformas de combate, ciberseguridad, simulación, salud en el campo de batalla, Mando y Control, Logística y transporte ha sido relativamente equilibrada en 2024.

4.1.2 Mercados por región

Europa, con un 30% del mercado de IA militar en 2023 tiene un peso destacado global, y ligeramente por debajo del nivel de América del Norte, aunque el desarrollo y operación de sus sistemas puedan depender de componentes, software y Propiedad Intelectual (IP) de otros países, fundamentalmente de Estados Unidos en el ámbito de la OTAN (*Precedence Research*, 2024)⁵⁰. Será el caso de los Estados miembros de la Unión Europea, o del Reino Unido, Noruega y Turquía, pero no aplicable en el caso de la Federación Rusa, también considerada europea en este análisis. Las cuotas de mercado por región en el año 2023 revelan que América del Norte representaba un 36%, Europa el 30%, Asia-Pacífico el 24%, América Latina el 6%, y Medio Oriente y África el 4%

Estas cifras, según el estudio de *MarketsAndMarkets* (2023), presentan una rápida expansión del mercado de IA en el ámbito militar, diferenciando la evolución por regiones de 2022 a 2028, y prediciendo crecimiento significativo en todas ellas durante ese periodo⁵¹. Mientras que en 2022 la IA alcanzó un valor estimado de 4.600 millones de dólares, apenas un año después ya era de 9.200 millones de dólares. Según esta fuente, en 2028 el volumen del mercado sería de 38.800 millones de dólares, lo cual significa una **tasa compuesta anual de crecimiento (CAGR) del 33.3% en apenas 5 años**.

El **dominio de América del Norte en cada período** es evidente tanto en el tamaño de los segmentos de la pila técnica (stack) de IA como en la inversión subyacente en tecnologías de IA, lo que refleja el papel de América del Norte como **pionera en la adopción de innovaciones de defensa avanzadas**.

Europa, por su parte, suele tener la segunda o tercera mayor porción, según el año, y aparece cercana en tamaño a Asia Pacífico. **La cuota de Europa también crece de manera constante, lo que sugiere que los presupuestos de defensa de la región están incorporando cada vez más capacidades impulsadas por IA**. Sin embargo, a pesar de este sólido creci-

50 <https://www.precedenceresearch.com/artificial-intelligence-in-military-market>

51 <https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-military-market-41793495.html>

miento, el mercado europeo sigue estando por detrás de América del Norte en términos de tamaño absoluto.

Asia Pacífico presenta una porción similar o ligeramente mayor que Europa, lo que subraya el fuerte gasto en defensa y los avances tecnológicos en países clave de la región. Aunque Oriente Medio y América Latina representan segmentos más pequeños del mercado, también muestran crecimiento en términos absolutos, lo que indica que, incluso con presupuestos de defensa más modestos, estas regiones están ampliando de forma constante sus inversiones en IA.

Centrando la atención específicamente **en Europa se estima un aumento sustancial en términos absolutos**, aunque la región permanece por detrás de la mayor participación de América del Norte. Entre 2022 y 2023, la porción de Europa casi se duplica a la par que el mercado total pasa de 4.600 millones de dólares a 9.200 millones de dólares. Para 2028, cuando se proyecta que el mercado total alcance los 38.800 millones de dólares, **la inversión de Europa en aplicaciones de IA para el ámbito militar es considerable, aunque todavía por debajo de la de América del Norte.**

En general, la evolución del mercado evidencia una tendencia clara: todos los segmentos experimentan un aumento significativo en el gasto en defensa relacionado con la IA desde 2022 hasta 2028. América del Norte se destaca como el principal inversor, mientras que Europa y Asia Pacífico mantienen participaciones sustanciales, pero menores. Oriente Medio y América Latina conservan participaciones más pequeñas, pero continúan expandiéndose de manera constante.

4.1.3 Relevancia de IA en el mercado de Defensa

De acuerdo con una publicación de *Business Research Insights* (2025)⁵², **el tamaño del mercado global de defensa fue de 2.494 miles de millones de dólares en 2024**, se estima que alcance los 3.340 miles de millones en 2030, y se proyecta que aumente a 3.871 miles de millones de dólares para 2033, con una tasa CAGR del 5,0% durante el período de previsión de 2025 a 2033. Ese total congrega la oferta de plataformas – aeronaves, buques y vehículos –, equipos y servicios.

Las cifras evidencian este impulso: el mercado global alcanzó los 9.671 millones de dólares en 2024, tras crecer a una tasa compuesta anual (CAGR) del 16,72 % desde 2019. Las proyecciones de distintas fuentes especializadas coinciden en anticipar un crecimiento sostenido y, en algunos casos, muy elevado. *Business Research Company* estima que el mercado alcanzará los 19.740 millones de dólares en 2029 y los 61.087 millones en 2034, con una CAGR de 20,57 %. Por su parte, *MarketsAndMarkets* proyecta un escenario aún más

52 <https://www.businessresearchinsights.com/market-reports/defence-market-109136>

dinámico, con un mercado de 38.800 millones de dólares para 2028 y una CAGR del 33,3 %, mientras que *Precedence Research* ofrece una estimación más conservadora, apuntando a 32.170 millones de dólares en 2034 con un crecimiento del 12,9 % anual entre 2024 y 2034.

Mientras que podría concluirse que **el peso económico de la IA en el mercado de defensa total es reducido** dado que la mayor parte del coste corresponde a las plataformas, el **impacto de la IA en la capacidad operacional supondría una magnitud superior**. Según *Business Research Company* (2025), el mercado de **IA ascendió en 2024 a 9.200 millones de dólares del mercado global de defensa**, correspondiente a un 0,003% del total. Muy poco, pero es probable que el uso real esté enmascarado en el desarrollo de plataformas o sistemas de armas que incorporan sistemas potenciados por algoritmos de IA que no se valoran separadamente.

4.1.3.1 Volumen de mercado en Europa

La **pandemia de COVID-19 tuvo efectos negativos** a corto plazo en el mercado de defensa europeo, ya que muchos fabricantes perdieron acceso al financiamiento para tecnologías emergentes como inteligencia artificial y *blockchain* (*Mordor Intelligence*, 2025)⁵³. Sin embargo, se espera que la región europea experimente un impulso positivo, ya que estas tecnologías pueden acelerar la digitalización y transformar sectores clave que fueron fuertemente afectados por la pandemia.

En 2024, el combinado de mercado de las tres principales naciones europeas – Reino Unido, Francia y Alemania – de **IA en defensa generó unos ingresos de 2.348,8 millones de dólares** (*Grand View Research*, 2025b)⁵⁴. Por segmentos, el software fue la oferta con mayores ingresos en 2024, consolidándose como el área más fuerte del mercado. Sin embargo, el hardware es el segmento más lucrativo, registrando el crecimiento más rápido durante el período de pronóstico. Se espera que el mercado de inteligencia artificial en el ámbito militar en Europa alcance unos ingresos proyectados de 4.090 millones de dólares para el año 2030.

Como dato agregado en el **mercado europeo de IA en defensa**, se prevé una **tasa de crecimiento anual compuesta del 9,8 %** durante el período 2025-2030.

En el caso de Francia, diversas iniciativas gubernamentales y desarrollo son los principales factores que contribuyen a este crecimiento. Además, este país está trabajando en nuevas estrategias de IA para su sector de defensa. El Ministerio de Defensa francés está impulsando proyectos clave, como contratos de desarrollo de *big data* e inteligencia artificial, que fortalecerán el uso de estas tecnologías en la defensa del país.

53 <https://www.mordorintelligence.com/industry-reports/europe-artificial-intelligence-and-analytics-in-defence-market>

54 <https://www.grandviewresearch.com/horizon/outlook/artificial-intelligence-in-military-market/europe>

Actualmente, se suele considerar a **Francia un líder europeo en I+D relacionada con la defensa**. Por un lado, aunque la investigación en IA ha crecido significativamente, el desarrollo de productos y servicios basados en esta tecnología no ha experimentado el mismo crecimiento en Francia en las últimas décadas. No obstante, Francia espera revertir esta situación mediante alianzas estratégicas con grandes empresas, con el objetivo de avanzar y consolidarse en el desarrollo de tecnologías de IA que proporcionen el impulso necesario para lograr un crecimiento significativo en este ámbito. En definitiva, **la mejora de sus capacidades militares se apoyará en el crecimiento del mercado de IA en defensa** en los próximos años.

Es importante considerar que, **si los países de la UE continúan comprando grandes cantidades** de sistemas y tecnologías, ya sea hardware, software o servicios, **a proveedores que no pertenecen a la UE, la industria de defensa europea seguirá siendo de menor tamaño del deseable** (Scazzieri, 2025). Es el caso de los dispositivos semiconductores GPU de NVIDIA para aplicaciones de AI. Un enfoque restrictivo hacia proveedores corre el riesgo de interrumpir la cooperación existente entre los países de la UE y naciones socias no pertenecientes a la UE. Esto significa que la UE debe valorizar sinergias que pueden aportar las alianzas como la OTAN. A la UE le convendría adoptar un enfoque caso por caso en la participación de socios en sus proyectos de desarrollo de sistemas militares.

El Reglamento Europeo de IA, en vigor desde el 1 de agosto de 2024⁵⁵, establece un marco legal pionero para regular el uso de la IA en la Unión Europea, imponiendo restricciones a su uso en la medida en la que sistemas de IA puedan limitar los derechos de los ciudadanos y crear riesgos a los Estados miembros. Sin embargo, **excluye explícitamente los sistemas de IA utilizados exclusivamente con fines militares, de defensa o seguridad nacional**, independientemente de si son desarrollados por entidades públicas o privadas; aspecto que se tratará con más detalle en un capítulo posterior de este informe.

4.1.3.2 Volumen de mercado en España

No existe una cifra pública y unificada que refleje con exactitud el volumen de mercado de la IA en el sector militar en España. En general, la inversión en tecnologías de IA aplicada a la defensa se encuentra en crecimiento, impulsada tanto por la transformación digital de empresas nacionales como por el aumento en la demanda de sistemas avanzados de seguridad y ciberdefensa.

Tentativamente se podría estimar el valor de las inversiones en IA para la defensa en España en función del porcentaje que la IA representa en el mercado global de Defensa. En 2024, el presupuesto para inversión de defensa de España era de 13,1 miles de millones de euros⁵⁶.

55 <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32024R1689>

56 <https://www.globaldata.com/store/report/spain-defense-market-analysis>

Aplicando un factor conservador de 0,3%, se estima que IA podría haber representado ingresos potenciales por encima los 40 millones de euros en España.

Es indudable que IA ya juega un rol relevante en la industria española de defensa y en el mercado doméstico. España está presente en grandes programas en los que IA juega un rol relevante, como *Aegis* (AMD), *Barracuda* (UAV), *BlueScan* (ASW), *Future Combat Air System* (FCAS, plataforma aérea), *Harpoon Block II* (misil), *Patriot* (AMD), *RQ-11 RAVEN* (UAV), *SWORD* (simulación), *ScanEagle* (plataforma aérea) o *nEUROn* (plataforma aérea), según una publicación de la OTAN (CCDCOE, 2021)⁵⁷.

España ya está desarrollando varios proyectos para **mejorar la eficiencia de la logística militar apoyada por aplicaciones de IA**. El informe de la *Oficina Nacional de Prospectiva y Estrategia* dependiente de la Presidencia del Gobierno de España de 2025⁵⁸, presentado durante el evento *HispanIA 2040*, destaca el proyecto *MPC16* del Ejército del Aire para el mantenimiento predictivo de las aeronaves Eurofighter, el *Sistema de Logística predictiva del Ejército de Tierra* (SILPE), el *gemelo digital integrado en las Fragatas F-110* o el *Módulo de Mantenimiento Predictivo Embarcado* (MAPRE) para buques de la Armada.

El Ministerio de Defensa de España ha creado *Idoia*, un asistente de IA desarrollado por el *Centro de Sistemas y Tecnologías de la Información y las Comunicaciones* (CESTIC) e *Imbox*, una aplicación de mensajería instantánea específica para el Ministerio de Defensa que ya contaba con cerca de 12.000 usuarios en 2024⁵⁹. El principal reto es **asegurar su total independencia de internet** y garantizar la máxima confidencialidad frente a otras soluciones tecnológicas comerciales que operan desde la nube pública. También se puede destacar un proyecto de **IA generativa específica** (del tipo de un chatbot) denominado *Gonzalo* desarrollado por el Estado Mayor del Ejército, el Mando de Adiestramiento y Doctrina, la Jefatura del Ciberespacio y de los Servicios de Asistencia Técnica, el Mando de Apoyo Logístico del Ejército de Tierra y por el INTA.

Como demuestra el conjunto de distintos programas en las Fuerzas Armadas españolas mencionados previamente, ya se ha incorporado la IA en todos ellos. **Su aplicación es todavía incipiente**, centrada en sistemas de comunicación o de guiado de munición, pero el conflicto en Ucrania ha desencadenado un mayor interés en el uso de la IA como ayuda para el mando militar en sus decisiones, y esta tendencia también se producirá en España. **El Ministerio de Defensa ha comenzado un proceso estratégico para integrar sistemas de IA en la toma de decisiones del Ejército de Tierra, tanto a nivel técnico como operativo**. En 2024, se definieron necesidades técnicas para explorar la mejor forma de automatizar este

57 https://ccdcoe.org/uploads/2021/12/Strategies_and_Deployment_A4.pdf

58 https://futuros.gob.es/sites/default/files/2025-01/HispanIA_2040.pdf

59 Idoia es un asistente de IA generativa que se aloja en los Centros de Procesamiento de Datos (CPD) del Ministerio de Defensa. Para más detalles puede consultarse <https://www.businessinsider.es/tecnologia/son-dos-asistentes-inteligencia-artificial-espanola-creados-defensa-1395725>

proceso mediante IA. Actualmente, la iniciativa se encuentra en una fase prospectiva, es decir, de estudio y exploración inicial.

Cabe destacar que esta área está sujeta a importantes **variaciones en función de las políticas de defensa**, el presupuesto asignado por el gobierno y la evolución de la tecnología, por lo que las cifras pueden cambiar rápidamente. Además, muchas inversiones se realizan a través de contratos y programas en colaboración con socios internacionales, lo que dificulta la obtención de un dato nacional consolidado y detallado.

4.2 Tecnología Industrial

Siendo el uso de IA en defensa innovador en diversos segmentos, es relevante el análisis de procesos de **patentes**, y la dispersión geográfica de la tecnología industrial resultante. La tabla 4.1 muestra la evolución de patentes registradas y concedidas dentro de la industria aeroespacial y de defensa, directamente relacionadas con IA en cada trimestre de 2020 a 2022. Los datos fueron obtenidos de la base de datos de *GlobalData Patent Analytics*⁶⁰.

Año	Trimestre	Sometidas	Concedidas	Total de Patentes	
2020	T1	330	148	478	2550
	T2	498	180	678	
	T3	429	185	614	
	T4	551	229	780	
2021	T1	483	219	702	3314
	T2	600	246	846	
	T3	630	298	928	
	T4	552	286	838	
2022	T1	516	278	794	3281
	T2	565	350	915	
	T3	428	363	791	
	T4	473	308	781	

Tabla 4.1 Patentes IA dentro de la industria aeroespacial y de defensa 2020-2022
Fuente: elaboración propia

La industria aeroespacial y de defensa global experimentó un aumento del 26% en la tasa de crecimiento anual promedio (AAGR) en el número de solicitudes de patentes relacionadas con la IA entre 2020 y 2022. El número total de concesiones de patentes relacionadas con la inteligencia artificial aumentó en un AAGR del 41% durante el mismo período, según la base de datos de análisis de patentes de GlobalData. El número de solicitudes de patentes relacionadas con IA en la industria aeroespacial y de defensa fue de 6.055 desde 2020 a

60 <https://www.globaldata.com/reports/patent-statistics-and-analysis/>

2022, mientras que se concedieron 3.090 solicitudes. La figura 4.1 detalla la actividad de patentes relacionada con la inteligencia artificial en la industria aeroespacial y de defensa global, de 2020 a 2022.

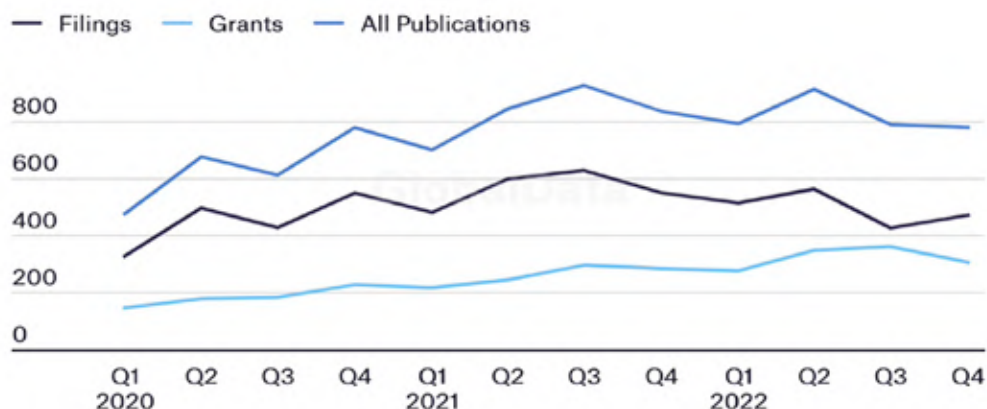


Figura 4.1 Variación de números de patentes relacionadas con la IA en la industria aeroespacial y de defensa global 2020-2022. Fuente: *GlobalData Patent Analytics*

La tabla 4.2 muestra un análisis geográfico de las patentes relacionadas con la inteligencia artificial en la industria aeroespacial y de defensa de 2020 a 2022. Los datos fueron obtenidos de la base de datos *GlobalData Patent Analytics*.

País		Patentes presentadas		Total
EE. UU.		3584		9145
China		3061		
UE, Reino Unido y Turquía	España	9	383	
	Francia	147		
	Reino Unido	107		
	Bélgica	2		
	Luxemburgo	2		
	Países Bajos	6		
	Dinamarca	2		
	Suecia	2		
	Finlandia	3		
	Turquía	12		
	Serbia	1		
	Italia	1		
	Grecia	2		
	Alemania	86		
	Lituania	1		
Rusia		38		
Australia		105		
Sudáfrica		2		
Arabia Saudí		2		
Túnez		1		
Japón		277		
Corea del Sur		592		
Filipinas		2		
Taiwán		18		
Canadá		61		
México		5		
Costa Rica		1		
Colombia		1		
Brasil		46		
Perú		2		
Argentina		4		
Chile		1		
Otros países		959		

Tabla 4.2 Patentes relacionadas con la IA en la industria aeroespacial y de defensa global por países 2020-2022 Fuente: elaboración propia

Podemos concluir que existe un dominio abrumador de Estados Unidos y China, según muestra el mapa de la figura 4.2. **La mayor proporción de publicaciones de patentes relacionadas con inteligencia artificial en la industria aeroespacial y de defensa desde**

2020 la tuvo Estados Unidos, con un 44 %, seguido de China (37 %) y Corea del Sur (7 %). El agregado de los principales países la UE, Reino Unido y Turquía sólo representa el 5,4% de las patentes presentadas en este ámbito.



Figura 4.2 Análisis geográfico mundial de la actividad de patentes relacionadas con inteligencia artificial en la industria aeroespacial y de defensa 2020-2022. Fuente: *GlobalData Patent Analytics*

Las cinco **principales empresas por número de solicitudes representaron el 21 % de las solicitudes de patentes**⁶¹. La figura 4.3 sintetiza el análisis de las solicitudes de patentes por titular, y muestra que Boeing presentó el mayor número de patentes relacionadas con inteligencia artificial en la industria aeroespacial y de defensa desde 2020, con un total de 411 patentes. Le siguen Thales (186 solicitudes), Raytheon Technologies (165 solicitudes), Honeywell International (101 solicitudes) y Baidu (88 solicitudes).



Figura 4.3 Principales titulares de solicitudes de patentes relacionadas con inteligencia artificial en la industria aeroespacial y de defensa a nivel mundial, 2020-2022
Fuente: *GlobalData Patent Analytics*

61 https://defence.nridigital.com/global_defence_technology_aug23/artificial_intelligence_patent_applications_aerospace_defence_industry_2020-2022

El informe de datos de GlobalData, “Aerospace, Defense & Security: Patents Trends Q3 2024”, ofrece información detallada sobre las tendencias de patentamiento, las estrategias de los principales actores y el enfoque geográfico en el sector durante los últimos tres años. El análisis de la actividad de patentes presentadas por empresas muestra que **Boeing fue la compañía que registró la mayor cantidad de patentes relacionadas con IA** en la industria aeroespacial, de defensa y seguridad durante el tercer trimestre de 2024. Boeing presentó 33 patentes vinculadas a inteligencia artificial en el trimestre, en comparación con 32 en el trimestre anterior. Le siguieron BAE Systems, con 20 solicitudes de patentes, Y RTX (con 17 solicitudes). **Dentro de la UE lidera la francesa Safran con 11 solicitudes en el mismo período**⁶².

La mayor parte de las solicitudes de patentes relacionadas con la inteligencia artificial en la industria aeroespacial, de defensa y seguridad en el tercer trimestre de 2024 se registró en EE. UU. Con un 45%, seguido de China (10%) y el Reino Unido (3%). La participación de EE. UU. fue un 22% mayor que el 23% que representó en el segundo trimestre de 2024.

Sin que haya proyecciones para el 2030, el número de nuevas patentes se espera que continúe creciendo, y que las actividades de I+D sigan existiendo, con apalancamiento de actores del sector privado industrial “legacy” de defensa y por las PYMES de innovación.

4.3 Estructura del ecosistema de defensa relacionado con la IA en la UE y en España

Los ingresos por venta de sistemas de armas de las 100 principales empresas de producción de armamento y servicios militares según el SIPRI alcanzaron los 632.000 millones de dólares en 2023, lo que representa un aumento del 4,2 % en términos reales en comparación con 2022⁶³. Hay una empresa europea en las 10 primeras, se trata de **BAE Systems** en el Reino Unido. No hay ninguna empresa de defensa de la UE entre las 10 primeras del mundo, como se puede constatar por la tabla 4.3 que las identifica de entre las principales por volumen de facturación en 2022. Entre las 20 primeras se puedan contar tres europeas, la italiana Leonardo y dos francesas, **Airbus** (que se puede considerar multinacional) y **Thales**.

62 La industria global aeroespacial, de defensa y seguridad experimentó una disminución del 50% en el número de solicitudes de patentes relacionadas con la inteligencia artificial en el tercer trimestre de 2024 en comparación con el trimestre anterior. El número total de concesiones de patentes relacionadas con la inteligencia artificial cayó un 2% en el tercer trimestre de 2024. Para más detalles puede consultarse: <https://www.army-technology.com/data-insights/patent-activity-artificialintelligence-aerospacedefensesecurity-industry/>

63 https://www.sipri.org/sites/default/files/2024-11/fs_2412_top_100_2023_0.pdf

Global top 10 and European top 10 defence companies by turnover, 2022					
Global rank	Company	Country	Armaments revenues, \$ billions	Total revenues, \$ billions	Armaments revenue as % of total revenues
1	Lockheed Martin Corp.	United States	59390	65984	90%
2	Raytheon Technologies	United States	39570	67074	59%
3	Northrop Grumman Corp.	United States	32300	36602	88%
4	Boeing	United States	29300	66608	44%
5	General Dynamics Corp.	United States	28320	39407	72%
6	BAE Systems	UK	26900	27712	97%
7	NORINCO	China	22060	82537	27%
8	AVIC	China	20620	82499	25%
9	CASC	China	19560	44458	44%
10	Rostec	Russia	16810	30295	55%
13	Leonardo	Italy	12470	15025	83%
14	Airbus	Trans-European	12090	61805	20%
17	Thales	France	9420	18479	51%
23	Dassault Aviation Group	France	5070	7288	70%
25	Rolls-Royce	UK	4930	15647	32%
28	Rheinmetall	Germany	4550	6742	67%
29	Naval Group	France	4530	4578	99%
32	MBDA	Trans-European	4380	4428	99%
34	Safran	France	4200	20021	21%

Tabla 4.3 Las 10 principales empresas de defensa a nivel global y las 10 principales en Europa por volumen de facturación en 2022. Fuente: SIPRI (2024)

Los ingresos totales por armas de las 41 **empresas con sede en Estados Unidos** crecieron un 2,5 % hasta alcanzar los 317.000 millones de dólares en 2023. Las 27 **empresas europeas** incluidas en el “Top 100” registraron un pequeño crecimiento del 0,2 %, alcanzando los 133.000 millones de dólares en ingresos por armas.

Los ingresos por armas de las dos **empresas rusas** de las que se dispone de datos aumentaron un 40 %, hasta un estimado de 25.500 millones de dólares, debido a un aumento significativo en pedidos y producción.

4.3.1 Caracterización del sector industrial de IA para la defensa

Las diversas empresas tecnológicas con posición importante en el mercado militar se ubican como Fabricantes de Hardware/Componentes, Proveedores de Software o Integradores de Sistemas.

Empresas de defensa con enfoque tecnológico – que van desde gigantes de semiconductores hasta grandes contratistas aeroespaciales y proveedores especializados de IA – ocupan funciones distintas, aunque a veces superpuestas. Sus diversas carteras, presencia global y tamaños variables ponen de manifiesto la complejidad del mercado militar moderno, donde el hardware, el software y la integración de sistemas completos desempeñan roles fundamentales en el desarrollo de capacidades de defensa avanzadas.

El diagrama de la figura 4.4 de *MarketsAndMarkets* (2023)⁶⁴ ilustra cómo diversas empresas tecnológicas se ubican en el mercado militar como fabricantes de hardware/componentes, proveedores de software o integradores de sistemas.

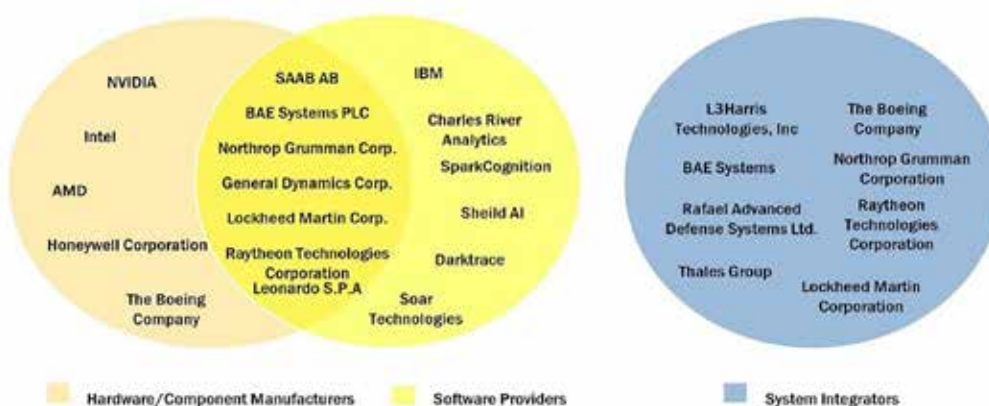


Figura 4.4 Tipos de empresas tecnológicas de IA militar.
Fuente: MarketsAndMarkets (2023)

Aunque muchas de estas compañías se centran en tecnología avanzada, difieren en sus ofertas principales y áreas de especialización. Algunas son grandes corporaciones multinacionales, mientras que otras son empresas de tamaño mediano o especializadas, y provienen de diferentes países alrededor del mundo. En el círculo medio se encuentran las empresas centradas principalmente en software, análisis y soluciones impulsadas por IA para el sector de la defensa. BAE Systems, las estadounidenses Northrop Grumman, General Dynamics, Lockheed Martin y Raytheon Technologies Corporation (RTX desde

64 <https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-military-market-41793495.html>

2023) – aunque son grandes contratistas de defensa – aparecen aquí por sus capacidades de software e IA⁶⁵.

De forma similar, Leonardo ofrece sistemas de defensa basados en software junto con su hardware aeroespacial. La sueca SAAB es una destacada empresa europea de defensa que proporciona soluciones de vigilancia y mando y control basadas en software, además de plataformas de hardware. IBM (Estados Unidos) es un líder tecnológico global reconocido por sus servicios de IA, computación en la nube y análisis de datos. Charles River Analytics (Estados Unidos), SparkCognition (Estados Unidos), Shield AI (Estados Unidos), Darktrace (Reino Unido) y Soar Technologies (Estados Unidos) son, por lo general, empresas más pequeñas o de tamaño mediano que se especializan en inteligencia artificial, ciberseguridad y sistemas autónomos.

Se perfilan compañías que integran sistemas y tecnologías complejos en soluciones militares integrales. L3Harris Technologies (Estados Unidos) es un importante contratista de defensa centrado en comunicaciones, guerra electrónica y sistemas de misión integrados. Boeing y Northrop Grumman también figuran aquí por su capacidad de reunir múltiples componentes – tanto de hardware como de software— en plataformas unificadas. La estadounidense RTX y BAE Systems actúan como integradores, ensamblando sistemas de radar, defensa antimisiles y soluciones electrónicas. Rafael Advanced Defense Systems (Israel) ofrece soluciones de defensa integradas, como sistemas de defensa aérea y armamento de precisión. Lockheed Martin (Estados Unidos) es un integrador líder de aviones de combate, sistemas de misiles y tecnologías espaciales, uniendo software y hardware avanzados en soluciones coherentes. Grupo Thales ofrece soluciones integradas en los campos aeroespacial, de defensa, transporte y seguridad, a menudo combinando sensores, comunicaciones y sistemas de mando.

4.3.2 Actores Industriales de defensa en Europa

La mayor parte de la industria de defensa de Europa se encuentra en sus Estados miembros occidentales, especialmente en Reino Unido, Francia, Alemania e Italia. Normalmente, estos países apoyan las iniciativas industriales de defensa de la UE, siempre y cuando piensen que sus propias industrias se beneficiarán. El mapa de la figura 4.5, elaborado por EOM partir de los datos de SIPRI del 2022⁶⁶, muestra las huellas del negocio de defensa de las naciones europeas.

⁶⁵ Las compañías que enfatizan la producción de componentes físicos y plataformas críticas para la tecnología militar. NVIDIA, Intel y AMD de Estados Unidos son fabricantes destacados de semiconductores y GPU, proporcionando la potencia de procesamiento necesaria para la IA y otras aplicaciones de defensa que manejan grandes volúmenes de datos. La estadounidense Honeywell es un gran conglomerado cuya división aeroespacial produce sistemas de aviónica y otros equipos críticos para misiones. Boeing es conocida por sus aviones, helicópteros, cohetes, satélites y misiles.

⁶⁶ <https://elordenmundial.com/mapas-y-graficos/empresas-armamento-mas-importantes-europa/>

Navantia es la única empresa española incluida en las 100 empresas de defensa más importantes a nivel mundial⁶⁸. Aunque se encuentra en el puesto número 88 en 2025, ha escalado 6 posiciones respecto al ranking anterior y en 2023 vio incrementados sus ingresos en un 13,3 %, alcanzando los 1.190 millones de dólares (alrededor de 1.150 millones de euros) en ventas de armamento durante el periodo analizado.

4.3.3 Actores Industriales de defensa en España

Según recoge el Catálogo 2023-24 de la Industria Española de Defensa⁶⁹, editado por el Ministerio de Defensa, la base industrial y tecnológica de defensa (BITD), contaba en el año 2021 con más de 520 empresas, aunque solo unas 350 suministraron productos o servicios en el ámbito de defensa. **El número de empleos directos en defensa fue de unos 22.000 empleos directos y la facturación asociada de 6.300 millones de euros**, lo que supuso un 15% de sus ventas totales (civiles y militares).

Esta actividad encuentra un efecto tractor principalmente en los grandes programas de armamento, especialmente para las empresas tipo Tier 1 y Tier 2, aunque también otros subcontratistas y las PYMES de la cadena de suministro. Estas últimas categorías suponen cerca del 85% del total de empresas de la industria de defensa española. En términos de cuota de mercado, **el 1,5% de las empresas aglutinan el 75% de todo el volumen del mercado**, como queda reflejado en la siguiente figura:



Figura 4.6 Cobertura de las ventas de Defensa por número de empresas
Fuente: Ministerio de Defensa de España (2023)

68 <https://www.estrelladigital.es/seguridad-defensa/20250109/industria-europea-defensa-a-la-cola/>

69 https://publicaciones.defensa.gob.es/pprevistas/REVISTAS_PDF23790/index.html

Las ventas internacionales, incluyendo los programas cooperativos, ascendieron a un 79% del negocio.

El informe de la DGAM sobre la Industria Española de Defensa de 2022⁷⁰ destaca que este sector es muy intensivo en I+D+i y demandante de inversiones. El desarrollo de capacidades se realiza en largos ciclos, sin garantías de comercialización salvo para el cliente lanzado. Este nivel de riesgo económico apela a la intervención de los poderes públicos para facilitar las inversiones del sector privado.

La estructura de la BITD es piramidal: una cúspide de pocos grandes plataformistas y sistemistas lideran los diferentes subsectores, traccionando del resto de la industria. En ésta aparecen acto seguido los suministradores de primer nivel (Tier 1) a los que hay que añadir una cadena de suministro de más de dos mil empresas de menor tamaño (mid caps, PYMES, startups) que suministran subsistemas o componentes. En comparación con los líderes europeos, nuestra industria muestra un déficit de tamaño.

El gráfico de la figura 4.7 muestra la distribución de las ventas de esta industria. Podemos resumir que las empresas que potencialmente pueden trabajar en Defensa lo hacen en mayor medida en el ámbito civil, y lo que hacen en Defensa es en gran medida en un contexto exportador o internacional y con alto grado de concentración.

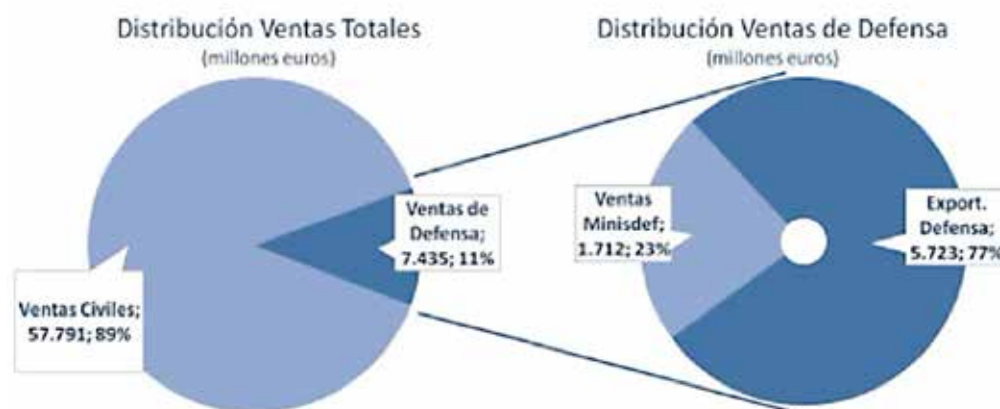


Figura 4.7 Ventas de defensa en España.
Fuente: Ministerio de Defensa de España (2024)

El gráfico de la figura 4.8 muestra la distribución de las ventas de defensa entre las principales empresas del sector, de acuerdo con Ministerio de Defensa de España. La empresa con mayor participación es la multinacional Airbus, que representa el 34,4% del total. En conjunto, el gráfico refleja una concentración significativa del mercado de defensa en unas pocas compañías principales.

⁷⁰ <https://publicaciones.defensa.gob.es/la-industria-de-defensa-en-espa-a-informe-2022-libros-pdf.html>



Figura 4.8 Top de empresas de defensa en España.
Fuente: Ministerio de Defensa de España (2024)

El gráfico de la figura 4.9 muestra las ventas de defensa desglosadas por subsector, tanto en millones de euros como en porcentaje sobre el total.

Ventas de defensa por subsector (millones de euros y porcentaje sobre el total)

	AERONÁUTICO	4.491 60,4%		RPAS	112 1,5%
	NAVAL	1.092 14,7%		MISILES	81 1,1%
	TERRESTRE	537 7,2%		ESPACIAL	59 0,8%
	AUXILIAR	458 6,2%		SIMULACIÓN	37 0,5%
	ELECTRÓNICO	391 5,3%		MATERIAS PRIMAS	0,2 0,0%
	ARMAMENTO	175 2,4%			

Figura 4.9 Ventas por sector de defensa en España.
Fuente: Ministerio de Defensa de España (2024)

El subsector con mayor peso es el aeronáutico, que concentra 4.491 millones de euros, equivalentes al 60,4% del total. Le sigue el subsector naval con 1.092 millones y un 14,7%, y el terrestre con 537 millones, lo que representa el 7,2%. En conjunto, el gráfico evidencia una fuerte concentración de las ventas de defensa en el sector aeronáutico, seguido a distancia por el naval y el terrestre, mientras que los demás subsectores tienen un peso mucho más reducido en el conjunto de la industria.

El gráfico de la figura 4.10 presenta las ventas al Ministerio de Defensa español clasificadas por subsector, tanto en millones de euros como en porcentaje sobre el total.

Ventas al Ministerio de Defensa por subsector (millones de euros y porcentaje sobre el total)

	NAVAL	523 30,5%		ARMAMENTO	43 2,5%
	AERONÁUTICO	409 23,9%		SIMULACIÓN	19 1,1%
	ELECTRÓNICO	294 17,1%		MISILES	16 0,9%
	AUXILIAR	183 10,7%		RPAS	4 0,2%
	TERRESTRE	180 10,5%		MATERIAS PRIMAS	0,2 0,01%
	ESPACIAL	43 2,5%			

Figura 4.10 Ventas al ministerio de Defensa de España por subsector
Fuente: Ministerio de Defensa de España (2024)

El subsector naval encabeza la lista con 523 millones de euros, lo que representa el 30,5% del total. Le sigue el subsector aeronáutico con 409 millones (23,9%) y el electrónico con 294 millones, equivalente al 17,1%.

En resumen, el gasto del Ministerio de Defensa está dominado por los subsectores naval, aeronáutico y electrónico, que en conjunto suman más del 70% del total, mientras que otros segmentos, como RPAS o misiles, tienen un peso marginal en el presupuesto.

Es muy importante destacar el papel de consorcios internacionales, sobre todo aeronáuticos, en la actividad exportadora. La figura 4.11 muestra el *ranking* de países destino de las exportaciones totales de defensa.

Ranking de países destino de las exportaciones de defensa totales

País		Exportaciones de defensa (millones €) y porcentaje sobre el total (%)
	Consortios Internacionales	2.025 (35,4%)
	Francia	636 (11,1%)
	Reino Unido	517 (9,0%)
	Arabia Saudí	444 (7,8%)
	Alemania	422 (7,4%)
	Estados Unidos	283 (4,9%)
	Luxemburgo	173 (3,0%)
	Emiratos Árabes Unidos	158 (2,8%)
	Canadá	114 (2,0%)
	Irlanda	74 (1,3%)
	Australia	71 (1,2%)

Figura 4.11 Destinos de exportaciones de defensa españolas
Fuente: Ministerio de Defensa de España (2024)

El principal receptor son los consorcios internacionales, que concentran 2.025 millones de euros, lo que representa el 35,4% del total exportado. Entre los países individuales, destaca Francia con 636 millones de euros (11,1%), seguida por el Reino Unido con 517 millones (9,0%), Arabia Saudí con 444 millones (7,8%), Alemania con 422 millones (7,4%) y Estados Unidos con 283 millones (4,9%). En conjunto, el gráfico refleja una concentración significativa de las exportaciones en consorcios y en países aliados estratégicos, tanto europeos como de Oriente Medio y América del Norte.

El gráfico de la figura 4.12 muestra la distribución del sector defensa por tipología de venta y tamaño empresarial, distinguiéndose dos tipos de empresas: grandes y PYMES. En el total de ventas de defensa (suma de contratos con Ministerio de Defensa y las exportaciones), las grandes empresas dominan claramente con el 89,9% del volumen, equivalente a 6.686 millones de euros, mientras que las PYMES solo representan el 10,1% (749 millones).



Figura 4.12 Distribución por tipología de ventas y tamaño empresarial de la industria de defensa española. Fuente: Ministerio de Defensa de España (2024)

En las ventas directas al Ministerio de Defensa, la participación de las grandes empresas baja al 73,6% (1.260 millones), permitiendo a las PYMES alcanzar un 26,4% (452 millones), su proporción más alta dentro del gráfico.

En cuanto a las exportaciones de defensa, las grandes empresas vuelven a tener un papel predominante con el 94,8% (5.426 millones), mientras que las PYMES apenas alcanzan el 5,2% (297 millones). Finalmente, en las ventas indirectas al Ministerio de Defensa, las grandes empresas representan el 83,6% (1.690 millones), y las PYMES el 16,4% (333 millones).

En resumen, el gráfico evidencia una fuerte concentración del mercado de defensa en grandes empresas, aunque las PYMES tienen una participación más relevante en las ventas directas e indirectas al Ministerio de Defensa, en comparación con el sector exportador.

Porcentaje de Ventas de Defensa según el carácter del capital social

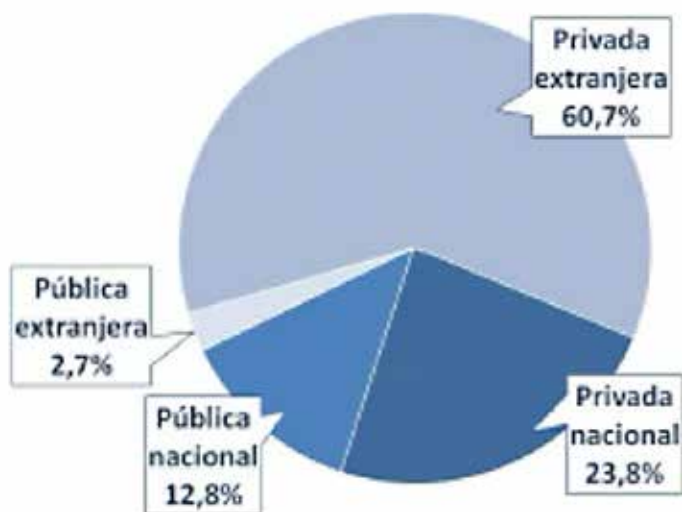


Figura 4.13 Distribución de ventas de defensa según carácter de capital social

Fuente: Ministerio de Defensa de España (2024)

En un momento de reflexión sobre autonomía estratégica, no está de más constatar que **dominan las ventas de empresas con capital extranjero**, como el gráfico de la figura 4.13 expone. El sector público participa como vendedor, con una cuota 15,5%. Efectivamente, hay que destacar el papel que juegan las empresas multinacionales europeas con fuerte presencia en España en el volumen de negocio industrial nacional⁷¹.

El **informe anual de la Dirección General de Armamento e Material de Ministerio de Defensa de España (2024)** apunta que en 2022 el total de ventas de la industria nacional de Defensa fue de 7.435 millones de euros, con ventas indirectas al Ministerio de Defensa de España de 2.023 millones de euros. Si se considera la parte nacional de Airbus, Rheinmetall (EXPAL) y MBDA las cifras de ventas de la industria de defensa española casi duplican. La tabla 4.5 siguiente contiene las principales 75 empresas de defensa en cuanto a su volumen de ventas al Ministerio de Defensa de España.

71 <https://publicaciones.defensa.gob.es/la-industria-de-defensa-en-espa-a-informe-2022-libros-pdf.html>

A							B						
2022	Empresa	Ventas al Ministerio de Defensa 2021 (millones de euros)	Ventas al Ministerio de Defensa 2022 (millones de euros)	Ratio 2022/2021	Ranking 2021	Ranking 2022	C: Evolución relativa del volumen de ventas						
1	ARMANDO TESTA E HIJOS	5.900	5.100	86%	1	2							
2	ARMUN MILITARY	1.291	1.000	77%	2	3							
3	ARMUN MILITARY	803	1.000	124%	3	1							
4	ARMUN	400	1.000	250%	4	4							
5	ARMUN	300	300	100%	5	5							
6	ARMUN	100	100	100%	6	6							
7	ARMUN	100	100	100%	7	7							
8	ARMUN	200	200	100%	8	8							
9	ARMUN	100	100	100%	9	9							
10	ARMUN	100	100	100%	10	10							
11	ARMUN	100	100	100%	11	11							
12	ARMUN	100	100	100%	12	12							
13	ARMUN	100	100	100%	13	13							
14	ARMUN	100	100	100%	14	14							
15	ARMUN	100	100	100%	15	15							
16	ARMUN	100	100	100%	16	16							
17	ARMUN	100	100	100%	17	17							
18	ARMUN	100	100	100%	18	18							
19	ARMUN	100	100	100%	19	19							
20	ARMUN	100	100	100%	20	20							
21	ARMUN	100	100	100%	21	21							
22	ARMUN	100	100	100%	22	22							
23	ARMUN	100	100	100%	23	23							
24	ARMUN	100	100	100%	24	24							
25	ARMUN	100	100	100%	25	25							
26	ARMUN	100	100	100%	26	26							
27	ARMUN	100	100	100%	27	27							
28	ARMUN	100	100	100%	28	28							
29	ARMUN	100	100	100%	29	29							
30	ARMUN	100	100	100%	30	30							
31	ARMUN	100	100	100%	31	31							
32	ARMUN	100	100	100%	32	32							
33	ARMUN	100	100	100%	33	33							
34	ARMUN	100	100	100%	34	34							
35	ARMUN	100	100	100%	35	35							
36	ARMUN	100	100	100%	36	36							
37	ARMUN	100	100	100%	37	37							
38	ARMUN	100	100	100%	38	38							
39	ARMUN	100	100	100%	39	39							
40	ARMUN	100	100	100%	40	40							
41	ARMUN	100	100	100%	41	41							
42	ARMUN	100	100	100%	42	42							
43	ARMUN	100	100	100%	43	43							
44	ARMUN	100	100	100%	44	44							
45	ARMUN	100	100	100%	45	45							
46	ARMUN	100	100	100%	46	46							
47	ARMUN	100	100	100%	47	47							
48	ARMUN	100	100	100%	48	48							
49	ARMUN	100	100	100%	49	49							
50	ARMUN	100	100	100%	50	50							
51	ARMUN	100	100	100%	51	51							
52	ARMUN	100	100	100%	52	52							
53	ARMUN	100	100	100%	53	53							
54	ARMUN	100	100	100%	54	54							
55	ARMUN	100	100	100%	55	55							
56	ARMUN	100	100	100%	56	56							
57	ARMUN	100	100	100%	57	57							
58	ARMUN	100	100	100%	58	58							
59	ARMUN	100	100	100%	59	59							
60	ARMUN	100	100	100%	60	60							
61	ARMUN	100	100	100%	61	61							
62	ARMUN	100	100	100%	62	62							
63	ARMUN	100	100	100%	63	63							
64	ARMUN	100	100	100%	64	64							
65	ARMUN	100	100	100%	65	65							
66	ARMUN	100	100	100%	66	66							
67	ARMUN	100	100	100%	67	67							
68	ARMUN	100	100	100%	68	68							
69	ARMUN	100	100	100%	69	69							
70	ARMUN	100	100	100%	70	70							
71	ARMUN	100	100	100%	71	71							
72	ARMUN	100	100	100%	72	72							
73	ARMUN	100	100	100%	73	73							
74	ARMUN	100	100	100%	74	74							
75	ARMUN	100	100	100%	75	75							

Tabla 4.5 Top 75 de empresas de defensa de ventas al Ministerio de Defensa de España
Fuente: Ministerio de Defensa de España (2024)

4.3.4 Ecosistema industrial de IA en Defensa en España

La IA está desempeñando un papel clave en la modernización de la defensa, con varias tendencias que marcan el desarrollo tecnológico en este sector, y que caracterizan la industria de defensa española. Una de ellas es la **IA en vehículos autónomos**, donde diversas empresas trabajan en **drones y vehículos no tripulados** equipados con inteligencia artificial para mejorar las capacidades operativas en el campo militar.

Otra área en crecimiento es la **guerra electrónica** con el desarrollo de sistemas de detección y neutralización de amenazas electrónicas mediante IA, lo que fortalece la capacidad de respuesta ante ataques cibernéticos y perturbaciones en las comunicaciones. En el ámbito de la **ciberseguridad**, España está invirtiendo en tecnologías basadas en inteligencia artificial para detectar y mitigar ataques en redes militares y plataformas críticas, protegiendo infraestructuras estratégicas.

Finalmente, la IA en análisis de datos y fusión de sensores está siendo integrada en centros de mando y control, permitiendo un procesamiento más rápido y preciso de la información operativa.

No se ha localizado en los estudios publicados sobre el sector industrial español una identificación exhaustiva de las capacidades existentes en el ámbito de la IA. Sin embargo, **puede considerarse que todos los sistemas harán un uso creciente de la IA**, por lo que cabe esperar

que todos los plataformistas y sistemistas o bien desarrollen algunas capacidades propias adicionales a algunas ya existentes, o alcancen colaboraciones con el ecosistema nacional e internacional de IA. En este contexto **entendemos por una capacidad “nacional” cuando exista una implantación de capacidades tecnológicas en nuestro país**. Lo mismo puede decirse del ámbito de la fabricación y de procesos de apoyo, en toda tipología de empresas.

El subsector afectado de manera más sistemática por la irrupción de la IA es el electrónico, definido como: componentes electrónicos de alta fiabilidad, sistemas electrónicos de comunicaciones, mando y control, equipos de radar, sonar, sistemas de teledetección y encriptado, control de vuelo y ayudas a la navegación, contramedidas electrónicas, robótica, así como equipos y sistemas informáticos.

En España, varias empresas del sector de defensa están incorporando soluciones de IA en sus proyectos y sistemas. Seguidamente, se indican algunas empresas representativas (no se pretende ser exhaustivo) Una de las más destacadas es **Indra**, que lidera la transformación digital en el ámbito militar a través de sistemas de simulación, análisis de datos y ciberseguridad, aplicando algoritmos de IA para mejorar la toma de decisiones y la eficiencia operativa en entornos complejos como **sistemas de mando y control (C2)**. Además, participa en el desarrollo del *Future Combat Air System (FCAS)*, el futuro caza europeo, donde la IA es clave en la toma de decisiones automatizada.

En el caso de **GMV**, integra tecnologías avanzadas, incluida la IA, en el desarrollo de sistemas de mando y control C4I e ISR, simuladores, soluciones de navegación satelital, sistemas espaciales y soluciones de ciberdefensa contribuyendo a modernizar los procesos de defensa y a optimizar la gestión de información crítica. GMV trabaja tanto con el Ministerio de Defensa español como con organismos internacionales como la OTAN, EDA y programas de la UE, participando en numerosos programas que implican el uso de la IA.

Airbus Defence and Space España aplica IA en el procesamiento de imágenes satelitales, mejorando la vigilancia y el reconocimiento en tiempo real. Además, emplea esta tecnología en sistemas de apoyo a la toma de decisiones en combate, optimizando la eficiencia operativa en escenarios militares. Airbus también tiene un papel fundamental en el desarrollo del *Future Combat Air System (FCAS)*, donde la IA será esencial para la fusión de sensores y el control de drones autónomos, impulsando la autonomía y la interconectividad en las futuras plataformas de combate aéreo.

SENER Aeroespacial y Defensa es una empresa especializada en el desarrollo de tecnologías avanzadas en optrónica, guiado, navegación y control, con una creciente aplicación de inteligencia artificial en sus productos de defensa. En el ámbito de la IA, SENER implementa algoritmos avanzados para el reconocimiento automático de objetivos (ATR), optimizando la precisión y eficacia de sistemas de misiles y plataformas de defensa. Además, trabaja en el desarrollo de sistemas de guiado autónomo mejorados con IA, lo que permite una mayor precisión y adaptabilidad en entornos operativos complejos.

EXPAL Systems, parte de *Rheinmetall* desde 2022, es una empresa tradicionalmente enfocada en municiones y sistemas de armamento, que ha comenzado a integrar inteligencia artificial en sus soluciones militares para mejorar la precisión y autonomía de sus sistemas. En este ámbito, EXPAL ha desarrollado tecnologías como *Smart Mortars* y *Smart Artillery*, que utilizan IA para el cálculo avanzado de trayectorias y la optimización de impactos en entornos de combate. Esta innovación permite una mayor eficiencia en el uso de municiones y una mejor capacidad de adaptación a escenarios tácticos dinámicos.

Tecnobit, parte del *Grupo Oesía*, es una empresa especializada en comunicaciones seguras, guerra electrónica y sistemas avanzados de defensa. Su enfoque en inteligencia artificial ha permitido el desarrollo de soluciones innovadoras en el ámbito militar. En cuanto a sus aplicaciones en IA en dominio de defensa, la compañía trabaja en procesamiento de datos en tiempo real para mejorar la toma de decisiones en combate, optimizando la rapidez y precisión de las respuestas operativas. Además, desarrolla sistemas de ciberseguridad autónoma, capaces de detectar y neutralizar amenazas en entornos militares, reforzando la protección de infraestructuras críticas y sistemas de defensa.

Amper ha decidido invertir en I+D en IA para la evolución de sus productos de defensa, concentrando su oferta en las áreas de comunicaciones, sensores y mando y control.

Swarming Technologies & Solutions, del grupo español *Zelenza*, es la primera empresa española especializada en enjambres de sistemas no tripulados. Desarrolla los enjambres *Starling*, sistemas multidominio con inteligencia distribuida y autónoma, capaces de reconfigurarse automáticamente y operar en entornos sin comunicaciones fiables, aumentando la supervivencia y eficiencia en misiones críticas.

También cabe mencionar a **Escribano Mechanical & Engineering**, empresa que desarrolla sistemas avanzados de defensa, incorporando IA en soluciones de vigilancia y control.

Otra relevante es **Aertec**, en el campo de los UAVs, singularmente de la mano de un programa de la Xunta de apoyo a la I+D y la industria en ese sector.

Estas empresas, junto con otras colaboraciones entre el sector público y privado, demuestran el compromiso de la industria militar española por incorporar la IA como herramienta clave para potenciar la seguridad, la innovación y la competitividad en el mercado global.

4.3.4.1 Industria internacional de defensa con filiales en España

Hay que subrayar que importantes **empresas multinacionales**, a través de sus filiales y oficinas en España, **contribuyen a la transferencia de tecnología, la innovación y la com-**

petitividad en el sector de defensa, fortaleciendo tanto las capacidades locales como la colaboración internacional en proyectos estratégicos.

La europea **BAE Systems** ha establecido filial en España, contando con oficinas y centros de investigación que desarrollan soluciones en defensa electrónica y sistemas integrados, lo que le permite colaborar estrechamente con el sector público y privado en el país. El grupo **Thales** posee una sólida presencia a través de varias empresas España, que agrupa diversas unidades de negocio dedicadas a la seguridad, las comunicaciones y la aviónica, colaborando en proyectos conjuntos con otras empresas y organismos del sector.

Leonardo, la compañía italiana, opera en el mercado español mediante su filial Leonardo España, que participa activamente en programas aeroespaciales y de defensa, ofreciendo soluciones integradas que combinan hardware y software de alta tecnología. Thales Alenia Space España es una empresa muy importante en comunicaciones por satélite, cuyos socios son Thales (66,6%) y Leonardo (33,3%).

El líder mundial en defensa **Lockheed Martin** cuenta con oficinas y unidades de soporte en España que se encargan de gestionar proyectos y contratos con las Fuerzas Armadas y organismos gubernamentales, facilitando la implementación de sus tecnologías avanzadas en programas europeos. **Boeing**, por su parte, mantiene presencia en España; por una parte, a través de su centro de desarrollo Boeing Research & Technology Europe (BRTE), situado en Madrid que forma parte de su división 'Boeing Global', y por otra parte, a través de oficinas de ventas y centros de soporte técnico, colaborando en proyectos de aviación militar y sistemas integrados que forman parte de la cadena de suministro aeroespacial en el país.

La empresa norteamericana **Raytheon Technologies** también tiene representación en España mediante subsidiarias o unidades locales que permiten la integración y soporte de sistemas de defensa, como misiles y radares, adaptándose a las necesidades específicas del mercado español. **Northrop Grumman** opera con oficinas regionales que facilitan la coordinación de proyectos, el soporte a contratos y la participación en iniciativas colaborativas con socios locales y organismos públicos.

4.3.5 Programas de I+D de IA en Defensa

Los programas de I+D en inteligencia artificial en el sector de la defensa son estratégicos para garantizar la superioridad tecnológica en escenarios de conflicto futuros. La convergencia entre programas públicos de I+D y el dinamismo del capital privado crea una **sinergia esencial** para acelerar la adopción de IA en defensa y mantener una ventaja competitiva sostenida.

El apoyo público a la I+D es una de las herramientas estratégicas para desarrollar una base tecnológica e industrial en Defensa. Cada país tiene una aproximación bien diferente

cuando se compara el % de la financiación pública a la I+D que se dedica a Defensa, como muestra un estudio de Bruegel (2024)⁷², como ilustra la figura 4.14:

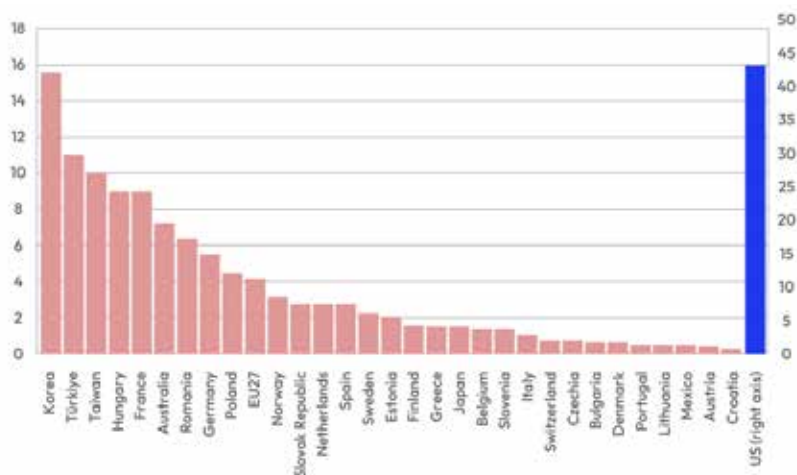


Figura 4.22 Financiación pública a la I+D por nación.

Fuente: Bruegel (2024)

Para poner en contexto estas cifras, la **Agencia Europea de Defensa (EDA)** estima los siguientes niveles de **inversión total anual en I+D en Defensa**⁷³:

- **EU**: 13.000 millones de euros (en 2024);
- **Estados Unidos**: 129.000 millones de euros (actividades de Investigación, Desarrollo, Pruebas y Evaluación en 2023);
- **China**: 21.000 millones de euros (en 2023).

Esta visión se extiende, en particular, al ámbito de la IA. En Estados Unidos, el 95% de la financiación del gobierno federal destinada a inteligencia artificial se realiza bajo el epígrafe *NAICS 54* (designación para servicios profesionales, científicos y técnicos). El 84% del valor total de la financiación bajo *NAICS 54* está vinculado a contratos relacionados con el *Departamento de Defensa (DoD)*. **La inversión total del gobierno federal en IA en 2022 fue de aproximadamente 3.300 millones de dólares**, complementando de forma totalmente direccional las inversiones masivas que ya realiza el sector privado en aquel país⁷⁴.

Este patrón es similar al que se produce en **China**, donde las inversiones aúnan el objetivo de satisfacer necesidades estratégicas en seguridad al tiempo que se impulsa la competitividad del sector industrial. China tiene, específicamente, una Estrategia de inteligencia artificial para defensa y seguridad.

72 <https://www.bruegel.org/policy-brief/european-defence-industrial-strategy-hostile-world>

73 <https://eda.europa.eu/docs/default-source/brochures/eda---defence-data-23-24---web---final.pdf>

74 <https://www.securityoutlines.cz/europe-and-ai-part-i/>

A diferencia de estos dos países, la tercera potencia mundial en IA, la **UE**, manifiesta una segmentación de las inversiones entre las instituciones comunitarias y nacionales (incluso regionales) y el menor alineamiento con los objetivos de Seguridad. Así, a los 1.000 millones de euros comunitarios anuales declarados en 2018 podrían sumarse cantidades comparables en algunos países individuales.

Rusia parte claramente con retraso respecto a los tres líderes antes mencionados, aunque está acelerando su toma de posiciones en la materia desde la aprobación en 2019 de su Estrategia Nacional de Desarrollo de la IA hasta 2030. En 2023 se estimaba una inversión en torno a los 5.000 millones de euros. En ese mismo año, el presidente Putin anunció un proyecto nacional de “Economía de Datos” que integraba líneas específicas en IA y ciberseguridad.

El **capital de riesgo** (VC) ha tenido un papel fundamental en el desarrollo y la expansión de la inteligencia artificial en los últimos años, funcionando como uno de los principales motores de innovación tecnológica. VC ha viabilizado miles de startups y empresas emergentes que han llevado la IA desde los laboratorios de investigación hasta aplicaciones concretas en sectores como la salud, la movilidad autónoma, el marketing digital, las finanzas y la ciberseguridad. Estas inversiones han permitido acelerar el desarrollo de algoritmos más eficientes, infraestructuras de datos escalables y sistemas autónomos cada vez más sofisticados, en un entorno donde el riesgo tecnológico es alto y los retornos son inciertos a corto plazo.

La figura 4.15 muestra la evolución de la inversión de capital de riesgo (VC) en tecnologías de inteligencia artificial según el sector industrial, desde 2012 hasta 2024, con base en datos de la OCDE de 2025⁷⁵.

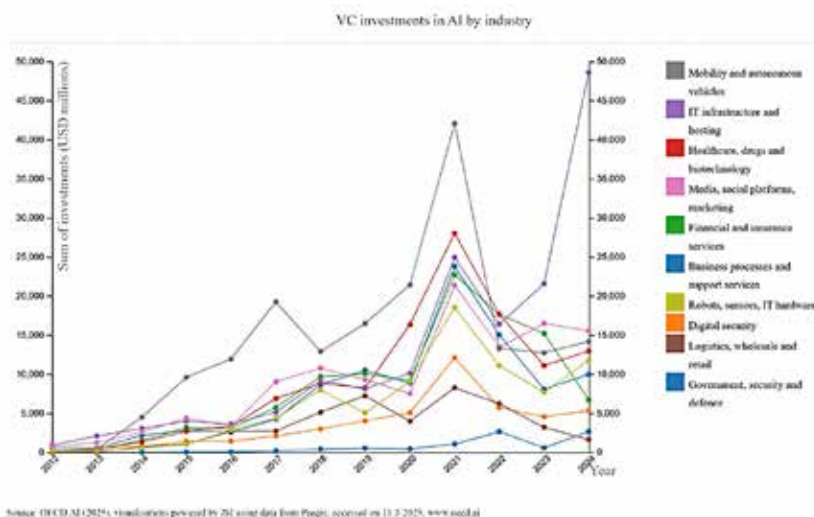


Figura 4.15 Inversiones de Venture Capital en IA
Fuente: OCDE (2025)

75 <https://oecd.ai>

El gráfico muestra que los principales sectores que han concentrado las mayores inversiones de capital de riesgo en IA durante el período 2012-2024 son movilidad y vehículos autónomos, infraestructura TI y servicios en la nube, salud, biotecnología y farmacéutica, y medios, plataformas sociales y marketing. Entre ellos, destaca especialmente el sector de **movilidad autónoma**. Le siguen la infraestructura tecnológica y el sector salud, ambos con crecimientos sostenidos a lo largo del período y picos significativos en los años de mayor inversión global.

En contraste, **áreas como las de gobierno, defensa y seguridad, han mantenido niveles de inversión considerablemente más bajos**, lo que indica una menor prioridad para los inversores privados de VC en estos campos. El hecho de que haya inversión en seguridad digital e infraestructura computacional de IA es un aspecto positivo para la defensa. Esta situación ya está cambiando, y lo va a hacer en mucha mayor medida en los próximos años.

A continuación, en esta sección se revisan diferentes actores y programas relevantes en el impulso público a la I+D en el mundo occidental en particular en la intersección entre la Defensa y la IA:

- Apoyo a la I+D en IA en defensa en Europa (EDA, PESCO y EDF);
- Apoyo a la I+D en OTAN (DIANA);
- Apoyo a la I+D en Defensa en USA (DARPA);
- Apoyo a la I+D en Defensa en España (COINCIDENTE);
- Apoyo a la I+D en IA en el programa marco (Horizonte Europa);
- Programas nacionales de potencial doble uso: PTA y CCAA.

4.3.5.1 I+D de IA en Defensa en Europa

El aumento significativo (del 13,4% interanual) en la inversión europea en I+D en los sectores de aeronáutica y defensa en 2023 es un claro indicador del creciente énfasis en el avance tecnológico y la seguridad. El gasto colectivo en I+D en estos sectores, financiado tanto por la industria como por los gobiernos, alcanzó valor un estimado de 23.400 millones de euros, según datos de ASD (2025)⁷⁶. La mayor asignación de fondos para iniciativas militares (61% frente al 39% del sector civil) refleja las tendencias globales en la priorización de las capacidades de defensa y subraya la importancia de la innovación para mantener una ventaja competitiva y afrontar los desafíos en constante evolución en el ámbito militar.

El siguiente cronograma resume la **evolución reciente de la Política de Defensa en la UE** (Bruegel, 2024), y los hitos cumplidos hasta ser consagrada la *Estrategia Industrial Europea de Defensa (EDIS)*.

⁷⁶ <https://www.asd-europe.org/news-media/facts-figures/key-data-overview/>



Figura 4.16 Evolución reciente de la política de Defensa en la UE.
Fuente: Bruegel (2024)

La *EDIS*, propuesta por la Comisión Europea el 5 de marzo de 2024, pretende, de hecho, lograr una **“Preparación de la UE a través de una industria europea de defensa receptiva y resiliente”**. Esta estrategia persigue reducir la fragmentación industrial y las importaciones de material de defensa: entre sus objetivos está conseguir que el 50% de las compras procedan de la base tecnológica e industrial de defensa europea.

Armonizar las políticas industriales y de Defensa y Seguridad europeas supone amplios desafíos, no siendo el menor el que se presenta en el ámbito institucional. Así, mientras la primera está ampliamente delegada en instituciones comunitarias, la segunda reside fundamentalmente en autoridades nacionales y, de facto, el espacio de cooperación internacional más relevante ha sido el que ofrece la OTAN. En todo caso, los países retienen también amplio margen de acción (ej.: en materia de Competencia) cuando nos referimos a la política industrial de defensa.

El contexto geopolítico que afronta la UE en el momento de redacción de estas líneas hace presuponer la **presión para alcanzar nuevos acuerdos de gran calado** en la materia, claramente en el apartado financiero, pero con alta probabilidad de que también se logren en la dimensión institucional y de estrategia industrial.

4.3.5.2 Europa – impulso a la IA en el marco de la EDA, PESCO y EDF

El *Fondo Europeo de Defensa* (EDF) de la UE, es un instrumento gestionado y ejecutado por la Comisión Europea, dotado con 8.000 millones de euros para el período 2021-2027, de los cuales 2.700 millones de euros se dirigen a investigación y 5.300 millones de euros a desarrollo en materia de defensa. La *“Permanent European Structured Cooperation”* (PESCO) agrupa de manera voluntaria a los países de la UE para cooperar en el desarrollo de capacidades de defensa.

Actualmente el *Fondo Europeo de Defensa*, abarca a 26 Estados miembros – toda la UE excepto Malta – que participan conjuntamente en proyectos en diferentes ámbitos mili-

tares (como la ciberdefensa, la defensa marítima y la defensa aérea). También participan Noruega, Islandia y Liechtenstein a través de acuerdos de asociación..

Agencia Europea de Defensa (EDA) y la IA

La *Agencia Europea de Defensa* (EDA), establecida en 2004 a través de una “*Acción Conjunta*” del Consejo de ministros, tiene cinco tareas centrales identificadas tras el “*Long Term Review*” de 2024⁷⁷:

1. Identificar las necesidades y prioridades compartidas a nivel de la UE para garantizar que las fuerzas armadas de los Estados miembros de la UE tengan las capacidades que realmente necesitan;
2. Permitir la investigación, la tecnología y la innovación colaborativas en materia de defensa para preparar el futuro de la defensa de la UE;
3. Armonizar los requisitos y participar en el desarrollo conjunto de capacidades, garantizando al mismo tiempo la interoperabilidad;
4. Agregar la demanda hacia la adquisición conjunta, para cubrir las deficiencias de capacidades;
5. Interactuar con las políticas civiles y de defensa de la UE, expresando las posiciones conjuntas de los Ministerios de Defensa.

La industria cuenta con el apoyo a la investigación y Tecnología desde la EDA. Para garantizar la identificación de las lagunas tecnológicas y las áreas de interés común para la cooperación, la **Agenda Estratégica General de Investigación (OSRA)**, la herramienta de planificación de I+D de la EDA desarrollada junto con sus Estados miembros, proporciona una visión compartida de los desafíos técnicos más importantes que deben investigarse a nivel europeo en las diferentes áreas de obtención de capacidades (“*CapTech*”). Estos “*Grupos de Tecnología de Capacidades*” especializados, están compuestos por expertos nacionales, organizaciones de la investigación y la industria. La EDA ofrece a los Estados miembros una plataforma a medida en la que pueden participar voluntariamente en proyectos de investigación de defensa colaborativos que sean de su interés. **Desde su creación en 2004, la EDA ha gestionado unos 250 proyectos de I+D, por un valor de más de 1.000 millones de euros.**

La EDA también garantiza que los Estados miembros hagan el mejor uso de la financiación existente y futura de la UE para la investigación relacionada con la defensa, especialmente la *Acción Preparatoria sobre Investigación en Defensa (PADR)* de la Comisión Europea, que gestiona la EDA, y proporciona aportaciones a un Programa de Investigación de Defensa de la UE plenamente desarrollado en el marco del EDF a partir de 2021.

La OSRA define los “**Technology Building Blocks**” (TBB) centrados en áreas específicas de I+D de defensa. Cada TBB desarrollado en los **CapTechs**, proporciona una evaluación en

⁷⁷ <https://eda.europa.eu/who-we-are/Missionandfunctions>

profundidad que incluye una hoja de ruta con ideas de proyectos concretos. En total, hay **15 CapTechs**, ubicados en la Dirección de Investigación, Tecnología e Innovación (RTI).

Las actividades de la **CapTech “Information”** están guiadas por su propia Agenda Estratégica de Investigación (SRA) que, en su versión actual incluye nueve prioridades principales, cada una corresponde a un TBB. El TBB07 aborda la prioridad *“Mejora de procesos de información mediante el uso de IA y big data”*. Dentro de este **CapTech** se desarrollan proyectos con IA:

- **CLAUDIA** (*“Cloud Intelligence for Decision Making Support and Analysis”*): desarrollo de una plataforma de análisis de software para investigar las posibilidades de apoyo al estudio y evaluación de escenarios militares, especialmente centrados en los relacionados con la guerra híbrida, a través de una amplia investigación y procesamiento de los diferentes datos involucrados.
- **CRAI** (*“Communications and Radar systems hardened with Artificial Intelligence in a contested electronic warfare environment”*): investigación de los posibles beneficios de la inteligencia artificial (IA) utilizada en una configuración combinada para la detección y el uso del espectro (comunicaciones y radar) para apoyar el conocimiento de la situación y, por lo tanto, los procesos de toma de decisiones en una aplicación militar.

En la **CapTech “Cyber”** hay un proyecto que contempla el uso de IA, que es el **MASFAD II** (*Sistema Multiagente para la Detección Avanzada de Amenazas Persistentes 2*). Como continuación de **MASFAD I**, es para desarrollar un prototipo con nuevas técnicas de detección de amenazas persistentes avanzadas a nivel de red.

Fondo Europeo de Defensa (EDF) y la IA

El EDF es el instrumento de la Comisión para apoyar la investigación y el desarrollo en materia de defensa. Sus principales objetivos son⁷⁸:

- Promover la cooperación entre empresas, incluidas las PYMES y los agentes de investigación en toda la Unión;
- Impulsar el desarrollo de capacidades de defensa mediante inversiones;
- Ayudar a las empresas de la UE a desarrollar tecnologías y equipos de defensa de vanguardia e interoperables.

El Fondo tiene un presupuesto de casi 7.300 millones de euros para el período 2021-2027. Cuenta 2.700 millones de euros asignados a la investigación colaborativa en materia de defensa y 5.300 millones de euros a proyectos de desarrollo de capacidades colaborativas que complementan las contribuciones nacionales. El apoyo financiero se ofrece principalmente a través de subvenciones de hasta el 100 % de los costes subvencionables en función de las

⁷⁸ https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en

actividades implicadas y un sistema de bonificación que tiene en cuenta a las PYMES, las empresas de mediana capitalización y la conexión con un proyecto de la PESCO.

Es interesante ubicar este instrumento en el marco del desarrollo de capacidades industriales europeas⁷⁹, como piedra basilar de la *Structure for European Armament Programmes (SEAP)*, propuesta en 2024.

Esta estructura complementaría el apoyo financiero existente incentivando la colaboración a lo largo de todo el ciclo de vida del equipamiento, desde la fase de I+D (EDF) hasta su retirada del servicio, incluyendo también el soporte operativo, que representa una parte significativa del coste total. Según un **estudio del Parlamento Europeo, el ciclo de vida de los equipos de defensa se reparte en un 10% para I+D**, un 30-35% para inversión (producción y adquisición), y un 55-60% para operación, mantenimiento y eliminación, como ilustra la figura 4.17.

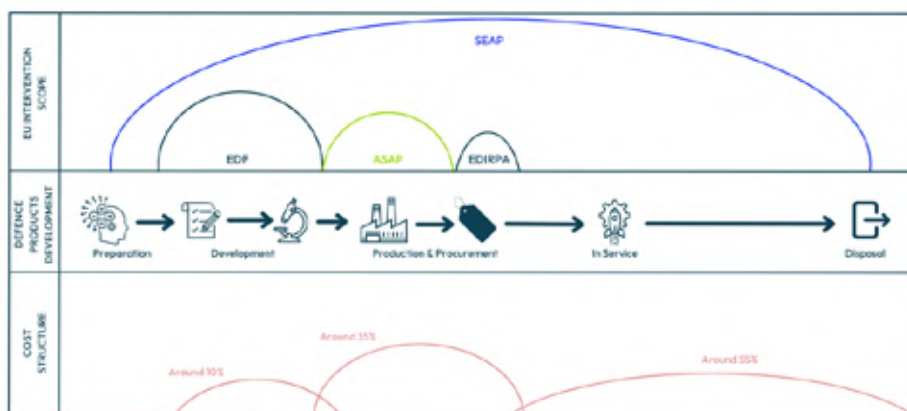


Figura 4.17 Herramientas y marcos de la UE para proporcionar apoyo en las etapas cruciales del ciclo de vida del equipamiento de defensa. Fuente: Comisión Europea (2024) https://defence-industry-space.ec.europa.eu/document/download/f1e6ba44-4720-4f14-a991-a3a7f3afb475_en?filename=Staff%20Working%20Document%20on%20EDIP.PDF

El EDF se ejecuta a través de programas de trabajo anuales estructurados en 34 categorías temáticas y horizontales de acciones en consonancia con los objetivos establecidos en el marco financiero plurianual 2021-2027. El programa lo ejecuta directamente la Comisión. En casos debidamente justificados y de conformidad con el Reglamento del EDF, la gestión de una subvención puede delegarse en una entidad encargada.

Los programas de trabajo anuales del EDF se definen en estrecha cooperación con los representantes de los Estados miembros en el Comité del Programa del EDF, incluida la participación de la Agencia Europea de Defensa y el Servicio Europeo de Acción Exterior (EEAA). El EDF construye sobre iniciativas anteriores, como la Acción Preparatoria sobre Investigación en Defensa (PADR) y el Programa Europeo de Desarrollo Industrial (EDIDP).

⁷⁹ https://defence-industry-space.ec.europa.eu/document/download/f1e6ba44-4720-4f14-a991-a3a7f3afb475_en?filename=Staff%20Working%20Document%20on%20EDIP.PDF

La figura 4.18 ilustra cómo funciona el ciclo de financiación del Fondo Europeo de Defensa durante el período 2021-2027, mostrando como se posiciona en el ciclo la investigación, el desarrollo y la adquisición de capacidades en el ámbito de la defensa a nivel de la Unión Europea.

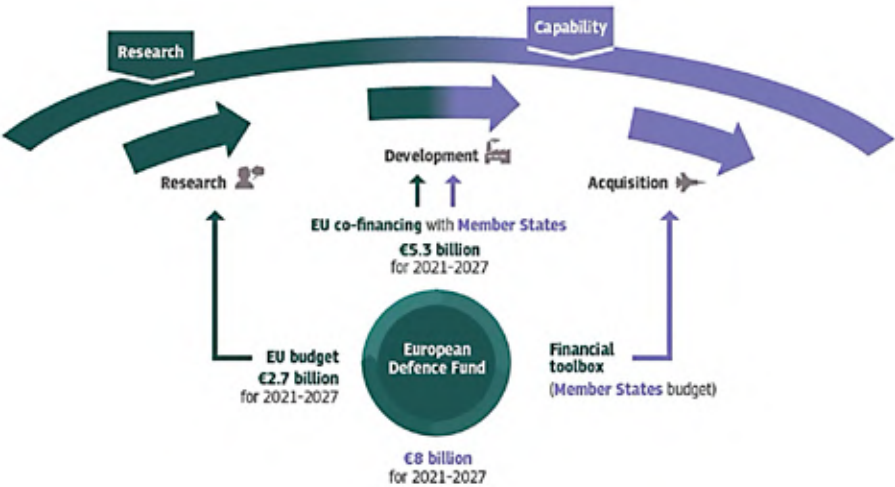


Figura 4.18 Relación entre EDF y otros programas
Fuente: Comisión Europea (2024)

La siguiente figura resume la contribución desde diferentes fuentes a la I+D colaborativa en el ámbito de la Defensa, notablemente la secuencia y complementariedad de los programas PADR, EDIDP e EDF.

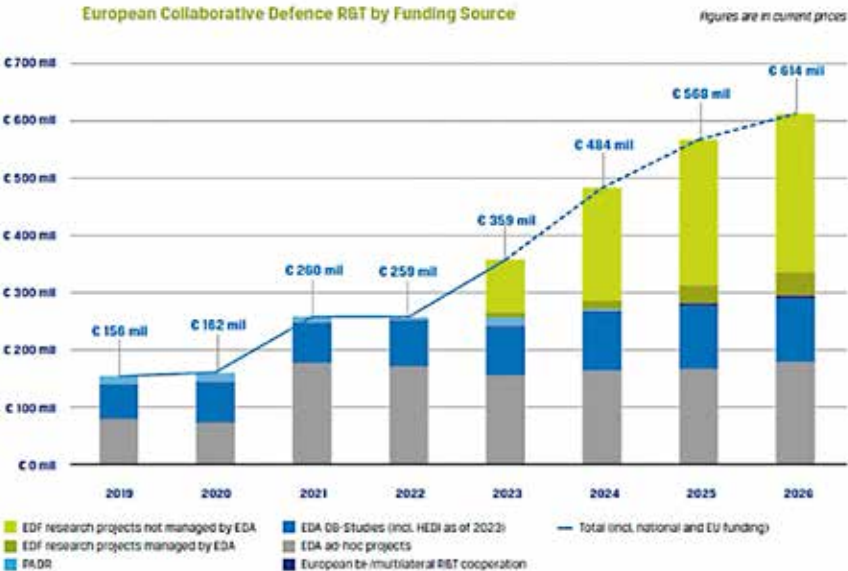


Figura 4.19 Investigación y Tecnología colaborativa en defensa en Europa según la fuente de financiación. Fuente: Comisión Europea (2024)

EDF lanzó la convocatoria de propuestas para 2024 con un presupuesto de 1,1 miles de millones de euros, abarcando 32 temas. La descripción de los temas prioritarios menciona explícitamente la IA en los siguientes 16 casos (tabla 4.6):

Temas de EDF-2024 en los que se trabaja en el ámbito de la Inteligencia Artificial:				
Topic	Titulo	Aplicación de IA	Posibles usos en defensa	Presupuesto Asignado
EDF-2024-RA-SENS-ART	Advanced radar technologies	IAMI, para procesamiento de señales y detección de amenazas	Mejora de radar de vigilancia y guerra electrónica	0,9M
EDF-2024-RA-DIGIT-ASMEP	Automated structural modelling for effect prediction	IA para predicción de efectos de ataques en estructuras	Evaluación de daños y planificación de ataques con IA	0,19M
EDF-2024-RA-PROTMOB-FMTC	Future mid-size tactical cargo aircraft	Autonomía colaborativa	Proyecto de generación de aviones de transporte táctico	0,9M
EDF-2024-RA-SIMRAIN-BRG-STEP	Methods for bridging capability gaps	Generación y simulación de escenarios	Planificación de misión, entrenamiento	0,19M
EDF-2024-LS-RA-DIS-NT	Non-thermal remote detection targeting disruptive technologies for defense	inspección	inspección	0,19M
EDF-2024-LS-RA-CHALLENGE-SENS-RADNP	Multi-sensor integration for robust autonomous drone navigation	IA para navegación autónoma de drones en entornos hostiles	Drones para misiones militares en áreas CNSS-denied	0,2M
EDF-2024-LS-RA-CHALLENGE-SENS-RADNO	Organisation of a technological challenge on robust autonomous drone navigation	IA para pruebas comparativas de navegación autónoma	Diseño de algoritmos y estándares para navegación autónoma en defensa	0M
EDF-2024-LS-RA-CHALLENGE-SPACE-MSAP	Multi-source satellite imagery analysis	IA para fusión de imágenes ópticas y radar	Mejorar el reconocimiento de objetivos militares desde el espacio	0,19M
EDF-2024-LS-RA-CHALLENGE-SPACE-MSIAO	Multi-source satellite imagery analysis	IA para fusión de imágenes ópticas y radar	Mejorar el reconocimiento de objetivos militares desde el espacio	0,10M
EDF-2024-DA-C4ISR-GEED-STEP	Small enhanced European UAS	Navegación y guiado autónomo	UAV de bajo coste	0,11M
EDF-2024-DA-C4ISR-AIMA-STEP	AI-based multifunctional aperture and transceiver	IA para gestión de espectro y comunicaciones tácticas	Resiliencia y optimización en comunicaciones tácticas militares	0,9M
EDF-2024-DA-CYBER-NGCR-STEP	Next-Generation Cooperative Cyber Range	IA para simulaciones de ciberdefensa y entrenamiento	Plataforma de entrenamiento en ciberseguridad para defensa	0,9M
EDF-2024-DA-GROUND-UGS-STEP	Multipurpose unmanned ground systems	IA para vehículos autónomos terrestres en combate	Vehículos autónomos de combate para operaciones militares	0,5M
EDF-2024-DA-NAVAL-FNP	Functional smart system of systems under an	IA para toma de decisiones	Sistemas de sistemas navales	0,9M
EDF-2024-LS-DA-SME	Non-thermal development action by Mica	inspección	inspección	0,3M

Tabla 4.6 Temas prioritarios con IA en convocatoria de propuestas EDF para 2024

Fuente: Elaboración propia con datos de la Comisión Europea (2024)

La convocatoria de propuestas de EDF para 2025 cuenta con un presupuesto de 1.065 millones de euros, abarcando 33 temas. La descripción de las prioridades para 2025 menciona explícitamente la IA en los siguientes 16 casos (tabla 4.7):

Temas de EDF-2025 en los que se trabaja en el ámbito de la Inteligencia Artificial:				
Topic	Titulo	Aplicación de IA	Posibles usos en defensa	Presupuesto Asignado
EDF-2025-RA-MODRN-AIE	Autonomous image and evaluation	Trabajo, estrategia, evaluación	Integración de campo de batalla con bajas militares	€12M
EDF-2025-RA-ENERENV-PSR	Propulsion system for next generation rockets	Monitorización y control	Motores de helicóptero de nueva generación	€25M
EDF-2025-RA-MATCOMF-CDA-STEP	Chiplet for Defense Application	Múltiples aplicaciones sobre chiplets	Múltiples aplicaciones sobre chiplets	€25M
EDF-2025-RA-SIMRAIN-UWAS	Multi-41 capabilities Design and Analysis Framework for Aerial Systems	Digital Twins (DT) con IA para optimización de diseño	Simulación de entornos, optimización de costo de vida, optimización de sistemas	€19M
EDF-2025-RA-SIMRAIN-LVC-STEP	Live, Virtual, Constructive training in interoperability - Joint operations and sensor-specific solutions	Entrenamiento de dispositivo, realidad virtual/aumentada	Entrenamiento en entornos LVC multi dominio	€19M
EDF-2025-LS-RA-CHALLENGE-DIGIT-RADNP-STEP	Privacy-preserving human-AI dialogue system - Participation in a technological challenge	Modelos de lenguaje y aplicaciones híbridas para preservación de privacidad	Chatbots y asistentes de IA para inteligencia militar y planificación estratégica	€20M
EDF-2025-DA-CYBER-CDCC-STEP	Improved cyber defense operations capabilities	Detección, cooperación, automatización de la respuesta, toma de decisiones	Automatización y aumento de la ciberdefensa distribuida, protección de software	€19M
EDF-2025-RA-GROUND-BWAS	Intelligent Weaponry and Ammunition Systems	IA para selección y ataque autónomo de objetivos	Municiones inteligentes, drones armados, precisión en el combate	No especificado
EDF-2025-DA-AIR-CAC	Collaborative Air Combat	IA para combate aéreo colaborativo y mando autónomo	Coordinación entre aviones tripulados y no tripulados, combate en red	€49M
EDF-2025-DA-AIR-DTE	Enhanced pilot awareness	IA y sensores para monitorización del estado cognitivo del piloto	Mejora en la organización del piloto, sistemas de asistencia en combate	€54M
EDF-2025-DA-CROKIND-LCC-STEP	Land collaborative combat including air-land	Mission planning	Mission planning, mando y control	€49M
EDF-2025-DA-PROTMOB-SS	Full-size demonstrators for next generation soldiers	Detección, asistencia a la toma de decisiones del combatiente	Apoyo al combatiente, comprensión situacional, detección y respuesta	€35M
EDF-2025-DA-NAVAL-DSNOC-STEP	Digital Ship and Naval Combat Cloud	Monitorización y detección de amenazas de las defensas	Naval Combat Cloud	€54M
EDF-2025-DA-UWAV-AUWV-STEP	Advanced underwater networks	Análisis de datos, monitorización, toma de decisiones	Unmanned Underwater Super Systems	€25M
EDF-2025-DA-NS-SPICEL-SOS	On-orbit operations and response	Threat intelligence	Tecnología y hardware para detectar, rastrear	€49M
EDF-2025-DA-NS-GROUND-UWMM	Drone-based affordable mass munition	Autonomía, colaboración	Municiones inteligentes para (enjambres de) drones	€49M

Tabla 4.7 Temas prioritarios con IA en convocatoria de propuestas EDF para 2025

Fuente: Elaboración propia con datos de la Comisión Europea (2025)

Del análisis de estas tablas cabe señalar lo siguiente:

- La aparición de la referencia a la IA en un tema prioritario no puede utilizarse directamente para obtener el grado de inversión específicamente en esta tecnología, que es una entre otras tecnologías habilitadoras en ese tema.
- Es palmaria la aplicación de la IA en todos los dominios (aéreo, espacial, marítimo, terrestre) y tipología de plataformas y sistemas de armamento.
- Se abordan diferentes ámbitos tecnológicos dentro de la IA (p.ej. ML, IA generativa, PLN) y aplicaciones (soporte a toma de decisiones, monitorización y control, autonomía/colaboración).

Varias **empresas españolas** han sido importantes beneficiarias de financiación del Fondo Europeo de Defensa (EDF) en diversos proyectos. Estas empresas han participado en proyectos relacionados con la **defensa hipersónica**, la **ciber resiliencia**, los **sistemas aeroespaciales** y las **capacidades navales**, poniendo de relieve el papel estratégico de España en la industria de defensa europea. En la última convocatoria 2024 de EDF, los participantes españoles obtuvieron 69 millones de euros (el 11,4% del total) y en la de 2023 149 millones (el 17,6%). A estas cantidades hay que sumar las cofinanciaciones nacionales procedentes del Ministerio de Defensa.

Programa europeo de doble uso aeronáutico: SESAR

La Empresa Conjunta **SESAR 3** (SESAR 3 JU) es una asociación público-privada institucional europea creada para acelerar, a través de la investigación y la innovación, la realización de la transformación digital del tráfico Aéreo en Europa; en otras palabras, el Cielo Digital Europeo. Para ello, desarrolla y acelera la adopción de las soluciones tecnológicas punteras para gestionar aviones convencionales, drones, taxis aéreos y vehículos que vuelan a mayor altitud. Es el pilar tecnológico de la política de Cielo Único Europeo de la UE y un facilitador clave de la Estrategia de Movilidad Sostenible e Inteligente de la Comisión Europea. SESAR define, desarrolla y despliega tecnologías para transformar la gestión del tráfico aéreo en Europa.

En los últimos años, con motivo de la guerra de Ucrania, SESAR ha iniciado actividades de integración de la gestión civil y militar del espacio aéreo. En todo caso, lo cierto es que, especialmente en el ámbito de los UAS (*Unmanned Air Systems*), existe un gran abanico de **sinergias tecnológicas, en el ámbito de la IA, entre los programas de SESAR y las aplicaciones militares de este tipo de vehículos aéreos**, como es el caso del proyecto AI4HyDrop, cuyo propósito es desarrollar un sistema dinámico holístico basado en inteligencia artificial para operaciones seguras de drones en zonas restringidas y urbanas⁸⁰.

80 <https://ai4hydrop.eu/>

Programas multilaterales OTAN: DIANA y NCIA

DIANA es el Acelerador de Innovación en Defensa para el Atlántico Norte (DIANA)⁸¹, una organización de la OTAN con la misión de localizar y acelerar la innovación de doble uso en toda la Alianza. DIANA proporciona a las empresas los recursos, las redes y la orientación para desarrollar tecnologías profundas para resolver desafíos críticos de defensa y seguridad, desde operar en entornos desfavorecidos hasta enfrentar amenazas a nuestra resiliencia colectiva.

DIANA trabaja con una red de aceleradores y centros de prueba para conectar a los usuarios finales con las mejores y más brillantes empresas emergentes, investigadores y tecnólogos en 32 naciones. Los innovadores que participan en DIANA ganan exposición a compradores gubernamentales y militares, inversores y usuarios finales en toda la Alianza.

DIANA busca resolver los principales desafíos de defensa y seguridad reuniendo a los usuarios finales militares y gubernamentales aliados con innovadores de tecnología avanzada y de uso dual.

DIANA apoya a los innovadores en este proceso brindándoles acceso a mentores, especialistas en adquisiciones y una red de inversores. El Servicio de Adopción Rápida (RAS) de DIANA brindará a las entidades nacionales aliadas la oportunidad de desarrollar y adquirir rápidamente las soluciones más prometedoras. DIANA se lanzó formalmente en 2023 y emitió su primer conjunto de desafíos poco después, en junio de 2023.

Las áreas tecnológicas de interés para los desafíos de DIANA incluyen, entre otras, redes de comunicación de próxima generación, inteligencia artificial, autonomía, tecnologías basadas en lo cuántico, biotecnología y mejora humana, energía y propulsión, nuevos materiales y fabricación, y aeroespacial.

Los participantes del Programa de Aceleración de DIANA obtendrán exposición a especialistas en inversión del Fondo de Innovación de la OTAN (NIF). La estrategia de inversión del NIF exige que éste priorice las inversiones en empresas aceleradas a través de DIANA que tengan su sede en cualquiera de los países que participan en el Fondo.

Se han establecido más de 60 test centres en países de la Alianza Atlántica que darán cobertura a los proyectos aprobados dentro del marco de DIANA en las áreas prioritarias de la OTAN. **Cinco de estos centros de investigación están ubicados en España desde 2023, y siete más fueron aprobados en 2024 (de MadQCI, Telefónica e Incibe)** dos de ellos en la UPM (*Neurotechnology and AI y Quantum Communications*) y otros dos en instalaciones del Ejército del Aire y del Espacio (*Flight Test Center – CLAEX – y el Centro de Instrucción de*

81 <https://www.diana.nato.int>

Medicina Aeroespacial – CIMA), junto al CEHIPAR *Canal de Experiencias Hidrodinámicas del Pardo*, adscrito al INTA, del Ministerio de Defensa.

La **Agencia de Información y Comunicaciones de la OTAN (NCIA)** desempeña un papel central en el avance e integración de tecnologías disruptivas como la inteligencia artificial dentro de la OTAN. Su trabajo en IA se centra en la investigación, el desarrollo, la integración y el apoyo operativo para fortalecer las capacidades de la Alianza. La NCIA ha estado apoyando a la Alianza con ciencia de datos, IA y análisis avanzado de datos, ofreciendo resultados prácticos para la comunidad de la OTAN desde 2018, cuando un grupo de científicos de datos e innovadores comenzó a colaborar con diferentes entidades de la OTAN. Con la creación de la *Oficina del director de Tecnología* en 2021, la NCIA lanzó oficialmente un equipo dedicado a **Ciencia de Datos e Inteligencia Artificial**⁸².

La agencia ha desarrollado algunos proyectos entre los que se destacan:

- El “*Data Science and AI Sandbox*” (SANDI), que proporciona un espacio seguro para desarrollar y probar herramientas de IA. Esta plataforma soporta el desarrollo de diversos proyectos clasificados dentro de la OTAN;
- Por su lado, el “*Science & Technology Ecosystem Analysis Model*” (STEAM) analiza sistemáticamente millones de documentos de investigación académica para identificar tendencias tecnológicas, en apoyo a la estrategia de la organización.

4.3.6 Desarrollos en IA militar en diversos países

Desarrollo de IA en EE. UU. – DARPA

DARPA (*Defense Advanced Research Projects Agency*) es la Agencia de Proyectos de Investigación Avanzada de Defensa de los Estados Unidos. Es un organismo del Departamento de Defensa de Estados Unidos encargado de desarrollar tecnologías innovadoras y disruptivas para mantener la superioridad tecnológica del país en el ámbito militar⁸³. La IA ha estado entre los retos abordados en DARPA durante décadas. En el momento de redactar este informe, alrededor del tema prioritario de “Artificial Intelligence” estaban abiertos los siguientes programas, que ilustran la orientación actual de su investigación:

- *AIQ: Artificial Intelligence Quantified.*
- *CODORD: Human-AI Communication for Deontic Reasoning Devops.*

82 <https://www.ncia.nato.int/about-us/technology-and-innovation/emerging-and-disruptive-technologies>

83 Creada en 1958, DARPA se enfoca en la innovación disruptiva, no en el enfoque incremental. Sin duda, se ha ganado un lugar entre las instituciones más destacadas a nivel mundial en el impulso a la innovación. Su Small Business Programs Office se especializa en el apoyo a pequeñas empresas a través de instrumentos como Small Business Innovation Research (SBIR) y Small Business Technology Transfer (STTR), que suponen el 3,2% and 4,5% de su financiación. También les ofrecen conexión con socios académicos y otras agencias federales. En 2024 tuvo un presupuesto de 4.122 millones de dólares, que financió acuerdos con 233 entidades de todo tipo.

- *EMHAT: Exploratory Models of Human-AI Teams.*
- *expMath: Exponentiating Mathematics.*
- *Heimdall (ML for targeting).*
- *LINC: Learning Introspective Control.*
- *SABER: Securing Artificial Intelligence for Battlefield Effective Robustness.*
- *SAFRON: Safe and Assured Foundation Robots for Open Environments.*
- *SBIR: Language Models for Veteran Suicide Prevention (LM4VSP).*
- *SBIR: Spectrum Monitoring and Awareness in Real-Time (SMART) – Open Topic.*
- *SCEPTER: Strategic Chaos Engine for Planning, Tactics, Experimentation and Resiliency.*
- *STTR: Addressing Underrepresentation Through Data Augmentation (Amended);*
- *STTR: Analyzing the Trade-off Between Bias and Accuracy.*
- *STTR: Bias Datasets for the Department of Defense (DoD).*
- *STTR: Mitigating Explicit and Implicit Bias Through Hybrid AI.*
- *STTR: Model-Agnostic Detection of Bias (MAD-Bias).*
- *STTR: Unlearning Bias.*
- *XENA: X-ray Extreme-range Non-imaging Analysis.*

En el tema prioritario de aprendizaje automático (“*machine learning*”) se pueden añadir los siguientes:

- **MOCHA:** Machine Learning and Optimization-guided Compilers for Heterogeneous.
- **OPEN:** Open Price Exploration for National security.
- **RIDDL:** Rapid Inhibitor Discovery and Development pipeLine.
- **TRS:** The Right Space.

Otras áreas relacionadas como “Analytics”, “Autonomy”, “Cognitive Science” añadirían aún más programas de entre los 267 accesibles a fecha de este informe.

Como ejemplo, el proyecto *Heimdall* de la iniciativa DARPA consiste en el uso de IA/ML para el control de disparos. El objetivo es madurar algoritmos de IA/ML para mejorar la eficacia del enfrentamiento de disparos navales a través de actualizaciones de software para el Sistema Informático de Armas Mk 160 (GCS) instalado en los combatientes de superficie de la Marina de los Estados Unidos. El Mk 160 GCS se utiliza para planificar y dirigir enfrentamientos de amenazas de superficie, incluida la capacidad de disparar disparos de advertencia, inhabilitar el fuego y lograr la misión de muerte contra estas amenazas. Forma parte de un sistema de armas de fuego, que también incluye un sistema de sensores electroópticos/infrarrojos (EO/IR) y monturas de armas.

Según DARPA, *Heimdall* se centra en la entrega rápida de nuevos componentes de software a la línea base de software Mk 160 GCS que ayuda o automatiza las actividades que actualmente realiza manualmente un operador. La intención es mejorar la precisión del seguimiento contra objetivos de superficie pequeños y rápidos, reduciendo el número de

rondas necesarias para un enfrentamiento exitoso. La agencia prevé una fase inicial de desarrollo de seis meses para Heimdall, en la que participarán varios actores que llevarán a cabo actividades de desarrollo de algoritmos de IA/ML.

Estos esfuerzos se centran en ayudar a los operadores a identificar objetivos a partir de las alimentaciones actuales de los sensores EO o IR y mejorar el seguimiento de los objetos seleccionados. Esta fase, para la que cada actor recibirá un contrato de 750.000 dólares, culminará con una evaluación de laboratorio del rendimiento en el entorno de simulación del Mk 160 GCS.

Una fase de integración de seguimiento, con un conjunto limitado de actores, incluye un evento de prueba de alcance y culmina con una prueba en el mar que demuestra la validez de la tecnología para obtener la certificación final para uso operativo. Esta fase también está valorada en USD 750.000 por cada intérprete.

Desarrollos de IA en Rusia

En 2024 Rusia presentó un nuevo plan de defensa a diez años que incluye una sección dedicada a la inteligencia artificial, lo que indica el enfoque de Moscú en desplegar armas autónomas.

Esta medida se produce mientras la invasión a gran escala de Ucrania por parte de Rusia ha desencadenado una carrera armamentista basada en IA en los campos de batalla, especialmente con drones aéreos y terrestres, que, según analistas, influirá en los conflictos del futuro. Elementos de inteligencia artificial han sido utilizados durante mucho tiempo en la industria militar rusa, que está estrictamente controlada por el gobierno. Por ejemplo, existe un conjunto de fabricantes de robots terrestres como los vehículos Marker, Plataforma-M, Soratnik y Uran-9, que han suministrado sus sistemas para la guerra en Ucrania.

El complejo misilístico del país también tiene una trayectoria en la incorporación de distintos grados de autonomía en los algoritmos de guiado, siendo el caso más conocido el del programa *Perimeter*, una secuencia algorítmica de la era soviética diseñada para coordinar un ataque nuclear de represalia.

El volumen del mercado ruso de IA en 2023 alcanzó casi los 650.000 millones de rublos (unos 7.300 millones de dólares), una cifra que queda muy por debajo del gasto conjunto de Occidente en diversas aplicaciones derivadas de esta tecnología.

La línea presupuestaria dedicada a la IA, cuyo monto aún no ha sido revelado por las autoridades, tiene como objetivo facilitar la transición hacia aplicaciones en defensa. Rusia anunció también la **creación de un departamento especializado en el desarrollo de inteligencia artificial dentro del Ministerio de Defensa ruso.** Por ejemplo, se está

desarrollando una capacidad de control basada en IA para el sistema de defensa aérea S-500, que permitirá evaluar amenazas y predecir daños ante un posible ataque con misiles balísticos.

La industria de defensa rusa desarrollará inteligencia artificial y sistemas automatizados aplicables a sistemas de defensa antimisiles, proyectiles de artillería y drones aéreos. Otra área de aplicación de la IA será en la aviación y la artillería, con el fin de aumentar su eficiencia. También se usará inteligencia artificial en la modelización computacional de campañas militares durante su fase de planificación. Rusia también tiene previsto utilizar IA para mejorar los procesos de producción de productos militares, mediante controles automáticos de calidad que detendrán la fabricación en caso de fallos.

A principios de 2022, el holding *Roselektronika* de la Corporación Estatal *Rostec* creó el Laboratorio de Investigación en Tecnologías de Inteligencia Artificial, dedicado a investigar el uso de la IA en sistemas de radiocomunicaciones, el desarrollo de tecnologías de realidad virtual, big data y el aprendizaje automático de redes neuronales profundas. La Fundación rusa ERA busca identificar nuevas tecnologías desarrolladas por empresas privadas y universidades. En agosto de 2024, la fundación seleccionó ocho proyectos -incluyendo una embarcación no tripulada, una torreta controlada a distancia, diversos drones y un sistema de detección de drones- que recibirán financiación para entrar en producción en masa.

Desarrollos de IA en Turquía

Turquía está logrando avances significativos en el ámbito de la defensa, especialmente en la integración de la Inteligencia Artificial (IA). A medida que el panorama global de la guerra evoluciona, Turquía es plenamente consciente del potencial transformador de la IA y está adaptando activamente sus estrategias de defensa para aprovechar dicho potencial.

Los sistemas autónomos están llamados a redefinir el futuro del combate, y el desarrollo de IA en defensa de Turquía se centra en mejorar las capacidades de estos sistemas. El enfoque no está solo en los sistemas autónomos en sí, sino también en los sensores y los sistemas de apoyo a la decisión que los complementan. **Turquía imagina un futuro en el que los humanos sigan siendo el núcleo de la toma de decisiones, con soporte de IA.**

La hoja de ruta de Turquía para la IA en defensa está bien documentada. Diversos documentos estratégicos oficiales e informes de grupos de trabajo en I+D ofrecen una visión clara de las intenciones y planes del país.

Desarrollos de IA en Israel

Israel se ha consolidado como un país líder en inteligencia artificial aplicada a vehículos aéreos no tripulados (UAV) y ciberseguridad, gracias a una combinación estratégica de inversión

gubernamental, innovación tecnológica y una estrecha colaboración entre el sector público, privado y militar. En el ámbito de los UAV, empresas israelíes como **Elbit Systems**, **Rafael** y startups como **Xtend** están integrando IA avanzada para permitir operaciones autónomas, reconocimiento inteligente y misiones de enjambre con mínima intervención humana.

Paralelamente, en ciberseguridad, Israel alberga uno de los ecosistemas más dinámicos del mundo, con el respaldo de unidades militares de élite como la Unidad 8200, que lidera el desarrollo de soluciones basadas en IA para detección de amenazas, defensa proactiva y análisis predictivo. Esta sinergia entre defensa y tecnología ha posicionado a Israel como referente global en el uso estratégico y ético de la inteligencia artificial para la seguridad nacional.

En enero de 2025, el Ministerio de Defensa de Israel puso en marcha la Administración de IA y Autonomía (AIAA) bajo la Dirección de Investigación y Desarrollo en Defensa (DDR&D). Esta administración tiene como misión supervisar la investigación, el desarrollo y la implementación de tecnologías de inteligencia artificial y sistemas autónomos en todas las ramas de las Fuerzas de Defensa de Israel (IDF). El objetivo de la AIAA es centralizar los esfuerzos para mejorar las capacidades en el campo de batalla y mantener la ventaja operativa de las IDF.

El **Programa Nacional de Inteligencia Artificial de Israel** es una iniciativa interministerial diseñada para asegurar el liderazgo a largo plazo del país en el ámbito de la IA. El programa se centra en el avance de la investigación en IA, el desarrollo del capital humano y la integración de la inteligencia artificial en diversos sectores, incluida la defensa. Pone especial énfasis en la colaboración entre el mundo académico, la industria y el gobierno para fomentar la innovación y una práctica ética en el uso de la IA.

4.3.7 I+D de IA en Defensa en España

España ha reconocido que el I+D en el área de IA debe contemplar el sector de Defensa en la *Estrategia Nacional de Inteligencia Artificial (ENIA)* publicada en 2020 por el Ministerio de Asuntos Económicos y Transformación Digital⁸⁴.

Adicionalmente, **en el año 2023 se publicó la Estrategia de IA del Ministerio de Defensa**. La estrategia, entre otras disposiciones, establece los **casos de uso de la IA**, que son una orientación para la innovación en la materia⁸⁵:

- Movilidad militar;
- Inteligencia;
- Guerra electrónica;

84 <https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/ENIA2B.pdf>

85 <https://publicaciones.defensa.gob.es/media/downloadable/files/links/2/0/20230706.pdf>

- Autonomía en el comportamiento de sistemas no tripulados;
- Apoyo logístico y alistamiento operativo;
- Conocimiento y vigilancia del entorno en los ámbitos terrestre, marítimo, aeroespacial, ciberespacial y cognitivo;
- Ciberdefensa. Identificación y actuación frente a ciberamenazas;
- Apoyo a la toma de decisiones;
- Análisis geoespacial, meteorológico y oceanográfico;
- Gestión de la información, de la infraestructura y los servicios CIS/TIC;
- Gestión del talento y formación.

En España, el desarrollo de la inteligencia artificial en el ámbito de defensa está impulsado principalmente por el sector privado, aunque este se compone de un conjunto heterogéneo de actores (Ricart, 2024). El sector industrial está protagonizado por unas pocas grandes empresas de defensa que concentran la mayor parte de las actividades en este ámbito. Sin ánimo de ser exhaustivos, se puede destacar a **Indra Systems** (empresa española de tecnología de la información y sistemas de defensa), **Navantia** (líder en seguridad marítima), **Escribano**, **GMV**, **Sener**, **Tecnobit** o **Telefónica**. **Amper** ha establecido un grupo de I+D en IA Generativa y desarrolla aplicaciones de ISR militar. Además, importantes compañías internacionales de defensa, como **Thales** y **Airbus**, también cuentan con oficinas y centros de I+D en España.

También podemos señalar la **actividad de pequeñas y medianas empresas (PYMES)** que frecuentemente han unido esfuerzos en clústeres como *Andalucía Aerospace* que representa el tejido empresarial del sector aeroespacial y de defensa en Andalucía. Otros clústeres de defensa se han empezado a crear en otras Comunidades Autónomas españolas.

Otro grupo de actores relevantes es el compuesto por instituciones de investigación, en su mayoría del sector público. Algunas de ellas forman parte del ecosistema militar, como el *Instituto Nacional de Técnica Aeroespacial Esteban Terradas (INTA)* y el incipiente *CETE-DEX (Centro Tecnológico de Desarrollo y Experimentación)* con una de sus áreas dedicado a la IA también dependiente del INTA. El Ministerio habla de su propia “comunidad de IA”. Aunque no encontramos un directorio “oficial”, en particular para aplicaciones de Defensa y Seguridad, podemos partir de la autoidentificación de los grupos de investigación que participan en **AEPIA**, la *Asociación Española de Inteligencia Artificial*⁸⁶. Por supuesto, como se ha indicado, emerge como un actor relevante el **Centro de Neurotecnología e IA** de la UPM, integrado como centro de pruebas en la red DIANA de la OTAN y en estrecha colaboración con el Ejército del Aire y del Espacio.

A destacar también, el papel de los centros tecnológicos. En el directorio de *Centros Tecnológicos de FEDIT* se posicionan en IA y el ámbito de la Defensa y Seguridad los CCTT

86 <https://www.aepia.org/grupos-de-investigacion/>

Cartif, Idonial, Leitat, Tecnalia, Gradiant, Naitec o Idecam⁸⁷. Muchos otros CCTT declaran actividad en IA, aunque no vinculada a Defensa.

Finalmente, debemos mencionar la participación de startups, en ocasiones spin-off universitarios, que trabajan principalmente para grandes empresas. Algunas de estas startups cuentan con sus propios portafolios, clientes e inversores, operan de manera independiente y ofrecen servicios a clientes internacionales. Un ejemplo exitoso y ya maduro es **Devo** (anteriormente *Logtrust*), una empresa tecnológica que desarrolló el primer software de big data en tiempo real en movimiento, permitiendo la recopilación y análisis de datos en tiempo real. **Devo** se convirtió en el **primer unicornio de ciberseguridad en España** y también ofrece soluciones de inteligencia artificial.

En el ámbito de startups que desarrollan actividad en Defensa podemos señalar también a la startup **XRF**, que desarrolla tecnologías para la toma de decisiones militares mediante el uso de realidad extendida e IA.

Para fomentar el crecimiento de startups y PYMES que trabajan en inteligencia artificial aplicada a la defensa en España, las **grandes empresas han comenzado a impulsar iniciativas para atraer a más pequeñas compañías a este campo tecnológico**. Un ejemplo es *Indra Sistemas*, que lanzó el “*FCAS Challenge*” (*Future Combat Air System*), con el objetivo de potenciar la capacidad innovadora del ecosistema industrial español mediante el desarrollo conjunto de tecnologías emergentes y disruptivas en el marco del programa FCAS. Esta iniciativa busca atraer PYMES con tecnologías avanzadas o proyectos altamente innovadores, con el fin de colaborar en el desarrollo, promoción y maduración de sus propuestas tecnológicas. Entre las áreas de mayor interés de la iniciativa destacan inteligencia artificial, gestión de datos en nubes distribuidas, sensores de baja observabilidad, simulación y representación de información, tecnologías ópticas y tecnologías de radiofrecuencia (RF) y microondas.

Además de los programas específicos de apoyo a la I+D en Defensa (ej.: COINCIDENTE), cabe mencionar el impulso innovador, en particular en la **aplicación de la IA, que surge de los grandes programas de desarrollo de plataformas y sistemas**, tales como las Fragatas F-100 y F-110, ZEUS (sistema CIS del ejército de tierra) y BACSI (Base Aérea Conectada, Sostenible e Inteligente).

4.3.7.1 El impulso a la IA en el marco de Programa COINCIDENTE

El programa COINCIDENTE (Cooperación en Investigación Científica y Desarrollo en Tecnologías Estratégicas) tiene como principal objetivo aprovechar las tecnologías de carácter civil desarrolladas en el ámbito del Plan Nacional de I+D para incorporar soluciones tecnológicas

⁸⁷ <https://fedit.com/sector/seguridad-y-defensa/>

innovadoras de interés para el Ministerio de Defensa, fomentando así el tejido industrial, científico y tecnológico dedicado a la defensa.

Los proyectos en el marco del programa COINCIDENTE deben ser tendentes al desarrollo de un demostrador con funcionalidad militar y deben suponer una novedad tecnológica significativa, que satisfaga una necesidad real o potencial del Ministerio de Defensa. Los proyectos son cofinanciados con un grado de participación del Ministerio de Defensa entre el 20% y el 80% dependiendo del interés de los mismos para la defensa nacional, de su carácter innovador, de su interés tecnológico, así como el tipo de empresa que lo presenta.

Desde su puesta en marcha en el año 1985, el programa COINCIDENTE ha sido un instrumento esencial para promover la capacitación de la base científica, tecnológica e industrial nacional en las áreas tecnológicas de interés para Defensa. El programa está abierto a la participación de empresas, universidades, centros de investigación, Organismos Públicos de Investigación, etc.

Dado que, desde 2014, no se publican los datos cuantitativos de las asignaciones económicas de cada proyecto, nos hemos centrado en un análisis del número de proyectos. La siguiente tabla 4.8 muestra la evolución del número de proyectos del programa COINCIDENTE, identificando de forma específica aquellos en los que parece que debe haber una componente de IA.

La identificación de los proyectos con componente de IA se ha realizado según el conocimiento técnico de los autores, considerando aquellos proyectos cuyo título muestra unas funcionalidades que deben integrar capacidades de tipo Inteligencia Artificial. Solamente en 2024 se incorpora, por primera vez, un área tecnológica específica de IA en la propia convocatoria y asignación de proyectos; por lo que los 3 proyectos identificados en este año son aquellos que el propio ministerio identifica como proyectos de IA. Para cada anualidad se diferencian los proyectos liderados por universidades (UNI), centros tecnológicos (C-T), empresas pequeñas (E-P), empresas medianas (E-M) y empresas grandes (E-G).

AÑO	Nº proyectos	UNI	C-T	E-P	E-M	E-G	Nº proy IA	UNI	C-T	E-P	E-M	E-G
2011	19	5		9	1	4	6	3		2		1
2014	20	8	1	9		1	5	3	1	1		
2018	22	8	4	1	6	3	7	3	1		1	2
2019	6	3		3	1		2	2				
2020	7		1	2	2	2	0					
2021	9	2	1	6			1		1	1		
2022	5		1	3	1		1				1	
2023	5	1		2	2		2			1	1	
2024	9	2		5	1	1	3			2		1

Tabla 4.8 Mapeo de actores participantes del Programa COINCIDENTE
Fuente: Elaboración propia

Desde el punto de vista de la tipología de actores, se aprecia claramente una **gran presencia de universidades**, que acaparan el 40 % de los proyectos de I+D, si bien esta presencia desaparece en los años más recientes. Cabe hacer notar que, **entre las empresas, hay una clara mayoría de empresas pequeñas en los proyectos con IA**, si bien, parece que en los últimos años empiezan a aparecer empresas medianas y grandes en este tipo de proyectos.

En cualquier caso, cabe suponer que los montantes empleados en este tipo de tecnología resultan muy alejados de los montantes dedicados por los grandes actores internacionales y, muy probablemente, también lejos de los principales actores europeos.

En los años 2011 a 2017 se aprecia que algunos proyectos debieron forzosamente incorporar tecnologías de algoritmia avanzada, según el estado del arte de la IA en aquellos momentos, para resolver los retos planteados en ciertos proyectos tales como *“Detección de anomalías y blancos en imágenes hiperspectrales”* en 2011 o *“Sistema Integrado de Gestión de Emergencias para embarcaciones Militares”* y *“Sistema de Predicción de Operación de Vehículos No Tripulados en plataformas navales”* en 2014. A ello se añaden algunos proyectos de esos años centrados en la simulación de diversos tipos de escenarios.

En las líneas tecnológicas de 2018, se identifican claramente al menos tres de ellas (Robótica aplicada a misiones militares, Detección y neutralización de IED en entornos terrestres y navales y Sistemas inteligentes de análisis y explotación de información aplicado a la resolución de problemas militares) en las que se puede presumir que es necesario que incluyan tecnologías de IA en algunos de sus componentes y subsistemas.

En esta misma línea se pueden identificar líneas prioritarias orientadas a tecnologías IA en los años posteriores: tales como *“Empleo innovador de vehículos aéreos remotamente tripulados”* en 2019, *“Tecnologías de detección para sistemas de protección activa”* en 2020, *“Sistemas de detección de artefactos explosivos improvisados”* y *“Robótica terrestre de apoyo al combatiente a pie”* en 2021 o *“Tecnologías de navegación y posicionamiento para plataformas aéreas no tripuladas en ausencia de GNSS para aplicaciones de defensa”* en 2022.

El paso adicional aparece claramente en 2023 cuando, por primera vez se identifica una línea específica de tecnología de IA titulada *“Generación de datos sintéticos para el entrenamiento de algoritmos de IA en aplicaciones de defensa”*. Esta novedad se mantiene en la convocatoria de 2024 con una línea prioritaria de *“Aplicación de la inteligencia artificial generativa a misiones militares”*.

En la convocatoria de 2025 no se ha incluido de forma explícita el área tecnológica de IA; no obstante, en dos de los tres ítems incluidos es bastante probable que las propuestas de proyectos incluyan algún tipo de algoritmia con componentes de IA, se trata de las temáti-

cas “Aprovechamiento de avances tecnológicos para el desarrollo de nuevas capacidades en municiones merodeadoras” y “Soluciones innovadoras y robustas para la navegación, posicionamiento y sincronización en entornos de defensa con denegación o degradación de la señal GNSS”.

4.3.7.2 Programas nacionales españoles de potencial uso dual: PTA y CCAA

No existen planes nacionales relacionados con la tecnología militar aparte del programa COINCIDENTE de la DGAM que se ha expuesto en otro apartado.

Tan solo el *Programa Tecnológico Aeronáutico (PTA)*, podría considerarse parcialmente como objeto del presente análisis. En el programa tecnológico aeronáutico existen cuatro líneas principales de desarrollo: Tecnologías enfocadas a la reducción de emisiones – avión cero emisiones; UAS; Sistemas; y Fabricación inteligente y avanzada – Digitalización. De todas ellas, una parte de las tecnologías de UAS podrían tener relevancia en el marco del presente análisis. En la siguiente tabla 4.9 se identifican las principales magnitudes, para las convocatorias de las anualidades de 2021, 2022 y 2023.

Año	Mtte asignado	Mtte movilizado	UAS - asignado
2021	39.999.767 €	78.854.360 €	1.538.501 €
2022	78.330.978 €	126.831.875 €	5.079.253 €
2023	109.059.943 €	71.420.078 €	7.422.182 €

Tabla 4.9 Proyectos de UAS soportados por el Programa Tecnológico Aeronáutico (PTA) de 2021 a 2023.
Fuente: Elaboración propia

Como se aprecia, el montante para actividades relacionadas con los UAS es una parte inferior al 10 % del total de del programa. Además, la mayoría de estas actividades no tienen relación con la IA.

4.3.7.3 Programas de I+D de las CCAA

En España las CCAA no tienen competencias en defensa, por lo que no tienen programas relacionados con esta actividad; no obstante, la *Xunta de Galicia* puso en marcha en 2015 la Iniciativa Estratégica “*Civil UAVs Initiative*” (CUI)⁸⁸.

Aunque esta iniciativa tiene la palabra “civil” específicamente en su denominación, se han desarrollado en su seno un conjunto de algoritmos que podrían ser fácilmente utilizados de forma dual por parte de las empresas que los han implementado; sin ánimo de realizar

⁸⁸ <https://www.civiluavsinitiative.com/wp-content/uploads/2021/08/Documento-regulador-ES.pdf>

una lista exhaustiva, de los materiales publicados en las jornadas técnicas realizadas en el marco de esta iniciativa, se pueden identificar al menos los siguientes como de interés para el tema objeto del presente informe:

- Algoritmos de detección de zonas de aterrizaje;
- Rutas de escape de brigadas antincendios;
- Rutas de acceso a puntos calientes en situaciones de emergencia;
- Identificación de obstáculos en vuelo;
- Sistemas cooperativos de tipo enjambre;
- Sistemas de resolución automática de contingencias en vuelo: pérdida de señal GPS, pérdida de energía, pérdida de control de la aeronave.

El montante total de fondos públicos invertidos por la Xunta en esta iniciativa desde 2015 asciende a más de 100 millones de euros, habiendo conseguido movilizar más de 300 millones de euros de actividad total, de los cuales una parte puede ser considerada relacionada con IA.

4.4 Evolución estimada del sector de la defensa hasta 2030

La IA en el ámbito militar se perfila como uno de los motores más dinámicos y estratégicos del desarrollo tecnológico global. Su impacto trasciende lo puramente operacional, actuando como catalizador de innovación industrial, autonomía estratégica y transformación socioeconómica.

Las cifras evidencian este impulso: el mercado global alcanzó los 9.671 millones de dólares en 2024, tras crecer a una tasa compuesta anual (CAGR) del 16,72 % desde 2019. Las proyecciones de distintas fuentes especializadas coinciden en anticipar un crecimiento sostenido y, en algunos casos, exponencial. *The Business Research Company* estima que el mercado alcanzará los 19.740 millones de dólares en 2029 y los 61.087 millones en 2034, con una CAGR de 20,57 %. Por su parte, la consultora *MarketsAndMarkets* proyecta un escenario aún más dinámico, con un mercado de 38.800 millones de dólares para 2028 y una CAGR del 33,3 %, mientras que *Precedence Research* ofrece una estimación más conservadora, apuntando a 32.170 millones de dólares en 2034 con un crecimiento del 12,9 % anual entre 2024 y 2034.

Este crecimiento acelerado responde tanto a factores estructurales – como el avance de tecnologías emergentes, el aumento del gasto en defensa y la digitalización de los conflictos – como a impulsos coyunturales derivados de tensiones geopolíticas y nuevas doctrinas operativas. Además, la participación del capital de riesgo y los programas de I+D en defensa, tanto en Estados Unidos como en Europa, están reforzando el ecosistema de innovación militar. En este contexto, la inteligencia artificial se consolida no solo como

una herramienta clave para la superioridad operativa, sino también como un activo geoestratégico y económico de primer orden, capaz de redefinir el equilibrio internacional en las próximas décadas.

El **software**, que ya representa cerca del 50 % del mercado, sigue siendo esencial, mientras que el **hardware especializado**, como procesadores y sensores, muestra fuerte expansión debido a la demanda de capacidades autónomas en tiempo real. El **aprendizaje automático** lidera por su valor en autonomía operativa, seguido por tecnologías como visión por computadora y procesamiento de lenguaje natural. Los sistemas terrestres serán la plataforma de crecimiento más rápido, reflejando su uso creciente en conflictos actuales.

En cuanto a regiones, **América del Norte mantendrá el liderazgo**, mientras que Europa, con proyecciones de 4.090 millones de dólares en 2030 y un CAGR del 9,8 %, refuerza su papel gracias a políticas de innovación, especialmente en Francia. A pesar de su rápida evolución, la IA aún representa una pequeña parte del gasto total en defensa, estimado en apenas 0,003 % en 2024. El desafío hacia 2030 será aumentar su impacto operativo, fortaleciendo la autonomía tecnológica europea sin romper alianzas clave como la OTAN. La IA redefinirá la defensa moderna, combinando capacidades inteligentes con nuevas estrategias de cooperación y desarrollo.

En España, aunque no hay una cifra oficial unificada, se estima que la inteligencia artificial en defensa podría haber generado más de 40 millones de euros en 2024, basándose en un 0,3 % del presupuesto nacional de defensa. La inversión está en crecimiento, impulsada por la transformación digital y la demanda de capacidades avanzadas.

El sector industrial de inteligencia artificial en defensa está compuesto por fabricantes de hardware, proveedores de software e integradores de sistemas. A nivel global, empresas como NVIDIA, Lockheed Martin, Raytheon, BAE Systems, Airbus, Leonardo y Thales lideran el uso de la IA en defensa. Navantia es la única empresa española entre las cien principales empresas a nivel mundial. La intensidad del resultado de la I+D tiene como un indicador el número de solicitudes de patentes en IA aplicada a defensa. En 2024, EE. UU. mantuvo el liderazgo con el 45 % de las nuevas patentes, muy por delante de China y Europa. Hacia 2030, se espera que esta tendencia continúe, con un fuerte papel de actores industriales consolidados y PYMES innovadoras.

Los programas europeos de I+D, especialmente el *European Defence Fund (EDF)*, son clave para impulsar la innovación en inteligencia artificial aplicada a defensa. Con un presupuesto de 8.000 millones de euros (2021–2027), el EDF financia investigación y desarrollo colaborativo, fomentando capacidades autónomas y soberanía tecnológica.

Frente al liderazgo inversor de EE. UU. y China, la UE apuesta por una estrategia industrial integrada a través de la EDA, la PESCO y el EDF, alineando tecnologías emergentes como IA, ciberseguridad y big data. **Esta financiación complementa el capital privado y fortalece la base industrial europea de defensa.** Hacia 2030, se prevé una ampliación del papel de la IA en todos los dominios operativos y plataformas, con participación creciente de empresas españolas.

En España, **el I+D de la IA en defensa está liderado por el sector privado**, dominado por un grupo reducido de grandes empresas como Indra, Navantia, Escribano, GMV, Sener, Tecno-bit y Telefónica. Entre ellas, Amper destaca por su grupo de I+D en IA generativa. También operan en el país multinacionales como Thales y Airbus, con centros de I+D activos. Estas son las entidades mejor posicionadas para liderar proyectos nacionales y exportar dentro de la UE y otros países OTAN, con una apuesta en la innovación apalancada en motores de I+D como los EDF.

En el radar de todas las entidades de la IA en Defensa está el plan *ReArm Europe / Readiness 2030*. Este plan se destina a **financiar la defensa de la UE** con 800.000 millones de euros, que es la cantidad que los Estados miembros aspiran a movilizar hasta 2030 para financiar un aumento masivo del gasto en defensa, como respuesta a los compromisos OTAN y otros desafíos, con un principio “*made in Europe*” de fortalecimiento de la industria de defensa. De él ya se ha aprobado en mayo de 2025 el reglamento del instrumento **SAFE** dotado de 150.000 millones de euros en créditos como se ha expuesto en el capítulo 2.

En relación con la situación de la Industria de Defensa Española, la matriz DAFO de la tabla 4.9 analiza el **posicionamiento estratégico de la Industria de Defensa Española en relación con el mercado emergente de la IA aplicada al ámbito de defensa hasta el año 2030**. Esta evaluación explora las fortalezas internas y debilidades estructurales del sector, así como las oportunidades externas y amenazas potenciales derivadas de los rápidos avances tecnológicos, la evolución del contexto geopolítico global y los desafíos propios del mercado europeo e internacional.

DEBILIDADES	AMENAZAS
• Tamaño de nuestras empresas (con las excepciones indicadas) • Escasez de actores en el ámbito de software base y plataformas tecnológicas • Escasez de plataformas de datos • Debilidad de enlaces entre entorno científico y empresa • Escasez de recursos financieros del Ministerio de Defensa • Escasez de recursos financieros públicos nacionales para el apoyo a la I+D • Escasez de inversión privada en I+D • Tamaño del sector nacional de Venture Capital • Inmadurez en la valoración y el tratamiento de los IPRs • Dependencia casi total en LLM no-UE	• Acceso a elementos críticos en la cadena de valor (ej.: chips) • Competencia de nuevos actores industriales internacionales • Priorización de políticas de adquisiciones a corto plazo (i.e. USA vs UE) • Pérdida de atractivo para el talento vs otros sectores • Falta de continuidad en la política nacional por ausencia de consensos básicos • Nuevos modelos tecnológicos demandantes de grandes economías de escala (ej.: LLMs) • Orientación de los grandes programas comunitarios de I+D e industrial hacia los intereses de otros países • Fragmentación de la OTAN
FORTALEZAS	OPORTUNIDADES
• Buena calidad de la base científica del país • Competitividad internacional de la industria española de Defensa • Presencia (en grado variable) en los grandes sistemas y plataformas (i.e. acceso al control cadena de valor y a datos) • Capacidades en el segmento de servicios de integración y desarrollo • Cohesión en el ecosistema institucional e industrial • Competitividad en programas colaborativos internacionales • Competitividad del talento STEM • Refuerzo institucional a la I+D en Defensa • Nuevos ecosistemas de startups • Buena relación histórica entre el Ministerio y la industria nacional	• Revolución tecnológica por la IA • Nueva estrategia europea de Defensa e inversiones – ReArm Europe • Nueva estrategia e inversiones nacionales • Nueva ley de Industria • Nuevos paradigmas tecnológicos accesibles para el desarrollo de la IA (sin grandes economías de escala), ej. modelos abiertos • Infraestructuras UE compartidas (ej.: factorías de IA) • Mercados internacionales no alineados • EDF para soporte a la innovación

Tabla 4.10 Matriz DAFO sobre posicionamiento estratégico de la Industria de Defensa Española en relación con el mercado emergente de la IA aplicada al ámbito de defensa hasta el año 2030

Fuente: Elaboración propia

Capítulo 5

CAPÍTULO 5.

DIMENSIÓN TÁCTICA, OPERATIVA Y ESTRATÉGICA DEL USO DE LA IA EN DEFENSA

5.1 Introducción progresiva de la IA en operaciones militares

Tras el análisis efectuado en capítulos anteriores sobre la situación y tendencias de las tecnologías que configuran la inteligencia artificial (desarrollado en el capítulo 3), y la dimensión socioeconómica, prestando especial atención a la estructura y evolución del mercado de la IA en defensa (desarrollado en el capítulo 4), el objetivo perseguido en el presente capítulo 5 es el de describir el **uso actual de la IA desde la dimensión táctica, operativa y estratégica en el ámbito de la defensa y su previsible evolución a lo largo de la presente década**. Son, precisamente las ventajas derivadas de este uso real de la IA en defensa, las que impulsan el desarrollo del mercado descrito en el capítulo anterior, y los profundos cambios en la forma en la que se desarrollan las operaciones militares. El incremento acelerado de las inversiones en defensa, están sirviendo también para acelerar determinadas **tecnologías relacionadas con el uso dual de la IA**.

El GT es consciente de que no es posible desarrollar en estas páginas todos los aspectos que cubren el uso de la IA por las fuerzas armadas en todo el mundo, y menos aún su eficacia real en el campo de batalla, información que en muchos casos, está clasificada y no es accesible. Por este motivo, se ha decidido focalizar la descripción en un **conjunto reducido de ámbitos que se consideran cruciales y representativos de la penetración de la IA en defensa**. Algunos de ellos presentan **condicionantes éticos y regulatorios** relevantes, que han merecido la atención para su desarrollo en un capítulo específico independiente (capítulo 6).

Existen otros usos de la IA en los procesos de **desarrollo de los sistemas de armas por la industria de defensa**, tanto de armas ligeras como de grandes plataformas militares (aviones, buques, tanques, etc.), y también de **equipos militares** (radios tácticas, redes de comunicaciones, nube de combate, sistemas de guerra electrónica, plataformas de toma de decisión en mando y control, etc.) o para su mantenimiento (mantenimiento predictivo, logística inteligente, etc.), que son cada vez más relevantes.

Muchos de ellos tienen un carácter eminentemente dual y son compartidos para el desarrollo de equipos de uso civil o son adaptaciones de ellos; así sucede con el apoyo logístico, con el mantenimiento predictivo de equipos y sistemas y con el desarrollo de productos basados en la denominada **ingeniería digital** que hacen uso creciente de técnicas de modelado y simulación apoyada por el uso de **gemelos digitales**. Sin embargo, su introducción en este

capítulo hubiese desenfocado el objetivo pretendido de prestar atención al **uso de la IA en las operaciones militares**.

Concretamente, en este capítulo 5 se abordan **tres grandes temas** en el ámbito de defensa **en los que la IA juega un papel esencial**: la evolución hacia lo que se denomina un **campo de batalla inteligente**, el creciente empleo de la IA en la denominada **guerra híbrida y cognitiva**, y la importancia que adquiere la IA en un dominio dual como es el del **espacio**, cuyo valor para la defensa multidominio es creciente. En todos los temas indicados el uso de la IA evoluciona rápidamente por lo que se prestará atención a las razones de su progresiva adopción y a las barreras existentes que limitan su uso.

En el primero de los temas seleccionados, evolución hacia un **campo de batalla inteligente**, se pretende dar cuenta del papel que la IA juega para disponer de una visión integrada basada en la captura y análisis de datos de la situación en el campo de batalla como base para la toma de decisiones autónomas o semiautónomas. El análisis se focalizará en el uso de la IA en **sistemas de mando y control**, en la necesidad de gestión de **sistemas de comunicaciones** integrados a varios niveles focalizado en el concepto de **nube de combate**, y en el relevante tema del empleo de **armas autónomas o semiautónomas** y sus condicionantes de uso por operadores humanos junto a armas convencionales.

Con el segundo de los temas seleccionados se aborda un ámbito de creciente relevancia como es la irrupción **de la IA en la expansión de la guerra híbrida y cognitiva**. En él se presta especial atención a la forma en la que se potencia el uso de la IA como factor esencial en la gradación de intensidad que va desde la **amenaza híbrida**, al **conflicto híbrido** y, finalmente, a la **guerra híbrida**, combinando acciones cinéticas, cibernéticas o de control de la información. Desde esta visión se pretende, asimismo, describir el **creciente uso de la IA en la guerra cognitiva** y, especialmente, de la importancia que han adquirido en las campañas de desinformación y generación de narrativas como un factor esencial de las guerras híbridas y convencionales cuya extensión y relevancia es creciente.

Finalmente, con el tercero de los temas seleccionados, el **uso de la IA en el sector espacial de la defensa**, se aborda su uso en un dominio eminentemente dual, dado que muchas de sus plataformas (ya sean satélites individuales o formando parte de constelaciones) en orbitas geoestacionarias, medias o bajas, asumen funciones civiles y militares para comunicaciones, observación y navegación. Todo ello, con independencia de la necesidad de desarrollar cargas útiles específicas para la defensa y el desarrollo de armas anti satélites (Bendett y Kirichenko, 2025).

Esta evolución está ligada a la creciente relevancia del **espacio como un dominio plenamente integrado** junto al terrestre, marítimo, aéreo, ciber y cognitivo, enmarcado en el

concepto de **operaciones multidominio** que se configura como un elemento clave del uso de la IA en las operaciones militares.

No se ha pretendido ofrecer un análisis exhaustivo en todos los países del uso militar de la IA, imposible de realizar, sino mostrar a lo largo del capítulo diversos **casos de uso de la IA en operaciones militares** que para la redacción del informe se ha considerado representativos del papel que juega la IA, y las tendencias más relevantes que incrementarán su despliegue a lo largo de la presente década.

Los ejemplos que indican el **empleo innovador de la IA** se han basado en referencias a **fuentes abiertas** con especial atención a *Europa* y *Estados Unidos*. Podría argumentarse que, en cualquiera de los ámbitos indicados, podrían existir otros casos de uso más avanzados que los descritos en proyectos de I+D desarrollados en centros o laboratorios de defensa, pero la información sobre ellos está clasificada. El GT es consciente de que su uso y despliegue, aunque sea de forma experimental, puede **acelerarse en el caso de continuación de conflictos militares de alta intensidad**, como el caso de los drones en la guerra en Ucrania ejemplifica de manera evidente en los últimos tres años.

El futuro del uso de la IA en defensa mostrará cambios aún más significativos cuando se produzca su **convergencia con las tecnologías cuánticas**, como ya intuye la Escuela de Guerra de Estados Unidos (Simmons *et al.*, 2024; Carlson, *et al.*, 2024); situación que se espera que se materialice en la próxima década, a pesar de que algunos experimentos sí se llevarán a cabo durante la actual.

5.2 Evolución hacia un campo de batalla inteligente

5.2.1 Introducción progresiva de nuevas tecnologías

La **introducción de sistemas tecnológicos en el campo de batalla** con los que se pueda obtener la superioridad frente al adversario ha sido una tendencia constante en la historia de la humanidad. Hacerlo **a tiempo y de manera efectiva, modificando, con su aplicación**, si fuera necesario, **las tácticas y estrategias militares empleadas**, ha constituido un factor clave para el éxito de su uso y su permanencia en el tiempo (Aznar, 2024).

En cada momento histórico que se considere, el **esfuerzo para disponer de nuevos sistemas tecnológicos** de combate que permitan superar las defensas del adversario o protegerse de los ataques también ha presionado a los bandos en conflicto para **utilizar la tecnología más avanzada disponible**, incluso, cuando ello lleva a aceptar **riesgos derivados de su falta de madurez**. Se trata de un escenario en el que se genera una sucesión continua de avances desde las perspectivas ofensivas y defensivas.

Son innumerables los ejemplos históricos que se pueden citar de la forma en la que los ejércitos han incorporado las nuevas tecnologías disponibles en cada momento en el nivel individual y colectivo, modificando con ello sus tácticas y estrategias. Puede decirse que **el “campo de batalla” siempre ha sido un laboratorio de experimentación y maduración de sistemas tecnológicos** que, con posterioridad, en caso de éxito, se han expandido por mimetización a todos los ejércitos, y que, en algunos casos, ha dado lugar a múltiples desarrollos civiles que han penetrado profundamente en la sociedad.

La situación en 2025 de la incorporación de nuevos sistemas tecnológicos al uso militar no es conceptualmente diferente a la señalada, aunque sí se conjugan actualmente tres **elementos característicos** que le confiere una mayor **relevancia y complejidad**:

1. la **velocidad** a la que se suceden los cambios tecnológicos en los sistemas de armas de ataque y defensa desplegados en el campo de batalla, muy superior a la ocurrida en etapas anteriores.
2. la utilización de **tecnologías duales** en su mayor parte generadas en el ámbito civil y, posteriormente, adaptadas al ámbito militar para satisfacer requisitos específicos.
3. la necesidad de disponer de **sistemas automáticos de ayuda a la decisión o a la ejecución de acciones** soportados por un uso creciente de la IA, que se han integrado en sistemas multitecnológicos de defensa interoperables muy complejos.

El primer factor mencionado relativo al incremento de la **tasa del cambio tecnológico** constituye un elemento clave para comprender la situación actual. Se trata con ello de considerar el **impacto generado por una aceleración tecnológica** en situaciones de conflictos militares de alta intensidad o de riesgo de su emergencia, en el que la tecnología puede jugar un papel disuasorio. El cambio tecnológico en el ámbito de la defensa es reflejo del que tiene lugar en múltiples sectores civiles, pero que, en el de la defensa, adquiere un protagonismo clave enfocado en asegurar, a través del uso de la tecnología, la **superioridad frente al adversario**.

Desde el siglo XX ha sido habitual que **cambios tecnológicos significativos para la defensa se sucedieran en periodos cada vez más cortos**, como demuestran los avances tecnológicos sucedidos en las dos guerras mundiales y conflictos posteriores en Asia y Oriente Medio. Posteriormente, en la Primera Guerra del Golfo Pérsico, del 2 de agosto de 1990 al 28 de febrero de 1991, fue el turno de la **tecnología digital**, que ha jugado desde entonces un papel esencial de una nueva era estratégica caracterizada durante unos años por un dominio político, económico, tecnológico y financiero de Estados Unidos (Gautier, 2023).

En el siglo XXI, como se ha hecho patente en el caso de la guerra de Ucrania, cambios relevantes en los sistemas tecnológicos empleados por ambos bandos se suceden en periodos que no se miden en años, sino en meses o semanas. El caso de la evolución de los **drones**

aéreos o marítimos letales es un ejemplo paradigmático de esta velocidad de incorporación al campo de batalla con ciclos de detección de problemas, desarrollo, experimentación y despliegue de una nueva solución tecnológica en pocas semanas; todo ello, con la consiguiente **modificación de las tácticas militares utilizadas** en base a la experiencia acumulada en su uso y en la valoración de su eficacia.

El segundo de los factores mencionados, el **creciente uso de tecnologías duales** que se adaptan al uso militar (Baldwin, 2024; León, 2024a y 2023) también demuestra la capacidad de aprovechar desarrollos preexistentes, aprovechando las enormes **inversiones realizadas en mercados civiles sobre algunas tecnologías habilitadoras**; este hecho contribuye al proceso de aceleración en la innovación tecnológica militar indicado previamente como primer factor.

Un ámbito en el que se constata expresamente este fenómeno es el de las **tecnologías microelectrónicas**. A diferencia de lo ocurrido en el comienzo de los circuitos integrados o de la Internet, en el que las necesidades militares impulsaron su desarrollo en la segunda mitad del siglo XX, **son ahora las fuerzas armadas quienes adaptan desarrollos civiles**. El caso de los microprocesadores, de las unidades de procesamiento gráfico (GPU), de los chips de memoria de gran ancho de banda, de arquitecturas de altas prestaciones en los centros de datos o de múltiples sistemas software para la gestión de enormes volúmenes de datos en la *nube* demuestran esta dinámica.

Obviamente, **a los requisitos habituales del mercado civil se suman otros específicos de su uso militar** que implican o pueden implicar la adaptación o el rediseño de algunos de estos sistemas para cubrir necesidades derivadas de un mayor rango de temperatura, vibraciones, radiación, y otras muchas.

El fenómeno indicado no solo tiene lugar en relación con los sistemas y componentes microelectrónicos integrados en un producto civil o militar, sino también con las **herramientas de diseño y fabricación de los circuitos integrados** cuya dualidad de uso es manifiesta y que explica el valor estratégico que adquieren en la confrontación geopolítica actual. Las restricciones establecidas por Estados Unidos a China para la comercialización de sistemas de *litografía ultravioleta extrema (EUV)*, empleados para la fabricación de chips, potencialmente de uso dual, como los empleados para aplicaciones de IA son paradigmáticas de la interacción de las herramientas de diseño con el desarrollo posterior de aplicaciones (Colussi, 2025).

Finalmente, el tercer factor referido a la **integración de algoritmos de inteligencia artificial en equipos militares y sistemas de armas para dotarles de una mayor inteligencia** ha tenido que esperar a una maduración mayor para un despliegue efectivo en el campo de batalla, porque los riesgos derivados de su uso son mayores (Pérez-Martínez, 2024). Sin embargo, debe reconocerse que su uso es creciente y acelerado (Black et al., 2025); simplemente, **sin el concurso de la IA no sería posible integrar y analizar un volumen creciente de datos capturados en tiempo real desde múltiples sensores**.

En este caso, los **riesgos y condicionantes éticos asociados a la automatización de decisiones** con consecuencias en la selección de objetivos o en la ejecución automática de las acciones derivadas (p.ej. en drones o misiles lanzados hacia coordenadas de un objetivo seleccionado previamente por un algoritmo de IA) obligó a una mayor prudencia en su adopción. Con ella se pusieron sobre el tapete las consecuencias de la menor intervención de operadores humanos y su papel futuro en la toma de decisiones (Moliner, 2024).

Como también ha ocurrido en el pasado con la incorporación de nuevos sistemas de armas, la adopción de sistemas tecnológicos disruptivos en el ámbito militar ha obligado a llevar a cabo **modificaciones sustanciales de las estrategias y tácticas militares** empleadas, así como la necesidad de **incrementar la preparación del personal** que las emplean, cuyo grado de especialización es creciente y requiere de actualización de conocimientos y re-entrenamientos continuos.

Tampoco este hecho constituye una novedad, puesto que la historia también demuestra repetidas veces la **estrecha interacción existente entre la evolución de las tácticas militares y el armamento empleado**. En unos casos, la necesidad de nuevas tácticas impulsa su desarrollo y, en otras, es la experiencia de su uso la que implica cambios en las tácticas y estrategias empleadas. El caso de la adopción y despliegue de la IA en las fuerzas armadas encaja en este contexto como se verá posteriormente.

Es precisamente la relevancia de la IA en la defensa la que ha motivado reacciones geopolíticas como las que han alimentado los **controles de exportación sobre los chips de IA** impuestos por Estados Unidos a China (combinación del interés de asegurar el dominio tecnológico y la superioridad militar), y la contra reacción derivada en China que ha llevado a fortalecer y acelerar su propio desarrollo microelectrónico o de sistemas de IA (Wang, 2025).

En definitiva, **la adopción de sistemas tecnológicos avanzados** en el ámbito de la defensa no es un proceso sencillo y rápido exento de riesgos. En el caso de la IA, de su inherente complejidad para entender la forma en la que los algoritmos han llegado a generar una determinada respuesta, y de las potenciales consecuencias sobre la vida de personas que pueda conllevar su uso, explica el hecho de que el **despliegue masivo de nuevos sistemas tecnológicos inteligentes en defensa se realice a un ritmo más lento que la introducción de sistemas con la misma tecnología en sectores civiles**.

En la siguiente sección se analizan las tendencias del uso de la IA en un campo de batalla inteligente prestando atención a la **visión multidominio** en el camino hacia una mayor transparencia de la situación en el terreno, el uso de la IA en **sistemas de mando y control multidominio**, en la implantación de la **nube de combate inteligente** y el creciente papel que juega la IA en la **guerra electrónica**.

El muy relevante tema de los **sistemas autónomos** y, en especial, el despliegue de las **armas autónomas o semiautónomas** y el papel que la IA juega en incrementar su efectividad, como parte del **campo de batalla inteligente**, se tratará posteriormente en una sección específica del presente capítulo.

5.2.2. Niveles de automatización

En muy pocos años múltiples **sistemas de armas inteligentes o sistemas de armas autónomos** con diversas soluciones basadas en IA se han incorporado, junto a sistemas microelectrónicos, sensores, y actuadores de todo tipo, en una carrera tecnológica en **búsqueda de la supremacía entre grandes potencias** sabedoras del papel que pueden jugar frente a las armas convencionales en el campo de batalla.

En todas ellas la idea básica consiste en **delegar en algoritmos de IA parcial o totalmente** (es decir, con o sin intervención del operador humano) **la toma de decisiones** con objeto de acelerar el proceso de decisión y ser capaces de manejar volúmenes de datos ingentes que un operador humano no podría analizar; menos aún si se requiere hacerlo en condiciones temporales muy estrictas. La información generada (p.ej. las coordenadas de un objetivo identificado) puede ser comunicada a otro sistema como sucedería en el caso de un dron para generar un ataque sobre uno de los objetivos seleccionados o puede generarse directamente por el dron, en interacción con el operador humano.

El rango de soluciones no responde a una clasificación binaria: decisión automatizada o no; en realidad, debe hablarse de una **gradación en las capacidades de automatización** como puede verse en la figura 5.1 en **diez niveles** diferenciados.



Figura 5.1. Niveles de automatización. Fuente: elaboración propia

Comenzando en el **nivel 1** en el que el sistema informático no tiene ninguna función y es **el operador humano el que toma todas las decisiones**, hasta el **nivel 10** en el que es el **sistema potenciado por la IA el que toma las decisiones** y el humano ninguna, existen muchos niveles intermedios.

Hasta el nivel 4 de automatización puede decirse que es el operador humano el que controla la decisión. Son niveles en los que el sistema informático dotado de algoritmos de IA que acceden a datos históricos y de tiempo real asume una **función de ayuda a la decisión, pero el operador humano está firmemente asentado en el bucle de decisión** (*human in the loop*). El uso en el ámbito militar de estos niveles es ampliamente aceptado. En el ejemplo del empleo de drones mencionado anteriormente, el sistema inteligente puede generar las coordenadas objetivo, pero es decisión del operador humano dar la orden al dron de ir a ellas, y actuar si procede.

Por otro lado, los niveles de automatización del 5 al 7, denominados en la figura como “*zona gris*” implican aceptar progresivamente una **responsabilidad mayor de los algoritmos** del sistema informático, permitiendo la aprobación (nivel 5), el veto temporal (nivel 6) o proporcionar la información a tiempo al operador humano para la toma de medidas alternativas que deshagan la acción iniciada²⁵⁴ (nivel 7). Puede decirse que el **humano está sobre el bucle de decisión** (*on the loop*). Finalmente, los niveles de automatización del 8 al 10 se corresponden con el uso de **algoritmos que toman la decisión**. El humano puede, o no, ser informado de ello, dependiendo del nivel considerado, pero está **fuera del bucle de decisión** (*out of the loop*).

Generalmente, ningún gobierno acepta públicamente que los sistemas de armas dispongan de un nivel de autonomía del 7 o superior, al menos con la madurez de los sistemas de IA actuales, cuando de ello se pueden desprender consecuencias irremediables sobre la vida de personas²⁵⁵. Como se analizará posteriormente, aunque no exista una regulación taxativa que lo impida, se plantean **problemas éticos considerables en la aceptación de estos niveles en sistemas de armas autónomos**.

5.3 Tendencias del uso de la IA en un campo de batalla inteligente

5.3.1 IA en el campo de batalla

La IA está cambiando la forma en la que se diseñan y llevan a cabo las operaciones militares al y la mejorar la toma de decisiones, el conocimiento de la situación en el campo de batalla

254 Por ejemplo, con la posibilidad de forzar la ejecución de un sistema de autodestrucción de un misil lanzado de forma automática mucho antes de alcanzar el blanco o abandonar el territorio propio.

255 Es interesante indicar, no obstante, que sí se han aceptado por la sociedad funciones totalmente automáticas en sistemas cuando ello repercute en el salud o bienestar del humano. Es el caso de algunos sistemas médicos de monitorización automática, o en vehículos para forzar la reducción de velocidad o parada ante la detección de un obstáculo o persona frente al vehículo. En ambos casos, no se causa perjuicio a un tercero.

de los diferentes activos (de las fuerzas propias y las del adversario) y la asignación dinámica de recursos. Así, la IA **permite el desarrollo de operaciones militares más eficaces y reduce potencialmente los riesgos para el personal militar** en la medida en la que puedan operar más alejados de la *zona de contacto*.

Desde el **punto de vista técnico**, las principales áreas de aplicación de la IA para la defensa que se documentan en la literatura son:

- **Gestión inteligente de grandes volúmenes de datos** integrando los históricos con los capturados en tiempo real. Se han aplicado al mantenimiento predictivo o la logística con objeto de maximizar el uso y eficiencia con objeto de **optimizar el uso de los recursos materiales** disponibles.
- **Guerra electrónica**: se refiere al uso de tecnologías digitales para interrumpir, deshabilitar o destruir los sistemas informáticos, las redes y la infraestructura del enemigo, lo que incluye el lanzamiento de ciberataques dirigidos, la defensa electrónica de las amenazas y las operaciones encubiertas.
- **Inteligencia, vigilancia y reconocimiento (ISR)**: implica el uso de sensores, drones, aviones y satélites con IA embebida para recopilar y analizar datos sobre posiciones, daños y movimientos del enemigo. La IA permite analizar grandes conjuntos de datos, o extraer conclusiones a partir de datos poco precisos y a una velocidad imposible de igualar por un operador humano.
- **Visión por ordenador**: consiste en el análisis y extracción de datos visuales de imágenes y vídeos para detección, seguimiento y reconocimiento de objetos, reconocimiento facial, comprensión de escenas, o elaboración automática de mapas, que luego podrán integrarse en sistemas autónomos, plataformas o robots con el fin de incrementar su funcionalidad.
- **Interfaces hombre-máquina (HMI)**: permiten a los humanos interactuar eficazmente con los sistemas de IA; pueden reducir la carga cognitiva y mejorar el conocimiento de la situación y la toma de decisiones en entornos de alto estrés. Entre estas técnicas está el procesamiento de lenguaje natural (PLN) y los grandes modelos de lenguaje (LLM) empleados para analizar y comprender el lenguaje humano, lo que facilita la interacción conversacional fluida de los operadores con los sistemas de armas.
- **Sistemas autónomos**: corresponden a cualquier tipo de vehículo no tripulado, terrestre, aéreo o marítimo (de superficie o submarino) que pueda funcionar de forma independiente pilotados remotamente o sin intervención humana. Suelen estar diseñados para realizar tareas de vigilancia, reconocimiento y combate complementando o sustituyendo a los seres humanos o mediante su integración junto a sistemas tripulados. En el caso

de incorporar armas y que el mismo sistema pueda controlar su uso, toman la denominación de **sistemas letales autónomos** o **sistemas de armas letales autónomas (SALA)**.

- **Inteligencia de enjambres**²⁵⁶: son algoritmos de IA que coordinan el comportamiento de múltiples sistemas autónomos homogéneos (terrestres, aéreos o marítimos) o heterogéneos para lograr un objetivo común. Esta subdisciplina dentro de la IA se creó sobre la base de las leyes que rigen el comportamiento de insectos sociales, bancos de peces o bandadas de aves y está vinculada al comportamiento de inteligencia grupal y a la forma en que el comportamiento de cada miembro individual contribuye al conjunto.
- **Mando y control (C2)**: apoyado por la analítica y la gestión de datos para procesar grandes volúmenes de información histórica o capturada en tiempo real, y su presentación, especialmente visual, al operador humano facilitando la toma de decisiones.
- **IA en el borde (edge AI)**: la IA en el borde implica el uso de algoritmos de IA para procesar datos en tiempo real en dispositivos situados en el borde de la red, como sensores o dispositivos de usuario, y su interacción o transmisión a otros dispositivos, lo que reduce la latencia y mejora la toma de decisiones en aplicaciones como los sistemas autónomos o la guerra cibernética.

Seguidamente, se analiza este último aspecto (*edge AI*) que, con el desarrollo de la microelectrónica y el **abaratamiento de los dispositivos y sensores**, ha adquirido una creciente importancia.

5.3.2 IA en la frontera y el continuo “borde-niebla-nube” (*edge-fog-cloud*)

La **computación en la frontera o en el borde de la red** (*edge computing*) tiene como objetivo **procesar los datos generados por los sensores cerca de estos, en nodos periféricos** de la red de comunicaciones que se denominan **pasarelas**. Este enfoque supone una evolución y mejora respecto al modelo convencional en el que los sensores recogen datos y los envían a la nube para su procesamiento posterior (“*sensors-to-cloud*”), lo que implica tiempos de latencia mayores, y consumo de recursos de la red, que pueden ser limitados en situación de conflicto.

La idea de **la computación en el borde es trasladar funciones de procesamiento de datos** (por ejemplo, la identificación de objetos móviles) **a nodos periféricos de la red**, cercanos o situados en los mismos sensores (por ejemplo, cámaras); con ello, **el tiempo de respuesta del sistema y la ocupación de la red mejora sustancialmente**.

²⁵⁶ Se tratará en detalle en una sección posterior del presente capítulo.

Sin embargo, estos nodos periféricos, aun soportando algunas funciones de procesamiento de datos, **no disponen de todos los recursos de cómputo o almacenamiento ni tampoco comunicaciones suficientes** para abordar todas las funciones necesarias del sistema, por lo que persiste la necesidad de su interacción con otros nodos más centralizados que sí los posean. Es en este contexto en el que aparece la idea de **continuo *edge-fog-cloud* en la operación de los sistemas de armas letales autónomas (SALA)**, en la que las capacidades de **cómputo, almacenamiento y comunicación están dispersas** en la red, con nodos situados en cada uno de los tres niveles, capaces de resolver funciones a cierta escala.

Así, un sistema de identificación de objetos móviles para defensa activa y vigilancia aérea (Rojas *et al.*, 2023) puede **recoger información visual de cámaras, realizar un primer análisis para detectar objetos móviles de interés en el nodo en el borde, con un tiempo de respuesta corto** (Abbasov, 2023), enviar imágenes seleccionadas para identificación de trayectoria a un nodo intermedio y almacenar las imágenes relevantes para su análisis detallado posterior en la nube.

La **reducción de latencia** que ofrece el **continuo *edge-fog-cloud*** es clave en entornos tácticos para sistemas de defensa, vigilancia y combate autónomo (Pióro, 2024) ya que mejora la comunicación y la eficiencia operativa en aplicaciones críticas como detección de amenazas, navegación autónoma de drones o defensa activa. Estudios recientes destacan también su papel en la mejora de la seguridad cibernética, la automatización de sistemas de defensa y la toma de decisiones descentralizada. Algunos países están implementando soluciones de IA en el borde para fortalecer sus estrategias de defensa, y, en breves plazos, se expandirá a todos los ejércitos avanzados.

Desde el punto de vista técnico, el **continuo *edge-fog-cloud*** es un modelo arquitectónico con datos y servicios en niveles de infraestructura de red distribuida, que extiende el modelo de computación en el borde. El **edge (borde) procesa los datos cerca del punto en el que se generan** por sensores, dispositivos de Internet de las Cosas (IoT), etc., buscando minimizar la latencia y reducir el ancho de banda de red consumido (Berkol y Demirtaş, 2023). Típicamente, los **procesadores en el borde (edge) son microcontroladores con capacidades de cómputo reducidas**, operando en entornos críticos u hostiles, con funcionalidades restringidas, y con el menor consumo energético posible.

En relación con su uso para **IA en el borde**, se pretende que sean capaces de **realizar inferencias, ejecutando modelos de IA reducidos**, aunque esa alternativa puede restarles precisión. Se trata de un campo de trabajo muy activo en el que diversas empresas de defensa han comenzado a ofrecer productos para aplicaciones que requieren sistemas de IA robustos, compactos y energéticamente eficientes, capaces de ejecutar modelos de inferencia avanzados en condiciones extremas²⁵⁷. Su uso será creciente en los próximos años.

257 <https://www.washingtontechnology.com/sponsors/sponsor-content/2025/04/future-defense-ai-edge-real-time-tactical-advantage/404000/>

El **nivel de niebla (fog)** está compuesto por **nodos intermedios** como encaminadores (*routers*) o servidores locales, dando servicio en un dominio táctico en el que puede haber centenares o miles de sensores con decenas de dispositivos en el borde. El nivel de **niebla** soporta modelos más complejos que el nivel de **borde**, con dispositivos provistos de mayores capacidades de computación, pero manteniendo unos niveles aceptables de latencia para una aplicación determinada. Para aplicaciones de IA, el **nivel de niebla** puede **ejecutar modelos entrenados con la agregación de la información de todos los sensores en su dominio**, o soportar el desbordamiento de las inferencias que los nodos inferiores -con menos capacidades- no han podido realizar en situaciones de alta carga de datos (ráfagas de eventos, por ejemplo).

El **nivel de la nube (cloud)** incorpora las funciones de **almacenamiento y procesamiento centralizado** y se suelen realizar en un gran centro de datos. Dispone de recursos potencialmente ilimitados, pero, por el contrario, tiene una mayor latencia y dependencia de la red, además de soportar la carga desbordada de todos los servidores de niveles inferiores. Se suele reservar como último recurso para aplicaciones IA, y para el entrenamiento de los modelos con conjuntos de datos históricos. Además de dar soporte distribuido a las aplicaciones basadas en IA, el continuo **edge-fog-cloud** utiliza internamente algoritmos de IA como aprendizaje profundo o por refuerzo para la asignación dinámica de recursos y optimización del rendimiento del propio sistema (Khalyeyev *et al.*, 2023).

Resulta imposible pensar en la aplicación de la IA en la frontera o sobre el continuo, sin el desarrollo de la **Internet de las Cosas Militares (IoMT)**, cuyo objetivo es proporcionar capacidades avanzadas de **captura y transmisión de datos a través de redes tácticas** para su recopilación y tratamiento por la IA. Las redes IoMT conectan una gran variedad de dispositivos y sensores en entornos militares, como drones, vehículos autónomos, redes de sensores de batalla y sistemas de vigilancia (Liu *et al.*, 2022). Algunas experiencias reportadas en la literatura científico-técnica en la que se aplica la IA en el contexto de IoMT son:

- El desarrollo de una solución basada en **cifrado ABE²⁵⁸ y cadenas de bloques (blockchain)** para proteger la transmisión de datos en redes militares IoT federadas, que permite compartir información de manera segura entre diferentes unidades militares y aliados sin comprometer la seguridad.
- La **optimización de la distribución de tareas** en redes de drones, mejorando la eficiencia en misiones de vigilancia y patrullaje autónomo (Wu *et al.*, 2024).
- La creación de **modelos de redundancia y recuperación de fallos** en IoMT para garantizar la comunicación continua entre unidades en el campo de batalla (Zieliński *et al.*, 2021).

²⁵⁸ Se trata de un tipo de cifrado asimétrico denominado criptografía basada en atributos. <https://egidacybersecurity.com/asegurando-la-confidencialidad-mediante-atributos-y-politicas-de-acceso-con-criptografia-cp-abe/>

- La propuesta de sistemas basados en **bibliotecas ligeras de IA (como TinyML) para la detección de ataques** y anomalías y respuesta rápida ante intentos de intrusión o sabotaje en redes de sensores militares en tiempo real (Saranya *et al.*, 2024).
- La fusión de datos de **cámaras y sensores AIS para mejorar la seguridad y autonomía de vehículos marítimos militares**.

Cuando las aplicaciones que se van a ejecutar sobre el borde o el continuo *edge-fog-cloud* están basadas en IA, se habla de **IA en el borde (edge IA)**, que es el enfoque basado en la ejecución de aplicaciones basadas en IA sobre una infraestructura *edge* o *edge-fog-cloud* (Srirama, 2024). Se trata de una infraestructura compleja, por lo que es necesario considerar varios aspectos tecnológicos para garantizar el rendimiento, la seguridad y la eficiencia en entornos exigentes, como son los tácticos:

- **Respecto al hardware:** los **dispositivos para las inferencias** (GPUs, TPUs o NPUs) se comunican con sensores avanzados como cámaras térmicas, radares, LIDAR, etc. y deben poder funcionar en entornos sin acceso continuo a fuentes de energía por lo que el consumo debe ser el menor posible.
- **Respecto a la red:** deben implantarse esquemas de **autenticación y control de acceso y arquitecturas Zero Trust (ZTA)** para garantizar interacciones seguras (Dhanapala, 2024), lo que puede incluir procesadores auxiliares para cifrado (Ayed *et al.*, 2022). Deben tener la capacidad de funcionar desconectados, en **entornos hostiles con contramedidas de guerra electrónica** (Kallenborn, 2022), con redes intermitentes (radio, 5G militar), y minimizar la dependencia de enlaces satelitales (Shwe y Aritsugi, 2024). Esta es una característica fundamental en operaciones de combate y zonas de conflicto (Masip-Bruin *et al.*, 2021). También implementan esquemas descentralizados de red como **las redes mesh para comunicación entre dispositivos** sin una infraestructura centralizada (Hildmann *et al.*, 2019).
- **Respecto a los modelos y algoritmos de IA:** deben permitir el **procesamiento local inmediato sin necesidad de conexión** a servidores centrales. Los modelos han de ser **resistentes a ataques de adversarios**, como los intentos de manipulación de datos de entrada²⁵⁹. Los modelos deben ser livianos, lo que se logra mediante el uso de técnicas como **cuantización, poda y destilación de conocimiento** que consiguen ejecutar modelos en hardware con recursos limitados (Park *et al.*, 2024). Otra característica deseable es el **autoaprendizaje y adaptación**: la implementación de IA debe poderse ajustar a condiciones operacionales cambiantes sin necesidad de reentrenamiento en la nube. En este aspecto las técnicas de **aprendizaje por refuerzo** muestran resultados prometedores en

²⁵⁹ Como ejemplo, el sistema EdgeShield (Xia *et al.*, 2024) permite detectar ataques de adversarios en los sistemas de IA, lo que es crucial para mantener la integridad operativa.

el laboratorio, pero son más **difíciles de implementar con éxito en casos reales** (Vergara *et al.*, 2023). Por supuesto, los **resultados deben de ser explicables** para garantizar transparencia y trazabilidad en las decisiones tomadas por la IA.

La aplicación de la IA sobre el *continuo edge-fog-cloud* que soporta el sistema “*Fuerzas en entornos virtuales*” ha demostrado una importante mejora en cuanto a precisión y eficiencia -aunque la mayor parte de los resultados se han obtenido en simulaciones y es necesario continuar el proceso de experimentación en entorno real (Mendi, 2023).

Con todo, el enfoque *continuo edge-fog-cloud* sigue siendo un fértil campo de investigación en el que se espera que los próximos años se consiga la **integración total del continuo mediante redes 6G e IA distribuida**, con colaboración entre dispositivos con **latencias por debajo del milisegundo y tasas de datos superiores a 1 Tbps**; implementado sobre dispositivos de bajo consumo y ofreciendo **seguridad robusta post-cuántica** para los datos críticos. Se trata de un proceso de innovación tecnológica progresivo que también implica la adaptación de las estrategias y tácticas en la conducción de operaciones militares.

5.3.3 Robots de combate terrestres y marítimos

Los robots de **combate terrestres y marítimos** se usan para operar en entornos peligrosos para los humanos; un ejemplo típico en el que se usan robot operados a distancia desde hace años es para llevar a cabo operaciones de *desminado*. Sin embargo, en los últimos años, el uso de la IA ha mejorado las capacidades autónomas de estos dispositivos hasta alcanzar en algunos casos la **toma de decisión autónoma inteligente**. Entre los desarrollos técnicos más recientes se pueden mencionar:

- **La detección y reconocimiento automático de objetivos (ATR)** mediante visión por ordenador y **redes neuronales convolucionales y YOLO²⁶⁰**, como el Proyecto *Convergence* del Ejército de EE.UU. en el que se identifican y marcan carros de combate enemigos de forma autónoma, permitiendo reducir el tiempo de respuesta en combate (Freedberg, 2020).
- **La conducción/navegación autónoma**: el software **OverDrive** de *Overland AI* permite el **movimiento autónomo de vehículos terrestres a altas velocidades** en terrenos irregulares sin intervención humana, utilizando el **aprendizaje por refuerzo profundo y la fusión de sensores** (Manuel, 2024). También, el buque *Sea Hunter* demostró ser capaz de navegar de forma autónoma en el océano, evitando colisiones y siguiendo **rutas conformes a las regulaciones internacionales** de tráfico marítimo, para lo que aplica **redes neuronales recurrentes** (C4ISRNET/AP, 2019).

²⁶⁰ YOLO significa (You Only Look Once). Se trata de un modelo de detección de objetos y segmentación de imágenes.

En la literatura podemos encontrar información sobre algunos desarrollos y casos de uso de robots de combate terrestres y marítimos (los aéreos se comentan en la sección sobre drones). Así, el Ejército de Estados Unidos ha probado vehículos autónomos terrestres en ejercicios de combate que han logrado **avanzar, flanquear obstáculos y atacar blancos con aprobación humana basados en aprendizaje por refuerzo profundo**. La Marina de Estados Unidos ha desarrollado buques no tripulados, como el *Sea Hunter* mencionado previamente, y el *Nomad*, con capacidad para patrullaje autónomo y guerra antisubmarina, en **misiones prolongadas, sin necesidad de tripulación** basados en redes neuronales recurrentes. También se han empezado a emplear para la identificación y evacuación de heridos en el campo de batalla.

Por su parte, Israel ya ha desplegado desde hace años el *Jaguar*, un vehículo terrestre semiautónomo que patrulla la frontera de Gaza, capaz de evitar obstáculos y equipado con sensores avanzados y redes neuronales profundas (Saballa, 2021).

Pero ha sido la guerra de Ucrania la que ha acelerado los desarrollos y puesta en funcionamiento de vehículos autónomos terrestres y navales en entornos de combate real. Rusia ha desplegado vehículos terrestres con capacidad de combate autónomo y teleoperación, pero las **limitaciones en comunicaciones y navegación han complicado su funcionamiento en combate**, lo que ha obligado a usar técnicas de ajuste fino sobre redes neuronales profundas²⁶¹. También Rusia ha comenzado a desplegar **botes no tripulados de vigilancia** en sus bases en Crimea, todavía sin uso significativo en combate (Gosselin-Malo, 2025), con modelos entrenados con **aprendizaje supervisado para detección de objetos en radares y sonar**.

Ucrania, por su parte, cuenta con el **robot autónomo *TheMIS*** para transporte logístico y **evacuación de heridos** (que planifican sus rutas mediante aprendizaje por refuerzo), y ha probado drones terrestres armados en ataques directos, destacando en operaciones en Járkov donde se usaron en combinación con drones aéreos (Kirichenko, 2025). También ha usado **lanchas no tripuladas con cargas explosivas** como el Magura V5, para atacar buques rusos en el Mar Negro, logrando **hundir el patrullero Sergey Kotov** en marzo de 2024 (C4ISR-NET/AP, 2024); sus sistemas de guiado están basados en redes neuronales convolucionales.

Entre las aplicaciones más comunes de los sistemas autónomos se encuentran:

- **Ciberdefensa autónoma:** el sistema *Autonomous Intelligent Cyber Defense Agents* (AICA) protege infraestructuras militares en entornos de guerra cibernética (Théron *et al.*, 2020).

²⁶¹ Los problemas derivados de opera en un entorno radioeléctrico muy degradado ha impulsado el que algunos de estos sistemas terrestres no tripulados estén conectados con el operador en base a cables de fibra óptica que, si bien son inmunes a estas interferencias también limitan su movimiento.

- **Guerra electrónica:** se pueden usar los **enjambres para interrumpir comunicaciones enemigas y desactivar sistemas de radar**. Un ejemplo son los drones con capacidades de interferencia, utilizados en conflictos recientes en el Medio Oriente.
- **Contramedidas y seguridad:** los sistemas de defensa **anti-enjambres** incluyen **interferencia de señales, drones interceptores**, redes de defensa automatizadas, pulsos de radiofrecuencia de alta potencia y guerra cibernética (Weinberg, 2022). No suponen una novedad; en el ataque a una base rusa en Siria en 2018, 13 drones en enjambre fueron neutralizados con sistemas de guerra electrónica (Hambling, 2018). Diariamente se reciben noticias de drones en Ucrania que son interceptados y destruidos por las contramedidas ucranianas y rusas.
- **Defensa perimetral automatizada:** sistemas como las torretas centinela, desplegadas en zonas fronterizas, detectan y responden a intrusiones sin intervención humana, **utilizando IA para diferenciar entre amenazas y no amenazas** (FUHEM, 2025). También en este caso, el uso se inició hace años.
- **Inteligencia, vigilancia y reconocimiento (ISR):** los drones, aislados o en grupo, se han usado en **misiones de vigilancia en zonas de combate para reducir la exposición de las tropas humanas** (Joshi *et al.*, 2024). Un ejemplo que tiene ya algunos años son los drones lanzados desde submarinos para ISR en zonas costeras por la Marina de Estados Unidos (White, 2017).
- **Drones autónomos para combate:** el uso de drones autónomos para **identificar y atacar objetivos en entornos urbanos complejos** reduce el riesgo para las tropas y mejora la precisión. Para ello, deben estar preparados para **atacar en entornos dinámicos e impredecibles**, adaptándose a cambios en tiempo real en su entorno lo que implica mayor inteligencia y capacidad de procesamiento a bordo para obtener una mejor conciencia situacional (Fossaceca, 2023).

5.3.4 Uso de la IA generativa en aplicaciones de defensa

La explosión de la **IA generativa** en los últimos tres años, con multitud de aplicaciones para usuarios finales, también ha llegado a las Fuerzas Armadas de muchos países, aunque con **restricciones y cautelas en su uso**.

La adopción de aplicaciones basadas en LLM está ligada a la **validez y utilidad de las respuestas que ofrecen a las preguntas realizadas (prompts)** por los usuarios en sistemas tipo “*chatGPT*”. La credibilidad de estas respuestas, a su vez, depende de los datos utilizados en el entrenamiento de los modelos que pueden generar respuestas incorrectas (“*alucinaciones*”).

La cuestión básica para aceptar su uso en el entorno militar es **determinar si se puede confiar en sistemas de IA generativa en los que el entrenamiento depende del uso de**

datos (muchos de ellos clasificados) que no se pueden verificar externamente. Más concretamente, algunos de los riesgos potenciales derivados del uso militar de los LLM son (Lavadia, 2025):

- La interacción con LLM en base a preguntas puede **exponer información clasificada**, amenazando la seguridad nacional. Los sistemas militares que incorporan LLM deben implementar sofisticados protocolos de ciberseguridad para identificar y contrarrestar los ataques de inyección rápida de manera efectiva.
- Los LLM entrenados con información confidencial o clasificada plantean el riesgo de **revelar datos protegidos** y acceder a estrategias militares sensibles, planes operativos o avances tecnológicos. Por este motivo, los datos militares utilizados para el entrenamiento o el funcionamiento de LLMs deben permanecer en entornos de nube seguros y cifrados para protegerlos contra el acceso no autorizado.
- Los LLM pueden **generar resultados sesgados o incorrectos** derivados de confiar en conjuntos de datos extensos y sin refinar que conducen a decisiones estratégicas erróneas, o asignación incorrecta de recursos con consecuencias no deseadas. Por ello, los LLM deben entrenarse con conjuntos de datos de alta calidad cuidadosamente seleccionados. Precisamente son estos datos de los que menos se dispone en la actualidad y los más difíciles de generalizar a distintos tipos de conflictos.
- La naturaleza de los LLM complica la **explicación de las decisiones tomadas**. Identificar el origen del error puede ser un desafío, porque puede provenir del LLM, de sus datos de entrenamiento o de la supervisión humana.
- El **uso de programas que transforman las salidas de LLM** en información de entrada para otros sistemas de software, como las plataformas de mando y control (C2) crean vulnerabilidades adicionales al propagar y amplificar los errores.

Como resultado de estos riesgos potenciales, los ejércitos de Estados Unidos y de las principales potencias militares han puesto en marcha **procesos internos de experimentación y validación** de las técnicas de IA Generativa antes de su adopción generalizada.

El *Departamento de Defensa* de Estados Unidos (DoD) creó en agosto de 2023 un grupo de trabajo especial denominado “*Task Force Lima*” para **analizar y evaluar el uso de la IA generativa en temas de seguridad nacional**, así como para recomendar su uso responsable y proveer de implementaciones seguras a todas las unidades del DoD. El objetivo es analizar hasta qué punto los potenciales adversarios pueden acceder y emplear esa tecnología y tratar de interrumpir el uso propio de las soluciones basadas en IA. Dicho de otra manera, **evaluar los riesgos asociados al uso de la IA generativa en las fuerzas armadas**.

En 2024 el DoD seleccionó a la empresa “**Scale AI**”, especializada en prueba y evaluación de LLM, para probar y evaluar la IA generativa en aplicaciones militares. El objetivo del contrato firmado con *Scale AI* es “*desarrollar un marco para implementar la IA de forma segura midiendo el rendimiento de los modelos, ofreciendo información en tiempo real a los combatientes y creando conjuntos de evaluación especializados del sector público para probar modelos de IA para aplicaciones de apoyo militar, como la organización de los resultados de los informes posteriores a la acción*”.

Scale AI ha desarrollado un LLM específico para aplicaciones militares denominado **Defense Llama**²⁶² construido sobre un LLM abierto, *Llama 3* de Meta. Se utilizaron técnicas de ajuste de datos para configurar los parámetros de *Defense Llama* y poder responder a preguntas y escenarios relacionados con la defensa.

Recientemente el DoD ha lanzado una plataforma de IA generativa “**Army Enterprise Large Language Model Workspace**”²⁶³, que muestra cómo el Ejército está aprovechando la IA para agilizar la comunicación, mejorar la eficiencia operativa e impulsar la innovación. Se aplica desde la redacción de comunicados de prensa hasta la reclasificación de las descripciones del personal, y otros servicios. La plataforma actúa como una herramienta transformadora tanto para los combatientes como para los procesos administrativos.

Un paso más en la dirección de adopción real de la IA es el lanzamiento en 2025 del programa “**Thunderforge**”²⁶⁴ de la Unidad de Innovación en Defensa (DIU) del DoD cuyo objetivo es integrar la IA en la planificación operativa militar a nivel de teatro de operaciones, y fusionar herramientas de modelado y simulación de última generación junto a agentes inteligentes de IA. Los usos previstos de los **agentes de IA** incluirán modelado y simulación, apoyo a la toma de decisiones, propuestas de acción e incluso flujos de trabajo automatizados. El objetivo final de **Thunderforge** es ofrecer un **ecosistema de planificación unificado en el que los agentes de IA simulan juegos de guerra y planifican escenarios y perfeccionan los cursos de acción propuestos**.

Su puesta en marcha se hace colaborando con empresas privadas como *Anduril*, *Microsoft*, *ScaleAI* y otras con el apoyo de la DIU para acelerar los procesos de desarrollo (Field, 2025). El sistema aprovechará las aplicaciones de agentes de IA de *Scale AI* y la experiencia en pruebas y evaluaciones de IA generativa. **Thunderforge** también incluirá la plataforma de software **Lattice** de *Anduril* y LLM de última generación proporcionado por *Microsoft*²⁶⁵ (Tucker y Hlad, 2025).

262 <https://scale.com/blog/defense-llama>

263 https://www.army.mil/article/285537/army_launches_army_enterprise_llm_workspace_the_revolutionary_ai_platform_that_wrote_this_article

264 <https://www.diu.mil/latest/dius-thunderforge-project-to-integrate-commercial-ai-powered-decision-making>

265 https://www.escudodigital.com/defensa/desarrollo-defensa/thunderforge-revolucion-ia-en-toma-decisiones-militares-pentagono_62950_102.html

Todos estos esfuerzos anuncian, si los resultados de estos proyectos son los previstos, una **aceleración en el uso de sistemas basados en agentes de IA apoyados por técnicas de IA generativa** en diversos ámbitos de planificación y toma de decisiones como complemento al decisor humano.

5.3.5 Visión multidominio

Las consecuencias derivadas de la **explosión en el desarrollo y despliegue de sensores terrestres aéreos o marítimos**, fijos o móviles, de bajo coste que captan **información detallada del terreno** combinado con su **procesamiento automatizado en tiempo real** para alimentar la toma de decisiones, y su interacción con sistemas robotizados, está acelerando un proceso de **cambio disruptivo en el campo de batalla**.

La conjunción de estos elementos conduce paulatinamente a la existencia de un **campo de batalla** que puede denominarse **“transparente”** en el que la ocultación de movimientos de tropas o equipos militares a media o gran escala durante tiempos prolongados no es posible²⁶⁶. La “transparencia” en el campo de batalla se refiere a la capacidad de un adversario de obtener información detallada y casi en tiempo real sobre las actividades y movimientos del enemigo combinando información de comunicaciones, de inteligencia y de capacidades de vigilancia (Frías, 2024; Pérez-Martínez, 2024).

La consecuencia operativa es la necesidad de **incrementar la movilidad de los sistemas de ataque o defensa** para que su posición se modifique a la mayor velocidad posible, antes de que sea detectada y pueda ser atacada por el adversario. Este condicionante obliga a cambios sustanciales en la logística empleada, y afecta a las tácticas de despliegue de las unidades militares en el frente.

En el caso de la guerra de Ucrania la “transparencia” conseguida en el terreno por un **despliegue masivo de múltiples drones y uso de satélites de observación de baja cota** permite la identificación rápida de objetivos en las líneas del frente, y planificar su ataque en ciclos de observación-decisión-acción muy rápidos. El resultado es un campo de batalla en el que (casi) todo lo que se encuentre presente, será detectado y localizado en breve tiempo, al menos, en áreas cercanas a la zona de contacto entre los dos bandos. Como consecuencia, las tácticas de combate empleadas han evolucionado en poco tiempo como respuesta a la necesidad de **incrementar la movilidad con unidades ligeras y autosuficientes** (Frías, 2024).

Un ejemplo de ello es que el **ciclo de posicionamiento, montaje, disparo y desmontaje de un sistema de misiles** para el ataque a un objetivo desde una posición determinada esté en el orden de los **minutos**; permanecer más tiempo en la misma posición física pondría

²⁶⁶ Utilizaremos este término de manera cualitativa y no ligado a una métrica cuantitativa de transparencia. Es obvio que no se consigue una transparencia total en todo momento y lugar, pero ese es el objetivo deseado.

en peligro el sistema y sus operadores ante un ataque del adversario que tendría tiempo para identificarlo y atacarlo. Posiblemente, esta tendencia se acentúe en el futuro con un ciclo en el que **la tendencia es que todas las operaciones en el terreno sucedan “en movimiento”** a velocidades crecientes.

De nuevo, en base a la experiencia de uso obtenida de conflictos militares actuales como son los casos de Ucrania, Oriente Medio o Sahel, aunque muy distintos entre ellos, se pueden identificar algunas **tendencias en el uso de la IA**. Brevemente, las tendencias identificadas por el GT son las siguientes:

- Uso creciente de la IA en la **identificación y selección automática de objetivos** en base a la integración y análisis de datos históricos y otros obtenidos en tiempo real de múltiples sensores.
- Introducción de **algoritmos de IA en las plataformas de ayuda a la decisión** tanto a nivel personal (en forma de asistente automatizado) como en el de sistemas de mando y control a diferentes niveles organizativos (pelotón, compañía, división, cuerpo de ejército).
- Utilización de **sistemas de armas autónomas o semiautónomas letales** aisladas o en enjambre con diferente grado de inteligencia.
- Sistemas inteligentes de **guerra electrónica**.

El otro elemento destacable que se suma al de **transparencia** anteriormente citado y, de hecho, lo posibilita es el de **“integración multidominio”**. En este caso se trata de combinar la información y la acción de sistemas propios de los dominios aéreos, espaciales, terrestres, marítimos, cibernéticos y cognitivos para mejorar la comprensión de lo que sucede en el campo de batalla y poder tomar decisiones. En la figura 5.2 puede verse la relación entre los dominios citados en los que la integración de tecnologías maduras y duales ha acelerado el proceso.

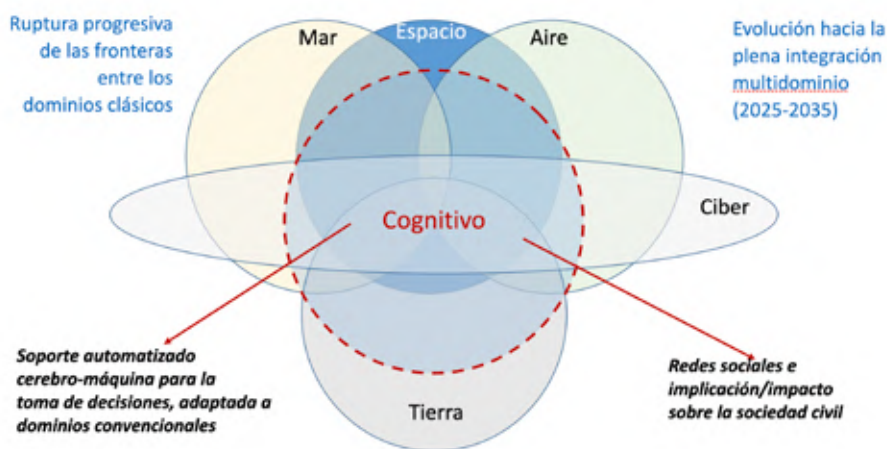


Figura 5.2. Visión multidominio de las operaciones militares.
Fuente: elaboración propia

Conceptualmente, la información a considerar por un sistema de decisión como ocurre en los sistemas de mando y control multidominio es muy voluminosa y cambia rápidamente con el despliegue de multitud de sensores. Por este motivo, es muy **difícil que el proceso de interpretación de los datos pueda ser llevado a cabo exclusivamente por operadores humanos en los sistemas de mando y control integrados** en el tiempo requerido para la toma de decisión.

El uso de la IA se ha convertido, por tanto, en una **tecnología ineludible de carácter horizontal** en este contexto, aunque ello implique determinar el nivel en el que se requiera mantener al operador humano en el bucle de decisión para preservar el control sobre decisiones que pueden implicar vidas humanas.

En todo caso, la funcionalidad y eficacia de un sistema de mando y control integrado e inteligente no puede ser analizado tácticamente de forma independiente en base al análisis de datos, sino que debe ser considerado como una **parte integrante del resto de los elementos de combate** (considerando de forma simultánea la potencia ofensiva, la capacidad defensiva y la movilidad) para que la toma de decisión tenga los efectos deseados; es decir, **acompañar la decisión con los medios para hacerla efectiva**.

El **proceso de toma de decisiones** ha evolucionado debido a la alta velocidad a la que se producen las amenazas y la dificultad para detectarlas²⁶⁷, lo que, a su vez, ha reducido al mínimo el tiempo disponible para reaccionar. Para solucionar esta debilidad se ha adoptado un proceso de delegación de funciones en hombres y equipos, reservándose el comandante el *control por veto*; de este modo, se distingue entre varios **niveles en el proceso de toma de decisiones**²⁶⁸ (Escobar, 2020) cuya implementación evoluciona con la disponibilidad de nuevas tecnologías.

Seguidamente, se analizarán las oportunidades y requisitos del uso de la IA en los **sistemas de mando y control (C2)**, en la denominada **nube de combate** y en la **guerra electrónica**. Los tres elementos se han convertido en áreas críticas para asegurar la superioridad militar.

5.3.6 Uso de la IA en los sistemas de mando y control

En el caso de los sistemas de mando y control la **macrotendencia tecnológica** clara es la **integración de la IA en los sistemas C2** aplicada al análisis de altos volúmenes de información y como soporte a los procesos de toma de decisión. Concretamente, **el objetivo**

267 Piénsese en el efecto que pueden tener los misiles hipersónicos en los sistemas de mando y control para su detección y la dificultad para tomar la decisión de su neutralización.

268 **Reacción automática.** Un equipo C2 detecta la amenaza, la evalúa e inicia automáticamente las medidas defensivas, activando diversos sistemas. **Respuesta pre-planificada.** Procedimiento tabulado que permite iniciar reacciones ante amenazas específicas. **Control por negación.** El comandante, delega funciones en diferentes niveles de su organización —para que éstos dispongan el empleo de los sistemas de armas de acuerdo con las doctrinas vigentes en sus respectivas áreas de responsabilidad— reservándose el derecho a veto.

deseado es que los sistemas C2 sean capaces de capturar, procesar y analizar datos de manera autónoma hasta el máximo nivel posible, acelerando la toma de decisiones y la predicción de comportamientos de los adversarios por parte del personal que opera el sistema.

Un nuevo concepto destacable en este sentido es la estrategia conocida como **JADC2** (*Joint All-Domain Command and Control*)²⁶⁹ propuesta por Estados Unidos en 2022 que refleja la necesidad de **asegurar la interoperabilidad entre todos los dominios** incorporando las nuevas tecnologías aplicables como la IA, redes de sensores, comunicaciones avanzadas o gestión dinámica de información de datos de combate. Se trata de un esfuerzo a largo plazo que ya está conduciendo a planteamientos similares en todos los países de la OTAN.

Este requisito implica disponer de una **arquitectura de referencia** sobre la que se puedan integrar diversos subsistemas de diferentes proveedores asegurando su interoperabilidad. En la figura 5.3 se presenta un **esquema conceptual de alto nivel de JADC2** cuya implementación se llevará a cabo durante varios años.

Más específicamente, la relevancia de **la IA en sistemas C2 se concreta en proporcionar las siguientes funcionalidades:**

- Análisis de datos en tiempo real.
- Automatización de la respuesta ante amenazas.
- Reconocimiento de objetivos y vigilancia avanzada: relacionado con la “computación en el borde”.
- Simulación y entrenamiento de operaciones.
- Mantenimiento predictivo y gestión logística.
- Apoyo en la toma de decisiones estratégica.
- Ciberseguridad y defensa contra amenazas digitales: relacionado con la “Seguridad integrada en C2 centrada en datos” (C2-2).
- Autonomía avanzada y sistemas de decisión colaborativa.
- Uso de IA en simulaciones hiperrealistas para entrenamiento: combinando IA, realidad virtual (VR), y realidad aumentada (AR).
- Drones autónomos y enjambres de drones inteligentes.
- Uso de IA en la logística avanzada y el mantenimiento predictivo: la tecnología avanzará hacia la automatización total de la logística.

269 <https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.pdf>

- Modelos de lenguaje específicos entrenados para sistemas C2 (generalmente, sobre la base de LLM genéricos confiables).
 - Obtención de datos etiquetados y relevantes que permitan entrenar a los algoritmos desarrollados.
- Procesamiento automatizado de datos geoespaciales para:
 - Detectar cambios en el terreno o movimientos del enemigo sin intervención manual.
 - Generar alertas automáticas cuando ocurren eventos en ubicaciones específicas, ayudando a la toma de decisiones inmediata.
- Interoperabilidad entre sistemas de mando y control y plataformas de defensa de distintas fuerzas armadas.

El proceso de hacer realidad el concepto de “*Combined Joint All-Domain Command and Control (CJADC2 o Combined JADC2)*” está acelerándose (Harper, 2024). En mayo de 2024 el Pentágono anunció un nuevo contrato con la empresa *Palantir* de 480 millones de dólares para emplear el **Maven Smart System (MSS)** en todos los servicios del Ejército, la Fuerza Aérea, la Fuerza Espacial, la Armada y el Cuerpo de Marines de Estados Unidos²⁷⁰.

El objetivo pretendido es conectar mejor las plataformas, los sensores y los flujos de datos de las fuerzas armadas de los Estados Unidos y socios internacionales clave para mejorar la toma de decisiones, la eficacia operativa y la eficiencia. Concretamente, se trata de obtener un **acceso ampliado a la integración de datos y herramientas de IA para mejorar la conciencia situacional del espacio de batalla**.

Un paso decisivo en este sentido es la **aplicación del MSS a la OTAN**. En abril de 2025 la *Agencia de Comunicaciones e Información de la OTAN (NCIA)* ha anunciado la adquisición del *Maven Smart System OTAN (MSS NATO)* de *Palantir* para su empleo dentro del *Comando Aliado de Operaciones (ACO)* de la OTAN, con el fin de modernizar las capacidades de combate habilitada por datos de la OTAN²⁷¹. A través de diversas aplicaciones de IA, desde grandes modelos de lenguaje (LLM) hasta aprendizaje generativo y automático. **Se pretende que con MSS NATO mejore la fusión de inteligencia y la selección de objetivos, el conocimiento y la planificación del espacio de batalla y se acelere la toma de decisiones.**

270 El Proyecto Maven se estableció en 2017 con el objetivo de ofrecer capacidades de IA al DoD. Maven proporciona la infraestructura en la nube, las capacidades de software y la IA de CJADC2.

271 <https://shape.nato.int/news-releases/nato-acquires-ai-enabled-warfighting-system->

5.3.7 Nube de combate inteligente

Poco a poco, datos y múltiples tecnologías para su captura y análisis empleando algoritmos de IA se integrarán en sistemas militares desplegados por las potencias militares formando parte de lo que se denomina **“nube de combate inteligente multidominio”**. Diversas empresas están generando productos orientados a proporcionar de forma integrada estos sistemas de decisión inteligente.

El estudio desarrollado por la Agencia Europea de Defensa (EDA) sobre la aplicación de las tecnologías de la nube en defensa en un proyecto denominado ***Claudia*** (*Cloud Intelligence for Decision Making Support and Analysis*) indica sus posibilidades y los problemas asociados. La complejidad de lo que supone su despliegue puede verse en el esquema conceptual de la figura 5.4.

Claudia ya ha demostrado en un proyecto piloto el tipo de rendimiento que se puede esperar en la aplicación del potencial de la nube a la guerra híbrida, ejemplificado en el **análisis de inteligencia de código abierto (OSINT) a través de fuentes de datos de señales cruzadas**. Esta actividad permitió recopilar información sobre las causas de las series de datos temporales obtenidos y contribuyó a mejorar la conciencia sobre la situación real del entorno.

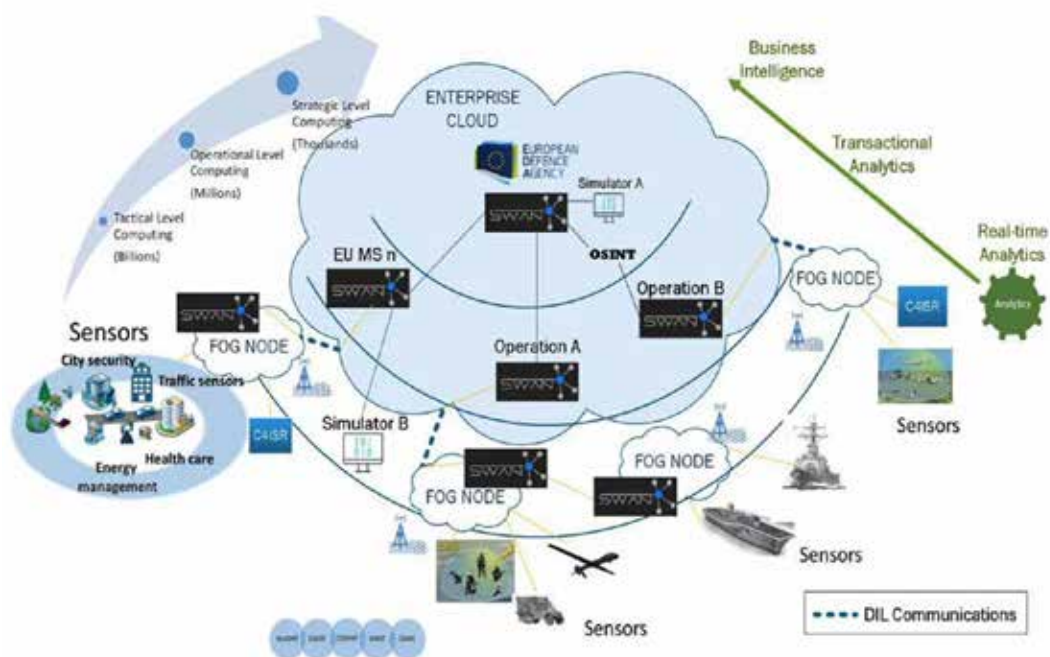


Figura 5.4 Arquitectura de una nube de combate multidominio: Fuente: EDA

Para el **Ministerio de Defensa** español²⁷² la **Nube de Combate** puede definirse como una *red de cobertura global dentro de un espacio de batalla que permite la gestión de la información y la prestación de servicios, con el fin último de tomar decisiones y ejecutar operaciones militares*. Es una solución tecnológica que **proporciona un ecosistema de servicios y un espacio de compartición de datos sustentado en un nuevo esquema de interoperabilidad**, donde se integran y procesan conjuntamente todos los datos recopilados por los sensores y sistemas conectados desde cualquier dominio.

Desde un punto de vista más técnico una **nube de combate** puede definirse como un *“Sistema de Sistemas, de carácter distribuido, donde diferentes elementos o activos de una fuerza operan integrados, proporcionando capacidades de combate colaborativo, gracias a la implantación de un modelo de hiperconectividad, computación distribuida y ecosistema de servicios de combate colaborativo y C2, a través del cual cada activo puede acceder a un espacio común de proceso de información y de prestación de servicios, que le permite disponer de la información adecuada en el momento preciso”*²⁷³.

Obviamente, no basta con disponer de soluciones tecnológicas avanzadas, aunque estén bien integradas y sean conocidas en el mundo civil; en el ámbito de la defensa es necesario **aprender de la experiencia** y saber cómo usar estas aplicaciones de forma responsable en diferentes niveles de la jerarquía de mando (desde los estados mayores a los soldados). Las experiencias acumuladas en varios países indican que **no es un proceso sencillo** dado que implica no solo el despliegue de sistemas técnicos avanzados, sino un **cambio profundo de mentalidad** basado en la confianza en sistemas inteligentes que permita su adopción real.

Las **futuras plataformas de combate** sean terrestres, navales o aeroespaciales, como nodos en el extremo táctico de la nube de combate, dispondrán de:

- Diversas aplicaciones software diseñadas para diferentes funciones operativas.
- Herramientas automatizadas de análisis, posiblemente compartidas con otros sistemas, implementadas a través de sus aplicaciones.
- Servicios informáticos comunes compartidos con otros sistemas, operando de forma transparente para los tripulantes y operadores.
- Almacenamiento virtual de grandes cantidades de datos.
- Conexión con otros usuarios, mediante una red móvil ad hoc o malla de nodos móviles tipo MANET, autoconfigurable y autorreparable, pero integrando otras capacidades avanzadas como enrutamiento dinámico inteligente y gestión de calidades de servicio extremo a extremo (*end-to-end*).

²⁷² <https://www.defensa.com/ciberespacio/nube-combate-multidominio-como-nuevo-escenario-estrategico>

²⁷³ La hiperconectividad es una característica que afecta a las comunicaciones y, por sí sola, no produce un efecto de nube, sino que debe combinarse con soluciones a otros niveles.

- La gestión de transferencia de datos por la red se realizará de forma transparente para la tripulación u operador de la plataforma, quienes verán los datos fusionados, pudiendo centrarse en aspectos exclusivamente operativos.

También **la IA se incorporará de manera general en los procesos de diseño de nuevos sistemas** con objeto de incrementar su flexibilidad y reducir los tiempos y costes de desarrollo. Tanto la generación de **datos sintéticos** que complementen la disponibilidad de datos reales difíciles de obtener, como el uso de **gemelos digitales** impulsan el uso de la IA.

Como ejemplo de esta tendencia, *Duality AI*, la compañía detrás de la **plataforma de simulación de gemelos digitales Falcon**, anunció en abril de 2025 la adjudicación de un contrato de la Oficina del Programa XM30, el equipo del Ejército de los Estados Unidos que construye la próxima generación del vehículo de combate de infantería M2 Bradley (Duality, 2025). El equipo del XM30 está desarrollando un robusto sistema de **Detección y Reconocimiento de Objetivos con IA (AiTDR)** antidrones para proteger de forma fiable al personal y a las tropas a bordo del vehículo. Para ello, aprovechará los datos sintéticos generados en la simulación de sensores virtuales en la plataforma *Falcon* para acelerar las primeras etapas del desarrollo.

5.3.8 IA en la guerra electrónica

El **dominio del espectro electromagnético** se ha convertido en un elemento clave para la conducción de los conflictos militares. Sin su control, defensa, y uso ofensivo si fuera el caso, no es posible asegurar el éxito en las operaciones militares. Por este motivo, el dominio del espectro electromagnético en una amplia banda de frecuencias, tanto para asegurar las comunicaciones propias como para impedir las del adversario, forma parte de lo que se denomina **guerra electrónica**. Estos sistemas han adquirido gran relevancia en un entorno radioeléctrico altamente disputado en el que coexisten múltiples actores con intereses divergentes como sucede en la actualidad en todos los conflictos militares²⁷⁴.

El concepto de guerra electrónica (EW) es muy amplio. Cubre desde los ataques a los sistemas de radar hasta la interferencia de los sistemas de comunicación y navegación, pasando por el enmascaramiento electrónico, el sondeo, el reconocimiento y la recopilación de inteligencia. La EW puede aplicarse en todos los dominios operativos: aéreo, terrestre, marítimo, espacial y cibernético. Las **subáreas más relevantes** de guerra electrónica son las siguientes:

274 Es interesante indicar que, si bien los recursos desde el final de la Guerra Fría se han concentrado en Occidente en reducir las amenazas en el ámbito de la ciberseguridad, en detrimento de la guerra electrónica, no ha sido ese el caso de Rusia. Esa ventaja relativa se manifestó en el Donbas (Ucrania) desde 2014.

- Guerra de Navegación satelital (NAVWAR).
- Inteligencia, vigilancia y reconocimiento (ISR/ISTAR).
- Operaciones de Inteligencia electrónica (SIGINT y COMINT).
- Operaciones de guerra electrónica (EW).
- Gestión del espectro (EMSO).
- Operaciones psicológicas.
- Operaciones con redes de ordenadores.
- Operaciones de ciberdefensa.

De un modo gráfico adaptado de un informe de RAND (Pérez-Martínez, 2024) puede describirse el ámbito de actuación de la guerra electrónica tal y como se indica en la figura 5.5. Obsérvense los diferentes solapes existentes entre las diferentes áreas.



Figura 5.5 Ámbito de actuación de la guerra electrónica. Fuente: Rand Corporation²⁷⁵

Los sistemas de EW no son elementos aislados y deberán estar coordinados con el resto de los sistemas que conforman las **Operaciones Electromagnéticas (EMO)** para un empleo eficiente y dinámico en un entorno electromagnético saturado y posiblemente denegado junto con los aspectos de ciberseguridad. De hecho, la referencia al concepto de “ciberespacio” implica su consideración como “un dominio caracterizado por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de la red, sistemas e infraestructuras físicas asociadas”.

²⁷⁵ Adaptada de <https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136055/convergence-of-cyberspaceoperations-and-electronic-warfare-effects>

La principal evolución de la Guerra Electrónica se concreta en la visión denominada **CEMA** (*Cyber and ElectroMagnetic Activities*) cuyo objetivo es la **sincronización y coordinación de las actividades de Guerra Electrónica con las de Ciberdefensa** que se ha convertido en un elemento esencial para el éxito de las futuras operaciones militares. La figura 5.6 representa la visión de Estados Unidos del concepto de CEMA.

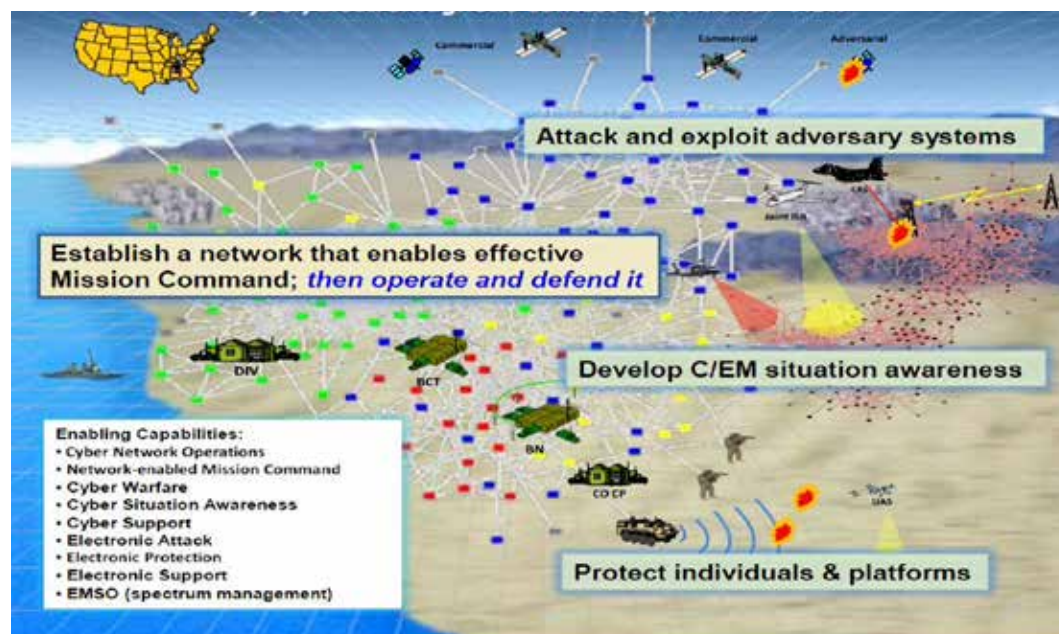


Figura 5.6 Concepto de CEMA. Fuente: <https://publicintelligence.net/us-army-cema/>

La **OTAN** también ha prestado atención a la Guerra Electrónica²⁷⁶. En el modelo de EW de la alianza, identificada como una **capacidad troncal**, se le añaden otras capacidades, conformando un todo que se denomina **“operaciones electromagnéticas”**: la gestión que permita el uso del espectro electromagnético (*spectrum management, SM*); el empleo de la capacidad de posicionamiento, navegación y sincronismo en lo que se denomina “guerra de navegación” (*navigation warfare, NAVWAR*); y la inteligencia de señales (SIGINT) (Oliva, 2024).

En este capítulo interesa analizar únicamente el **uso de la IA en la guerra electrónica** y no otras técnicas de control del espectro radioeléctrico. En una era en la que los avances tecnológicos están remodelando el panorama de la guerra, la **integración de la IA, el aprendizaje automático y los sistemas autónomos en las estrategias de defensa ya no es un concepto futurista, sino una evolución realista para mejorar las capacidades de la EW** con ventajas significativas en términos de velocidad, eficiencia y complejidad de las operaciones. El empleo de tecnologías de IA y Big Data pueden servir como base para el

276 El Comité NEWAC (NATO Electromagnetic Warfare Advisory Committee), Comité Asesor de Guerra Electromagnética de la OTAN, es el principal foro dentro de la OTAN para guerra electromagnética. https://www.nato.int/cps/en/natohq/topics_80906.htm

desarrollo de sistemas autónomos que no solo analicen señales, sino que también respondan de manera automática a las amenazas electrónicas.

La IA puede procesar grandes cantidades de datos de sensores y redes de comunicación para proporcionar conocimiento de la situación y apoyo para la toma de decisiones en tiempo real. La IA puede predecir posibles acciones enemigas en función de los datos históricos y las condiciones actuales, lo que **permite tomar medidas proactivas en la guerra electrónica**.

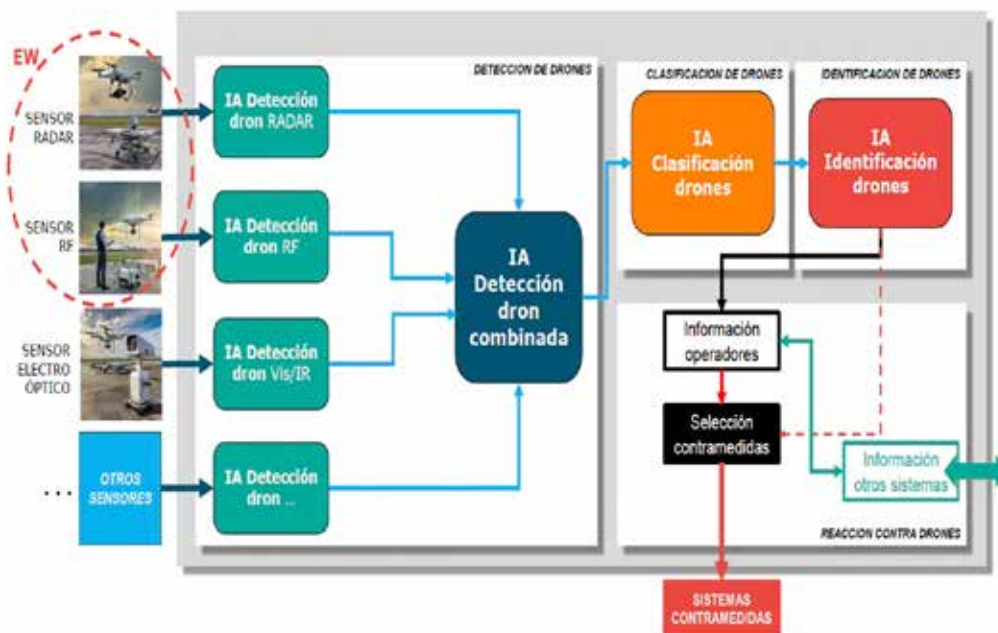


Figura 5.7 Esquema de guerra electrónica con IA en su uso contra drones.
Fuente: Inetum

La IA aplicada a la guerra electrónica e inteligencia de señal permite la identificación y clasificación de señales, implementar técnicas para ataque electrónico y sistemas inteligentes de protección de plataformas. Seguidamente, se describen tres áreas dentro de la guerra electrónica en la que está aumentando el uso de la IA:

5.3.8.1 IA en inteligencia de señal

Los sistemas de inteligencia de comunicaciones (COMINT) y de inteligencia electrónica (ELINT) recogen un creciente volumen de información procedente de comunicaciones por radiofrecuencia (RF), de emisiones electromagnéticas de radares y de otros sistemas electrónicos. Las tecnologías de Big Data se han empleado para estructurar y analizar estos flujos de datos masivos y no estructurados, mientras que **la IA aplica algoritmos de aprendizaje automático y aprendizaje profundo para detectar señales críticas y clasificarlas en función de su origen, naturaleza y relevancia operativa**.

La automatización del análisis y explotación de señales a través de IA y Big Data permite la identificación de actores enemigos, la ubicación de emisores electrónicos y la estimación de las intenciones o capacidades del adversario en tiempo real, ofreciendo una alerta temprana de amenazas potenciales o actividades hostiles.

5.3.8.2 Innovación en análisis predictivo

La IA en los Sistemas de EW deben emplearse como ayuda a los analistas y operadores en el manejo de la información que facilite a estos la toma de decisiones, llegando, en ciertos escenarios cambiantes donde la respuesta debe ser inmediata a ser capaz de tomar decisiones sobre los sistemas de EW de forma autónoma. Concretamente, **el uso de la IA combinada con el análisis de Big Data puede prever acciones hostiles basándose en patrones de comportamiento detectados previamente, permitiendo a las fuerzas armadas anticipar los movimientos del adversario.**

Un método para superar la interferencia adversaria es **STAP** (*space-time adaptive processing*) basado en IA²⁷⁷ que utiliza algoritmos de aprendizaje automático para sondear, detectar y caracterizar amenazas de forma autónoma y adaptativa y, a continuación, generar automáticamente contramedidas para nuevas amenazas indefinidas en tiempo real²⁷⁸.

5.3.8.3 IA en Operaciones Autónomas en la guerra Electrónica

La inteligencia artificial (IA) en operaciones autónomas de ciberdefensa y guerra electrónica implica la implementación de sistemas que pueden **ejecutar decisiones y contramedidas sin la intervención humana**. Estos sistemas están o estarán equipados con algoritmos avanzados de IA que aprenden de manera continua, mejorando su capacidad para identificar amenazas y responder en tiempo real.

En el dominio de la guerra electrónica, **se pretende que la IA pueda desplegar contramedidas electrónicas de manera autónoma**, ajustando las frecuencias y los métodos de interferencia en función de las señales detectadas. Esto mejora la capacidad de respuesta frente a ataques de guerra electrónica que evolucionan rápidamente, y reduce la dependencia de operadores humanos, lo que es crucial en entornos de alta demanda. Estados Unidos también está invirtiendo en un **sistema de guerra electrónica cognitiva basada en IA (AI-based CEW)**²⁷⁹. Estas tecnologías ayudan a las fuerzas armadas a interferir o falsificar el radar de un adversario de manera más efectiva.

277 <https://www.gpsworld.com/anti-jam-technology-demystifying-the-crpa/>

278 <https://www.defenseone.com/insights/cards/how-ai-changing-way-warfighters-make-decisions-and-fight-battlefield/3/>

279 <https://www.c4isrnet.com/c2-comms/2016/12/16/what-is-the-difference-between-adaptive-and-cognitive-electronic-warfare/>

La irrupción de **la IA convertirá a los sistemas de Guerra Electrónica en cognitivos y autónomos** en pocos años, adquiriendo el uso de drones un papel principal. A más largo plazo, probablemente en la próxima década, las tecnologías cuánticas en su convergencia paulatina con la IA pueden generar una nueva revolución en las operaciones de Guerra Electrónica.

5.3.9 Sistemas de armas inteligentes

5.3.9.1 Definiciones

El interés en esta sección se focaliza en el **uso de sistemas autónomos empleados como armas** que se denominan oficialmente por las Naciones Unidas **Sistemas de Armas Letales Autónomos, SALA** (*“Lethal Autonomous Weapon Systems, LAWS”*). Una definición empleada ampliamente las define como: *“sistemas de armas que utilizan inteligencia artificial (IA) para identificar, seleccionar y atacar objetivos sin intervención humana”*.

En todo caso, no existe una definición consensuada. Para el gobierno de Estados Unidos, en la directiva DODD 3000.09, se define los **SALA** como *“sistema[s] de armas que, una vez activados, pueden seleccionar y atacar objetivos sin más intervención de un operador humano”*. Este concepto de autonomía también se conoce como **“autonomía total”**.

Las **armas totalmente autónomas**, se caracterizan por la **capacidad de completar autónomamente el ciclo de enfrentamiento sin intervención del operador humano**. Ello implica disponer de la capacidad de: 1) buscar e identificar objetivos enemigos, 2) decidir atacar o no según el análisis de datos en tiempo real y sus algoritmos de reglas de enfrentamiento predefinidos, y 3) atacar el objetivo seleccionado para destruirlo o inutilizarlo determinando autónomamente cuándo y cómo hacerlo, empleando, en su caso, el arma más adecuada del conjunto de armas que posea.

No se ha llegado a un consenso global en la definición de los SALA; la razón detrás de esta dificultad es que **la discusión de la definición no es neutral** porque los participantes en los debates para su control siguen sus intereses políticos y estratégicos. Y, por lo tanto, proponer una definición en vez de otra no es un mero problema técnico, sino que puede servir a intereses políticos o estratégicos, lo que complica llegar a un consenso. No obstante, sí ha crecido la preocupación de que **la falta de regulación sobre los SALA y su rápida expansión puede dificultar su control** (Trager y Luca, 2022).

Otra categoría relevante y mucho más empleada actualmente son los **sistemas de armas semiautónomos**, es decir, aquellos en los que se mantienen a los **“humanos en el circuito”** (*“humans in the loop”*) con responsabilidades en la **toma de decisiones significativas** (Moliner, 2024). En este caso *“solo atacan objetivos individuales o grupos de objetivos”*.

específicos que han sido seleccionados por un operador humano”, pero tienen que esperar su orden de ataque para actuar.

Las armas semiautónomas incluyen las llamadas armas de “disparar y olvidar”, como ciertos tipos de armas que producen efectos en objetivos identificados por humanos utilizando **misiles guiados** con funciones autónomas, o en el caso de los **drones militares no tripulados** empleados habitualmente la decisión de disparar a un objetivo con consecuencias potencialmente letales la toma un operador humano de forma remota. De hecho, algunos **SALA semiautomáticos** ya son capaces de “merodear” (*loitering munitions*) en un área para encontrar objetivos que los algoritmos de aprendizaje automático les han entrenado para reconocer, incluidos sistemas de radar enemigos, tanques, barcos e incluso individuos concretos. Si lo encuentran, comunican al operador humano el hecho y “esperan la orden de atacar”.

La diferencia básica es que con **armas totalmente autónomas la decisión la toman solo los algoritmos de IA incorporados en el sistema**, una vez entrenados y definido el objetivo, **y en los sistemas semiautónomos media un operador humano** que da la orden final de atacar o no a objetivo identificado. En realidad, no se trata únicamente de un problema técnico que desarrollos tecnológicos futuros de la IA pueden resolver, sino de **asegurar que las situaciones reales se interpreten adecuadamente por un humano para evitar daños irreversibles.**

5.3.9.2 Uso de armas autónomas

Disponer de un sistema de armas totalmente autónomo no es una mera posibilidad futurista sí, como parece, **su uso ya tiene lugar en Ucrania, aunque sea de forma experimental** y, probablemente, en Gaza, aunque la clasificación de la información impide determinar hasta qué punto se han alcanzado los tres últimos niveles de la figura 5.1.

Aunque hoy día la mayor parte de estas armas son **tripuladas remotamente**, ya sean drones **aéreos** con visión en primera persona (*First person View, FPV*), o **marítimos** (fundamentalmente de superficie) o **terrestres** (incluso, con “cable” para evitar interferencias en la señal), se están produciendo avances tecnológicos considerables y muy rápidos para dotarlos de mayor inteligencia²⁸⁰.

La aparición de **UAV armados o «suicidas»** (un ejemplo de **municiones merodeadoras**), su relativamente bajo coste y el escaso riesgo para el personal que los opera hacen que se empleen con profusión como vectores de ataques en todas las distancias del campo de batalla. Los más complejos, se emplean para ataques profundos, pero también se usan UAV comerciales modificados a distancias típicas del empleo de la artillería de campaña y los morteros (Frías, 2023).

280 No se pretende en este capítulo desarrollar todos los tipos de sistemas no tripulados de uso militar existentes actualmente; su evolución, además, es muy rápida.

Dentro de la categoría de “*drones armados*” existen (conceptualmente) los denominados “**drones autónomos armados**” capaces de tomar decisiones en base a los datos recibidos en tiempo real, sus algoritmos, y la planificación previa de la misión que es el foco de la presente sección.

En 2023 la empresa ucraniana de drones *Saker* afirmó que había desplegado un arma totalmente autónoma, ***Saker Scout***, pero no está corroborado su uso real y eficacia. Se trata de un dron desarrollado inicialmente para fines agrícolas en 2021 y desplegado activamente en el frente en 2023 por el ejército ucraniano contra Rusia²⁸¹.

Focalizándose en drones militares más complejos y con capacidades autónomas Estados Unidos posee el denominado ***XQ-58A Valkyrie***, *dron de ataque sigiloso* (véase figura 5.8). Hasta ahora, los drones denominados “autónomos” seguían instrucciones simples preprogramadas, por ejemplo, para regresar a una ubicación predeterminada después de perder contacto con su operador.

Pero los experimentos realizados con el dron *XQ-58 Valkyrie* han permitido experimentar con una forma más sofisticada de autonomía en la que, **fijado un objetivo, el dron decide qué configuración de aceleración, qué ángulo de inclinación, qué altitud, o qué ángulo de inmersión debe hacer para alcanzar el objetivo**, además de colaborar en “modo patrulla” con un avión tripulado (véase figura 5.8 derecha). Por ahora el coste de desarrollo de cada unidad supera un coste de 6 millones de dólares; la intención de EEUU parece ser contar con una flota de más de mil unidades.



Figura 5.8 Izquierda: Dron XQ-58^a Valkyrie de Estados Unidos. Derecha: XQ-58^a Valkyrie volando junto a un F-16 Fighting Falcon de la USAF

Muchos de los drones de combate actuales se han desarrollado a partir de **drones comerciales adaptados** para llevar un arma como el que se ve en la figura 5.9 a partir de un

281 <https://www.forbes.com/sites/davidhambling/2023/10/17/ukraines-ai-drones-seek-and-attack-russian-forces-without-human-oversight/>

cuadróptero *DJI Mavic 3* adquirido a la empresa china DJI modificado y empleado por el Ejército de Ucrania. En estos casos, se trata de drones tripulados de forma remota y su **nivel de comportamiento autónomo y prestaciones son muy limitadas**.



Figura 5.9 Uso del cuadróptero DJI Mavic 3 armado con una bomba por parte de militares ucranianos de la 17ª Brigada de Tanques. Foto: 17th Kostiantyn Pestushko Tank Brigade – Mil.gov.ua (Wikimedia Commons / CC BY 4.0). Fuente: Martí (2024).

Si se confirmase la disponibilidad de sistemas de armas con **capacidades autónomas superiores al nivel 5** (no creemos que existan problemas técnicos ni de coste insalvables a corto plazo), y la voluntad de usarlos se incrementa por ejércitos de múltiples países en situaciones límite (como parece probable que suceda en conflictos de alta intensidad con armamentos de este tipo por ambos bandos en liza), **el tiempo para reaccionar** definiendo bien lo que es un SALA y llegar a un acuerdo global para establecer limitaciones de uso consensuadas **se está acortando muy rápidamente**.

En los últimos años, países como Estados Unidos, Reino Unido, India, Israel, Irán, Corea del Sur, Rusia y Turquía han invertido fuertemente en la integración de la Inteligencia Artificial (IA) en el desarrollo de SALA; al principio, empleando drones comerciales que, rápidamente, se han militarizado. Actualmente, **ejércitos de todo el mundo utilizan más de 130 sistemas de armas que pueden rastrear y atacar de forma autónoma a sus objetivos** (Channa, 2024)²⁸².

282 En la Revisión Estratégica de la Defensa del Reino Unido, la relevancia asignada a la autonomía y la IA en el proceso de transformación de sus fuerzas convencionales es un punto que se destaca en ese sentido (SDR, 2025). En la Revisión Estratégica se pide que el Ejército británico sea diez veces más letal. Se planea que esto se logre combinando más personal y capacidades blindadas con defensa aérea, comunicaciones, inteligencia artificial (IA), software, armas de largo alcance y enjambres de vehículos aéreos no tripulados (UAV).

Un **ataque a larga distancia** (cientos de kilómetros) y que es llevado a cabo por un arma que se dirige de forma autónoma debe disponer de un sistema de guiado muy preciso. Por eso, la mejor defensa ante estas armas es obvia: interferir su sistema de guía, anularlo o engañarlo. Ante las dificultades de usar la señal del sistema satelital GPS poco inmune a interferencias o suplantación, es normal **utilizar sistemas inerciales** de respaldo. Estos se basan en tomar un punto de partida de referencia y, a partir de ahí, medir mediante acelerómetros y magnetómetros (equivalente a una brújula) el movimiento realizado para calcular la nueva posición. El problema del sistema inercial es que se producen errores de cálculo que se van acumulando. Cuanto más lejos está el objetivo, menor es la precisión.

Ante estas dificultades, los sistemas más sofisticados incorporan al GPS y al inercial el llamado **sistema Tercom** o de *seguimiento del terreno*. Se basa en captar imágenes del terreno sobre el que se sobrevuela, comparándolas con las que el navegador lleva grabadas en su memoria para localizar la posición con gran exactitud²⁸³ lo que necesita una cartografía muy precisa para comparar las imágenes.

Otro enfoque se basa en la **obtención de imágenes digitales del terreno**, tecnología DS-MAC, que consigue mediante un módulo con cámara óptica. Este enfoque realiza capturas continuas del terreno y las va comparando, una a una, con las anteriores; como se conoce el punto de partida, se puede lograr un cálculo muy preciso del desplazamiento que ha realizado sin necesidad de reconocer el terreno.

El **misil inteligente de bajo coste** denominado **RUTA** (véase figura 5.10) realizado por la empresa de drones suiza *Destinus* y la española *UAV Navigation* del *Grupo Oesia* se utiliza en Ucrania con una **técnica de ataque en enjambre sofisticada**²⁸⁴. La plataforma vuela a una velocidad de crucero de Mach 0.8, tiene un alcance de hasta 500 Km y una precisión de impacto final de 15 metros cuadrados.

En cada misión se utilizan **veinte drones señuelo y cuatro misiles RUTA**. Los señuelos se lanzan sobre secciones del frente para provocar que se activen las defensas rusas. A continuación, se buscan los puntos más débiles para penetrar el telón defensivo. Si alguno de los 20 lo consigue, el resto de supervivientes lo seguirán automáticamente para tratar de producir daño, pues todos van con carga explosiva (aunque menor a la del misil). Una vez **localizado un pasillo viable**, sobre él se lanzan desde diferentes ubicaciones cuatro misiles, que vuelan en formación a baja cota y utilizando la orografía hacia su objetivo. Cuando los misiles ya se encuentran cerca del objetivo, la formación se disgrega y cada unidad adopta un rumbo y altura diferente, buscando converger sobre su objetivo desde diferentes direcciones para tratar de confundir a las defensas enemigas.

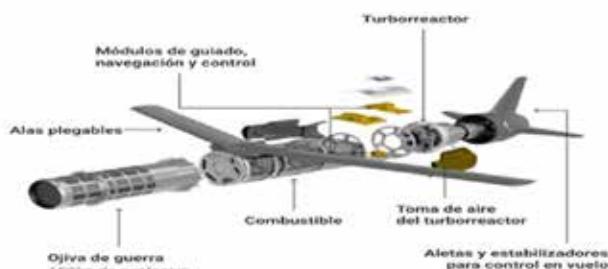
283 La ventaja es que es inmune a cualquier tipo de perturbación. La desventaja estriba en que este método necesita de una cartografía muy precisa (Fernández, 2025).

284 Se trata de un misil de cuatro metros de largo, con un peso de 300 kg (150 Kg de cabeza explosiva) y 300 Km de alcance.



Misil RUTA

Peso máximo: 310 kg
Velocidad de crucero: 0,8 Mach



Fuente: Destinos | El Confidencial

Figura 5.10. Misil RUTA. Fuente: https://www.elconfidencial.com/tecnologia/2025-05-22/ataques-ucranianos-misil-ruta-1hms_4134140/

Una tendencia tecnológica y operativa es **agrupar sistemas tripulados y no tripulados** para mejorar la eficiencia de las misiones. *Anduril*, junto con *General Atomics*, ha sido elegida por el Gobierno de Estados Unidos para crear el prototipo de una nueva clase de avión de combate autónomo llamado **Avión de Combate Colaborativo** (*Collaborative Combat Aircraft*, o *CCA*) para las Fuerzas Aéreas y la Marina de Estados Unidos con una inversión prevista de 6.000 millones de dólares de 2024 a 2028 para disponer de 1.000 drones de esta nueva generación²⁸⁵.

²⁸⁵ <https://www.airforce-technology.com/projects/collaborative-combat-aircraft-cca-usa/>

Se pretende que los nuevos drones del tipo CCA sean más capaces e independientes que los actuales que siguen dependiendo de operadores en tierra para una amplia gama de misiones, como reconocimiento, ataques aéreos y guerra electrónica, **en colaboración con aviones pilotados por un humano** (p.ej. asignando dos drones a cada F-35) **o actuando de forma autónoma**. Una parte esencial del programa CCA es el **desarrollo de un nuevo software de inteligencia artificial (IA)** para controlar las aeronaves que funcione de manera autónoma en una gama más amplia de situaciones que los sistemas militares existentes, que suelen ser autónomos únicamente en circunstancias limitadas.

Merece la pena referirse al desarrollo de **drones marítimos** cuya efectividad está alcanzando resonancia por su uso en la guerra de Ucrania. Se trata de drones autónomos, fundamentalmente de superficie (USV), aunque también los hay submarinos, capaces de lanzar torpedos o misiles aéreos o estrellarse contra objetivos de mucho mayor coste. También pueden cubrir misiones de vigilancia costera o salvamento marítimo.

La efectividad de los pequeños USV (7 u 8 metros de eslora) está modificando la guerra naval y de hecho, se empiezan a incorporar también a otros buques tripulados de mayor tonelaje como fragatas o corbetas como sistemas complementarios. El éxito de los USV desarrollados por Ucrania del tipo **Magura V5** (utilizado contra la flota rusa o helicópteros) o el más reciente **Magura V7** (dotados de misiles y capaz de derribar cazas rusos Su-30) ha supuesto un aliciente para el desarrollo de otros muchos por todas las potencias tecnológicas²⁸⁶.

España participa de esta tendencia con el desarrollo de USV como el **Sead 23** de la empresa **Seadrone** que se presenta en la figura 5.11. Desde 2023 ha sido integrado en diversos buques de la Armada española para diferentes tipos de misiones.



Figura 5.11. Sead 23. Fuente: Sead Drone

286 https://www.elespanol.com/omicrofono/defensa-y-espacio/20250510/magura-v7-dron-naval-ucraniano-teme-aviacion-putin-derriba-primera-vez-cazas-mar/1003743742006_0.html

Finalmente, es necesario referirse a la situación de los **vehículos terrestres no tripulados (UGV)** empleados en el contexto militar. Las dificultades comparadas con los empleados en el mundo civil son claras al tener que desplazarse en terrenos accidentados y no carreteras y con los problemas conocidos de perturbaciones de la señal. Aún con estas dificultades se han empleado en Ucrania para diversas tareas militares, incluyendo logística, reconocimiento, limpieza de minas e incluso operaciones ofensivas más de ochenta modelos diferentes. Uno de los últimos sistemas desarrollados adoptados por las fuerzas ucranianas es el denominado **Krampus** (véase figura 5.12).



Figura 5.12. UGV Krampus. Fuente: <https://thedefensepost.com/2025/05/21/ukraine-krampus-flamethrower-ugv/>

Sus principales características son las **cámaras de video** para inteligencia y detección de amenazas, así como el **lanzallamas termobárico** propulsado por cohetes RPV-16 para su uso contra tropas enemigas y vehículos blindados de clase ligera.

En la figura 5.13 puede verse la plataforma robotizada **Liut** (*Furia* en ucraniano) que está siendo empleada en el frente de Járkov en condiciones reales de campo de batalla. Está equipado con una ametralladora de 7,62 mm. Puede identificar y atacar objetivos de día y de noche, posee un motor eléctrico silencioso y su construcción robusta le permiten operar en terrenos difíciles y en condiciones climáticas adversas²⁸⁷.

²⁸⁷ <https://kyivindependent.com/ukraines-military-intelligence-releases-footage-of-robotic-ground-vehicle-attacking-russian-positions/>



Figura 5.13 Plataforma robótica armada Liut (Furia). Fuente: <https://kyivindependent.com/ukraines-military-intelligence-releases-footage-of-robotic-ground-vehicle-attacking-russian-positions/>

5.3.10 Enjambres de sistemas militares no tripulados

Una evolución muy relevante desde el punto de vista tecnológico, pero también desde el punto de vista táctico militar, es el paso del uso de sistemas autónomos individuales a **“enjambres de sistemas autónomos”**. Este proceso evolutivo, tecnológico y doctrinal, se está realizando a una gran velocidad inicialmente en enjambres aéreos y más lentamente en los terrestres y marítimos. La definición propuesta por Ekelfof y Paoli (2021) es la de *“sistemas multi-robot dentro de los cuales los robots coordinan sus acciones para trabajar colectivamente hacia la ejecución de un objetivo”*. La clave de la utilidad de los enjambres de drones, por tanto, no es su número sino la **inteligencia con la que coordinan sus acciones**.

En el campo de los vehículos autónomos aéreos que son los más desarrollados, un enjambre consiste en disponer de **grupos de vehículos aéreos no tripulados que operan de manera coordinada** mediante redes de comunicación avanzadas. Los enjambres dependen en gran medida de la IA para coordinar sus movimientos -lo que es necesario dado que **los drones tácticos de combate** deben ser capaces de tomar decisiones autónomas a gran velocidad y adaptarse a **entornos dinámicos** en tiempo real (Kori *et al.*, 2024).

El término *“enjambre”* se ha recuperado de la naturaleza en la que **múltiples especies de insectos, aves, peces y otros animales actúan de forma coordinada para conseguir sus objetivos**. La inteligencia de un enjambre de animales o enjambre natural, tal y como se

observa en la naturaleza, se refiere a los **comportamientos colectivos emergentes que surgen de la coordinación descentralizada entre organismos** (SDI, 2024). Cuando cada miembro del enjambre sigue individualmente las reglas locales, la acción combinada de estos miembros crea **comportamientos grupales complejos e “inteligentes”**. Desde un punto de vista más abstracto, el comportamiento de enjambre es el **movimiento colectivo de un gran número de entidades autopropulsadas**.

En el caso de los **enjambres artificiales** compuestos de drones, la **inteligencia de enjambre** (*swarm intelligence*) se refiere a la **capacidad de los drones para imitar los comportamientos de animales e insectos para seguir reglas que permiten capacidades y eficiencias cada vez más inteligentes**. Para conseguir que los robots cooperen, la robótica de enjambre emplea principios como la **comunicación**, la **coordinación** y la **colaboración**. La colaboración entre varios robots puede conducir a un tiempo de finalización de tareas más rápido en comparación con la utilización de un solo robot complejo.

Los algoritmos de enjambre se han aplicado tanto a drones como a grupos de robots de combate terrestres para la planificación de misiones y la coordinación de los elementos del grupo. Un ejemplo es el sistema Marker de Rusia, que integra visión artificial y comunicación en enjambre con **redes neuronales profundas** (Bendett, 2024).

Su capacidad para actuar como una entidad colectiva los hace útiles en misiones de **reconocimiento, vigilancia, ataque masivo, defensa y guerra electrónica** (Márquez, 2023). Los enjambres pueden constituir desde una pequeña formación de pocas unidades, hasta grupos muy numerosos de drones; por lo que se sabe, **China y Estados Unidos están desarrollando enjambres con decenas de miles** (Mezzacappa *et al.*, 2024).

El **coste unitario por dron** es un parámetro esencial que hará que los enjambres sean efectivos (o no); aunque hay drones comerciales de calidad suficiente por pocos cientos de euros, el rango sube hasta los 50.000 euros para drones avanzados (Dobija, 2023). Pensar en drones de bajo coste, empleados para misiones suicidas los acerca al concepto de “munición inteligente” y no de un activo permanente. Para el gobierno de Ucrania este tipo de drones se consideran material fungible en lugar de inventariable, lo que simplifica y acelera los trámites burocráticos para su adquisición, única forma de gestionar la adquisición y renovación de cientos de miles de drones²⁸⁸.

288 Los sistemas autónomos -ya sean drones, robots terrestres o marino- han adquirido gran relevancia en el contexto de la guerra de Ucrania (Gady, 2023). Ambas partes han desplegado drones equipados con IA para misiones de reconocimiento y ataque a infraestructuras estratégicas. Ucrania, por ejemplo, ha desarrollado drones de bajo coste que pueden identificar y atacar objetivos con alta precisión gracias a la IA. Según aparece en la prensa, Ucrania ha usado un robot armado con una ametralladora que se puede manejar remotamente -el Droid TW 12.7-. Los drones de muy bajo coste serán empleados profusamente. <https://www.huffingtonpost.es/global/los-drones-tirados-precio-toman-control-guerra.html>.

El buen funcionamiento y el éxito en la misión de un enjambre de drones, requiere **integrar las capacidades** de los drones individuales, para conseguir un **comportamiento colectivo**²⁸⁹. Pueden establecerse tres **enfoques básicos de coordinación de enjambres** de menor a mayor complejidad (véase figura 5.14):

- **Centralizado.** Todas las interacciones se realizan con el operador que recibe información de los drones individuales, decide y envía órdenes a cada uno de ellos. No existe comunicación entre los drones.
- **Descentralizado semi autónomo.** El operador humano se comunica con un dron para la recepción y transmisión de datos y órdenes, y este dron maestro se comunica con el resto de los miembros del enjambre. Algunas acciones derivadas de más bajo nivel podrían realizarse de forma autónoma sin necesidad de comunicación con el operador humano.
- **Descentralizado totalmente autónomo.** No existe operador humano. Cada dron intercambia información con todos o con algunos de los drones cercanos del enjambre para decidir los siguientes movimientos y acciones siguiendo comportamientos para los que sus algoritmos de IA han sido entrenados.

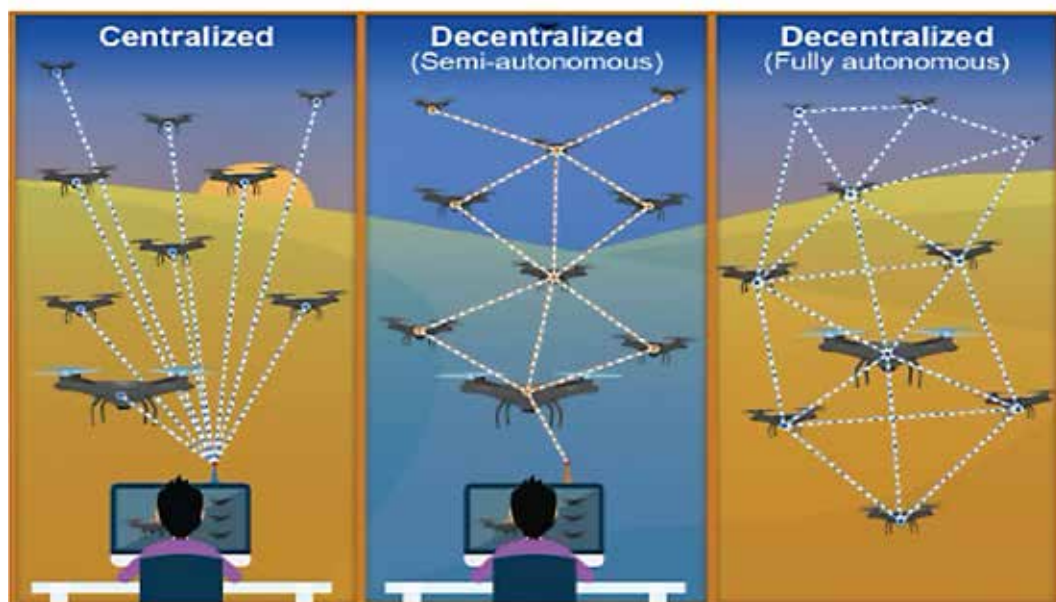


Figura 5.14. Enfoques básicos de coordinación de enjambres. Fuente: GAO Analysis

²⁸⁹ Debe tenerse cuidado en la interpretación del uso que se hace habitualmente del término de “enjambre” en la guerra de Ucrania o en la de Gaza porque en la mayor parte de los casos se trata de ataques simultáneos con “muchos drones” individuales, pero no existe un *comportamiento de enjambre* dado que no cooperan entre ellos para coordinar sus movimientos o acciones.

En los **casos descentralizados**, una vez que los operadores humanos hayan proporcionado las órdenes al enjambre (o a unidades específicas dentro del enjambre) y el software de control haya determinado cómo se distribuirán las órdenes entre los miembros, **el enjambre en su conjunto tiene que coordinar su comportamiento y acción colectiva para ejecutar las tareas asignadas**. Se han aplicado algoritmos diseñados manualmente o diseñados automáticamente (por ejemplo, basados en heurística, basados en evolución, basados en aprendizaje, para implementar varios comportamientos de enjambre (p. ej. vuelo en formación y detección distribuida) para lograr un objetivo deseado (p. ej., planificación de rutas, asignación de tareas, control de vuelo, reconfiguración de formaciones y prevención de colisiones).

Algunos enfoques comunes para facilitar la coordinación interna del enjambre (es decir, las decisiones de acción) son: **líder-seguidor**, **algoritmos de consenso**, **funciones de utilidad** y **coordinación emergente** (Ekelhof y Paoli, 2021). Aunque es más probable que algunos métodos de coordinación se utilicen en combinación con arquitecturas específicas (como líder-seguidor en el control jerárquico), podrían aplicarse a cada una de las cuatro arquitecturas básicas: control centralizado, control jerárquico, control a nivel de conjunto y control conductual.

Conseguir un comportamiento de enjambre se apoya en el **uso de la IA en el borde**, un dron puede considerarse como un sensor con actuador, con **apoyo de dispositivos en el borde del continuo edge-fog-cloud**, mejorado con capacidades autónomas. De nuevo sólo es posible desarrollar estos sistemas mediante las capacidades aumentadas que la IA proporciona en los siguientes aspectos, entre otros:

- En cuanto a **coordinación autónoma y control distribuido**, se usan algoritmos como las **redes neuronales convolucionales**, la **optimización basada en enjambres de partículas (PSO)** o los **algoritmos genéticos** para operar como una entidad colectiva sin intervención humana constante. Esto es necesario para **evitar colisiones y optimizar sus trayectorias** (Karadeniz *et al.*, 2023); **distribuir tareas entre los drones** de manera eficiente sin necesidad de un controlador central, y **adaptarse a fallos individuales** manteniendo la misión operativa incluso si algunos drones son derribados o sufren fallos de funcionamiento. Un ejemplo es el experimento EEUU *Perdix*, donde **103 microdrones** lanzados desde aviones F/A-18, operaron **en enjambre** con algoritmos basados en **redes neuronales recurrentes**, sin control humano directo.
- En lo relativo a las **estrategias de ataque y defensa**, usan **redes neuronales profundas** para planificar y ejecutar estrategias en el campo de batalla. Por ejemplo, al realizar ataques coordinados a infraestructuras enemigas con **decisiones autónomas sobre selección y el ataque de objetivos prioritarios**; en la defensa contra amenazas aéreas mediante redes de **drones interceptores con algoritmos predictivos basados en árboles de decisión y bosques aleatorios**; o al aplicar tácticas de guerra electrónica, incluyendo interferencias

y **ataques cibernéticos con redes adversarias generativas** (Kott, 2018). La organización de enjambres **masivos necesita modelos de optimización** como *Grey Wolf Optimization*.

- Mediante el **aprendizaje automático**, los enjambres de drones pueden **mejorar su rendimiento con cada misión**. Pueden ir aprendiendo por **refuerzo** o con otras técnicas como **regresión logística y redes neuronales profundas**, para predecir y evadir, como radares enemigos y sistemas de defensa aérea; **optimizar los patrones de vuelo y cobertura del terreno** en misiones de vigilancia con optimización basada en colonia de abejas; o mejorar su autonomía en la toma de decisiones tácticas, minimizando la necesidad de control humano por medio de **sistemas multi-agente** (Dobija, 2023). Se ha demostrado que los drones pueden aprender mediante **algoritmos por refuerzo profundo patrones de defensa** para superar barreras electrónicas.
- La recogida y procesado de la información mejora su rendimiento en tareas como la de **analizar imágenes y vídeos en misiones de reconocimiento** recogiendo información de múltiples sensores como radares, cámaras infrarrojas y LiDAR **para la detección de objetivos** (Mikulski *et al.*, 2014). También pueden identificar y **rastrear objetivos móviles en entornos hostiles** mediante **redes neuronales profundas, aprendizaje reforzado y fusión de datos**. En un experimento de hace algún tiempo, un enjambre de 25 drones fue capaz de ajustar su formación de vigilancia en función de las necesidades operativas.

Todas las grandes potencias están trabajando en el **desarrollo de enjambres de drones con fines militares**. Los países que actualmente están desarrollando algún proyecto sobre tecnología de enjambres de drones son: Estados Unidos, Reino Unido, Finlandia, Alemania, Francia, Turquía, Rusia, Ucrania, India y China (Borchert 2024). En **Estados Unidos**, los desarrollos se producen a través de **acuerdos entre empresas tecnológicas** (como Boeing o Raytheon) y **laboratorios de investigación** (MIT Media Lab) para aplicaciones tanto militares como comerciales. Destacan los experimentos con **grandes modelos de lenguajes (LLM) para dar soporte al mando y control de enjambres**, enfoque que comienza a observarse en la literatura científica (Onsu 2024). En todo caso, la realidad operativa alcanzada por estos enjambres es desconocida.

Esta tecnología no está solo en manos de grandes potencias tecnológicas. En Ucrania, nuevas empresas de base tecnológica están desarrollando sistemas de inteligencia artificial (IA) para **automatizar el vuelo de un enjambre de drones**, llevando la guerra a territorio inexplorado mientras los combatientes compiten para obtener una ventaja tecnológica en la batalla. **Ucrania ha creado una nueva rama de sistemas no tripulados**, empujada por las necesidades de la guerra. Una empresa start-up creada en 2023 tras el inicio de la invasión de Ucrania que trabaja en el desarrollo avanzado de drones para defensa es **Swarmr** (<https://www.getswarmr.com/>) posee un **sistema software para gestionar enjambres de drones** (véase en la figura 5.15 el tipo de drones desarrollado).



Figura 5.15. Desarrollo de drones de Swarmer. Fuente: Pool (2025). <https://www.eetimes.eu/drones-with-edge-ai-the-future-of-warfare/>

El sistema, llamado **Styx** (sistema avanzado de Mando y Control para la gestión de varias unidades de UAV con autonomía colaborativa, diseñado para la próxima generación de operaciones) dirige una red de drones de reconocimiento y ataque, tanto grandes como pequeños, en el aire y en tierra. Cada miembro del enjambre sería capaz de planificar sus propios movimientos y predecir el comportamiento de los demás en el enjambre. Las decisiones elaboradas por **Styx** se pueden implementar instantáneamente en todo el grupo, y solo un humano interviene para dar validar los objetivos y dar la orden de los ataques automatizados. Volviendo a la escala de la figura 5.7 puede decirse que se trata de un nivel 5, al comienzo de la zona gris.

También pueden mencionarse otras **empresas europeas** con similares niveles de automatización declarados (listado no exhaustivo).

- La empresa ucraniana de drones **Saker** afirmó que había desplegado un arma totalmente autónoma que “utiliza **IA para tomar sus propias decisiones** sobre a quién atacar en el campo de batalla. El dron había llevado a cabo **ataques autónomos a pequeña escala**”²⁹⁰. También se informa del desarrollo de un sistema **Tryzub** (Trident) para **derribar aeronaves enemigas a más de dos kilómetros** de distancia, representando un avance significativo en las capacidades defensivas²⁹¹.

²⁹⁰ <https://saker.airforce/home>

²⁹¹ Trident, la nueva arma láser en poder de Ucrania capaz de derribar aviones a más de 2 kilómetros. Disponible en línea: <https://as.com/actualidad/politica/trident-la-nueva-arma-laser-en-poder-de-ucrania-capaz-de-derribar-aviones-a-mas-de-2-kilometros-n/>

- La empresa alemana **Quantum Systems** desarrolla drones de reconocimiento para Ucrania y recientemente colaboró con *Airbus* y el desarrollador de software alemán *Spleenlab* para demostrar un enjambre de siete vehículos aéreos no tripulados controlados por IA como parte de un estudio para las Fuerzas Armadas de Alemania que ha sido probado en Ucrania.
- La empresa francesa **Thales** ha desarrollado una arquitectura de sistema basada en IA para enjambres de drones con diferentes niveles de autonomía que son “capaces de percibir y analizar su entorno local, compartir información sobre objetivos, analizar las intenciones del enemigo y priorizar las misiones”.
- La empresa alemana **Helsing**, con sede en Berlín, desarrolla software de IA en el borde y fabrica drones de ataque desplegados en Ucrania. Su software *Altra* conecta los drones con los operadores humanos y está diseñado para acelerar la identificación de objetivos mediante la combinación de la IA con las redes y el software de la estación terrestre. Disponen de sistemas de control para enjambres de drones de ataque HX-2 (véase figura 5.16).



Figura 5.16. Enjambre de drones HX-2 de la empresa Helsing empleados en Ucrania.

Fuente: https://www.elconfidencial.com/tecnologia/novaceno/2024-12-09/musk-pilotos-combate-plan-imposible_4018166/

- La empresa británica **BlueBear IA** dependiente de *Saab* ha realizado pruebas de drones de la Alianza AUKUS en los que un solo operador comandaba un enjambre diverso de drones autónomos. En la figura 5.17 puede verse uno de estos enjambres heterogéneos empleados en una demostración.



Figura 5.17. Enjambre de drones heterogéneos de BlueBear AI.

Fuente: <https://www.eetimes.eu/saab-robert-lindegren-on-drone-swarms-edge-ai-and-the-future-of-autonomous-warfare/>

También las **capacidades españolas en el desarrollo de UAV para aplicaciones en defensa** están incrementándose muy rápidamente, no solo en relación con el desarrollo de drones aéreos aislados, sino también en **enjambres de drones**²⁹². A ello contribuyen inversiones significativas desde 2024 del INTA y del JCISAT (Jefatura de Ciberespacio y Asistencia Técnica) del Ejército de Tierra (ET) apoyadas por fondos del programa *Next Generation EU*. Sin pretender ser exhaustivos, se mencionan algunas capacidades relevantes.

La empresa española **Swarming Technologies & Solutions**²⁹³, perteneciente al *Grupo Zelenza*, ha desarrollado un sistema de enjambre multidominio denominado MINERVA que permite: 1) Operación de diferentes tipos de vehículos (ala fija, VTOL, multicoptero, UGV y USV), 2) Operación de diferentes tipos de cargas útiles (EO/IR, guerra electrónica, NRBQ, altavoces, letales, carga, sistemas de localización sonora y otros) simultáneamente, y 3) Integración entre tripulados y no tripulados con aeronaves, vehículos terrestres y marítimos. En la figura 5.18 se puede ver el sistema de control del enjambre en un ejercicio de la OTAN.

²⁹² De hecho, las capacidades españolas en relación con enjambres de drones se remontan a 2016. La DGAM del Ministerio de Defensa deseaba incorporar la tecnología de enjambres de drones al proyecto RAPAZ de aeronaves no tripuladas para “valorar el estado del arte y las aplicaciones que puedan tener los enjambres de drones desde el punto de vista militar con objeto de estudiar su posible aplicación” <https://www.defensa.com/espana/swarming-technologies-solutions-primera-empresa-espanola-no>

²⁹³ <https://swarmingts.com/>



Figura 5.18. Izquierda. Centro de operaciones de Swarming TS con un enjambre Minerva en el ejercicio REPMUS294 de la OTAN en 2023. Derecha: Sistema C2 para control del enjambre. Fuente: <https://www.defensa.com/industria/swarming-technologies-solutions-supera-20-horas-vuelo-enjambre>

La progresiva puesta en marcha del **CETEDEX** (Centro Tecnológico de Desarrollo y Experimentación) como parte del INTA situado en Jaén, y dentro de él el **CEADRON** (Centro de sistemas y tecnologías antidrón) constituye una oportunidad para mejorar las capacidades españolas en enjambres. En este contexto, se adjudicó en 2024 a la empresa española

294 REPMUS es un ejercicio anual en aguas portuguesas en el que las armadas de la OTAN desarrollan capacidades para ofrecer equipos tripulados-no tripulados en operaciones multidominio. <https://seapowermagazine.org/a-must-do-repmus-is-primary-means-for-nato-to-develop-maritime-uncrewed-capability/>

Swarming Technologies & Solutions²⁹⁵ un contrato para el suministro de un sistema de enjambre de drones compuesto por 4 vehículos aéreos no tripulados, incluyendo 3 plataformas ‘multicóptero’ y 1 plataforma de ala fija con capacidad de **despegue y aterrizaje vertical** (VLOT).

El pliego de prescripciones técnicas indica que debe constituirse como un **“sistema ‘multiagente’ distribuido y no jerárquico para que, mediante la coordinación por consenso entre todas las plataformas del sistema, éstas sean capaces de organizarse autónomamente para llevar a cabo diferentes tipos de misiones simultáneamente de acuerdo”**. Además, se hacía constar que, para que la toma de decisiones no estuviese centralizada (sino que pudiera realizarse de manera distribuida y colaborativa entre las diferentes plataformas), era necesario que cada una contase con un **módulo de inteligencia embarcada potente y suficientemente capaz**²⁹⁶. Debe tenerse en cuenta que el CETEDEX constará también con un Centro de Inteligencia Artificial (CIA)²⁹⁷.

El sistema de un **enjambre de cuatro drones del tipo VLOT** ofrecerá, entre otras, las siguientes funcionalidades:

- Extender la cobertura 5G a zonas a las que no se puede dar servicio con la estación base terrestre.
- Mejorar y extender la calidad del servicio 5G en zonas urbanas, donde la atenuación de la señal sea muy elevada.
- Asignar una plataforma UAV del enjambre a un convoy de manera que proporcione cobertura 5G a dicho convoy de manera desatendida.

El enjambre de drones debe tener la inteligencia necesaria para planificar y replanificar sus rutas de manera autónoma, sin intervención humana. Para ello, se usarán algoritmos de enjambre, que tendrán en cuenta la orografía, la calidad de la señal, la localización del resto de drones, la potencia de radio recibida y la localización de los dispositivos que dispongan de esa información para calcular la localización óptima de cada uno de los drones del enjambre.

Finalmente, como ejemplo de desarrollo de vehículos terrestres no tripulados (UGV) en la UE, es destacable la participación de las empresas españolas **GMV** y **Escribano** en el proyec-

²⁹⁵ <https://swarmingts.com/>

²⁹⁶ <https://www.elradar.es/enjambre-drones-cetdex/>

²⁹⁷ Esas capacidades españolas también se complementarán con el suministro de un sistema de comunicaciones táctico (FANETC - Flying Ad-hoc NETWORK & distributed mobile Tactical Cloud) que permita establecer redes 5G terrestres y no terrestres, éstas últimas mediante la utilización de drones, para dar cobertura inalámbrica al despliegue de una unidad tipo Brigada del Ejército de Tierra. Este sistema incorporará capacidad de computación en el borde (edge computing) para permitir la ejecución de algoritmos de IA, disminuir el tiempo necesario para la toma de decisiones y facilitar la creación en el futuro de una nube táctica distribuida.

to denominado **iMUGS2** (*Integrated Modular Unmanned Ground System 2*)²⁹⁸ de la última convocatoria de EDF, continuación de uno anterior de 2023²⁹⁹. Su objetivo es desarrollar y validar capacidades autónomas y de enjambre para sistemas no tripulados terrestres con el objetivo de mejorar la protección, la interoperabilidad y las operaciones multidominio.

El sistema se ha probado con UGVs del tipo **ThEMIS** (*Tracked Hybrid Modular Infantry System*) desarrollado por la empresa de Estonia *Milrem Robotics*, como el que se ve en la figura 5.19. que ha sido desplegado en Ucrania.



Figura 5.19 UGV ThEMIS, Fuente: Izquierda. <https://www.army-technology.com/projects/themis-hybrid-unmanned-ground-vehicle/> Derecha: <https://thedefensepost.com/2025/05/23/ukraine-ugv-estonia-france/>

En este tema coinciden las **prioridades de desarrollo en Rusia y China. Israel y Turquía presentan actividades de desarrollo** en este ámbito buscando la reducción de bajas. También se informa sobre **Irán y Corea del Sur como países proclives a incorporar mayores cotas de autonomía en el armamento**, para tratar de compensar el envejecimiento demográfico y la reducción de efectivos.

En el caso de un enjambre con inteligencia limitada, **un dron puede actuar como supervisor** para otros drones que están realizando un ataque alimentando a los otros operadores de drones con información para hacer que el ataque sea más efectivo. Los enjambres con drones más avanzados automatizarían gran parte de este proceso, de modo que cuando un dron del enjambre detecta un sistema anti-drones, puede transmitir los detalles de la amenaza al resto del enjambre. Luego, el enjambre puede tomar medidas evasivas de forma autónoma para aumentar su probabilidad de completar su misión. Los **algoritmos necesarios**

²⁹⁸ <https://imugs.eu/>

²⁹⁹ GMV ha sido la responsable en el proyecto iMUGS de coordinar el subproyecto de mando y control e interoperabilidad C4ISR (que engloba sistemas de mando, control, comunicaciones, informática, Inteligencia, vigilancia y reconocimiento). <https://www.gmv.com/es-es/comunicacion/eventos/demostracion-final-del-proyecto-imugs>

para este nivel de automatización requieren una toma de decisiones descentralizada, pero sincronizada en un entorno dinámico, a menudo en presencia de interferencias enemigas³⁰⁰.

También se han empezado a considerar el despliegue de **enjambres de drones aéreos, terrestres y marítimos cooperando entre sí y con el apoyo de satélites**. En la figura 5.20 pueden verse cómo se combinan este tipo de unidades apoyados por satélite y estaciones terrenas (Munashinge et al., 2024). Aún persisten problemas técnicos para que esta cooperación UAV-UGV sea efectiva, particularmente en términos de optimización de la comunicación, la coordinación y la eficiencia operativa en escenarios complejos como ocurre en el caso de la defensa.

En los próximos años, según vaya madurando la tecnología, **los enjambres de sistemas aéreos no tripulados se integrarán como parte de una arquitectura general de sistema de sistemas** para permitir el desarrollo de verdaderas operaciones multidominio. Esto permitirá que drones de inteligencia, vigilancia y reconocimiento se integren directamente en la cadena de fuego (asumiendo en función de su tipo las funciones de identificación, ataque y neutralización de un objetivo).

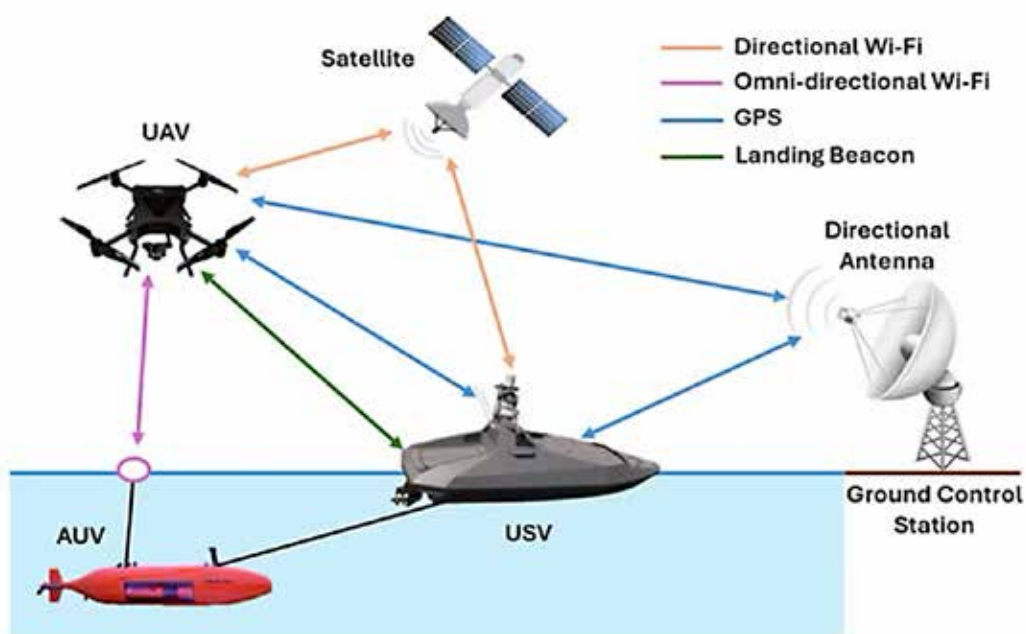


Figura 5.20. Enjambre de vehículos no tripulados aéreos y marítimos. Fuente: <https://doi.org/10.3390/jsan13060081>

A pesar de que, según los fabricantes, muchos drones tienen diferentes tipos de capacidades autónomas, éstas son aún limitadas y, **aunque algunos países (como Ucrania) utilizan o pueden estar cerca de utilizar drones semiautónomos, hay pocos o ningún dron totalmente**

300 <https://www.forbes.com/sites/vikrammittal/2025/01/02/swarming-drones-will-be-on-the-russian-ukrainian-battlefield-in-2025/>

autónomo en servicio regular. Sin embargo, dado el ritmo al que se está desarrollando la inteligencia artificial en el ámbito militar y la presión para incorporar innovaciones disruptivas en el campo de batalla, **esta situación podría cambiar radicalmente en uno o dos años desde el punto de vista técnico.** Otra dimensión diferente es si se decide usarlos en operaciones totalmente autónomas o no o como parte de “cadenas letales”. En este sentido, será necesario establecer límites de uso como se analizará en un capítulo posterior.

5.3.11 Consecuencias tácticas

Tanto *Ucrania* como *Rusia* están acelerando el desarrollo de diferentes tipos de drones y sistemas robóticos en el campo de batalla, tanto individuales como en enjambres impulsados por la necesidad de precisión, el empleo masivo para abrumar al adversario, la resistencia contra las contramedidas y la **reducción de los riesgos para las vidas humanas.** Esta evolución tecnológica hacia el uso masivo de drones y de enjambres de drones implica la posibilidad de **reducir significativamente los efectivos humanos empleados en el frente de batalla,** aunque no necesariamente el total de efectivos.

Esta importancia no se detiene en los drones aéreos; también ha tenido un **efecto muy relevante en el uso de drones marítimos** que, en el caso de Ucrania ha obligado a la flota rusa a retirarse de áreas cercanas a la península de Crimea. Su uso para atacar a buques rusos (empleando drones tipo *Magura V5*) ha sido muy efectivo, y también empieza a serlo contra helicópteros y aviones en su evolución *Magura V7* incorporando misiles tierra-aire *AIM-9 Sidewinder*³⁰¹. En la figura 5.21 se ve el dron marítimo *Magura V7* armado con los misiles citados.



Figura 5.21 *Magura V7* armado con dos misiles *Sidewinder*. Fuente: <https://www.navalnews.com/naval-news/2025/05/first-image-of-ukraines-sidewinder-armed-magura-v7-surface-drone/>

301 Un dron *Magura V5* derribó en diciembre de 2024 dos helicópteros rusos *Mi-8*, y en abril de 2025 se ha informado que uno de estos drones (*Magura V7*) ha sido capaz de derribar un caza *Su-30* con un misil (es la primera vez que se informa de un ataque de este estilo. Para más detalles puede consultarse https://www.larazon.es/tecnologia/primera-vez-dron-naval-derriba-avion_2025050468170d85319ae75da4bfb4eb.html

La consolidación de la **efectividad de estos sistemas**, y el **incremento de su inteligencia** para detectar objetivos y la **progresiva reducción del coste** frente a alternativas tripuladas, acelerará su uso y modificará las tácticas empleadas. Con ello, se obligará a las fuerzas aéreas a operar a mayor distancia del objetivo empleando para su defensa armas mucho más costosas. Los efectos que la **evolución de las operaciones basada en el uso generalizado de drones** genera en el campo de batalla son muy relevantes, aunque exista una **curva de aprendizaje** que durará tiempo para asimilar y transformar la doctrina y las tácticas militares empleadas.

No es sencillo evaluar a partir de fuentes abiertas la **efectividad de los enfoques con drones**, aunque los avances son rápidos con la introducción de la IA en la computación en el propio dron (Pool, 2025). Una aproximación a este escenario ya se empieza a producir en Ucrania. En diciembre de 2024, las fuerzas ucranianas llevaron a cabo el **primer ataque totalmente autónomo** con UAVs y UGVs cerca de *Lyptsi* (un pueblo cercano a *Kharkyv*). El ataque implicó docenas de vehículos terrestres no tripulados (UGV) y drones (UAV) con visión en primera persona (FPV) sin participación de la infantería (Bondar, 2025).

El **ataque multidominio** mencionado permitió que los UGVs equipados con cañones y munición realizaran tareas de desminado y fuego directo mientras que los drones FPV apoyaron la operación desde el aire en un contexto de **ataque coordinado multidominio (aire-tierra)**. A la finalización del ataque sobre las posiciones rusas, los sistemas robotizados supervivientes volvieron tras las líneas ucranianas. En todo caso, **la operación no supuso la eliminación de los operadores humanos que tuvieron el control de la operación**, pero manteniéndose alejados del escenario de combate.

El anuncio efectuado en julio de 2025 por el ejército ucraniano del uso en el frente de Járkov, por primera vez, de un **ataque combinado de drones aéreos y vehículos terrestres logrando capturar tropas rusas sin intervención humana directa**, supone, desde el punto de vista tecnológico, un ejemplo de la rapidez con la que se adoptan nuevas tácticas de combate con enjambres de vehículos autónomos heterogéneos pilotados remotamente. **La evolución hacia el campo de batalla inteligente se acelera.**

La evolución tecnológica hacia **“enjambres de drones inteligentes”** basados en **cientos o miles de drones** en los que cada uno de ellos puede identificar objetivos en tiempo real y comunicarse con sus drones vecinos, supondrá un cambio cualitativo con efectos en las tácticas militares. La combinación de enjambres con toma de decisiones IA en tiempo real parece apuntar hacia el desarrollo de **sistemas complejos de reconocimiento y ataque totalmente autónomos** capaces de operar bajo condiciones adversas en el espectro electromagnético; sin embargo, por ahora su **uso principal es en tareas de inteligencia, vigilancia y reconocimiento (ISR) para mejorar la información disponible o para apuntamiento y disparo.**

Con enjambres de esta dimensión ya **no es factible pensar en que un operador humano sea capaz de analizar toda la información y decidir qué objetivo atacar y por cuál de los**

drones del enjambre, y hacerlo en segundos; es imposible. Si, además, se pretende conseguir **mayor resiliencia del enjambre** ante el caso de derribo de algunos de ellos mediante la reasignación dinámica de tareas en los demás, el software necesario basado en algoritmos de IA es más complejo. Debe tenerse en cuenta que muchos de estos enjambres son heterogéneos: están **compuestos por drones de diferentes tipos y con diferentes modelos de interacción con operadores humanos**.

Al final, si la evolución de enjambres de drones continúa, **será un sistema centralizado potenciado por IA o serán los mismos drones los que tomarán la decisión**, dejando al humano fuera del ciclo de decisión salvo en la determinación de objetivos estratégicos en el planeamiento de la misión y, la decisión sobre las reglas de enfrentamiento. En pocos años, un país tecnológicamente avanzado puede ser capaz de desarrollar un enjambre de 10.000 drones, y otros muchos países podrán adquirirlos, empleando sofisticados algoritmos de IA cuyo desarrollo es un factor prioritario. Sin embargo, para ser efectivo, ese enjambre debe ser desplegado en el campo de batalla para lo que se requieren **capacidades de logística, mantenimiento y producción para sostenerlos**. La diferencia es que, si los 10.000 drones llegan al campo de batalla, es probable que, aunque muchos de ellos sean inhabilitados o destruidos en combate, el resto del enjambre aún pueda lograr su objetivo: **la resiliencia de un enjambre es mucho más elevada que con sistemas independientes**.

Un paso más disruptivo sería disponer (¿en pocos años?) de **enjambres de SALA inteligentes** que durante el desarrollo de una misión **intercambien información en tiempo real entre ellos** y, en función del análisis de los datos recibidos, sean capaces de modificar sus objetivos y estrategia, y hacerlo sin intervención humana o sin que ésta sea significativa en determinados supuestos.

Para los **soldados individuales** también supone un cambio sustancial como refleja el testimonio de un soldado ruso al rendirse (Bondar, 2025): *“En el campo de batalla no vi ni un solo soldado ucraniano. Solo drones”. Los vi (soldados ucranianos) solo cuando me rendí. Solo drones, y hay muchos. Es una guerra de drones*”. El entrenamiento del soldado individual en la defensa ante drones, **incluso la psicológica**, también deberá cambiar.

Dado que los drones totalmente autónomos podrían proporcionar importantes ventajas tácticas, la presión para conseguirlos y emplearlos es muy fuerte. Es una situación que **empieza a producirse en la guerra en Ucrania** y que, progresivamente, penetrará en todos los ejércitos³⁰²; esta evolución ha llevado en 2024 a Ucrania, y posteriormente a Rusia, a crear un **mando de combate específico para sistemas no tripulados** (Bendett y Kirichenko, 2025). Su responsabilidad estriba en integrar estos elementos en el resto de las unidades “más convencionales” y adaptar las tácticas y estrategias a ello.

302 El general Mark Milley, jefe del Estado Mayor Conjunto, ha pronosticado que en los próximos diez o quince años, hasta un tercio del ejército estadounidense podría consistir en sistemas robóticos. Al respecto puede consultarse <https://mwi.westpoint.edu/battlefield-drones-and-the-accelerating-autonomous-arms-race-in-ukraine/>

Como Watling y Reynolds (2025) indican en su análisis de la situación en febrero de 2025, tras tres años de guerra, **ambos bandos han adaptado sus tácticas de protección de posiciones, ataques de artillería, movilidad o aprovisionamiento** de manera rápida en base a la experiencia obtenida con el uso masivo de sistemas no tripulados.

Individualmente, **todas estas innovaciones suponen avances notables en la tecnología de drones, pero no implican por sí mismas una “revolución” táctica y estratégica**. Las revoluciones tecnológicas en asuntos militares requieren algo más que la adopción generalizada de nuevas tecnologías: los ejércitos deben desarrollar nuevos conceptos operativos, integrar nuevas capacidades en sistemas militares más amplios y adaptar su cultura y estructura organizativas; todo eso requiere acumular experiencia y lleva tiempo.

No es sorprendente, por tanto, que existan **dificultades para lograr una revolución efectiva derivada del uso de drones autónomos** a pesar del incremento de informaciones procedentes de los bandos implicados en conflictos militares abiertos afirmando que lo han conseguido; forma parte de la *“niebla informativa”* que acompaña a los conflictos bélicos.

Si bien la mayoría de los drones inicialmente contruidos en Ucrania (más allá de los recibidos de otros países como Turquía, Irán o Estados Unidos) eran **sistemas derivados de drones comerciales**, la tecnología ha madurado y se ha difundido rápidamente entre todos los bandos; con ello, no ha proporcionado una ventaja duradera a ninguna de las partes. Sin embargo, en los más de tres años de guerra transcurridos, se han producido múltiples **ciclos rápidos de diseño y adaptación**, en los que ambos bandos aprendieron el uno del otro, adoptando tácticas y tecnologías utilizadas con éxito para mejorar sus defensas o la precisión y efectividad de los ataques incorporando a múltiples startups con diseños originales.

La consecuencia es que con el desarrollo tecnológico conseguido es posible disponer de una red densa y superpuesta de vehículos aéreos no tripulados. Su impacto es la **“transparencia” del campo de batalla a menos de 3 km de la línea de contacto**, con una densidad de observación decreciente hasta 15 km de profundidad, aunque se puede disponer de capacidades de reconocimiento con fidelidad y latencia razonables hasta 40 km de profundidad. Más allá de este alcance se emplea reconocimiento satelital para determinar las áreas de interés para los UAV de mayor alcance (Watling y Reynolds, 2025).

El uso de sistemas basados en enjambre de drones masivos se ha empezado a considerar por la OTAN como una línea de defensa para defender áreas extensas o proteger fronteras. La **iniciativa denominada Muro de Drones** que se pretende desplegar en la frontera oriental de la OTAN en Europa³⁰³, está diseñada para servir como una **red permanente de alerta temprana y reconocimiento**, especialmente en las zonas vulnerables fronterizas con Rusia. Prevé el despliegue de una capa continua de UAV de reconocimiento impulsados

303 Liderada por Alemania con la participación de seis países de la OTAN (<https://www.huffingtonpost.es/global/arranca-plan-otan-impedir-invasiones-extendiendo-muro-antidrones.html>)

por IA, respaldados por una red de sensores, vigilancia satelital y plataformas móviles de contramedidas que se extenderá desde Noruega hasta Polonia y aprovechará tecnología de vanguardia para defenderse de incursiones y tácticas de guerra no convencionales.

En el horizonte (¿lejano?) dada la aceleración en el desarrollo tecnológico se puede vislumbrar la posibilidad de un **combate entre enjambres de drones de cada bando, sin intervención humana**; la situación asimétrica de un dron de combate neutralizando un dron de observación está al alcance técnico. En todo caso, nos encontramos en los **albores de una nueva era de combate dominada por la IA cuyas consecuencias tecnológicas, operativas, éticas y geopolíticas están aún muy poco definidas**.

Un último factor de riesgo e incertidumbre es la posibilidad de que grandes potencias tecnológicas nucleares combinen el **uso de drones autónomos con armamento nuclear**, ya sean aéreos o submarinos, **para ataques nucleares tácticos**. Rusia, como parte de una estrategia de elevar el tono de la amenaza nuclear en la invasión de Ucrania, parece que lo **está analizando** (Scharre, 2024); se trata de una posibilidad que debe ser considerada seriamente. Situaciones de riesgo similares en el contexto europeo pueden producirse en el mar *Báltico* o en el Ártico en los próximos años.

Finalmente, como puede entreverse en esta sección no es desdeñable el cúmulo de **aspectos éticos relacionados con el uso de SALA para los que la sociedad no tiene aún una respuesta consensuada**. Su análisis, sin embargo, es muy relevante para **determinar sí y cómo deberían emplearse** en el campo de batalla futuro. Su importancia hace que estos aspectos éticos y el marco regulatorio y normativo derivado sean tratados expresamente en el **capítulo 6** de este informe.

5.4 Relevancia de la IA en la guerra híbrida y cognitiva

5.4.1 Concepto y contexto de guerra híbrida

La importancia de la IA no solo ha crecido en **conflictos militares convencionales** entre estados, sino también en **conflictos asimétricos** y, especialmente, en la denominada “**guerra híbrida**”. Sobre la base de la guerra híbrida, en esta sección se analizará su evolución en un concepto ya consagrado en el contexto de la OTAN como es el de “**guerra cognitiva**” con la que se pretende influir sobre la población mediante la construcción de *narrativas colectivas* en temas de interés estratégico, político o militar, y en las tomas de decisión derivadas.

Esta sección caracteriza previamente el concepto de **guerra híbrida**, que es el caldo de cultivo en el que ha crecido el uso y relevancia de la **guerra cognitiva** que se expondrá posteriormente.

La estrategia de utilizar la tecnología disponible para influir en la población objetivo no es nueva, pero lo que no tiene precedentes, y explica la urgente atención que ha alcanzado en el discurso político y de seguridad en Europa, es el **desarrollo y ubicuidad de los medios digitales de comunicación**, cuyo impacto y riesgos como los de ciberseguridad han crecido potenciados **por el uso de la IA** (Lahman, 2024).

Son los medios de comunicación de la sociedad, empleados conscientemente por los gobiernos en sofisticadas campañas de (des)información, apoyadas por ataques cinéticos o ciberataques de forma combinada a los mismos, los que permiten acelerar la toma de decisiones en una determinada dirección con efectos sobre las personas e instituciones. Por tanto, no se trata solo de considerar el impacto de la IA de manera aislada, sino de su **convergencia con otras tecnologías emergentes** (Impiombato *et al.*, 2024).

La rápida adopción de lo que se denominan **“tecnologías persuasivas”** (entendidas como cualquier sistema digital que moldee las actitudes y comportamientos de los usuarios explotando las reacciones o vulnerabilidades fisiológicas y cognitivas) pondrá a prueba la seguridad nacional: *“Las tecnologías persuasivas emergentes, como la inteligencia artificial (IA) generativa, y la neurotecnología interactúan con la mente y el cuerpo humanos de formas mucho más íntimas y subconscientes, y a una velocidad y eficiencia mucho mayores que las tecnologías anteriores”*.

En este contexto, la **guerra híbrida** es un término de creciente relevancia que intenta capturar la complejidad de la guerra del siglo XXI en los que se involucra a una multiplicidad de actores y se difuminan las distinciones tradicionales entre tipos de conflictos armados y entre situaciones de guerra y paz. Responde a una visión perturbadora en la que **el principal campo de batalla está en la mente** por lo que las guerras de nueva generación, además del uso de la panoplia de armas de todo tipo que caracteriza a los conflictos convencionales, dependerán cada vez en mayor medida de la forma en la que interacciona la información con la psicología de los combatientes.

La enorme relevancia que ha adquirido la guerra híbrida lo demuestra los recientes datos procedentes de una investigación realizada por el *Instituto Internacional de Estudios Estratégicos* (IISS) (Voo y Singh, 2025) en el que se han identificado **al menos 134 estados y territorios afectados por operaciones de desinformación e interrupciones de cables submarinos, y al menos 84 que se sabe que están llevando a cabo operaciones cibernéticas** e invirtiendo en cables submarinos, actividades que dan forma de manera proactiva a las capas físicas, lógicas y virtuales del ciberespacio. También el CCN (2024) informa de un incremento en el número de ciberataques en España.

El **origen de la guerra híbrida** es antiguo, y se puede ver ya reflejado en contiendas del siglo XIX. Más recientemente, el concepto fue enunciado formalmente por Thomas Huber (1996), aunque fue Frank Hoffman (2007) quién en su libro *“Conflict in the 21st Century: The Rise*

of *Hybrid Wars*” lo reformula en términos cercanos a la situación actual. Para Hoffman, la **guerra híbrida** puede definirse como la *“combinación en el tiempo y en el espacio de fuerzas convencionales e irregulares, tácticas terroristas, desórdenes criminales y métodos no militares como la guerra cibernética, la desinformación y la coerción económica. Con ella se busca obtener ventajas psicológicas y físicas mediante el uso integrado de herramientas militares y no militares, incluyendo operaciones de información, electrónicas y cibernéticas, así como presión económica y acciones de inteligencia”*³⁰⁴.

Esta definición tan amplia, incluye muchos tipos y niveles distintos de *hibridación*. Algunos autores³⁰⁵ distinguen entre **tres tipos de situaciones “híbridas”** (amenaza, conflicto y guerra) que aluden a una **gradación en intensidad** y en el impacto social e involucración militar que conllevan:

- **Amenaza híbrida (*hybrid threat*):** Fenómeno resultante de la convergencia e interconexión de diferentes elementos que, en conjunto, constituyen una amenaza más compleja y multidimensional. La *“amenaza”* es empleada como elemento de disuasión o de posicionamiento ante procesos negociadores en los que se pretende sacar provecho de la reacción intimidada del contrincante³⁰⁶.
- **Conflicto híbrido (*hybrid conflict*):** Situación en la cual las partes se abstienen del uso abierto de la fuerza (armada) y actúan combinando la intimidación militar (sin llegar a un ataque convencional) y a la explotación de vulnerabilidades económicas, políticas, tecnológicas y diplomáticas mediante acciones planificadas y sincronizadas.
- **Guerra híbrida (*hybrid war*):** Situación en la que un país recurre al uso abierto de la fuerza (armada) contra otro país o contra un actor no estatal, junto al uso de otros medios de coerción (por ejemplo, económicos, políticos o diplomáticos) combinados con operaciones encubiertas o no de menor intensidad.

Otra definición relevante de guerra híbrida, abundando en la ambigüedad, es la procedente del **Centro Europeo de Excelencia para la Lucha contra las Amenazas Híbridas (*Hybrid CoE*)**³⁰⁷, establecido en 2017 en Helsinki conjuntamente por la OTAN y la Unión Europea. El *Hybrid-CoE* describió tales acciones como aquéllas: *“caracterizadas por la ambigüedad, ya que los actores híbridos difuminan las fronteras habituales de la política internacional y operan en las interfaces entre lo externo y lo interno, lo legal y lo ilegal, y la paz y la guerra”*.

304 https://www.marshallcenter.org/sites/default/files/files/2020-05/pC_V10N1_en_Wither.pdf

305 <https://campus-stellae.com/que-son-las-guerras-hibridas/>

306 Un ejemplo clásico es la amenaza del uso del arma nuclear frente a otro país o países que no la poseen como sucede actualmente en el caso de Rusia en la guerra de Ucrania con el fin de impedir a países occidentales de las potenciales consecuencias derivadas de permitir el uso en Ucrania o en la misma Rusia de determinados sistemas de armas.

307 <https://www.hybridcoe.fi/>

Se trata, por tanto, de un **término difícil de interpretar** puesto que los “*umbrales*” de aplicación no están definidos *a priori*, de forma objetiva, sino que varían en el tiempo y dependen del contexto de cada bando en conflicto que permite valorar su gravedad. Además, como señala Ålander (2024) para valorar su impacto sobre la sociedad no debe considerarse únicamente la gravedad de un incidente aislado, sino la **reiteración de decenas o centenares de pequeños incidentes en un breve lapso** afectando a múltiples entidades para detectar la existencia de una guerra híbrida de suficiente entidad. Muchas veces, estas acciones se concentran en una determinada área geográfica.

Un factor básico necesario para que una acción híbrida tenga éxito es la **sincronización y escalada de acciones**, tanto desde una perspectiva de *escalada horizontal* entre diferentes dominios del poder en una sociedad como de *escalada vertical* con diferentes niveles de intensidad y visibilidad de la actuación híbrida en el conjunto de la población. En la figura 5.22 se indican diversos **instrumentos de poder** sobre las que las acciones de guerra híbrida deben sincronizarse para asegurar el éxito: los **militares**, los **políticos**, los **económicos**, los **civiles**, y los de **información**.

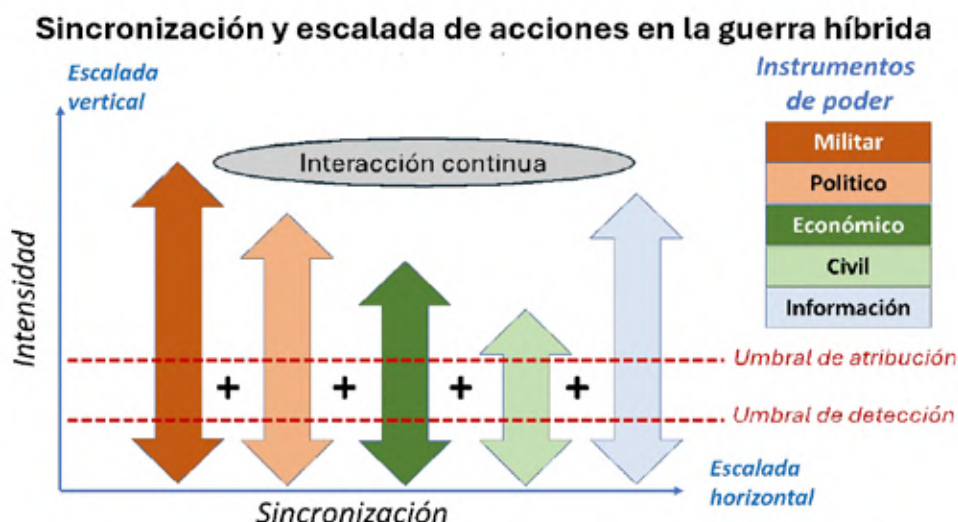


Figura 5.22 Sincronización y escalada de acciones en la guerra híbrida. Fuente. Adaptada de https://assets.publishing.service.gov.uk/media/5a8228a540f0b62305b92caa/dar_mcdc_hybrid_warfare.pdf

Se han representado en la figura dos **umbrales de visibilidad** relevantes para caracterizar con precisión este fenómeno:

- **Umbral de detección:** nivel mínimo de intensidad de la acción híbrida que permite a un gobierno detectar que se está produciendo una amenaza, conflicto o guerra de carácter híbrido; si el umbral se sitúa en un punto demasiado alto, habrá situaciones no detectadas a tiempo, pero si el umbral se sitúa demasiado bajo, todos los eventos serán considerados como parte de la guerra híbrida con el riesgo de saturar los sistemas de respuesta de la

sociedad atacada. Téngase en cuenta que un gobierno puede detectar acciones de guerra híbrida en su contra, pero, no necesariamente, puede desear hacer partícipe de ello a la población en su conjunto con objeto de controlar el nivel de alarma social. También influye en este caso la actividad y posicionamiento de los medios de comunicación.

- **Umbral de atribución:** nivel mínimo de intensidad que permite atribuir de forma convincente (una vez detectado) quién es el actor que la provoca para poder ejercer acciones (como serían las de represalia o de actuación ante organismos internacionales) con solidez y no rebatibles. Este umbral se gestiona de forma dinámica por los actores implicados en relación con su propia estrategia y los datos obtenidos.

La guerra híbrida se desarrolla como un **proceso temporal** en el que el **nivel de escalada** (incremento de la intensidad del conflicto) fluctúa, no es lineal, y se ve salpicado de diversas “crisis” y acciones de “desestabilización” en el transcurso del tiempo. Esta gradación no es una cualidad de la propia guerra híbrida, donde se utilizan medios y recursos de uno u otro dominio a criterio del decisor, sino de una **decisión estratégica sobre el nivel de enfrentamiento que se desea alcanzar con esas acciones** en respuesta al impacto obtenido y la potencial respuesta del adversario. Asimismo, también evolucionan en el proceso las técnicas empleadas.

Debe tenerse en cuenta que, para el actor que provoca una guerra híbrida, o una acción determinada dentro de ella, no siempre es deseable que su acción sea visible, y casi nunca desea que sea atribuible (salvo en el caso de organizaciones terroristas o gobiernos para las que la reivindicación de una acción concreta puede formar parte expresa de su estrategia). Es, de nuevo, un ejemplo del **escenario de borrosidad** imperante y, como tal, se desea preservar por muchos actores implicados³⁰⁸.

Para que la tecnología ligada a la guerra híbrida cumpla sus fines es necesario que se incorpore a las tácticas y estrategias militares **combinando la acción** (no necesariamente armada) **en el máximo número de los cinco dominios militares convencionales** (espacio, cibernético, marítimo, aéreo y terrestre) dentro de campañas híbridas que involucran las dimensiones político-económicas, socioculturales e informativas.

Para el Centro de Excelencia *Hybrid-CoE*, **la tecnología es uno de los principales impulsores de la guerra híbrida y de las teorías de la guerra híbrida**; de hecho, ha sido la rápida evolución de las tecnologías de la información y las comunicaciones (TIC) y, en especial, del uso de algoritmos de IA quien ha estimulado su uso como se demuestra en el caso del Báltico (Praks, 2024). Un análisis realizado en el proyecto *HYFUTEC*³⁰⁹ identificó **19 tecnologías** relevantes:

308 Téngase en cuenta que algunas actuaciones de guerra híbrida se llevan a cabo por actores interpuestos (proxies) y no directamente por los bandos en conflicto.

309 https://www.hybridcoe.fi/wp-content/uploads/2020/09/20200915_HYFUTEC_info.pdf

- Tecnologías orientadas a la **manipulación del acceso radioeléctrico a la información** mediante el uso de técnicas de guerra electrónica para generar interferencias de la señal radioeléctrica, suplantación de identidad u otros ciberataques. En estos casos no se actúa sobre el contenido de la información, sino para impedir que ésta llegue correctamente al destinatario.
- Orientadas a la **manipulación de la información y su narrativa** actuando sobre los servicios ofrecidos por las plataformas digitales (p.ej. interfiriendo en las redes sociales o los accesos a información contenida en la nube mediante cuentas falsas, bots, agentes inteligentes), generando “desinformación” mediante la generación de noticias falsas o tendenciosas. En este caso, sí interesa que llegue información al destinatario, pero alterada en la dirección perseguida por el atacante.
- Uso de **tecnologías emergentes** como las neurotecnologías, sistemas autónomos, realidad extendida (p.ej. realidad virtual, realidad aumentada) o, en un próximo futuro, la interacción de la IA con las tecnologías cuánticas.

En la figura 5.23 se han integrado todos los elementos indicados previamente. Obsérvese la posición de los **dos umbrales de detección y de atribución** señalados previamente cuya posición va a variar en el transcurso del tiempo. Un elemento relevante es la visibilidad que estas acciones tienen en la población no combatiente cuándo, sin frentes geográficos de batalla definidos, **toda la sociedad está en el frente**.

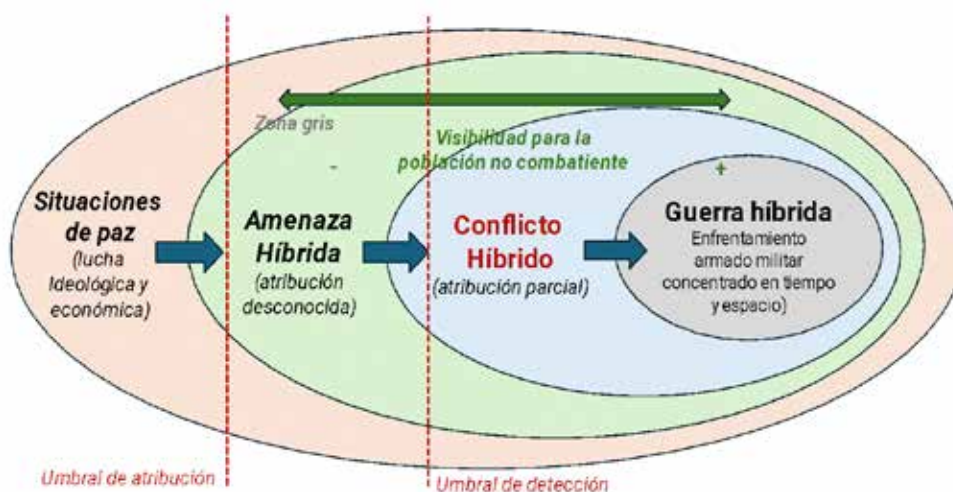


Figura 5.23. Relación entre amenazas, conflictos y guerra híbrida. Fuente: elaboración propia

La **evolución en el tiempo** de la guerra híbrida puede verse, de manera práctica, en la guerra en Ucrania. Se identifican dos fases diferenciadas: en el periodo entre la ocupación de Crimea hasta el ataque general a Ucrania (desde 2014 a 2022) y **después del ataque general** hasta la actualidad (desde 2022 a 2025).

En el periodo que media entre 2014 y antes de la invasión general en febrero de 2022 se produjeron múltiples **acciones típicas de guerra híbrida**, con niveles de detección y de atribución muy cercanos entre sí, que no se consideraron por muchos países occidentales suficientemente graves para actuar de forma decisiva y que, probablemente, alentaron a Rusia a pasar a una segunda fase. Obviamente, si fueron evidentes, graves y persistentes en la población de la zona del Donbas y en otras áreas del sur de Ucrania.

En la **segunda fase (2022-2025)** esta situación da un vuelco significativo al estallar un **conflicto militar convencional** con invasión terrestre en cuatro regiones limítrofes con Rusia, y ataques aéreos en toda Ucrania que se **superpone al conflicto híbrido** limitado en la fase anterior a una parte del territorio de Ucrania (con diferentes niveles de intensidad). En esta segunda fase, el **conflicto híbrido supera el umbral de visibilidad para la población de los países europeos**³¹⁰ y, también el de atribución.

Los **riesgos de escalada como consecuencia de los ataques híbridos** no son siempre fáciles de determinar *a priori*. Como se indica en la figura 5.24 adaptada de Cullen y Reichborn-Kjennerud (2017), un ataque militar de alto impacto en el dominio de la información puede conducir a un efecto de primer orden en los dominios políticos (desestabilización) y económicos (pérdidas empresariales y cambios bruscos en las valoraciones bursátiles) que **pueden conducir a una crisis sistémica**.

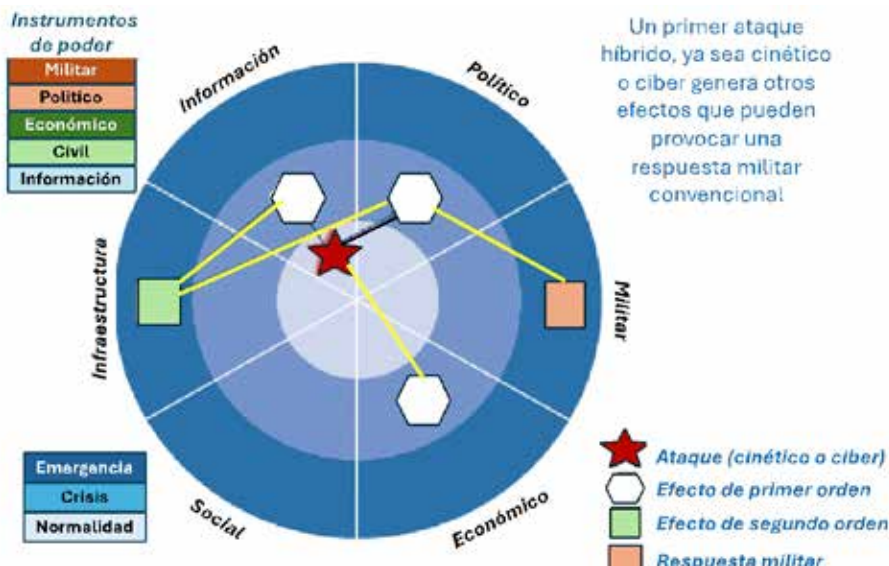


Figura 5.24. Efectos de escalada derivados de un ataque híbrido
Fuente: adaptada de Cullen y Reichborn-Kjennerud (2017).

310 Puede argumentarse que el umbral de visibilidad estaba claramente superado desde 2014 (o, incluso antes) en las zonas ruso-parlantes de Ucrania y obviamente, en el Donbas y Crimea. Sin embargo, para la mayor parte de la ciudadanía de la UE alejada de la zona de conflicto no existía una consciencia clara de que existía una guerra híbrida o que era de muy baja intensidad, y no era necesario preocuparse de ello.

Esta situación también puede conducir a un **efecto de segundo orden en el dominio de la infraestructura de comunicaciones** (p.ej. con interrupción en servicios de internet si se atacan cables submarinos, satélites de comunicaciones u observación, o centros de datos) o **energética** (p.ej. con ataques a los sistemas de control de las redes eléctricas o a las propias subestaciones o a las conducciones de gas o petróleo). A su vez, y **como represalia**, el país atacado puede provocar la adopción de sanciones económicas e, incluso, una **respuesta militar empleando ataques híbridos similares o mediante el empleo de medios convencionales**. El análisis de riesgo de escalada no es sencillo de realizar porque convive con información parcial (en base a datos históricos y de inteligencia) de las posibles reacciones del contrario.

El impacto potencial de estos ataques híbridos se acelera por el **empleo de sistemas automatizados** debido al uso de sistemas de IA capaces de analizar múltiples datos de contexto en un volumen tal que imposibilita su procesamiento por parte de analistas humanos. El uso de la IA en ejercicios de **simulación de negociaciones diplomáticas** parece que tiende también a acelerar la probabilidad de una escalada del conflicto (Rivera *et al.*, 2024)³¹¹.

El proceso de **escalada híbrida** ha venido acompañado de la creación de un discurso elaborado cuidadosamente y mantenido en el tiempo: “**narrativas**” de apoyo a las posiciones de los bandos en conflicto, junto a un incremento y sofisticación de la **desinformación** con la generación de campañas específicas apoyadas por el uso de tecnologías como la IA. Se entra con el uso de la IA en un ámbito de explosión de la capacidad de la “**guerra cognitiva**”, superpuesto a las actuaciones de naturaleza híbrida, cuyas características se abordarán en la siguiente sección.

5.4.2 Concepto de guerra cognitiva

Seguindo la definición de la OTAN³¹², la **Guerra Cognitiva** incluye: “*actividades llevadas a cabo en sincronización con otros instrumentos de poder, para afectar actitudes y comportamientos, influyendo, protegiendo o interrumpiendo la cognición a nivel individual, grupal o poblacional, para obtener una ventaja sobre un adversario. Diseñada para modificar las percepciones de la realidad, la manipulación de toda la sociedad se ha convertido en una nueva norma, y la cognición humana se ha convertido en un ámbito crítico de la guerra.*”

La **guerra cognitiva** supone una **focalización y especialización del proceso de hibridación centrado en el manejo de la información con fines de interés militar** que contará con estrategias, recursos económicos y organizativos, y el uso de herramientas tecnológicas como la IA. Desde una perspectiva militar puede considerarse que el ámbito cognitivo abarca a todos los demás puesto que nada existe si no se pueda percibir o provocar una emoción

311 Según las conclusiones de un estudio publicado de enero de 2024 basados en simulaciones de conflicto empleando cinco grandes modelos de lenguaje, el uso de la IA “tiende a desarrollar una dinámica de carrera armamentística, que conduce a conflictos más importantes y, en casos contados, al despliegue de armas nucleares”. Disponible en línea: <https://www.swissinfo.ch/spa/la-ia-en-la-guerra%3A-un-avance-fulgurante-y-un-control-humano-dudoso/75522183>

312 <https://www.act.nato.int/activities/cognitive-warfare/>

en el receptor. Desde este punto de vista, el ámbito cognitivo abarcaría todos los dominios físicos y electromagnéticos además de los emocionales.

Bebber y Marshal (2024) proponen una **definición de guerra cognitiva en el que el empleo de la tecnología juega un papel predominante**: *“El empleo de la ciencia y la tecnología que altera la cognición dentro de los individuos, grupos y poblaciones, lo que conduce a cambios en la comprensión, la emoción y el comportamiento. Su objetivo es incurrir en una influencia disruptiva de manera propagativa directa o indirecta alterando las sensaciones, percepciones, creencias, patrones de pensamiento, emociones y comportamientos resultantes de individuos y colectivos para desestabilizar y manipular direccionalmente el statu quo sociocultural, ecológico, económico, político y militar y, por lo tanto, permitir la influencia y el poder intencionales”*.

Como **marco de referencia para el análisis**, la figura 5.25 concibe la guerra cognitiva como una **estrategia superpuesta a la hibridación** cuyo objetivo es el dominio de la información para la construcción y difusión de narrativas orientadas a lograr objetivos políticos.

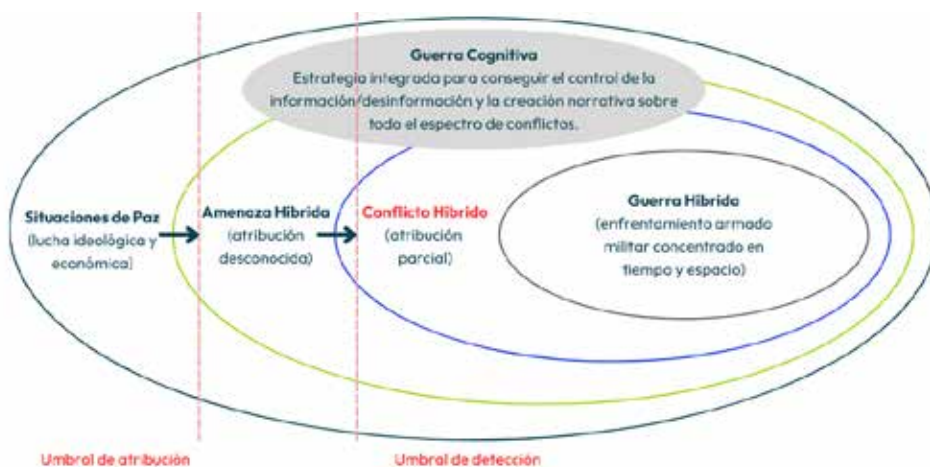


Figura 5.25. Interacción entre amenazas, conflictos y guerra híbrida, y la guerra cognitiva.
Fuente: elaboración propia.

No habría sido posible alcanzar en la situación actual el impacto de la **guerra cognitiva** sin el uso como “arma” de las **redes sociales**, y el lanzamiento (automatizado) de sofisticados **ciberataques** con el **concurso de la IA**. La **forma en la que se aborda**, sin embargo, depende de los objetivos considerados en cada momento.

Un elemento clave para valorar el uso de la guerra cognitiva y la necesidad de defensa es conocer el **impacto real** que este tipo de campañas tiene en Occidente, tanto desde el punto de vista **económico**, relativamente sencillo de estimar, como también, más difícil de estimar, en el **efecto de “desánimo”** o reducción de la moral de combate **de la sociedad** (en el contexto de la “trinidad de Clausewitz” que implica al pueblo, ejército y gobernantes) tras un uso prolongado de este tipo de ataques y de la relativa ineficacia de las contramedidas desarrolladas.

De cara al futuro, la influencia será más relevante cuando la **tecnología implicada para el diseño de estos ataques alcance un nivel mucho mayor de sofisticación con el uso de sistemas de IA** (p.ej. mediante la generación automática de mensajes multimedia personalizados con *bots* empáticos, distorsión de la realidad o generación sintética de la misma, y su difusión masiva en grupos de la población objetivo).

5.4.2.1 Uso del dominio cognitivo en diferentes países

Uso militar por Rusia del dominio cognitivo

Rusia ha prestado creciente atención a la guerra cognitiva tomando como base la **consideración de las redes sociales** como elemento clave para la difusión de mensajes englobados en narrativas a largo plazo. No se trata de un hecho nuevo, pero su relevancia con el incremento de la tensión geopolítica entre grandes potencias es mayor y ha generado preocupación en la Unión Europea y otros países.

En el contexto de la guerra de Ucrania, **Rusia está involucrada en una agresiva campaña de subversión y sabotaje contra objetivos europeos y estadounidenses**, que complementan la guerra convencional en Ucrania con ciberataques y campañas de desinformación. El número de ataques rusos en Europa casi se triplicó entre 2023 y 2024, después de cuadruplicarse entre 2022 y 2023 (Jones 2025a y 2025b). Se trata de *“operaciones subversivas planificadas y llevadas a cabo por el ejército y los servicios de inteligencia rusos para destruir Occidente desde dentro”*³¹³.

La **estrategia de desinformación de Rusia** es bastante sofisticada: desde el diseño de una narrativa apropiada para cada objetivo, al uso de medios de comunicación controlados y convertidos en armas, pero creíbles, con objetivos temporales preidentificados y medición de la reacción. Técnicamente, la forma de operar consiste en **clonar los sitios web de medios de comunicación de renombre, comprando dominios de aspecto similar e imitando su diseño y estilo**. Los artículos falsificados son luego amplificados por cuentas similares a *bots* en redes sociales. Esto permite que su propaganda y desinformación parezcan proceder de fuentes legítimas, y facilitar su aceptación como verídica por el usuario objetivo. Este uso se combina con ciberataques en los que el método preferido ha sido la **denegación de servicio distribuida (DdoS)**³¹⁴.

Además, **el uso de IA** permite abandonar el modelo básico seguido en el pasado, que se podía detectar fácilmente, con correos electrónicos sin editar; actualmente, los correos electrónicos son escritos por algoritmos de IA, con muy buena sintaxis. Y muchas veces con ataques personalizados.

313 <https://www.kew.org.pl/en/2024/11/27/destroy-from-within-russias-cognitive-warfare-on-eu-democracy/>

314 <https://www.state.gov/russias-pillars-of-disinformation-and-propaganda-report/>

La reacción de las sociedades atacadas, si es posible realizar una atribución de responsabilidades supone sancionar de diversas formas a los responsables identificados. El 8 de octubre de 2024, la UE adoptó un **nuevo marco de sanciones contra los responsables de actividades desestabilizadoras contra la UE y sus Estados miembros**³¹⁵. Este nuevo marco permite a la UE actuar sobre personas y entidades que participan en acciones y medidas de Rusia que menoscaban los valores fundamentales de la UE y sus Estados miembros, su seguridad, independencia e integridad, así como las de organizaciones internacionales y terceros países.

A pesar de ello, **los ciberataques rusos a Ucrania no han cesado**. En el último año los ciberataques se han focalizado principalmente en instituciones asociadas a la producción de equipamiento bélico y tecnologías de uso dual, así como en unidades militares, fuerzas de seguridad y gobiernos locales situados en zonas cercanas a la frontera oriental de Ucrania³¹⁶. De igual manera, el gobierno de Ucrania también ha incrementado sus ataques en territorio ruso o en las zonas ocupadas.

Guerra cognitiva en China

En China la guerra cognitiva adopta el término de “**guerra cognitiva algorítmica**”. Su origen, sin embargo, deriva de otras doctrinas militares de China anteriores. La **doctrina de las «Tres Guerras»** (三戰战略), desarrollada por China, constituye una **estrategia integral de influencia y manipulación del entorno informativo**. Se compone de tres elementos fundamentales (Goberna, 2025):

- **Guerra Psicológica** (心理战): Su objetivo principal es socavar la voluntad, cohesión y moral del adversario mediante el uso de propaganda, desinformación y técnicas de manipulación psicológica.
- **Guerra Mediática** (媒体战): Se orienta a controlar la narrativa y el flujo de información tanto a nivel nacional como internacional. Esto se logra a través del dominio de los medios de comunicación, la propaganda y estrategias de relaciones públicas.
- **Guerra Legal** (法律战): Se basa en la utilización y reinterpretación del marco jurídico internacional con el fin de legitimar las propias acciones y deslegitimar las del adversario.

El objetivo de la guerra cognitiva algorítmica de China es **obtener el máximo provecho de la combinación de algoritmos de análisis de datos y de recomendaciones en redes sociales** para influir eficazmente en el comportamiento del individuo. Se apoya en técnicas de segmentación de la información (“granularidad de los datos”) para ejercer una influencia precisa e individualizada.

315 <https://www.consilium.europa.eu/es/policies/sanctions-against-russia/>

316 <https://www.escenariomundial.com/2025/04/07/informe-revela-un-exponencial-aumento-de-los-ciberataques-contra-la-industria-militar-y-de-defensa-de-ucrania/>

La clave de la **visión china de la guerra cognitiva algorítmica** se sustenta en el aprovechamiento intencionado de las enormes cantidades de datos disponibles del comportamiento de personas y entidades (fácil en el contexto de la regulación de datos en china y con centenares de miles de cámaras instaladas en lugares públicos) para entrenar algoritmos de IA que puedan analizar el comportamiento de las personas y comprender sus preferencias, estado mental y relaciones con otras personas de su entorno³¹⁷. Las actividades se **potencian por el uso de herramientas de IA para el análisis de datos personales** que permite la legislación china.

Guerra cognitiva en el contexto de la OTAN

El *Mando Aliado de Transformación de la OTAN* está desarrollando el **Concepto de Guerra Cognitiva** con la contribución directa de más de 20 países miembros de la OTAN, académicos y expertos de la industria³¹⁸. Su objetivo es integrar el dominio de las **operaciones psicológicas** (PSYOPS) con el dominio de la **guerra cognitiva**, buscando la discapacidad cognitiva, mediante la combinación de diversas técnicas desde un enfoque multidisciplinar.

Para la OTAN (Deppe and Schaal, 2024) la guerra cognitiva emerge desde la **relación entre los tres elementos combinados** (véase figura 5.26): **ataques cognitivos** (disrumpir el bucle de decisión, manipular la cognición, las actitudes y el comportamiento), **conflicto bélico** (para conseguir ventaja sobre el adversario, degradar sus capacidades y atacar al vector de la sociedad) y uso de la **tecnología** (madura y emergente).

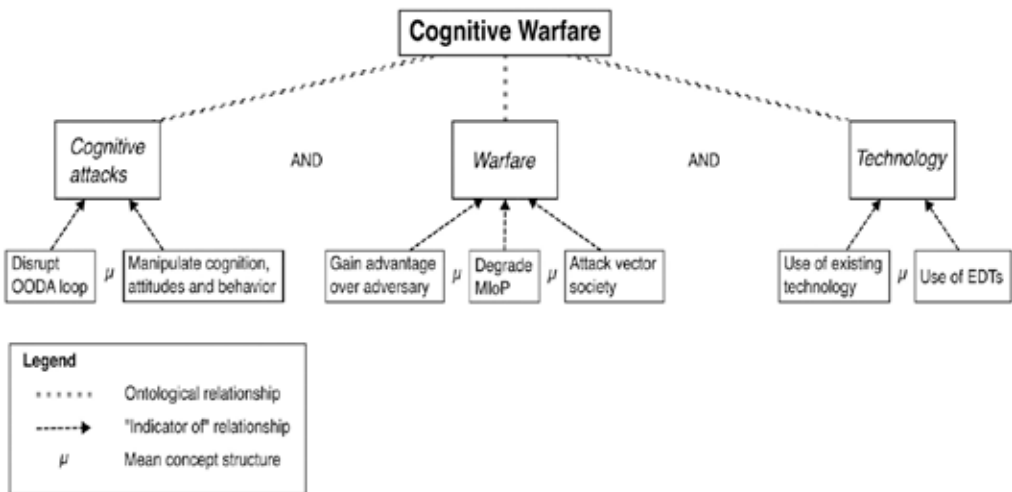


Figura 5.26. Componentes de la guerra cognitiva. Fuente: Deppe and Schaal (2024)

317 <https://scsp222.substack.com/p/algorithmic-cognitive-warfare-the>

318 <https://www.act.nato.int/article/cogwar-concept/>

Para Deppe y Schaal (2024) el mencionado **solape conceptual entre guerra híbrida y cognitiva** sugiere que *“la guerra cognitiva podría integrarse efectivamente como un elemento táctico dentro de estrategias de amenaza híbrida más amplias, mejorando así la profundidad analítica y la comprensión de los efectos híbridos al situar las operaciones cognitivas dentro de un contexto establecido y multifacético”*.

Una vez descritos los elementos conceptuales que caracterizan a la guerra cognitiva en el contexto de conflictos y guerras híbridas, y advertidos de sus efectos perniciosos sobre la sociedad, es necesario que unidades especializadas de los gobiernos responsables de las mismas dispongan de **un modelo integrado de defensa cognitiva** que permita integrar todas las actuaciones necesarias para su defensa y neutralización.

5.4.3 Evolución de la guerra cognitiva

5.4.3.1 Modelos de guerra cognitiva

Un **modelo de guerra cognitiva debe estar centrado en la cognición** a la que se subordinan las actuaciones físicas en el terreno, y sobre los sistemas de información ligados a la **difusión de narrativas** en el dominio cognitivo a nivel nacional e internacional. La dificultad subyace en el elevado número de conceptos a tener en cuenta y sus complejas interacciones.

Para abordarlo de forma sistémica, Bebbler y Marshal (2024) han elaborado una **ontología de la guerra cognitiva**, entendido como un sistema formal para organizar el conocimiento sobre este tema, construido en base a **cinco dimensiones instrumentales**:

- **Herramientas que explotan los sesgos cognitivos y la percepción:** Estas amenazas manipulan los sesgos cognitivos y las vulnerabilidades perceptivas de las personas para dar forma a sus opiniones y comportamientos.
- **Herramientas relacionadas con la neurociencia y la biología:** Los adversarios aprovechan los avances en neurociencia y biología para influir y controlar los procesos cognitivos de los individuos.
- **Herramientas que explotan la psicología social y la dinámica de grupo:** Los adversarios aprovechan la psicología social y la dinámica de grupo para manipular el comportamiento del grupo, crear polarización o influir en la toma de decisiones colectivas.
- **Herramientas que emplean aplicaciones tecno-sociales:** Los adversarios utilizan la tecnología de la información para difundir narrativas, participar en ingeniería social y realizar operaciones de información.

- **Herramientas relacionadas con la tecnología de la información:** La tecnología de la información proporciona herramientas para los ciberataques, las campañas de desinformación y la interrupción de infraestructuras críticas.

Gran parte de la relevancia que ha adquirido la guerra cognitiva en los últimos años procede del reconocimiento de que **en las cinco dimensiones citadas se están produciendo avances tecnológicos muy rápidos que alimentan la capacidad de integrar su uso en procesos específicos muy elaborados de guerra cognitiva.**

El enfoque seguido por la UE se basa en el **fortalecimiento de un ecosistema de resiliencia integral** basado en promover el esfuerzo intersectorial de toda la sociedad aprovechando las interrelaciones cruciales entre temas que, a menudo, se abordan por separado. La idea subyacente es que es necesario crear un **“ecosistema de lucha contra la guerra híbrida”** que implique la coordinación y el intercambio de información entre diferentes tipos de actores. Con ello se pretende **aumentar la resiliencia contra las amenazas híbridas** incluyendo la anticipación a los objetivos estratégicos del adversario (Jungwirth *et al.*, 2023)

Los **elementos básicos de este modelo** son: **espacio cívico, espacio de servicios y espacio de gobernanza**, con tres capas de actuación en cada uno de ellos: local, nacional e internacional. En los espacios citados se identifican unos **“dominios” de actuación** que actúan de puntos de entrada o “escudos” contra las herramientas híbridas con el fin de **incrementar la resiliencia de la sociedad** (véase figura 5.27).

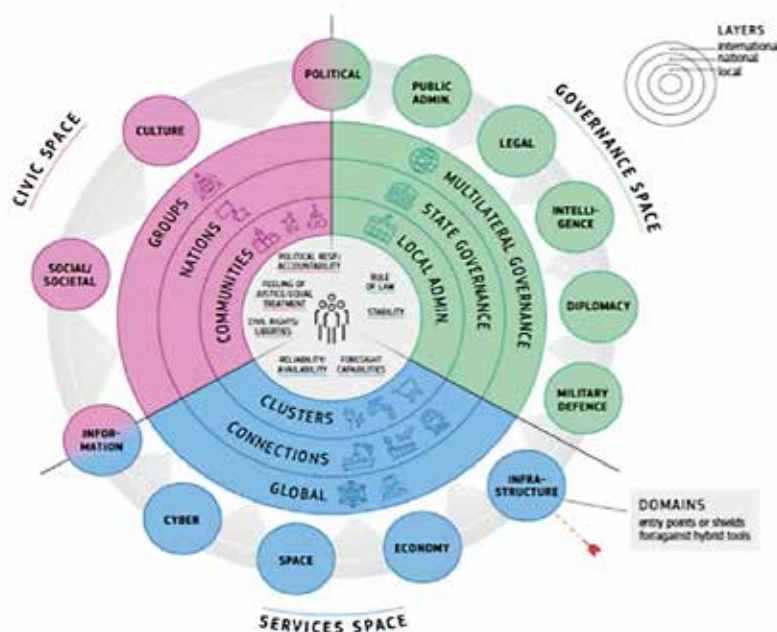


Figura 5.27. Fuente: https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf

Las **interconexiones entre dominios son cruciales para desarrollar la resiliencia frente a las amenazas híbridas**. A medida que los efectos de las amenazas híbridas puedan extenderse a través de dominios, es necesario interrumpir su propagación y contener los efectos. Esto no significa que los dominios deben estar desconectados, sino que las conexiones entre ellos deben ser resilientes.

5.4.3.2 Guerra informativa: desinformación

Un elemento básico para implementar la guerra cognitiva es el de la **desinformación**. Se trata de un **fenómeno social complejo** en el que, si bien las tecnologías juegan un papel relevante, no pueden limitar una concepción limitada de la desinformación.

El éxito de las **operaciones de influencia basadas en la desinformación** depende del cumplimiento de tres condiciones principales. En primer lugar, deben producir **narrativas** que transmitan de manera efectiva y persuasiva el mensaje diseñado para un objetivo concreto; en segundo lugar, deben ser capaces de **difundir ese mensaje** a un público objetivo lo suficientemente amplio como para influir en las decisiones políticas a nivel nacional o institucional; y, en tercer lugar, deben **persuadir** a una proporción suficiente de personas de la veracidad y relevancia de ese mensaje para que sus comportamientos generen una cadena de reacciones que logren el objetivo pretendido.

Una forma de reducir el impacto es considerar el **entrelazamiento de las dimensiones social, económica y estratégica como una característica definitoria de los fenómenos de desinformación**. Esas tres dimensiones de la desinformación convergen en torno a la naturaleza intencional de la desinformación: se trata de procesos planificados de carácter estratégico que buscan efectos concretos en el marco de las dinámicas de influencia social (Aguado *et al.*, 2024).

El **incremento de la desinformación**, apoyado y potenciado por el desarrollo de la IA, ha penetrado en gobiernos, instituciones y ciudadanos con un **efecto desestabilizador** al generar una duda persistente sobre la veracidad del mensaje. La **Asamblea General de las Naciones Unidas** ha expresado su preocupación por la proliferación de la desinformación y requiere promover la **cooperación internacional en la lucha contra la desinformación**.

El informe del Secretario General de la ONU de agosto de 2022 titulado *“Contrarrestar la desinformación para promover y proteger los derechos humanos y las libertades fundamentales”* (ONU, 2022) reclama esa **cooperación internacional**, al mismo tiempo que requiere preservar derechos y libertades esenciales del ser humano; equilibrio difícil de conseguir. Supone un cambio de actitud de las Naciones Unidas frente a una interpretación habitual de prohibir el uso de la “fuerza” solo cuando se trata de acciones con “efectos cinéticos” para extender el ámbito de actuación a otros supuestos de desinformación (Bernal *et al.*, 2020).

La oportunidad de lanzamiento de campañas de desinformación puede ser múltiple, pero es habitual que se intensifiquen en periodos electorales con el objetivo de **influir en los resultados de la votación** mediante el empleo de herramientas de control del acceso a la información y su difusión hacia el votante. En todo caso, no se plantean para poner el énfasis en las campañas electorales cuando sus límites temporales se extienden mucho más que los periodos establecidos y, sobre todo, porque los estados de ánimo del potencial votante y las propuestas políticas de los candidatos no se construyen solo en campaña.

Debe tenerse en cuenta que **con el uso de acciones de desinformación no se busca convencer al adversario: lo que se pretende es confundir**; es decir, crear un estado de confusión en la sociedad que le impida tomar las decisiones correctas.

En una de las **medidas propuestas por el Parlamento Europeo** se propone: *“contrarrestar con rapidez y firmeza la desinformación y la manipulación de la información y las injerencias extranjeras por parte de Rusia a fin de proteger la integridad de sus procesos democráticos y reforzar la resiliencia de las sociedades europeas, entre otras cosas promoviendo activamente la alfabetización mediática..., así como apoyando la investigación sobre las nuevas tecnologías de influencia híbrida”*.

Existe una considerable superposición conceptual entre la guerra cognitiva y conceptos próximos como son la **Manipulación e Interferencia de Información Extranjera** (*Foreign Information Manipulation and Interference, FIMI*), las amenazas híbridas, el conflicto híbrido, y, finalmente, la guerra híbrida. El *Servicio Exterior de la UE* (EEAS) define el **FIMI**³¹⁹ como *“un patrón de comportamiento que amenaza o tiene el potencial de afectar negativamente a los valores, procedimientos y procesos políticos”*. Dicha actividad es de carácter manipulador, llevada a cabo de manera intencional y coordinada. Los actores de dicha actividad pueden ser actores estatales o no estatales, incluidos sus representantes dentro y fuera de su propio territorio.

El EEAS informó en enero de 2024 (EEAS, 2024)³²⁰ de **750 incidentes FIMI** desde enero a noviembre de 2023 en casi cincuenta países. El 3º informe de marzo de 2025 sobre FIMI (EEAS, 2025) informa que **los incidentes de 2024 fueron 505 implicando 38.000 canales diferentes** (solo la red social X supuso el canal elegido en el 88% de los casos) **en 90 países** (la mitad de ellos ataques contra Ucrania). Como resultado de estos análisis, el 15 de julio de 2025, el Consejo, siguiendo otras decisiones similares con anterioridad, decidió imponer medidas restrictivas adicionales contra nueve personas y seis entidades responsables de acciones desestabilizadoras de Rusia en el extranjero, incluidas las relacionadas con FIMI³²¹.

319 https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en

320 https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

321 https://www.eeas.europa.eu/delegations/ukraine/russian-hybrid-threats-eu-lists-nine-individuals-and-six-entities-responsible-destabilising-actions_en

Como **estrategia de la UE para defenderse contra la desinformación** se han creado estructuras especializadas como el **Sistema de Alerta Rápida (SAR)** para permitir actividades conjuntas con otras instituciones de la UE y los Estados miembros. El objetivo es desarrollar un marco y una metodología integral para la recopilación sistemática de pruebas de incidentes FIMI facilitada por un *Centro de Análisis e Intercambio de Información* (FIMI ISAC). El conjunto de medidas puestas a disposición de los Estados miembros de la UE para defenderse de este tipo de incidentes de interferencia externa (*FIMI toolbox*) es muy amplia. El objetivo es **incrementar la resiliencia de la sociedad europea frente a la interferencia externa procedente de otros gobiernos** facilitando el intercambio rápido de información y el aprendizaje mutuo.

5.4.4 Relevancia de la IA en la generación y lucha contra la desinformación en la guerra cognitiva

5.4.4.1 Evolución tecnológica de la guerra cognitiva

Actualmente, el **dominio de las plataformas tecnológicas digitales potenciadas por la IA** forma parte de las estrategias de las grandes potencias tecnológicas para **influir en la opinión pública** en todo el mundo; sobre todo, aprovechando la enorme difusión y uso de las **redes sociales** y el impacto de la opinión de determinadas entidades y personas conocidas como “*influencers*”, con millones de *seguidores* en las mismas. Desde el punto de vista de **interés político**, el procesamiento de esta información personal también permite **analizar o introducir sesgos** hacia determinadas ideologías, partidos políticos, miembros del gobierno, representantes o candidatos en elecciones actuando sobre determinados estratos de la población.

Concretamente, la IA ha permitido incrementar y automatizar las campañas de manipulación y desinformación alcanzando un nivel más elevado de sofisticación e impacto potencial³²². La irrupción de la **IA generativa**, combinada con el aprendizaje automático y su capacidad de “*aprender*” de la interacción con sus interlocutores, permite **crear contenido altamente realista**, con el que llegar de manera personalizada a individuos dentro de un público objetivo de manera eficiente y efectiva mediante la generación de indicaciones automatizadas en el momento adecuado, con **poca intervención humana**, logrando una **mayor verosimilitud del mensaje**.

Específicamente, herramientas especializadas de IA han permitido crear automáticamente **campañas de desinformación con realidades sintéticas** difíciles de contrarrestar. De hecho, con las nuevas herramientas de **IA generativa multimodal** es difícil conocer si una infor-

322 <https://www.ie.edu/university/news-events/news/deceptive-use-ai-technology-is-turning-mind-main-battlefield-21st-century-according-ie-university/>

mación (texto, datos, video, imágenes, etc.) es real o ha sido creada de forma sintética o manipulada a no ser que se empleen herramientas especializadas.

La **IA generativa multimodal** (clonando no solo la imagen, sino también la voz en videos hiperrealistas) se combina con otro tipo de herramientas como la **realidad virtual** (con la generación de modelos realistas 3D) para permitir ataques cognitivos basados en un área creciente como es la **manipulación emocional** aprovechando los **entornos de realidad virtual** (*Virtual Reality Environment, VRE*); experimentos y estudios de casos de psicoterapia han demostrado la capacidad de los VRE para inducir emociones negativas como el miedo o la ansiedad, haciendo que una determinada persona esté más predispuesta o susceptible a aceptar falsos rumores o teorías de conspiración (Fenstermacher *et al.*, 2023).

En imágenes relacionadas con **conflictos bélicos**, las falsificaciones se diseñan expresamente para provocar una **fuerte reacción emocional** en su receptor (p.ej. al incluir los cuerpos de bebés, niños o familias). En la figura 5.28 se pueden ver tres ejemplos analizados como **noticias falsas ligadas a la guerra de Israel con Hamas en Gaza**.



Figura 5.28. Imágenes manipuladas por IA. Fuente: <https://www.dw.com/en/fact-check-ai-generated-images-of-children-in-gaza/a-68146699>

En experimentos realizados en la Universidad Complutense de Madrid (García-Huete *et al.*, 2025) se ha evaluado la capacidad efectiva de persuasión de la IA generativa capaz de crear mediante patrones y algoritmos imágenes bélicas. La idea es añadir herramientas automatizadas de detección para evaluar la capacidad de los sistemas actuales de identificar la generación (es decir, la no autenticidad) de esas imágenes. Se aplicaron técnicas *LUT* (*Look Up Tables*) a las imágenes para incrementar su realismo, hasta un punto en que puedan ser percibidas como auténticas, lo que podría contribuir a campañas de *fake news* para aumentar su realismo percibido. Este enfoque ayudará a evaluar de forma efectiva el

potencial de la IA Generativa en la aplicación de manipular a la población, y a contribuir al debate sobre las implicaciones éticas de la IA generativa en el campo de la desinformación³²³.

Esta tendencia se consolida con el concepto de **corporeización de los dispositivos inteligentes** (que acompañan de forma continua a los usuarios) y de la **transparencia creciente de las interfaces**, que las hace menos intrusivas y, por lo tanto, más naturales.

En la edición de la feria CES de 2025 la empresa coreana *LG Electronics* presentó su visión de **“Inteligencia Afectuosa”** (*Affectionate Intelligence*), donde las tecnologías de IA se integran de manera más humana y personalizada en la vida de los usuarios mediante sistemas de IA capaces de generar conexiones más humanas, **adaptándose a las emociones, necesidades y preferencias de los usuarios**³²⁴. Su uso en aplicaciones duales podría ser relevante en el futuro.

La tentación de **actuar sobre la regulación** para evitar estos casos de abuso de la buena intención es evidente, aunque ello implique efectos secundarios negativos sobre el proceso de innovación. Sin la existencia de **robustas salvaguardas legislativas** los sistemas de IA pueden hacer que la censura, vigilancia y expansión de la desinformación sea más rápida, barata y efectiva. **La guerra cognitiva establece un campo de batalla compartido entre diferentes unidades gubernamentales**. A medida que se difuminan las líneas entre el conflicto militar tradicional y las operaciones de información, es esencial una colaboración más estrecha entre los actores implicados (órganos de Inteligencia, y órganos de cooperación internacional).

La respuesta legislativa cambia significativamente de un país a otro. Los casos de la UE limitando el uso de cámaras para reconocimiento facial en sus regulaciones digitales se contraponen al de China y otros muchos países de Asia u Oriente Medio, o el mismo Reino Unido (Londres es la quinta ciudad con más cámaras por habitante), permitiéndolos en gran medida, responden a respuestas legislativas muy diferentes en las que asegurar la privacidad es un valor básico, por encima de la seguridad (caso de la UE³²⁵) o al revés (caso de China).

La legislación contra la desinformación varía en función de la **ideología** del gobierno, de la **extensión y conocimiento de la población** sobre estas técnicas, y del grado de aceptación de **medidas coercitivas** por la sociedad. En conjunto, deberá responder a la percepción del

323 García-Huete, E. et al. (2025). IA generativa y sistemas serverless en desinformación bélica con LUTs: impacto y ética. Documento de Opinión IEEE 45/2025. Disponible en línea: IA generativa y sistemas serverless en desinformación bélica con LUTs: impacto y ética - CESEDEN

324 Un ejemplo destacado fue la integración de la tecnología de “inteligencia afectuosa” en los televisores OLED de próxima generación de LG, que ofrecen recomendaciones de contenido basadas en el estado de ánimo detectado por sensores biométricos y cámaras especializadas. <https://www.altaidigital.co/post/lg-nos-muestra-su-affectionate-intelligence>

325 La Ley de IA de la UE restringe la creación de noticias falsas al exigir a quienes utilizan sistemas de IA para generar o manipular contenidos (ya sean imágenes, audio o vídeo) la obligatoriedad de indicar si esos contenidos han sido creados o modificados artificialmente.

equilibrio entre libertad y seguridad presente en cada sociedad; factor que evoluciona en el tiempo de acuerdo con el contexto de seguridad.

El uso de **herramientas de IA** ofrece mejoras a diferentes actores implicados en la guerra cognitiva para conseguir el efecto deseado. Con un poco más de detalle:

- El contenido que se publica y comparte se puede analizar mediante técnicas de IA como el **procesamiento del lenguaje natural (NLP)**.
- Varias herramientas de clasificación, como los bosques de decisión y las redes neuronales LSTM, facilitan la **traducción automática**.
- La **tecnología de grafos** aprovecha el potencial de la IA para analizar las relaciones entre puntos de datos.
- Los sistemas de aprendizaje automático pueden crear herramientas para **detectar imágenes que han sido manipuladas**, por ejemplo, buscando rastros dejados por los sistemas utilizados para capturar imágenes alteradas.
- Las aplicaciones de IA también pueden ser entrenadas para **detectar desinformación en las redes sociales** y emitir advertencias. Al analizar bloques de datos procedentes de intercambios en redes como *Twitter* y *Telegram*, las IA pueden reconocer elementos estilísticos típicos de las noticias falsas.
- También pueden ser entrenados para **identificar contenido potencialmente problemático** y ayudar a los operadores a comprender por qué se ha marcado.

En el futuro, la IA se combinará con **realidad aumentada (RA)**, **realidad virtual (RV)**, **interfaces cerebro ordenador (BCI)**, y el análisis de los datos neuronales que genera su uso. Ello puede permitir a actores maliciosos **hackear la “realidad” que nos rodea**, nuestros estados de ánimo y reacciones, y con ello dar forma a nuestro comportamiento en las direcciones buscadas por los atacantes.

5.4.4.2 Impacto de la IA en la generación de desinformación

Ante el hecho de que la **construcción y difusión de narrativas** alimenta el proceso de deliberación y realimenta las posiciones de partida, la forma de crear las narrativas ha adquirido gran importancia. El **factor habilitador** procede del uso de la IA en la que los argumentos individuales se ven enmascarados por elementos de **desinformación generados automáticamente por herramientas de IA** (Pawels, 2024) en los siguientes pasos:

- **Fase 1. Elección de un tema de interés** (político o social) en una sociedad que justifique el desarrollo de una campaña de desinformación basada en una “narrativa” que pueda ser construida para el fin deseado.
- **Fase 2. Generación de información susceptible de crear opinión en redes sociales** mediante la creación automática de cuentas falsas en números significativos, generación de contenido multimedia “creíble” multilingüe, difusión del contenido y generación de respuestas en cadena, uso de “influencers”, repercusión en medios, y monitorización de “tendencias” (difusión geográfica y persistencia en el tiempo).
- **Fase 3. Provocación de respuesta política** que refuercen o contradigan la narrativa creada. Esta respuesta puede ir dirigida a gobiernos (amigos y enemigos), organizaciones multilaterales con posiciones oficiales, y grupos de oposición política.
- **Fase 4. Impacto físico en el terreno** por parte de la población con manifestaciones de repulsa o atentados terroristas.

En la tabla 5.1 puede verse esta relevancia en términos de **argumentación para el uso de la IA y su efecto**.

De igual manera que la IA alimenta la desinformación, también puede emplearse para luchar contra ella basado en la **comprobación automática de la veracidad de determinada información**.

Se puede decir que **los modelos de IA generativa son un intento innovador de hacer frente a las noticias falsas**, ya que presentan herramientas complementarias a las disponibles actualmente (Nayuni, 2024). Aprovechando la capacidad de los modelos de procesamiento de datos en lenguaje natural, aprendizaje automático y generación de datos sintéticos, **los modelos podrían ayudar en el futuro a la identificación de información falsa y fraudulenta**. Para ello, es necesario reducir los sesgos introducidos en los procesos de entrenamiento que sigue siendo un problema no resuelto.

Estas tecnologías analizan la estructura, semántica y fuentes de las noticias, comparándolas con bases de datos verificadas para identificar patrones de desinformación. Existen actualmente diversas herramientas de IA para **determinar si una “frase”** (mensaje en los medios) **está respaldada por hechos para considerarla veraz** (un hecho es una sentencia que puede ser verificada, una opinión no es un hecho). Un requisito previo es disponer de conjuntos de datos como **LIAR**³²⁶ que proporcionan **datos etiquetados para entrenar modelos de IA, lo que permite un mejor rendimiento en la identificación de noticias falsas**

326 <https://www.kaggle.com/code/hendrixwilsonj/liar-data-analysis>

en diversas plataformas. En la tabla 5.1 se resume la justificación y situación actual en el uso de las diversas herramientas.

Argumento	Explicación	Efecto
Incremento del volumen de desinformación	Debido a la facilidad de acceso y uso, la IA generativa puede emplearse para crear información falsa a gran escala sin coste para individuos y actores organizados.	Un volumen mayor de desinformación permite a actores mal intencionados inundar una zona con información incorrecta sembrando confusión.
Incremento de la calidad de desinformación	Debido a sus capacidades técnicas y facilidad de uso las herramientas de IA generativa pueden usarse para crear información falsa de mayor calidad.	Una desinformación de mayor calidad tiene un mayor potencial persuasivo más difícil de detectar y verificar que provocaría una "crisis epistémica" y pérdida de confianza
Incremento de la personalización de la desinformación	Debido a sus capacidades técnicas y facilidad de uso las herramientas de IA generativa pueden usarse desinformación de alta calidad personalizada a los gustos y preferencias del usuario.	Generación de una mayor persuasión en los consumidores de la desinformación, con resultados similares al de la calidad y con fortalecimiento de la pertenencia al grupo.
Generación involuntaria de información falsa, pero plausible	La IA generativa puede generar contenido útil, pero también información plausible pero inexacta sin pretenderlo, contribuyendo así a generar y difundir desinformación potencialmente dañina.	Usuarios de desinformación generada por herramientas de IA generativa y potencialmente con los que compartan la información sin ser conscientes.

Tabla 5.1. Argumentos y efectos del uso de herramientas para la desinformación.
Fuente: elaboración propia.

En general, los **servicios de verificación de hechos e imágenes** proporcionan una aplicación móvil y una extensión del navegador que ofrece, combinando IA y verificadores humanos una evaluación de la confianza en la veracidad de la información. Las herramientas denominadas “**verificadores de datos**” leen un documento e identifican y extraen todo el contenido que necesita verificación de hechos (Gutiérrez-Caneda y Vázquez-Herrero, 2024). Las herramientas analizan afirmaciones, opiniones y eventos, monitorizando en tiempo real más de un millón de dominios web y plataformas de redes sociales para evaluar la veracidad de la información.

Un ejemplo de este tipo de herramientas es **Logically**. Otra herramienta de verificación de datos automatizada es **ClaimBuster**³²⁷. Esta herramienta se basa en el **procesamiento del lenguaje natural y el aprendizaje supervisado** (basado en un conjunto de datos codificado por humanos) para identificar información fáctica y falsa. Las herramientas de **FactCheck.org**³²⁸ integran el aprendizaje automático con el análisis de redes sociales para rastrear las tendencias de desinformación. Una herramienta de este tipo es la proporcionada por

327 Logically (<https://logically.ai/>); ClaimBuster (<https://idir.uta.edu/claimbuster/>)
328 <https://www.factcheck.org/>

Google (*Google Fact Check Explorer*)³²⁹ y sobre las que empresas de distribución de noticias (agencias) han elaborado sus propios verificadores automáticos.

También los gobiernos han puesto en marcha **plataforma específicas para combatir las noticias falsas y la desinformación**. Israel ha creado la herramienta **Stand4Israel** (<https://stand4israel.net/>) para recopilar “la verdad oficial del gobierno” sobre eventos sucedidos en Israel, obtenida directamente de medios de comunicación oficiales que contrarresten otros externos.

Asimismo, empresas startups como **AdVerif.ai** emplean algoritmos que detectan inconsistencias entre titulares y contenido, generando **informes detallados sobre la probabilidad de falsedad**³³⁰. Su algoritmo actúa en varias fases:

- **Detección de irregularidades en el contenido:** Escanea titulares y cuerpos de texto para identificar inconsistencias, como titulares que no coinciden con el contenido, uso excesivo de mayúsculas o lenguaje emocional.
- **Verificación en bases de datos:** Contrasta las noticias con una base de datos que incluye miles de publicaciones legítimas y falsas, actualizada semanalmente, para identificar patrones o coincidencias.
- **Generación de informes:** Proporciona a los clientes un informe con una puntuación que indica la probabilidad de que el contenido sea falso o problemático.
- **Reconocimiento avanzado:** Puede identificar sátiras, analizar tendencias políticas del medio y detectar incongruencias en perfiles sociales, como cuentas automatizadas o “bots”.

Agencias en España como *Newtral*, y *Maldita.es* son miembros de la *International Fact Checking Network*³³¹ y siguen estándares internacionales para garantizar el máximo rigor en sus verificaciones³³². También la agencia EFE³³³ y RTVE emplean herramientas de este estilo³³⁴. El riesgo es que algunas de estas agencias se conviertan en auditores de la competencia y en supuestas garantías de fiabilidad de los medios afines. De hecho, *Newtral* se ha convertido en una fuente de noticias por sí misma con el riesgo en casos muy polarizados ideológicamente de actuar de juez y parte o percibirse como tal.

329 <https://newsinitiative.withgoogle.com/es-es/resources/trainings/google-fact-check-tools/>

330 https://clubinterprensa.org/una-ia-capaz-de-detectar-fake-news/?utm_source=perplexity

331 Lanzada en 2025 por el Instituto Poynter agrupa a 170 organizaciones comprobación de hechos de todo el mundo <https://www.poynter.org/ifcn/>

332 https://www.ttandem.com/blog/contenidos-asi-funcionan-los-verificadores-de-noticias/?utm_source=perplexity

333 EFE Verifica https://verifica.efe.com/?t&utm_source=perplexity

334 Herramientas como el proyecto IVERES (“Identificación, Verificación y Respuesta. El estado democrático ante el reto de la desinformación interesada”) implementado por RTVE, utiliza la IA para analizar textos, imágenes y audios, evaluando su autenticidad en tiempo real <https://rubik-audiovisual.com/tecnologia-para-la-lucha-contra-la-desinformacion-y-la-discriminacion/>

Aunque la IA generativa es una fuente de noticias falsas, también parece prometedora para su detección. La eficiencia está ligada a la **mejora gradual de las tecnologías de IA multimodal** (con imágenes, voz, audios, videos, etc.), a la forma de abordar cuestiones éticas y a la evolución de la regulación para hacerlas más útiles y facilitar su adopción, en lugar de ser un sustituto de las prácticas tradicionales de verificación manual.

5.4.5 Análisis de sentimientos con herramientas de IA

Valorar el impacto de un determinado documento como factor de influencia en la sociedad, más allá de su veracidad, es un factor de creciente relevancia. Un enfoque basado en IA empleado para ello es el **análisis de sentimientos**³³⁵: se refiere al proceso de analizar grandes volúmenes de texto para determinar si expresa un sentimiento positivo, un sentimiento negativo o un sentimiento neutro, o estados de ánimo sobre algún ámbito tratado en el documento.

La clasificación de sentimientos ha evolucionado para proporcionar **análisis de sintaxis multilingüe o análisis de entidades**. Se trata de una aplicación de la IA en el campo del **procesamiento del lenguaje natural (PLN)** empleada para clasificar un texto en varios tipos de “*sentimientos*”, como positivos o negativos, felices, tristes o neutros.

Las soluciones de análisis de sentimiento **combinan técnicas de aprendizaje automático, procesamiento de lenguaje natural y estadísticas avanzadas** integrados en sistemas multiagente inteligentes para mejorar las experiencias de los usuarios. El desarrollo de técnicas de IA generativa multimodal permite extender y complementar este uso de texto escrito a la **voz** (teniendo en cuenta parámetros vocales como el tono y la modulación) y al lenguaje corporal en el caso de **videos** (movimiento de las manos, ojos, sudoración, etc.); factores que no son posibles de obtener con técnicas de procesamiento de lenguaje natural.

Actualmente, **existen varios paquetes de software de análisis de sentimientos** con interfaces de aplicación para el usuario (*Application Interface, API*), como *Google Cloud Natural Language API*, *Microsoft Azure Text Analytics API* o *Lexalytics Saliency*³³⁶ que se pueden personalizar para la investigación de mercado, la gestión de marcas y el análisis de productos/servicios. Otro ejemplo es *IBM watsonx Assistant*³³⁷, plataforma de inteligencia artificial conversacional impulsada por modelos de lenguaje de gran tamaño (LLM) que permite a las organizaciones usuarias crear agentes de voz y chatbots con IA con el que ofrecer soporte de autoservicio automatizado en una interfaz conversacional.

335 <https://www.ibm.com/es-es/topics/sentiment-analysis>

336 <https://www.lexalytics.com/saliency/>

337 <https://www.ibm.com/es-es/products/watsonx-assistant>

El uso de análisis de sentimientos en el marco de la guerra cognitiva plantea **preocupaciones éticas si se combina con técnicas de manipulación de los sentimientos**, de difusión de desinformación o tácticas psicológicas para influir en las creencias y comportamientos de las personas, y, específicamente, del personal militar. Conceptualmente, estas prácticas pueden afectar negativamente a las personas, las sociedades y los procesos democráticos, pero también a la **capacidad de resistencia** frente a adversarios³³⁸.

5.4.6 Uso de la IA en la negociación de conflictos militares

La emergencia de la IA generativa y el uso de agentes inteligentes permite a los gobiernos su **integración en la toma de decisiones relativas a conflictos militares y de política exterior** de alto riesgo favoreciendo el análisis de escenarios en los que se analizan opciones entre diferentes “bandos”. Especialmente, la aparición de modelos avanzados de IA generativa en los “juegos de guerra” (escenarios simulados de conflictos) permite analizar la **dinámica de los procesos de escalada**.

Varias empresas en Estados Unidos, entre ellas *Palantir Technologies Inc.* y *Anduril Industries Inc.* están desarrollando plataformas de decisión basadas en IA por lo que es muy importante conocer cómo los sistemas de IA generativa responden a diversas situaciones y si sus respuestas están polarizadas por el modelo de lenguaje (LLM) empleado. Dadas las diferencias existentes entre distintos sistemas de IA generativa es necesario analizar expresamente si un LLM elegido condiciona las respuestas y, por tanto, las decisiones en menor o mayor medida que otros posibles LLM.

En una experiencia llevada a cabo por Rivera *et al.* (2024) los investigadores observaron que los modelos tienden a desarrollar una dinámica de “carrera armamentista”, lo que conduce a un mayor conflicto y, en casos excepcionales, incluso al despliegue de armas nucleares; cambiando las reglas internas de funcionamiento de la simulación, los resultados muestran una **escalada inicial estadísticamente significativa para todos los modelos**.

5.4.7 Responsabilidades y límites en la detección de noticias falsas para los proveedores de plataformas digitales

Una discusión que ha emergido con fuerza en los dos últimos años es la de determinar la **responsabilidad legal**, no solo ética, que tienen o deben tener las grandes empresas ya sean proveedoras o usuarias de servicios digitales en la detección de noticias falsas impulsada por IA. Sus responsabilidades dependen del país y del marco legal aplicable, mucho más estricto en la UE que en Estados Unidos, pero pueden incluir:

338 <https://tdhj.org/blog/post/artificial-intelligence-cognitive-warfare-twitter/>

- **Monitorización activa:** Implementar herramientas de escucha en la sociedad (*social listening*) para identificar menciones y posibles bulos en redes sociales y medios digitales en tiempo real.
- **Protocolos de crisis:** Diseñar manuales específicos para gestionar crisis relacionadas con noticias falsas, evaluando las acciones tomadas para mejorar continuamente.
- **Colaboración y transparencia:** Asociarse con organizaciones de verificación de hechos y mantener canales oficiales como fuentes confiables para contrarrestar la desinformación.
- **Uso de tecnología avanzada:** Adoptar tecnologías como Inteligencia Artificial Explicable (XAI) para detectar y verificar información falsa de manera eficiente.
- **Educación interna y externa:** Capacitar a empleados y otras partes interesadas en la identificación de noticias falsas y fomentar la alfabetización mediática entre el público.
- **Acciones preventivas:** Suspender ingresos publicitarios en plataformas que promuevan desinformación, cerrar cuentas falsas y fomentar la transparencia en la publicidad programática.

Utilizando un enfoque de “**autorregulación**” promovido por diversos países, las grandes empresas proveedoras de servicios digitales han desarrollado o adquirido herramientas de IA específicas como Google con su “*Google News Initiative*” que utiliza la IA para priorizar el contenido confiable y de alta calidad en su plataforma; o Meta (en su red social Facebook) que ha implementado una herramienta de IA para detectar patrones de desinformación y colabora con verificadores de datos humanos para proporcionar contexto adicional para el contenido marcado. En todo caso, **el marco regulatorio es confuso** y su implementación depende de las políticas empresariales³³⁹.

Más allá de introducir mejoras tecnológicas, se requiere disponer de un **marco legislativo integrado** que abarque leyes consensuadas, y una aplicación con el establecimiento de prácticas óptimas para la integridad y la seguridad de los datos. Todo ello, junto a la puesta en marcha de procesos educativos que aseguren no solo disponer de personal especializado, sino de una **población bien formada** para saber defenderse.

339 Meta ha informado en enero de 2025 que va a detener estos procesos de verificación de datos por terceros en Estados Unidos (no, por ahora, en el resto del mundo), reemplazándolo con un modelo de “Community Notes” que permitirá a los usuarios añadir contexto a publicaciones potencialmente engañosas, similar al sistema de la red X. Las razones aducidas eran que los sistemas automatizados de Meta eliminaron publicaciones que cumplían con las normas debido a infracciones menores, afectando a millones de usuarios y comprometiendo el derecho a la información. Para más detalles puede consultarse https://www.rtve.es/noticias/20250107/meta-abandona-sistema-verificacion-datos-por-terceros-estados-unidos/16397475.shtml?utm_source=perplexity

Cómo **lograr esos objetivos mediante regulaciones coercitivas**, al mismo tiempo que se asegure el **mantenimiento de los valores y libertades democráticas** de las sociedades europeas, y se siga promoviendo el proceso de innovación sigue siendo un capítulo abierto a discusión y no resuelto.

5.4.8 IA y cibercrimen

La frontera entre las áreas de defensa y seguridad en el contexto de guerra híbrida y cognitiva es tenue y, desde el punto de vista tecnológico, muy borrosa. Un ámbito en el que la tecnología de IA influye directamente es en su **relación con la ciberseguridad** y, específicamente, con aquellas actuaciones procedentes de grupos ligados a actores gubernamentales cuando su objetivo no son entidades o población civil (objetivo habitual de los ciberdelincuentes para vender o chantajear con la información robada) sino entidades públicas o personas relevantes en los gobiernos si con ello se consigue un **efecto desestabilizador** que es el objetivo perseguido.

El uso de la IA generativa permite a los profesionales de seguridad profundizar en preguntas muy específicas utilizando agentes inteligentes. Un ejemplo es el asistente de **Microsoft Security Copilot**³⁴⁰ con el que se pretende **simplificar las operaciones de seguridad** para analistas y otros profesionales de seguridad al **sintetizar los datos en recomendaciones y conclusiones procesables** para guiar las investigaciones de incidentes. También permite **crear informes y presentaciones legibles** para ayudar a otros usuarios de la organización a comprender lo que está sucediendo, y **responder a preguntas sobre un incidente** o una vulnerabilidad en lenguaje natural o mediante gráficos.

Obviamente, de igual manera que la IA se emplea por las fuerzas y cuerpos de seguridad, también lo hacen los ciberdelincuentes. De acuerdo con el informe de 2024 del Centro Criptológico Nacional (CCN, 2024) el **malware como servicio (MaaS)** ha proliferado apoyado por herramientas sencillas de usar por los delincuentes con conocimientos tecnológicos limitados. La falta de conocimientos tecnológicos para llevar a cabo acciones ha derivado en el **“Hacking as a Service (HaaS)”**, donde individuos con conocimientos técnicos proporcionan sus productos online a todo aquél que esté dispuesto a pagarlos. Además, **grupos ciber-criminales integran el uso de la IA generativa en sus ciberataques** para aumentar sus probabilidades de éxito y hacer más rentable su modelo de negocio.

Los **ciberataques en situaciones de conflictos militares** se han sofisticado enormemente mediante la participación de unidades especializadas de los gobiernos. Así sucede en Ucrania en los que **el mecanismo de ataque es altamente dirigido**, donde los correos electrónicos incluyen archivos adjuntos en formato Excel que, a simple vista, parecen documentos ad-

340 <https://www.microsoft.com/es-es/security/business/ai-machine-learning/microsoft-security-copilot>

ministrativos legítimos, pero **contienen macros con código malicioso oculto**, que se activan al abrir el archivo y otorga acceso remoto al sistema infectado. En la figura 5.29 se puede ver un ejemplo de **infección mediante documentos manipulados**.

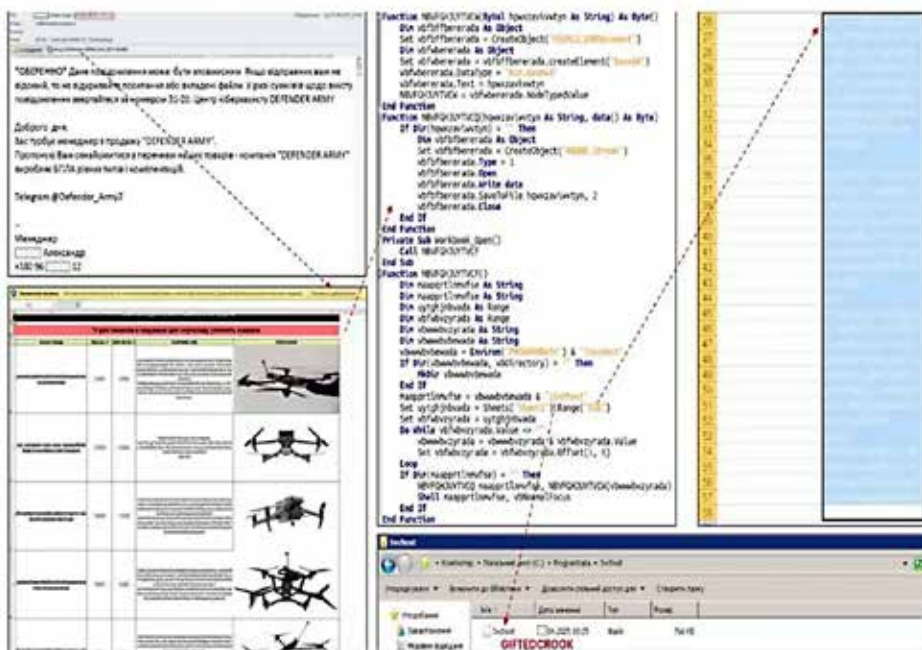


Figura 5.29. Estrategia de infección mediante documentos manipulados. Fuente: <https://www.escenariomundial.com/2025/04/07/informe-revela-un-exponencial-aumento-de-los-ciberataques-contr-la-industria-militar-y-de-defensa-de-ucrania/>

Desde febrero de 2025, el **CERT-UA**, dependiente del *Centro Estatal de Ciberseguridad de Ucrania*, ha documentado múltiples intentos de intrusión que apuntan a comprometer la seguridad de entidades clave del complejo militar-industrial del país³⁴¹. En muchos casos, los atacantes utilizan interfaces web de servicios de correo para enviar los mensajes, lo que podría indicar una **explotación sistemática de credenciales robadas en campañas anteriores**.

Otro ámbito en el que la IA ha tenido una difusión creciente es en el denominado **“fraude de identidad”** o **“fraude biométrico”**. En el caso de acceso a servicios digitales mediante una información de carácter biométrico (p.ej. la cara del usuario comparada con otra almacenada en el sistema) la IA generativa puede generar una imagen falsa³⁴². En los casos en los que las regulaciones requieren un video corto para la verificación en vez de una única foto, el problema de identificación no se resuelve totalmente **porque la IA generativa de**

341 Durante el primer trimestre de 2025, el CERT-UA de Ucrania, registró más de 1.500 incidentes cibernéticos. Supone ya más de un tercio de los 4.300 incidentes registrados en todo 2024, año en el que se produjo un aumento récord del 70%. <https://united24media.com/es/opinion/la-nueva-estrategia-de-defensa-digital-de-ucrania-contr-el-ciberataque-ruso-7747>

342 Un ejemplo de herramienta de IA para luchar contra ello es la proporcionada por SumSub denominada Liveness verification <https://docs.sumsub.com/docs/liveness>

tipo multimodal es capaz de generar videos difíciles de diferenciar de uno real. El sistema de verificación de identidad biométrica le pide al usuario que diga una frase al azar para determinar si es quien dice ser, además de un pequeño video.

El documento generado por el **NIST** (*National Institute of Standards and Technology*) de Estados Unidos en enero de 2025 (NIST, 2025) pretende dar un paso más proponiendo un conjunto de **directrices voluntarias para mejorar la seguridad, la protección y la confiabilidad de los modelos de verificación de doble uso**. Será necesario esperar a conocer el **recorrido real de unas directrices voluntarias**, pero, al menos, reflejan la necesidad de actuar de forma consensuada.

Como exponente de esta preocupación, el 6 de junio de 2025 el Consejo Europeo ha aprobado el **Plan Director de Ciberseguridad de la UE**³⁴³. Con él se propone hacer frente a un panorama de ciberamenazas cada vez más complejo reforzando las redes existentes de la UE, fomentando la cooperación entre los Estados miembros y los actores implicados y superando los obstáculos que puedan existir³⁴⁴.

En este plan director se destaca el hecho de que la sociedad esté cada vez más interconectada y digitalizada conlleva también un aumento del riesgo de incidentes de ciberseguridad y ciberataques. Las **campañas híbridas y los ciberataques pueden afectar directamente a la seguridad y la economía de la UE**. Se pretende también mejorar la puesta en común de **lecciones extraídas** entre los Estados miembros.

5.4.9 Evolución tecnológica futura de la guerra cognitiva

5.4.9.1 Relación de la (neuro)tecnología con el dominio cognitivo

El dominio cognitivo aprovecha que la IA y las neurociencias han alcanzado la capacidad de penetrar en la mente humana, de forma invasiva o no, para conseguir sus objetivos. El **reconocimiento de la vulnerabilidad de la mente humana** ha permitido pensar en lograr la **“superioridad cognitiva”**, convirtiendo a los investigadores en neurociencias e IA en nuevos actores en el ámbito de la defensa y la seguridad (León, 2024; McCreight, 2023).

En León (2024) se establece un **marco conceptual de los esfuerzos para mejorar las capacidades humanas**. Se ha planteado como un proceso continuo que parte de las mejoras del rendimiento de las capacidades innatas del ser humano comunes, a otra en la que se emplea un conjunto de prótesis externas, a otra fase más avanzada con el uso de prótesis

343 Proposal for a COUNCIL RECOMMENDATION for an EU Blueprint on cybersecurity crisis management COM(2025) 66 final 2025/0036 (NLE). Brussels, 24.2.2025

344 <https://www.consilium.europa.eu/es/press/press-releases/2025/06/06/eu-adopts-blueprint-to-better-manage-european-cyber-crises-and-incidents/>

internas y, finalmente, a una fase en la que las mejoras genéticas pueden implicar que esa mejora se transmita a otras generaciones. En todas las fases señaladas es posible emplear un conjunto de **tecnologías físicas** (semiconductores, IA, nanomateriales, sensores, robótica, etc.) y otras de carácter **biológico** (biología celular, genómica, biología sintética, etc.) cuya integración está acelerando la capacidad de conseguir los efectos deseados.

En el contexto de la **guerra cognitiva** son las **capacidades cognitivas** las que merecen mayor atención. En la figura 5.30 se indican algunos ejemplos de las tecnologías empleadas en las diferentes fases. La **mejora cognitiva del ser humano** que es la que afecta a la obtención, análisis y uso de datos de la actividad cerebral es aquella sobre lo que los algoritmos de IA tienen un papel relevante e indican en la eficacia de la guerra cognitiva. Debe recordarse que una de las prioridades tecnológicas establecidas por la OTAN es el desarrollo de tecnologías para el incremento de capacidades humanas, y la cognitiva es una de las más relevantes.

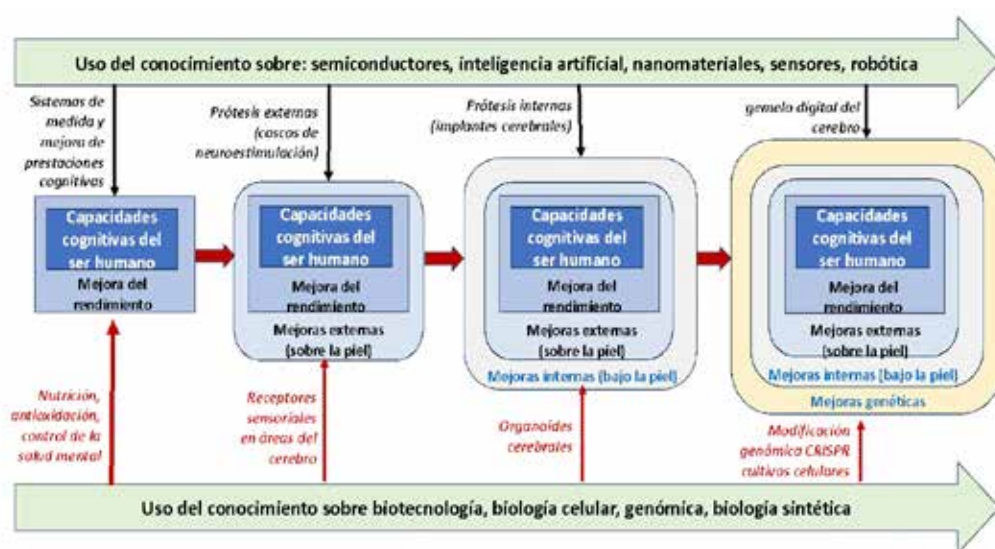


Figura 5.30. Aumento progresivo de capacidades cognitivas humanas.

Fuente: Adaptada de León (2024)

Así, la **mejora del rendimiento cognitivo puede “entrenarse”** como se hace con los músculos (p.ej. para retardar el deterioro cognitivo como se aplica con personas de la tercera edad); también pueden emplearse **prótesis externas** como son cascos de monitorización y estimulación cerebral dotados de sensores que permiten obtener información de la actividad cerebral (p.ej. la obtención de electroencefalogramas para analizar y actuar en función de ellos para mantener niveles de alerta), o **prótesis internas** como los implantes cerebrales (p.ej. para permitir la neuromodulación profunda con precisión suficiente en un área específica del cerebro).

Más lejos en el tiempo puede considerarse la posibilidad de obtener **mejoras cognitivas basadas en terapias génicas** empleando técnicas como CRISPR. En todos estos casos, el análisis de la información cerebral empleando algoritmos de IA se ha convertido en una herramienta esencial para la mejora cognitiva.

A pesar de las dudas sobre los niveles actuales de eficacia derivados de su falta de madurez, todos los indicios apuntan hacia un futuro en el que **la neurotecnología se utilizará ampliamente en diferentes áreas de la sociedad**. Muchos de estos desarrollos han estado motivados por ayudar a superar las necesidades de personas con dificultades cognitivas aplicadas en el contexto del sector médico. Sin embargo, **No hay limitaciones técnicas que impidan que no se puedan aplicar a personas sanas con el objetivo de mejorar sus capacidades cognitivas por encima de las de una persona media**.

Aunque tal vez sea inevitable, la difusión de la neurotecnología puede tener **efectos perturbadores en los valores humanos fundamentales**. Es probable que se empleen dispositivos que alteren inadvertida o intencionalmente el comportamiento y la personalidad de los usuarios. No se olvide que las neurotecnologías interactúan directamente con el cerebro, el órgano responsable de las funciones vitales, así como con todas las experiencias humanas, incluidas la percepción, la inteligencia, la emoción y el comportamiento.

La **traslación inmediata al ámbito militar de la neurotecnología** es evidente dada su caracterización como tecnología dual. Pensar en las ventajas derivadas de tener personal militar con capacidades mejoradas ha despertado un interés creciente por parte de las agencias de investigación de defensa. Para Claverie (2025) la guerra cognitiva puede aprovechar las tecnologías digitales para alterar funciones cognitivas específicas (memoria, atención, comunicación, emociones, etc.) en individuos específicos. **El objetivo es alterar el pensamiento a corto plazo influyendo en la atención, la toma de decisiones y la reacción**.

En este contexto, como se aborda expresamente en la siguiente sección, se ha comenzado en explorar el uso de la neurotecnología como tecnología dual para la **mejora de las capacidades cognitivas del personal militar**.

5.4.9.2 En búsqueda de un nuevo dominio militar basado en el cerebro

En un informe de la OTAN (du Cluzel, 2021) se lee: *“El cerebro será el campo de batalla del siglo XXI, y los humanos son el dominio en disputa”*. Esta visión está en el origen del concepto de guerra cognitiva desarrollado en el presente documento y anticipado por varios autores (Gómez, 2019)³⁴⁵. Ahora, con la convergencia de múltiples tecnologías emergentes surge la reflexión sobre la emergencia de un sexto dominio de operaciones denominado

345 https://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEO14_2019ANGGOM-GuerraGente.pdf

“cognitivo” que complementaría los dominios de operaciones de aire, tierra, mar, espacio y ciber considerados ya como “clásicos” en el ámbito de la defensa.

Si bien es creciente la importancia de las neurociencias y la neurotecnología en la sociedad, sobre todo en el ámbito médico, **sus impactos todavía están lejos de poder aplicarse de forma rutinaria en el campo de batalla real** sobre personas sanas. Desde un punto de vista científico, es un **dominio altamente interdisciplinar** en el que convergen cuatro dominios disociados hasta el siglo XXI:

- **Nanotecnología** (nanorobótica, nanosensores, nanoestructuras, energía...)
- **Biotecnología** (tecnología biogenómica, Crisp-Cas9, neurofarmacología...),
- **Informática** (tecnologías de la información, informática, microelectrónica, IA...)
- **Cognética** (tecnología cognitiva, ciencia cognitiva y neuropsicología).

Todas las grandes potencias han comenzado a explorar seriamente a dónde puede conducir este sexto dominio, a monitorizar su desarrollo en los próximos años, y a evaluar su potencial uso militar. Es probable que algunos países se esfuercen por aprovechar los *neurodatos* obtenidos del funcionamiento del cerebro para obtener ventajas en la capacidad de información, social, legal y militar, a medida que los países competidores invierten en investigación en neurociencias. Es un ámbito multidisciplinar porque no solo se necesita una comprensión de la neurociencia, sino también de la cognición, del comportamiento social y de su relación.

China y Estados Unidos son, posiblemente, las potencias militares más decididas en iniciar este proceso con el desarrollo de programas y recursos específicos. La filosofía del conflicto militar de China está evolucionando para considerar **el cerebro humano como un nuevo dominio operativo**. Imaginan para el futuro seres humanos mejorados cognitivamente por las TIC como algún tipo de **desarrollo evolutivo transhumano**. La idea de *guerra inteligente* fue conceptualizada por China en el informe de la “*Defensa Nacional de China en la Nueva Era*” desde julio de 2019.

También lo está haciendo Estados Unidos. DARPA, a través del programa **N3** (*Next-Generation Nonsurgical Neurotechnology*)³⁴⁶, financia investigación orientada al uso de combinación de estímulos de luz, ultrasonido o energía electromagnética para “leer y escribir” la actividad

346 <https://www.darpa.mil/research/programs/next-generation-nonsurgical-neurotechnology>. Uno de los proyectos financiados por DARPA es BrainSTORM cuyo objetivo es inyectar a través de los vasos sanguíneos unos dispositivos denominados MenT (magnetolectric nano transducer). <https://magnetismmag.com/magnetism-plays-key-roles-in-darpa-research-to-develop-brain-machine-interface-without-surgery/>

cerebral utilizando técnicas no invasivas o mínimamente invasivas. Sus resultados están lejos de aplicarse de forma directa a un número elevado de personas, pero marca un camino.

La figura 5.31 representa también la visión de la *Escuela de Guerra de Estados Unidos* (US Army War College) en su informe de 2023 sobre la **evolución del conflicto militar hacia 2035** basado en la convergencia de diversas tecnologías emergentes hacia lo que denomina “*guerra tecno-sentiente*” (Carlson *et al.*, 2023). Obsérvese que, de acuerdo con el informe citado, en solo diez años es casi seguro que tengamos enjambres de drones autónomos con comportamiento inteligente. En nuestra opinión, se va a producir antes de los diez años.



Figura 5.31. Elementos de la futura guerra “tecno-sentiente”.

Fuente: Adaptada de Carlson *et al.* (2023)

El segundo elemento, considerado altamente probable, es **disponer de soldados con prestaciones físicas y mentales incrementadas** (exoesqueletos, fármacos o interfaces cerebro máquina) . También se considera muy probable la guerra cognitiva ligada al campo de batalla de los medios sociales. En la estimación que hicieron Carlson y sus colegas en 2023 **se considera posible disponer en 2035 de “humanos mejorados”**, participando en operaciones militares junto a robots y vehículos no tripulados potenciados por IA con hardware neuromórfico especial.

Más allá de lo que actualmente es posible, en un terreno mucho más especulativo a partir de experiencias de laboratorio actuales, si se consiguiera **conectar directamente en red los cerebros humanos**, se podría acelerar la transmisión en tiempo real de datos en el campo de batalla y mejorar las capacidades cognitivas de toma de decisiones de los mandos y facilitar la comunicación entre ellos y sus unidades (Latheef, 2023; Vakilipour y Fekrvand, 2024).

5.4.9.3 El papel de la neurotecnología en la guerra cognitiva

La convergencia entre la IA y las neurotecnologías conduce hacia la potencial **militarización de su uso en la guerra cognitiva**. Los esfuerzos internacionales en la investigación sobre el cerebro podrían conducir, a una **competición para obtener capacidades militares ligada al cerebro** como diversos países están intentando (De Franco *et al.*, 2020)³⁴⁷.

Las **neuroarmas** se definen como tecnologías y sistemas para mejorar o dañar las capacidades cognitivas y/o físicas de un combatiente o de un objetivo, o atacar de otro modo a las personas o a la infraestructura crítica de la sociedad (De Franco *et al.*, 2019), (Pabst, 2024). Las neuroarmas son herramientas que aprovechan la neurociencia y la neurotecnología para influir o alterar el cerebro y el sistema nervioso humanos. Estas armas pueden **mejorar o degradar las funciones cognitivas, emocionales y motoras de las personas con fines militares y de inteligencia**. Hacerlo a distancia puede ser disruptivo. Este proceso también ha implicado mayor atención a la forma de defenderse de estas neuroarmas (Washington *et al.*, 2023; Grigsby *et al.*, 2023).

Las **neuroarmas** incluyen varios tipos: agentes bioquímicos, fármacos neurofarmacológicos, sistemas de energía dirigida e interfaces cerebro-máquina (*Brain Computer Interfaces, BCI*) ya sea de forma invasiva (p.ej. con implantes cerebrales) o no invasiva (p.ej. con sensores en cascos externos) (León, 2024). Veamos algunos ejemplos.

- **Neurofarmacología.** Fármacos que influyen en la cognición y el comportamiento humano mediante la reingeniería de neuronas, moléculas y el sistema nervioso.
- **Armas de energía dirigida.** Utiliza energía como micro, radio, ondas acústicas y electromagnéticas para crear armas que van desde aquéllas que pueden tener consecuencias fatales hasta las que no. Su interés surgió hace unos años con el denominado Síndrome de La Habana. Puede ser una **opción en conflictos híbridos** debido a sus características encubiertas y no atribuibles³⁴⁸. Algunos ejemplos son:
 - ─ Sistema activo de denegación. Aprovecha las ondas de frecuencia extremadamente alta para simular la sensación de fuego y “crear una sensación de ardor en la piel” (Skelton, 2012).
 - ─ Dispositivo Acústico de Largo Alcance. Utiliza frecuencias de sonido audibles o inaudibles para paralizar, herir o matar enemigos. Capaz de emitir sonidos de hasta 160, 180 y 200 decibelios, suficientes para inducir náuseas, cavitación corporal, contracción muscular, pérdida temporal de la visión, daño pulmonar, arritmia cardíaca, deformación celular y muerte.

347 <https://corbettreport.substack.com/p/the-battle-for-your-brain-is-already>

348 https://cttp.sanford.duke.edu/wp-content/uploads/sites/16/2023/06/2021-Hayes_FSRP-Presentation_v3.pdf

- **Interfaces Cerebro-Ordenador (Brain Computer Interfaces, BCI).** Tecnologías que conectan las ondas cerebrales con dispositivos externos como computadoras, armas y drones, lo que permite a los humanos controlar máquinas sin estar físicamente presentes.

Un caso de uso que se está explorando es el **control mental de drones mediante cascos no invasivos** que monitorizan las señales cerebrales y las transfiere a un dron, lo que permite a las personas volar el dron con su mente. Aunque se trata de tecnologías inmaduras, las interfaces cerebrales para controlar mentalmente un dron han mejorado rápidamente.

Hay muchas experiencias en este sentido no solo en Occidente, sino también en China o Rusia. Un ejemplo fue el sistema **NIMBUS** (*Neurological Intelligent Monitoring and Brain Utilisation System*) desarrollado desde el año 2022³⁴⁹. En Rusia la empresa Neurorobotics en 2023 ha desarrollado un sistema de control mental de un pequeño dron (Tomaswick, 2025).

Un sistema desarrollado por investigadores de China utiliza un sistema neuromórfico basado en un chip *memristor* compuesto por componentes electrónicos integrados que pueden “recordar” qué voltaje se les aplicó cambiando su resistencia.

Los sujetos de prueba pudieron controlar con éxito el movimiento de un dron sorteando obstáculos simplemente **pensando cómo querían que un dron se moviera en una dirección específica**. El casco sensorizado del humano recogía las señales cerebrales, las traducía en la “intención” del sujeto y luego movía el dron en la dirección prevista. Otro algoritmo de aprendizaje automático se actualizaba continuamente con nueva información sobre las señales cerebrales del usuario, con el fin de incrementar la precisión de las estimaciones de intención del sujeto³⁵⁰.

El uso de **interfaces no invasivas** como las indicadas basadas en electrodos incluidos en cascos cerebrales no son muy precisas. En una línea de **interfaces invasivas** la empresa *Neuralink* anunció en septiembre de 2024 el desarrollo de un implante denominado “**Blindsight**” para restaurar la visión a las personas ciegas. A diferencia de otros implantes de retina innovadores que envían señales desde una cámara a electrodos que van directamente a los nervios de la retina, **Blindsight es un implante cerebral que estimula directamente el área de la corteza visual del cerebro**. El sistema no emplea el nervio óptico.

No es el único caso de avance disruptivo. El **ojo biónico** “*Gennaris Bionic Vision System*”, desarrollado por investigadores de la Universidad Monash de Australia, en colaboración con *Alfred Health* consiste en una potente **minicámara montada en un casco personalizado que graba su entorno y lo transmite a un implante cerebral inalámbrico**. A diferencia de *Neuralink Blindsight*, que funciona en un implante de matriz de microelectrodos, el **Gennaris Bionic Eye** utiliza múltiples (hasta 11) implantes diminutos (9 mm) que se pueden colocar

349 <https://neuro8.com/static/media/Nimbus.cd72131bee2e10595c77.pdf>

350 Un video del sistema puede verse en <https://youtu.be/PR3KPwkeyQc>

en la superficie del cerebro para estimular partes específicas relacionadas con la visión³⁵¹. Cuando se implantan en la corteza visual, **estos impulsos eléctricos pueden interpretarse como información visual**, proporcionando al receptor formas y contornos básicos que pueden ayudar con la navegación, el reconocimiento de objetos y otras tareas cotidianas básicas³⁵².

Es necesario que la tecnología madure lo suficiente como para hacer realidad ese objetivo en el sector médico, o en personas sanas; un objetivo lejano³⁵³. Si se consigue mejorar la capacidad sensorial y cognitiva de las personas, no solo de los pacientes, nos encontraremos en una **nueva fase de la guerra cognitiva**.

Ante estos avances y las predicciones de su aceleración no es extraño que las grandes potencias tengan interés en financiar, analizar y experimentar con el uso militar de la neurotecnología. En junio de 2022, el Departamento de Defensa de Estados Unidos lanzó la **Iniciativa de Salud Cerebral de los Combatientes (Warfighter Brain Health Initiative)**³⁵⁴ en un enfoque unificado para **optimizar la salud cerebral y contrarrestar las lesiones cerebrales traumáticas del personal militar** con los siguientes objetivos específicos:

- Optimizar el rendimiento cognitivo y físico.
- Identificar, monitorizar y mitigar las exposiciones cerebrales.
- Prevenir, reconocer y minimizar los efectos de las lesiones cerebrales traumáticas.
- Reducir o eliminar los efectos a largo plazo o tardíos de las lesiones cerebrales.
- Avance de la ciencia de la salud cerebral de los combatientes.

La **Unidad de Innovación de Defensa (Defense Innovation Unit, DIU)** ha colaborado con empresas como *Garmin* y *Oura Ring* para proporcionar dispositivos portátiles para **rastrear 165 biomarcadores** entre 8.500 soldados, generando análisis predictivos de salud. Este programa se une al denominado “*The Next-Generation Nonsurgical Neurotechnology (N3)*”³⁵⁵ financiado por DARPA desde 2021 cuyo objetivo es el de desarrollar interfaces cerebro-máquina bidireccionales de alto rendimiento para militares sanos. Dichas interfaces permitirían disponer de la tecnología necesaria para el control de vehículos aéreos no tripulados y sistemas de defensa cibernética activos o la combinación con sistemas informáticos para realizar múltiples tareas con éxito durante misiones militares complejas.

Desde el punto de vista técnico **la tecnología N3 pretende superar las limitaciones de la tecnología existente al ofrecer un dispositivo integrado que no requiere implantación quirúrgica**. Por ejemplo, un equipo de Battelle está estudiando la forma de insertar en el

351 <https://www.sify.com/science-tech/neuralink-blindsight-and-gennaris-bionic-eye-the-future-of-ophthalmology/>

352 <https://www.monash.edu/mada/design-health-collab/projects/product-design-and-wearables/gennaris-bionic-eye>

353 <https://spectrum.ieee.org/neuralink-blindsight>

354 <https://www.health.mil/Military-Health-Topics/Warfighter-Brain-Health>

355 <https://www.darpa.mil/research/programs/next-generation-nonsurgical-neurotechnology>

cerebro minúsculos dispositivos denominados “transductores”. Estos dispositivos modificarían las señales eléctricas del cerebro para que puedan leerse desde el exterior³⁵⁶.

El **Ejército de China** (*Popular Liberation Army, PLA*) está explorando activamente las operaciones cognitivas como un nuevo dominio de la guerra, posicionándolo junto a la tierra, el mar, el aire, el ciberespacio y el espacio. El PLA está desarrollando actualmente **tecnología portátil y un sistema de apoyo psicológico dedicado para manipular el estado mental de las tropas enemigas** mientras fortalece sus propias fuerzas contra tales esfuerzos.

Una iniciativa del PLA es el **Sistema Inteligente de Monitorización Psicológica**. Este sistema subraya la importancia que se concede al bienestar mental de los soldados. Cada vez son más las unidades de PLA que están equipadas con **brazaletes sensores inteligentes que proporcionan datos fisiológicos en tiempo real**. Cuando sea necesario, el sistema puede enviar de inmediato a un “consejero psicológico” para recibir asesoramiento. También permite el **registro continuo de la información facial**, lo que facilita la evaluación en tiempo real de los estados psicológicos de los soldados. Además, el PLA utiliza **simulaciones de realidad virtual de alto estrés para mejorar la preparación para el combate de los soldados** (Mohino, 2019)³⁵⁷

Un ejemplo de actuación gubernamental de carácter dual es el **Programa militar de China sobre el cerebro** (*Military Brain Sciences, MBS*)³⁵⁸. En la Tabla 5.2 se pueden ver los objetivos planteados de los que algunos de ellos (no solo el último de la tabla referido a las neuroarmas) tienen un valor dual.

Comprender el cerebro	Comprender los factores de riesgo de las lesiones cerebrales causadas por las actividades militares
Proteger el cerebro	Prevención específica del daño cerebral causado por las actividades militares
Monitorizar el cerebro	Monitorización de la función cerebral a través de nuevas tecnologías y equipos
Dañar al cerebro	Promover la investigación y el desarrollo de armas sonoras, ligeras, explosivas, magnéticas y otros nuevos tipos de armas
Interferir el funcionamiento del cerebro	Causar disfunción cerebral y pérdida de control con métodos “sin humo”
Reparar el cerebro	Lograr la reconstrucción de la función cerebral con tecnología médica novedosa avanzada
Aumentar las capacidades cerebrales	Mejorar el nivel de la función cerebral del personal que realiza tareas especiales
Simular el cerebro	Inteligencia robótica inspirada en el cerebro y predicción de decisiones humanas
Armar el cerebro	Estudiar la forma de armar el cerebro, con las interfaces del cerebro y la máquina como foco

Tabla 5.2. Programa militar de China sobre el cerebro. Fuente: <https://www.sciencedirect.com/science/article/pii/S1008127517303188?via%3Dihub>

356 <https://english.mathrubhumi.com/features/technology/darpa-brain-helmet-military-operations-explainer-1.10067851>

357 https://emad.defensa.gob.es/Galerias/CCDC/files/USOS_MILITARES_DE_LA_INTELIGENCIA_ARTIFICIALx_LA_AUTOMATIZACION_Y_LA_ROBOTICA_xIAxRx-_VV.AA.pdf

358 <https://www.sciencedirect.com/science/article/pii/S1008127517303188?via%3Dihub>

Tianjin se ha convertido en un centro para la innovación en interfaces cerebro ordenador (BCI) de China. El Laboratorio Haihe de Interacción Cerebro-Computadora e Integración Humano-Computadora (脑机交互与人机共融 海河实验室) en la Universidad de Tianjin es un importante instituto de investigación en BCI con numerosos socios comerciales y militares. Dado el concepto de fusión civil-militar de China, la investigación hace poca distinción entre las instituciones de investigación, el gobierno, el sector privado y el ejército de China.

Las **tecnologías persuasivas emergentes interactúan de manera más intrusiva con los estados neurológicos y fisiológicos de los usuarios**, ofreciendo técnicas cada vez más sofisticadas para influir en el comportamiento humano. Los avances en IA generativa serán el principal impulsor de esta nueva generación de cambio tecnológico, particularmente a través de conceptos como:

- **Hiperpersuasión:** se refiere a la aplicación de modelos de aprendizaje automático que explotan los sesgos cognitivos para influir en las creencias y los comportamientos a niveles sin precedentes. Los sistemas de IA pueden identificar, dar forma y explotar las demandas de los usuarios y, a continuación, suministrar contenidos personalizados. La *hiperpersuasión* es una forma más sutil y estratégica de explotar las vulnerabilidades de los usuarios individuales para guiar a las personas a tomar decisiones que no son las mejores para ellos.
- **Hiperacicates (*hyper nudging*):** se trata de una extensión impulsada por IA de los “acicates” (*nudging*) tradicionales³⁵⁹ (intentar influir en las personas de una manera predecible, suave y reconocible) que utiliza grandes conjuntos de datos en tiempo real para implementar arrastres dinámicos y personalizados, al mismo tiempo que genera y recopila nuevos datos. Esto hace que los hiperacicates sean significativamente más agresivos, menos reconocibles y potencialmente más manipuladores.

En definitiva, la **carrera armamentista prevista por la superioridad cognitiva** da lugar a un **dilema de neuro seguridad** mucho más amplio que el concepto convencional de ciberseguridad: a medida que las neurociencias se imbrican con la seguridad, las prácticas neurocientíficas surgen simultáneamente como una vulnerabilidad central, condicionando su trabajo al cumplimiento de las prácticas de seguridad (Ördén, 2024).

Aún es pronto para poder evaluar si las tecnologías emergentes mencionadas madurarán lo suficiente para que puedan desarrollarse productos de uso real que puedan emplearse en operaciones militares. Con la información disponible en las fuentes abiertas empleadas para la elaboración de este documento no parece sencillo que su adopción masiva por las fuerzas armadas se produzca a corto plazo.

359 El acicate (*nudging*) digital convencional se basa en un diseño del entorno de elección en el que se presenta la información, que puede ejercer una influencia subconsciente en el resultado. Utiliza elementos de diseño de la interfaz de usuario para guiar el comportamiento de las personas en entornos de elección digital en formularios o preguntas.

5.4.10. Estimación de la aparición de eventos disruptivos relacionados con la guerra cognitiva hasta 2030

La evolución tecnológica relacionada con la guerra cognitiva puede plantearse en **cuatro fases tecnológicas** de las que nos encontramos en la fase 3, con algunas experiencias en proyectos de investigación de la fase 4 que podrán ser efectivos a partir de 2030. Considerando las fechas simplemente orientativas, estas fases son:

La **Fase 1**, transcurrida desde finales del siglo XVIII hasta el año 1980 (más de 200 años), se refiere al estado de **guerra cognitiva analógica**. En ese periodo no se había producido aún el proceso de digitalización masiva de la sociedad y la guerra cognitiva empleaba **técnicas analógicas de difusión de mensajes** empleando inicialmente la prensa, seguida posteriormente con la adopción social de la radio y la televisión. En esta fase era muy difícil disponer de mensajes “personalizados” para un usuario concreto que modulasen su comportamiento, y los mensajes iban acompañados de discursos políticos en evento multitudinarios. Algunos eventos característicos de esta fase de **guerra cognitiva analógica** son:

- Democratización del acceso a la prensa libre (en papel).
- Mensajes comerciales o políticos difundidos en el espacio público (vallas, pasquines, uso de fotocopadoras, eslóganes, mítines, etc.).
- Consideración de la “propaganda” como un medio empleado por los gobiernos.
- Emisoras de radio con programas de opinión y retransmisión en directo de discursos políticos.
- Emisoras de TV con programas de opinión, entrevistas, retransmisión en directo y documentales.
- Campañas de propaganda oficial gubernamental para modular la opinión pública sobre temas concretos.

La **Fase 2** desde 1980 a 2015 (25 años) se refiere al estado de **guerra cognitiva digital** caracterizada por la explosión progresiva de la digitalización de la información, del despliegue de las redes de comunicación fijas y móviles, y el intercambio de mensajes, primeros textuales y luego multimedia, entre millones de personas a través de las redes sociales y las plataformas digitales. Debe tenerse en cuenta que los medios empleados en la fase 1 siguen existiendo. Algunos eventos característicos de esta fase de **guerra cognitiva digital** son:

- Continuación de las técnicas empleadas en la Fase 1.
- Difusión del correo electrónico como medio de intercambio de información personal o grupal.
- Intercambio de información personal a través de redes físicas y desde el siglo XXI en redes móviles con la expansión de la conexión a Internet y los teléfonos móviles inteligentes.
- Expansión de los sitios Webs con interacción asíncrona, blogs, foros, etc. y almacenamiento en la nube.
- Emergencia de las redes sociales de intercambios de texto (p.ej. Facebook, Twitter).
- Análisis de datos (*big data*) por parte de empresas de marketing y gobiernos.
- Emergencia de un problema de ciberseguridad sobre la información personal.

La **Fase 3**, desde 2015 a 2030 (15 años) se refiere al estado de **guerra cognitiva inteligente** en el que **la IA se convierte en la tecnología habilitadora** para un nuevo desarrollo de herramientas de desinformación personalizadas y de modulación del comportamiento de los individuos. Algunas tendencias sugieren que nos encontramos en medio de esta fase y el presente informe refleja esta situación. Debe tenerse en cuenta que los medios empleados en las fases 1 y 2 siguen existiendo. Algunos eventos característicos de esta fase de **guerra cognitiva inteligente** son:

- Uso de la **IA generativa** para la construcción y difusión de “narrativas” orientadas a modular la opinión pública o de segmentos específicos.
 - Monomodal (texto) y multimodal (texto, voz, imagen, video).
 - Generación automática de noticias falsas (*fake news*).
 - Herramientas para la detección de información falsa
- Expansión de las **redes sociales multimedia** con miles de millones de usuarios combinado con acceso en todo momento desde dispositivos inteligentes.
 - Papel de los gestores de comunidad (“*community managers*”) en el filtrado y difusión de la información,
 - Papel de los “*Influencers*” en la sociedad.
 - Emergencia de bots (redes sociales híbridas)
- Plataformas digitales con **agentes inteligentes**.
 - Algoritmos de recomendación.
 - Análisis de comportamiento de usuarios.
 - Personalización sencilla de agentes inteligentes.
- Información contenida en la Web **oscura** (*dark web*) y en la Web **profunda** (*deep web*).
- Preocupación creciente sobre la **ciberseguridad de la información** (p.ej. alteración de información, robo y rescate de información personal o institucional).
- **Sistemas de múltiples agentes inteligentes** para la gestión automática de campañas de (des)información.

La **Fase 4**, desde 2030 en adelante, se refiere al estado que denominaría de **guerra neurocognitiva** en el que se producirá una **convergencia real entre la IA y la neurotecnología** auxiliada por nuevos conceptos de procesamiento neuromórfico y sensores inteligentes implantados (o subcutáneos) que puedan actuar con el cerebro humano para incrementar capacidades. Algunos eventos característicos de esta fase en relación con la guerra cognitiva podrían ser los siguientes:

- Maduración de **neurotecnologías con la capacidad de interpretar (leer y escribir) la actividad cerebral** empleando técnicas invasivas, mínimamente invasivas o no invasivas en personas sanas (fuera del contexto de la medicina).
- **Comunicación cerebro-cerebro bidireccional** (probablemente limitado en la próxima década a dos personas y no grupal).

- Chips implantados con capacidad de procesamiento neuronal y **neuromodulación funcional del comportamiento humano**.
- **Interfaces más transparentes y ubicuas**. La incorporación a nuestra cotidianeidad de los móviles los hace mucho más potentes para interiorizar las narrativas que dispositivos menos corporeizados.
- **Sistemas holográficos** de comunicación que pueden hacer más convincentes los mensajes y las narrativas.
- **Comunicación extendida** de tipo “conversacional” con no-humanos (humano-animal y humano-robot).

Aunque referidos a una ventana temporal restringida a la presente década (2020-2030) es posible estimar la **aparición de algunos eventos disruptivos de carácter tecnológico** (entendidos como la primera introducción en el mercado de un producto o servicio disruptivo) **relacionado con la guerra cognitiva**. Su análisis permite la **adopción temprana de medidas tanto tecnológicas como operativas** con el fin de minimizar o maximizar su impacto en función del objetivo que se desee desde una perspectiva dual. Debe tenerse en cuenta que si se lograra el **abaratamiento sustancial del uso de estas técnicas** (p.ej. cascos, implantes) también se va a **incrementar su ritmo de adopción en personas sanas** para mejorar sus prestaciones en actividades civiles o militares, y, por tanto, su impacto y relevancia en la sociedad (León, 2024).

Los eventos identificados más relevantes son los que se indican en la figura 5.32. En el caso de que todos estos eventos se produzcan, **la tecnología asociada a la guerra cognitiva habrá dado un paso de gigante**, y deberemos estar preparados para ello.

Destacan dos **eventos relevantes del uso de la IA en la guerra cognitiva**, con gran impacto, aunque con probabilidades de materialización no muy elevadas (<50%).

- Hacia 2027 se debería producir los primeros pasos de un acuerdo en relación con el uso de técnicas de guerra cognitiva estableciéndose ciertos límites en la aplicación de la IA. Es probable el establecimiento por parte de organismos internacionales de determinados “*códigos de conducta*” o directrices de aplicación voluntaria entre países.
- Al final de la presente década se ha incluido como evento la emergencia de la sinergia entre la computación cuántica y la IA. En relación con la guerra cognitiva esta sinergia permitiría disponer de la capacidad de procesamiento suficientes para disponer de gemelos digitales ciberfísicos del cerebro y poder conocer en tiempo real el efecto de determinados neuro impulsos para la neuromodulación del comportamiento.

También destacan dos **eventos relevantes del uso de la neurotecnología en la guerra cognitiva**, también con probabilidades no elevadas (<50%).

- Emergencia de **prótesis mentales** en personas sanas de manera rutinaria. Se trata, por tanto, de un uso más allá del ámbito médico, sino con el objetivo de incrementar las prestaciones del ser humano.
- **Comunicación cerebro-cerebro** aplicadas a operaciones de defensa. Aunque nuestra estimación de que suceda de forma abierta en el mercado tiene probabilidades bajas, estimamos que la tecnología madurará lo suficiente para poder llevar a cabo experiencias en entornos controlados.

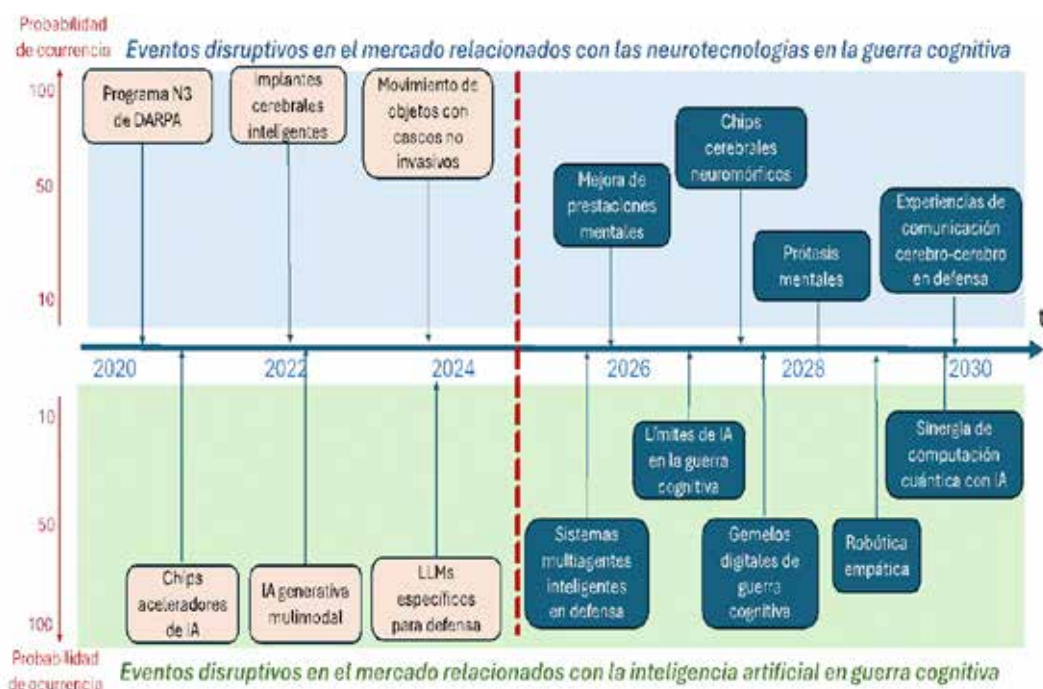


Figura 5.32 Eventos disruptivos relacionados con la guerra cognitiva.

Fuente: elaboración propia.

5.4.11. Consideraciones finales sobre la IA en la guerra híbrida y cognitiva

El análisis realizado presenta un panorama en el que las guerras híbridas y la guerra cognitiva como parte de ella están adquiriendo una mayor relevancia en las confrontaciones entre países. El **proceso de digitalización de la sociedad** ha actuado de caldo de cultivo para disponer de herramientas que permiten **generar y difundir información falsa y narrativas intencionadas** que modulan la opinión pública y de actores concretos como instituciones públicas y el personal militar con impactos muy relevantes.

En este escenario, las tecnologías de IA ofrecen soluciones prometedoras para la detección y eliminación de información errónea o falsa mediante procesos de verificación automatizados; concretamente, la IA permite identificar debilidades en la opinión pública y la información, evitando futuros ataques. Dado el carácter dual de la IA, las mismas herramientas que pueden prevenir la información falsa también se pueden usar para “atacar” la mente de las personas. De la presente sección pueden extraerse las siguientes conclusiones:

- La **relevancia de los conflictos híbridos** ha crecido en las últimas dos décadas con implicación de actores estatales y no estatales con sofisticados conocimientos.
- El **carácter multidimensional de los conflictos híbridos** obliga a actuar en varias dimensiones simultáneamente empleando técnicas procedentes de las TIC, especialmente de la IA, de la psicología y de las neurociencias.
- El **uso de herramientas de IA junto a big data** ha supuesto un cambio disruptivo en la forma en la que se detecta la escalada de los conflictos híbridos, se generan campañas de desinformación, y se crean capacidades de mitigación de los riesgos asociados.
- La **IA generativa** ha empezado a adquirir un mayor protagonismo en la generación de narrativas e información multimedia combinada con ciberataques.
- La **convergencia entre la IA y la neurotecnología** abre una nueva fase en la guerra cognitiva que se desarrollará plenamente en la próxima década.
- Todos los estados se han provisto de unidades **especializadas dotadas de tecnología avanzada de IA para luchar de forma integrada en conflictos híbridos** en estrecha interacción con entidades civiles cooperando con países aliados.
- La **OTAN** y la **UE** prestan una atención creciente a este fenómeno focalizado en las acciones llevadas a cabo por Rusia y, en menor medida, China e Irán desde 2010 sobre países occidentales.
- Se detecta una **creciente convergencia entre la neurotecnología y la IA aplicada a la guerra cognitiva** que alimenta el desarrollo de neuroarmas de carácter disruptivo.

Dada la relevancia que ha adquirido el uso de la IA, y la necesidad de responder a sus crecientes efectos en un contexto de amenazas, conflictos y guerra híbrida como los expuestos, parece que todo sería posible desde una perspectiva tecnológica a corto plazo. Consensuar los valores y principios que deben informar la **definición de un marco ético y regulatorio consensuado alrededor de la guerra cognitiva** es un objetivo urgente que será abordado en el siguiente capítulo.

5.5. IA en el sector espacial de la defensa

En una sociedad altamente tecnificada como es la actual, al menos desde la perspectiva de los países avanzados, la **importancia del sector espacial** es creciente. Aunque sólo un grupo reducido de países poseen las capacidades necesarias para desarrollar, poner en órbita y operar satélites, cubriendo toda la cadena de valor, la capacidad de desarrollo de **aplicaciones basadas en la información satelital** tanto en el ámbito civil como en el militar alcanza a un número muy superior de países. Aún más, atendiendo al **uso de aplicaciones satelitales**, ya sea de forma consciente o no, **millones de ciudadanos de todo el mundo son diariamente usuarios de estas aplicaciones**.

Para la Comisión Europea (JOIN, 2023) el **ámbito espacial comprende todo elemento pertinente para el funcionamiento de los sistemas espaciales y la prestación de servicios espaciales en la UE y los Estados miembros**. Ello incluye, por ejemplo, el entorno del espacio ultraterrestre, las diversas órbitas y vehículos espaciales y la información conexas sobre los sistemas a los que pertenecen, la infraestructura terrestre y de lanzamiento, los enlaces por radiofrecuencia, las terminales de usuario y los aspectos de ciberseguridad. También incluye las entidades que forman el sector espacial industrial subyacente y los organismos reguladores de su uso a nivel nacional e internacional.

A ello se suma el impacto que la tecnología espacial tiene para permitir la **exploración del espacio profundo**, desde las misiones a la Luna, nuestro satélite natural, hasta el conocimiento de otros planetas o de los satélites que les orbitan en el sistema Solar, o de otros objetos más pequeños, asteroides o cometas, pero con un potencial peligro en el caso de que impactaran en nuestro planeta. Se alienta con ello el deseo del ser humano de conocer mejor el mundo que le rodea.

El **sector espacial** que interesa en el contexto del presente informe ligado a la defensa es el fundamentalmente focalizado en el desarrollo y operación de sistemas espaciales relacionados con el planeta Tierra y no con la exploración del espacio profundo. Durante décadas el sector espacial ha servido de **impulso al desarrollo de tecnologías y aplicaciones disruptivas**, tanto en el segmento espacial como en el de estaciones en tierra necesarias para su control y operación, incluyendo la tecnología de cohetes lanzadores. Estas tecnologías han servido de base para el desarrollo de plataformas satelitales, aisladas o formando parte de constelaciones, así como aplicaciones basadas en la **explotación de datos espaciales** de utilidad en múltiples sectores, desde la pesca y agricultura o el medio ambiente al transporte, las comunicaciones, o la defensa y la seguridad.

La relevancia del sector espacial se observa no solo en términos cuantitativos medidos por el **incremento constante del volumen del mercado espacial**, sino también en su **relevancia para la sociedad**. Baste para ello con referirse a la relevancia y penetración que han alcanzado los sistemas de **navegación satelital** como el *GPS* o el *Galileo*, empleados por millones de

ciudadanos, el desarrollo de cámaras de alta resolución en diferentes frecuencias (desde ópticas a infrarrojas) para la observación del planeta, o su uso en los sistemas de telecomunicaciones satelitales digitales ya sea en **órbitas bajas** (LEO)³⁶⁰ basada en constelaciones de miles de satélites, como en **órbitas geoestacionarias** (GEO) que proporcionan servicios de respaldo o en zonas en las que no hay cobertura por redes terrestres, o sistemas que combinan órbitas bajas y medias.

Un elemento clave para comprender la relevancia actual del sector espacial y las limitaciones surgidas en la cooperación internacional es el reconocimiento de que **la tecnología espacial posee un carácter dual**, hecho evidente desde su inicio a mediados del siglo XX y, por tanto, muchas de sus aplicaciones. Por ello, no es de extrañar que el dominio tecnológico del sector espacial haya tenido, tenga y tendrá una **dimensión geopolítica** muy relevante, históricamente ligada a la **confrontación entre grandes potencias**, con una creciente implicación de las Fuerzas Armadas y de la industria de defensa.

El creciente **papel que está jugando la tecnología espacial en los conflictos armados** del siglo XXI ha fortalecido esta visión: desde las telecomunicaciones, a la observación de la Tierra o a la navegación espacial, incluyendo el desarrollo de armas cibernéticas o cinéticas espaciales que inhabiliten o destruyan respectivamente a satélites, las grandes potencias se han dotado de medios y **organizaciones espaciales específicas en sus fuerzas armadas**.

5.5.1 Situación del sector espacial militar

El sector espacial se puede agrupar en **tres subsectores** con características diferenciadas: **civil**, de **seguridad nacional** (es decir, plataformas y aplicaciones para defensa e inteligencia) y **comercial** ya sea en modelos de negocio entre empresas (B2B) o proporcionados al consumidor (B2C). Cada subsector opera con sus propios objetivos y activos, aunque dependen de una **base industrial, de talento cualificado y de infraestructura espacial** que puede ser común en base a la caracterización dual de muchas de las tecnologías implicadas y a la necesidad de optimizar los recursos de operación y explotación³⁶¹ (Bataille, 2024).

Como dato relevante, de los satélites orbitando la Tierra en 2023 el **70% eran militares o de doble uso**. Solamente **en 2023 se lanzaron 107 satélites militares** con lo que su número total supera los 900 y se estima alcanzar los 2.500 satélites militares en los próximos diez años. La distribución del volumen de mercado por países refleja una **situación fuertemente concentrada en unos pocos países**: Estados Unidos, China, Rusia, y Francia, seguidos a bastante distancia por Japón, Reino Unido, la UE (programas comunitarios), Alemania, e India.

360 Las órbitas se clasifican por la altitud a la superficie de la Tierra en bajas (entre 150 y 2.000 Km), medias (entre 2.000 y 35.786 km) y geoestacionarias (de 35.768 Km con lo que su periodo es igual al de rotación de la Tierra. Ahora también se empieza a prestar atención a órbitas ultra bajas (por debajo de los 150 Km).

361 https://www.spacefoundation.org/space_brief/space-sectors/

Centrando el análisis en los aspectos clave del **mercado de satélites militares** en 2024 existen **discrepancias apreciables** entre los informes consultados derivados de la forma de contabilizar los usos duales de los satélites. Como ejemplo, el informe de “*The Business Research Company*” estima que en 2024 se han alcanzado los 63.600 millones de dólares y estima que en 2028 se alcanzarán los 74.400 millones de dólares con un CAGR moderado del 4%. Para *Fortune business* el tamaño mundial del mercado de satélite militar se valoró en 17.110 millones de dólares en 2024 y espera que el mercado crezca de 18.440 millones en 2025 a 30.000 millones para 2032 a una tasa compuesta anual de 7.2% más de 2025-2032³⁶². Otros informes como el de *Precedence Research* estiman cifras más bajas³⁶³. Para esta empresa **Europa tiene un destacable 21%**, exponente de la relevancia del sector espacial en la UE y el Reino Unido.

La mayor parte de los satélites actuales son de **uso comercial**, y se corresponde con **satélites pequeños** (“*smallsats*”) con una masa en el lanzamiento entre 181 y 500 Kg situados en órbitas bajas (OECD, 2023). Existen datos actualizados sobre los objetos espaciales existentes como los publicados por la ESA en septiembre de 2024.

En la figura 5.33, con datos procedentes de la *Agencia Europea del Espacio (ESA)*, puede verse su evolución en el tiempo atendiendo a la **masa del objeto**. Actualmente, más de 20.000 objetos, desde satélites hasta desechos espaciales, orbitan la Tierra, y una oleada de nuevos lanzamientos de satélites comerciales previstos podría triplicar este tráfico en pocos años. Ello conlleva el incremento de riesgos asociados derivados de impactos con los desechos espaciales.

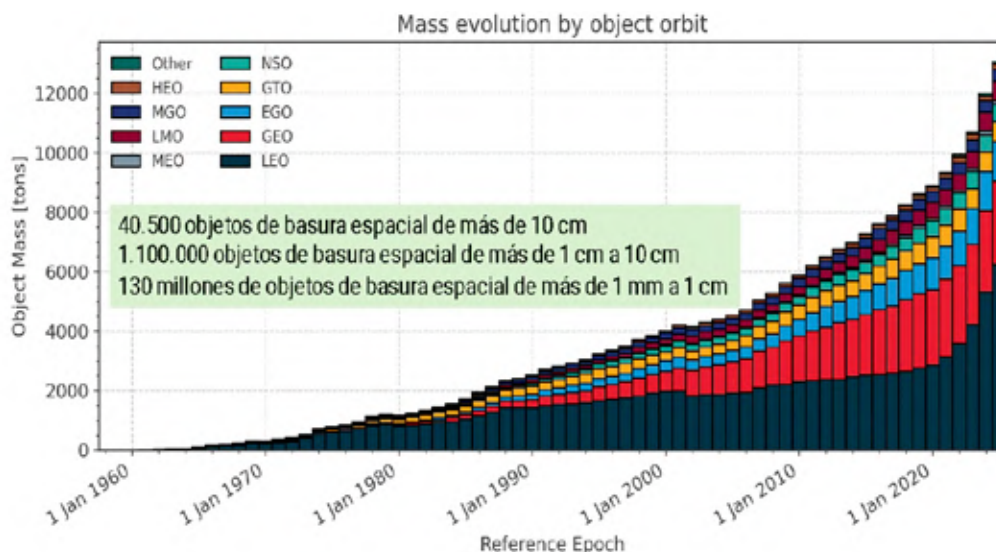


Figura 5.33. Evolución en el tiempo de objetos espaciales

Fuente: <https://sdup.esoc.esa.int/discosweb/statistics/static/allEvoTypeCnt.png>

362 <https://www.fortunebusinessinsights.com/es/military-satellite-market-106401>

363 <https://www.precedenceresearch.com/military-satellite-market#:~:text=The%20global%20military%20satellite%20market,6.95%25%20between%202024%20and%202034>

El **espacio**, en distancias cercanas al planeta, **se ha convertido en un dominio disputado entre las grandes potencias**. No se trata de un dominio aislado que se gestiona independientemente, sino que **se integra con los dominios clásicos de mar, tierra y espacio**, y con los menos clásicos de **ciberespacio y sociocognitivo** en una **visión multidominio** muy influenciada por la convergencia de tecnologías maduras y el aprovechamiento de tecnologías duales.

Desde el inicio de la denominada “*carrera espacial*” a mediados del siglo XX, el uso dual del espacio siempre ha sido un tema candente entre países a pesar de que ha sido considerado por las Naciones Unidas como un espacio “*abierto a la cooperación y a la paz*”. A nivel mundial, el **Tratado sobre el Espacio Ultraterrestre (OST)** de 1967 que todavía se encuentra en vigor³⁶⁴, tiene un **efecto disuasorio limitado** sobre el uso de armas no nucleares en el espacio u otras armas de destrucción masiva, pero **no contempla otros usos militares del espacio que la tecnología ha hecho posible desde entonces**. También, producto de la ampliación del OST efectuada en 1979, se ha aprobado impedir que los estados se arroguen la soberanía de satélites naturales como la Luna o partes de ella, así como de otros objetos en el espacio.

A pesar de todo ello, no es tan evidente que el acuerdo tácito del uso pacífico del espacio pueda preservarse en el futuro, como demuestra el hecho de la emergencia y despliegue (afortunadamente, todavía no el uso) de **armas antisatélite (ASAT)** por parte de varios países. La preocupación compartida por muchos países es que el incremento de satélites militares y el despliegue de diversos tipos de ASAT podría tener consecuencias importantes para la seguridad mundial, lo que, a su vez, podría dar lugar a una posible **aceleración de la carrera armamentista en el espacio** como ya ocurre en otros dominios.

Además de las potencias occidentales, según informes de inteligencia no clasificados citados en Berkowitz (2024), Rusia y China están adquiriendo u operando varios sistemas basados en el espacio de **armas cibernéticas, de guerra electrónica (EW), de energía cinética, de energía dirigida, nucleares y orbitales antisatélite (ASAT)**. El gobierno de los Estados Unidos también ha confirmado recientemente que Rusia ha desarrollado y se está preparando para desplegar un sistema antisatélite con armas nucleares en órbita. Además, Irán y Corea del Norte operan capacidades cibernéticas, de EW y de misiles que pueden interferir con los activos y operaciones espaciales de otros países. Las cuatro naciones mencionadas han llevado a cabo operaciones de **ciberguerra naval** contra el sistema de navegación y posicionamiento americano GPS.

364 Existen diversos Tratados de las Naciones Unidas (Tratados y Principios de las Naciones Unidas sobre el Espacio Ultraterrestre <https://www.unoosa.org/pdf/publications/STSPACE11S.pdf>) que inciden en el uso pacífico del espacio.

Ante la situación indicada, no es extraño que la UE en la **Estrategia Espacial de la UE para Seguridad y Defensa**³⁶⁵ aprobada en marzo de 2023 (EU, 2023) preste atención preferente a estas amenazas como parte de la *Brújula Estratégica* de la Unión.

Baste observar en la figura 5.34 (obtenida de la UE) que las **amenazas para el uso del espacio** no proceden solo de las características naturales del espacio (p.ej. la existencia de una radiación que puede inutilizar los sistemas o la existencia de asteroides que pueden provocar impactos a enormes velocidades³⁶⁶), sino de otras muchas provocadas por el ser humano, desde los impactos con fragmentos de naves espaciales, los ciberataques provocados por otras potencias, hasta las armas cinéticas antisatélite, o, desde un punto de vista de tecnologías aún menos maduras, los brazos robóticos que pueden “robar” o desplazar un satélite de su órbita inicial para hacerlo inoperativo.

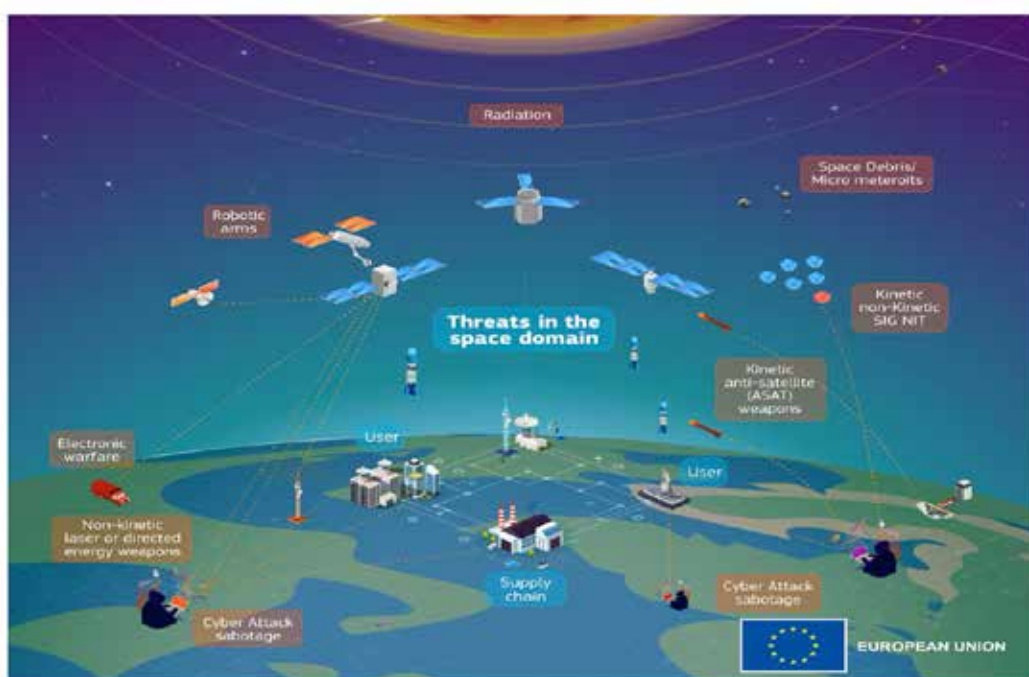


Figura 5.34. Amenazas en el espacio

Fuente: https://defence-industry-space.ec.europa.eu/eu-space/eu-space-strategy-security-and-defence_en

En resumen, nos encontramos en un momento en el que **el dominio y explotación del sector espacial se ha convertido en un factor decisivo desde la perspectiva de su uso en la defensa**. Un ámbito en el que la utilización de nuevas tecnologías juega un papel esencial y en el que, gracias a la consideración dual de muchas de ellas, los avances son muy rápidos.

365 EU Space Strategy for Security and Defence for a stronger and more resilient European Union. https://defence-industry-space.ec.europa.eu/eu-space-strategy-security-and-defence-stronger-and-more-resilient-eu-2023-03-10_en

366 Es interesante indicar que, si bien el tamaño del objeto es relevante, lo es más la velocidad a la que se produce un impacto porque la energía cinética depende del cuadrado de esa velocidad.

No es extraño, por ello, que **la inteligencia artificial (IA) juega y jugará un papel esencial** como se aborda explícitamente en la siguiente sección.

5.5.2 Aplicación de la IA en el sector espacial de defensa

5.5.2.1 Áreas relevantes de aplicación

La **rápida evolución del nivel de madurez** de técnicas de IA como el aprendizaje automático (*machine learning, ML*) o la IA generativa está haciendo que su uso en el espacio sea creciente, a pesar de tratarse de su aplicación en un **entorno complejo** como es el espacial en el que los errores acaecidos en un sistema tecnológico en órbita son muy caros y difíciles de resolver.

Desde una visión conceptual se ha representado en la figura 5.35 los **grandes impulsores del uso de la IA en el espacio**. En la parte central de la figura se han indicado dos *meta impulsores* ligados a la necesidad de **reducir el coste y el tiempo de desarrollo** de un satélite u otro objeto espacial y, al mismo tiempo, **mantener la máxima confianza en los procesos de verificación y validación** de componentes y subsistemas, procesos típicos en el sector espacial dadas las dificultades inherentes a la resolución de problemas una vez puesto en órbita. A ello se une la **necesidad de reducir los costes de lanzamiento** para que el **acceso al espacio** esté al alcance de muchos más países y entidades.



Figura 5.35. Impulsores del uso de la IA en el espacio. Fuente: Elaboración propia

En la parte superior de la figura 5.35 se ven tres **retos tecnológicos** cuyo abordaje requiere disponer de nuevas tecnologías adaptadas a su integración en el espacio:

1. Necesidad de **incrementar las capacidades de procesamiento a bordo** del satélite o nave espacial para poder disponer de sistemas espaciales más inteligentes en su propia gestión de la plataforma (p.ej. cambios en su órbita o de los paneles solares) y de las cargas útiles, incluyendo la cooperación entre satélites en el caso de formar parte de una constelación.
2. Necesidad de **reducir el volumen de transferencia de los datos** capturados por las cargas de pago del satélite (p.ej. cámaras o radares) a las estaciones terrestres con el objetivo de reducir la dependencia de los enlaces satelitales.
3. **Robustecer los sistemas de comunicaciones** de banda ancha, tanto ante eventos naturales en el espacio como es la radiación o los impactos, como frente a ciberataques provocados para inhabilitar el funcionamiento del satélite.

En la parte inferior de la figura precedente pueden verse cuatro **desarrollos tecnológicos relacionados con el uso espacial de la IA** que sirven de “*habilitadores*” frente a los retos indicados en la parte superior. Su maduración permite acelerar el desarrollo de las plataformas y las cargas útiles de satélites militares:

1. **Desarrollo de chips de altas prestaciones**, resistentes a las condiciones espaciales y de bajo consumo para el (re)entrenamiento de modelos de IA y para la extracción de inferencias³⁶⁷.
2. Generación de **gemelos digitales ciber-físicos** para facilitar y acelerar el proceso de diseño rápido de sistemas espaciales sobre la base de un modelo digital preciso del sistema a diseñar u operar conectado, si fuera posible, con componentes o sistemas reales.
3. Uso de la **IA generativa** basada en el uso de modelos grandes de lenguaje (LLM) adaptados a las necesidades del espacio y la defensa, aprovechando la tendencia en reducir el tamaño y, por tanto, las necesidades de computación.
4. Empleo de la **robótica inteligente** para facilitar operaciones en el satélite basados en brazos robóticos para reparación de módulos, gestión de vehículos autónomos asociados, o la recogida de desechos espaciales, entre otros muchos.

367 El concepto de “carga útil” (*payload*) en este ámbito se refiere a aquellos elementos de la nave espacial dedicados específicamente a producir datos de la misión y luego transmitir esos datos a la Tierra. Incluye elementos como cámaras, sistemas de comunicación, etc.

A pesar de todos estos avances la experiencia ha demostrado que llevar al espacio aplicaciones de IA muy extendidas en el planeta Tierra no es sencillo (Boozallen, 2025). De hecho, el modelo de **disponibilidad tecnológica** conocido como TRL (*“Technology Readiness Level”*) fue ideado por la NASA para asegurar que la tecnología estaba “suficientemente madura” para poder ser embarcada en una misión espacial con los menores riesgos posibles y evitar problemas de mantenimiento posteriores costosos o, incluso, imposibles. Se refleja en ello una **concepción conservadora de la adopción de la tecnología en el sector espacial**.

Por su parte la *Agencia Europea del Espacio (ESA)* como parte del programa de **Preparación para el Futuro de la Investigación Avanzada en Sistemas de Telecomunicaciones (ARTES)** ha financiado un estudio con el objetivo de conocer la forma en la que la industria espacial puede usar la **IA generativa para transformar los procesos de diseño de sistemas de comunicaciones con satélites**³⁶⁸.

Más concretamente, en la figura 5.36 se han representado las áreas concretas de aplicación de la IA en el sector espacial de la defensa en las que existen experiencias publicadas en fuentes abiertas en los últimos años.



Figura 5.36. Áreas de aplicación de la IA en el sector espacial de la defensa
Fuente: elaboración propia

Brevemente, las áreas identificadas son:

1. **Mejora del conocimiento del dominio espacial (SDA).** Su objetivo es comprender y gestionar los activos espaciales situados en el espacio y su posición real con objeto de

368 El estudio de carácter exploratorio está coordinado por Applied Data Science Partners (ADSP) <https://connectivity.esa.int/news/european-space-agency-kicks-groundbreaking-generative-ai-project-satellite-communication-design>

identificar otros objetos cercanos, amenazas derivadas de ello, y reducir los riesgos de la operación de una plataforma espacial.

2. **Defensa de la navegación satelital.** El objetivo es disponer de métodos que permitan conocer si la señal de navegación GNSS³⁶⁹ está alterada o es imposible de obtener ofreciendo técnicas de navegación alternativas a otros objetos aéreos o no para no depender de la señal satelital.
3. **Análisis inteligente de imágenes satelitales.** Capacidad de procesamiento de imágenes tomadas desde el satélite, ya sea desde el propio satélite o en estaciones terrenas para identificar objetos determinados de interés, y alimentar con la información obtenida la toma de decisiones en plataformas específicas basadas en IA. Puede formar parte de subobjetivos de SDA o para fines de seguridad marítima o terrestre apoyada por satélites.
4. **Ajustes automáticos de la órbita para evitar colisiones.** Conocimiento de la distancia y ajustes de la órbita de los satélites desde estaciones terrenas o por el mismo satélite si cuenta con sensores y capacidad de procesamiento suficiente a bordo para evitar impactos con otros objetos en el espacio (p.ej. desechos espaciales o asteroides) o para mejorar su funcionalidad.
5. **Mantenimiento predictivo de satélites.** Utilización de algoritmos de IA para planificar los procesos de mantenimiento del satélite en base al análisis de series temporales de datos combinados con otros datos capturados en tiempo real. Estos algoritmos pueden ejecutarse en estaciones terrenas o en la propia plataforma satelital cuando la capacidad de procesamiento a bordo lo hace factible.
6. **Optimización de comunicaciones militares espaciales.** Conseguir comunicaciones robustas de banda ancha con estaciones terrenas o entre satélites, inmunes a interferencias naturales en el medio espacial o las provocadas por el hombre.
7. **Ciberseguridad espacial.** La relevancia de los datos hacia o desde satélites, ya sean datos generados por las cargas útiles a bordo (p.ej. imágenes) o señales de control formando parte de redes de navegación o comunicaciones ha hecho que se conviertan en un objetivo de ciberataques, en gran medida, impulsados por otros gobiernos. Ello ha obligado a mejorar los sistemas de defensa frente a ciberataques.
8. **Robótica espacial inteligente.** Robots autónomos fijos (p. ej. brazos robóticos) o móviles (p.ej. antropomórficos cooperando con humanos, vehículos de explotación espacial)

369 GNSS significa Sistema Satelital de Navegación global (*Global Navigation Satellite System*). Es el término general que engloba todos los sistemas de navegación por satélite que proporcionan datos de posicionamiento globales.

para realizar múltiples misiones sin intervención humana con el mayor nivel de autonomía posible.

9. **Marcos comunes para la simulación e interoperabilidad de datos espaciales.** El uso de diversas plataformas y aplicaciones satelitales de uso militar se beneficia de la posibilidad de compartir datos obtenidos entre fuerzas armadas aliadas. Como sucede en el ámbito terrestre, la interoperabilidad de los datos espaciales es un elemento clave para disponer de sistemas y aplicaciones multifuente y multiproveedor.
10. **Integración de la IA con tecnologías cuánticas.** Su objetivo es analizar la forma en la que la IA puede integrarse con el uso de tecnologías cuánticas (comunicaciones, sensores o computación) en aplicaciones espaciales. Aunque se trata de un área en un estado experimental, merece la pena indicar las posibilidades y experiencias en marcha porque es previsible que su maduración (sobre todo, en comunicaciones y sensores cuánticos) va a ser rápida.

Además de las áreas de aplicación indicadas en el que el uso de la IA es creciente, y en el contexto de las tecnologías para el desarrollo es relevante mencionar el creciente interés suscitado en el **desarrollo y uso de gemelos digitales de sistemas espaciales**. Su objetivo es aprovechar las técnicas de **ingeniería digital** para disponer de modelos de datos y de simulación que permitan explorar opciones y acelerar los tiempos de desarrollo y mantenimiento de sistemas espaciales (plataformas satelitales, cargas útiles, modelos de entornos espaciales, etc.).

No se trata de áreas totalmente disjuntas, sino que **una correcta gestión global de los activos espaciales implica disponer de técnicas complementarias y de la explotación compartida de los datos obtenidos** lo que también ha impulsado acuerdos sobre estándares o formatos de datos interoperables.

5.8.2.2 Mejora del conocimiento del dominio espacial (SDA)

La **mejora del conocimiento del dominio espacial** (*Space Domain Awareness, SDA*) en base a información capturada sobre los objetos situados en el espacio y su posición real se ha convertido en un objetivo básico para comprender y gestionar los activos espaciales con el fin de **identificar amenazas y reducir riesgos** en la operación y funcionamiento de estos activos. La **proliferación de objetos en el espacio** requiere emplear nuevos enfoques para **conocer su situación real y poder tomar decisiones a tiempo**.

Aunque conceptualmente el objetivo de SDA es dual, civil y militar, **ha sido en el contexto de la defensa en la que ha cobrado mayor relevancia** puesto que suelen ser unidades militares las que operan los sensores empleados para recopilar datos (e inteligencia) de

cualquier objeto en el espacio para saber qué es y cómo podría afectar la seguridad de los activos espaciales de un país (Kratos, 2024).

El incremento de la complejidad del SDA hace que el uso de la IA se haya convertido en una técnica esencial. Para hacerse una idea de la complejidad, la Fuerza Espacial de Estados Unidos rastrea casi 45.000 objetos en órbita; si se tienen en cuenta factores como las condiciones atmosféricas y el clima solar, las variaciones en el campo gravitatorio de la Tierra, los cálculos necesarios para predecir las órbitas y advertir sobre posibles colisiones superan rápidamente la potencia computacional disponible (Tran et al., 2024), (Waterman, 2024). El uso de técnicas de IA ofrece a los analistas de inteligencia **mayor capacidad para el análisis de los datos** con restricciones temporales lo que, a su vez, permite simplificar la planificación de misiones, la optimización de recursos y la toma de decisiones en entornos espaciales complejos.

Como ejemplo de actividades de interés militar de SDA, el **Proyecto de Innovación Espacial Global (GSIP)** de la *Unidad de Innovación de Defensa (DIU)* de DARPA³⁷⁰ pretende **aprovechar la IA para recopilar, analizar y visualizar una red global de datos** de sensores comerciales y gubernamentales, terrestres y espaciales. Existen herramientas como *DEEP-Sight (Data Exploitation and Enhanced Processing)*³⁷¹, *KnownSpace*³⁷², o *ARC* de *Katalyst*³⁷³ para automatizar **el procesamiento de los datos de los sensores SDA mediante técnicas de aprendizaje automático.**

Tres enfoques complementarios del uso de la IA asociados a SDA son: el **uso de IA generativa** para disponer de **agentes inteligentes** para la ejecución de operaciones espaciales, el **uso de datos sintéticos** para calcular distancias entre satélites en constelaciones, y la **detección de satélites con comportamientos anómalos** en constelaciones de satélites. Se describen, brevemente, a continuación:

- Uso de agentes inteligentes

El uso de los **grandes modelos de lenguaje (LLM)** se está expandiendo más allá de las aplicaciones basadas en texto para convertirse en **agentes inteligentes de lenguaje** (Rodríguez-Fernández *et al.*, 2024) para la **planificación y operación de misiones espaciales**. Los LLM pueden ser utilizados como base para el desarrollo de agentes autónomos inteligentes capaces de tomar decisiones y acciones basadas en el procesamiento de datos digitales e información procedente de entornos complejos.

370 <https://www.diu.mil/latest/commercial-space-industry-providing-tools-to-advance-and-augment-space>

371 <https://nstxl.org/riverside-research-leading-three-nontraditional-organizations-on-space-domain-prototype/>

372 <https://www.kratosdefense.com/systems-and-platforms/space-systems/military-and-government/space-domain-awareness>

373 <https://www.katalystspace.com/arc>

Los resultados obtenidos por Rodríguez-Fernández *et al.* (2024) ponen de manifiesto las **limitaciones de los métodos tradicionales del aprendizaje por refuerzo** (*reinforcement learning*, RL) en aplicaciones espaciales dado que los algoritmos de RL suelen requerir un gran número de simulaciones y una “función de recompensa” bien definida para “aprender” políticas de control efectivas. Sin embargo, en el ámbito espacial, las simulaciones son escasas y difíciles de realizar, y definir una **función de recompensa** adecuada puede ser compleja si no se dispone de grandes conjuntos de datos. Debe tenerse en cuenta que en usos duales o directamente militares la compartición de datos para el entrenamiento de modelos es muy escasa.

- Detección de satélites con comportamientos anómalos

Otro ámbito de interés relacionado con SDA y facilitado por el uso de algoritmos de IA es la **detección de satélites con comportamientos anómalos en constelaciones de satélites**. Dado el crecimiento previsto en el lanzamiento de satélites para los próximos años³⁷⁴, se necesita emplear tecnologías de IA para monitorizar las constelaciones de satélites y rastrear el creciente número de objetos en el espacio y, si fuera posible, su comportamiento.

Como ejemplo, **Agatha** es una herramienta de IA desarrollada por *Slingshot Aerospace* (Slingshot, 2024) para identificar satélites atípicos dentro de grandes constelaciones en órbita baja (LEO)³⁷⁵. La tecnología se desarrolló en un programa financiado por DARPA sobre el uso de la IA para generar información sobre el dominio espacial y encontrar naves espaciales anómalas en grandes constelaciones de satélites. *Agatha* utiliza diversas técnicas de IA para procesar los datos de entrada con el fin de **detectar diferencias en las características y comportamiento de los satélites** y señalar aquellos con comportamientos potencialmente peligrosos, cambios en el perfil de la misión, o mal funcionamiento.

- Análisis inteligente de imágenes satelitales

La tecnología de observación de la Tierra desde el espacio está avanzando desde dos perspectivas complementarias: la **mejora en la capacidad de procesamiento a bordo** empleando sistemas de IA para analizar la información obtenida y reducir el flujo de datos a Tierra, y **transición desde la observación de satélites individuales a la integración de información procedente de constelaciones de satélites**.

Desde el punto de vista de la defensa, los **satélites** ofrecen ventajas críticas para funciones de **inteligencia, vigilancia y reconocimiento (ISR)**, lo que permite a las Fuerzas Armadas **saber, detectar, responder, y estar siempre preparado** ante amenazas si esta información

374 A principios de 2023, la Unión Internacional de Telecomunicaciones había recibido solicitudes para más de 300 constelaciones que representarían más de 1 millón de satélites.

375 <https://www.slingshot.space/news/slingshot-darpa-agatha-ai>

es capturada con la suficiente resolución, enviada y procesada a tiempo para la toma de decisiones. Como ejemplo, el uso de la IA para cruzar la información procedente de imágenes satelitales con inteligencia de señales podría proporcionar una visión integral de los movimientos militares. En pocas palabras, se trata de integrar la IA para fusionar la información procedente de sensores en el espacio, combinarlos con información desde sensores terrestres, extraer inteligencia de forma autónoma y construir modelos predictivos de lo que observan.

Si bien estas aplicaciones se ejecutan en estaciones terrestres, el problema es que implica recibir continua o muy frecuentemente un **volumen de imágenes muy elevado** lo que, a su vez, requiere enviar enormes cantidades de datos en tiempos limitados para que sean útiles, lo que conlleva el uso de canales de comunicación de gran ancho de banda. La solución proviene de la **mejora de la capacidad de computación a bordo** combinada con técnicas de IA en los propios satélites. Este análisis y el consiguiente filtrado de datos permite, además, **reducir el flujo de datos hacia estaciones terrestres** haciendo que ese procesamiento pueda hacerse en el satélite.

El Centro para el Avance de la Ciencia en el Espacio, que gestiona el *Laboratorio Nacional de la Estación Espacial Internacional (ISS)*, ha acordado en mayo de 2024 la realización de un proyecto con la empresa **LEOcloud**³⁷⁶ (proveedor de servicios espaciales en la nube adquirida por *Voyager Technologies* en 2025) para demostrar su infraestructura de **computación espacial en el borde como servicio**. Concretamente, **LEOcloud** instalará su **microcentro de datos virtualizado “Space Edge”** de primera generación en la ISS.

Más recientemente, el proveedor de servicios de seguridad y espacio *Voyager* ha anunciado en enero de 2025 un proyecto junto con *LEOcloud* para avanzar en la **tecnología de computación en el borde en el espacio con un enfoque en tecnología de neuro procesamiento**. El proyecto, tiene la intención de mejorar la fusión profunda de datos impulsada por la IA, la investigación y el desarrollo de microgravedad y las operaciones autónomas para usuarios finales comerciales y de defensa.

Por su parte, la Agencia Europea del Espacio (ESA) ha experimentado el uso de la IA para crear **nuevas capacidades en mini satélites inteligentes** desde 2022. Un ejemplo ha sido **FSSCat**³⁷⁷. Se trató de una misión innovadora de **dos CubeSats 6U federados**³⁷⁸ en apoyo de los servicios de Medio Ambiente Terrestre y Marino de Copernicus.

Un parámetro crítico para aplicaciones de defensa (inteligencia) es la **resolución alcanzada por la imagen** lo que, a su vez, permitirá o no un realizar un análisis posterior más preciso.

376 <https://www.leocloud.space/>

377 <https://earth.esa.int/eogateway/missions/fsscat>

378 Un satélite 6U es un CubeSat compuesto por seis unidades, “bloques” estandarizados de aproximadamente 10 cm³. De ahí viene el nombre de la clasificación de los satélites, los cubos que componen su estructura más que su forma completa. un CubeSat de 6U mide aproximadamente 30 cm x 20 cm x 10 cm.

Esencialmente, cuanto mayor sea la resolución, más pequeños serán los objetos que se pueden discernir en la imagen³⁷⁹.

Un ejemplo relevante en este sentido es el de la constelación de la empresa de Estados Unidos *Maxar Technologies* denominada **WorldView Legion**³⁸⁰. Se trata de una **constelación de seis satélites de observación** con uso dual civil y militar disponibles desde abril de 2025³⁸¹. *Maxar* ya dispone de 80 satélites en órbita y proporciona imágenes de inteligencia a 40 gobiernos, entre ellos Ucrania para ayudar a determinar objetivos rusos³⁸². La mejora en la resolución alcanzada en el caso de *WorldView Legion* puede verse en la figura 5.37.



Figura 5.37. Diferencias en la resolución de imágenes. Fuente: <https://ongeo-intelligence.com/blog/satellite-image-resolution>

También la IA se está empleando en sistemas de visión empleadas para la **observación de la Tierra en aplicaciones duales** con el objetivo de reducir el volumen de información enviada incrementando la capacidad de procesamiento a bordo. Sin procesamiento a bor-

379 Si la resolución es de 1 metro, cada píxel de la imagen representa un área cuadrada con una longitud de lado de 1 metro en la superficie de la Tierra

380 <https://ongeo-intelligence.com/blog/worldview-legion-advanced-satellite-imaging>

381 La constelación de Maxar puede recopilar más de 6 millones de kilómetros cuadrados de imágenes de la Tierra por día, incluidos hasta 3,6 millones de kilómetros cuadrados de imágenes de clase de 30 cm. <https://www.maxar.com/press-releases/maxar-successfully-launches-fifth-and-sixth-worldview-legion-satellites>

382 El uso de imágenes detalladas con fines militares hace también que su uso esté sometido a decisiones de los gobiernos en función de sus planteamientos geoestratégicos. Desde el 7 de marzo de 2025 Maxar ha comunicado que no puede proporcionar sus fotos a Ucrania (utilizadas con fines militares, pero también para la protección de civiles). La decisión se produce sólo unos días después de que la administración Trump confirmara la suspensión del intercambio de información y datos de inteligencia con el ejército ucraniano.

do se necesitan varias horas para procesar la información, y con procesamiento a bordo, cerca del tiempo real.

Uno de los casos en los que esta técnica ha demostrado utilidad es el de la **identificación de naves encubiertas** (“*buques oscuros*”) que se ha basado tradicionalmente en la descarga de imágenes ópticas de alta resolución capturadas por cámaras de observación de la Tierra. Sin embargo, dado que la capacidad de transmisión de datos como el almacenamiento son muy limitados, no siempre se pueden transmitir a una estación terrestre. Y cuando se reciben deben ser analizadas por humanos para identificar buques con la información del sistema AIS (*Automatic Identification System*)³⁸³. Se requiere emplear otra tecnología espacial para acelerar el proceso.

Este mismo enfoque de IA se está empezando a utilizar en pequeños satélites (Chintalapati *et al.*, 2024). Como un ejemplo más de uso de la IA vale la pena mencionar el desarrollo de Φsat-2 de la *Agencia Europea del Espacio* (ESA)³⁸⁴. Se trata de un mini satélite de tipo “*6u CubeSat*” diseñado para demostrar cómo las tecnologías de IA pueden **optimizar la observación de la Tierra (EO) desde el espacio** mejorando las capacidades de procesamiento a bordo.

El satélite **emplea herramientas de IA y sistemas de imágenes multispectrales** diseñados para 1) eliminar imágenes que están nubladas, 2) detectar y clasificar embarcaciones marítimas, 3) transformar imágenes de una forma a otra para la generación de mapas en tiempo real, 4) detectar anomalías en los ecosistemas marinos y detectar incendios forestales, y 5) herramientas para comprimir imágenes a bordo y reconstruirlas en tierra para reducir la descarga de datos.

5.5.2.3 Defensa de la navegación satelital GNSS

Un **Sistema de Navegación satelital** tiene como objetivo proporcionar servicios continuos de **posicionamiento, navegación y temporización (PNT)** a usuarios civiles, comerciales y de seguridad nacional en todo el mundo. La **navegación satelital del tipo GNSS**³⁸⁵ incluye el **GPS** de los Estados Unidos, el **GLONASS** de Rusia, el **Galileo** de Europa y el **BeiDou** de China.

Un sistema de navegación satelital se emplea habitualmente para **conocer la posición de un objeto en 3D y guiarle en su recorrido en base a la información recibida en tiempo real desde cuatro o más satélites** para poder determinar correctamente la posición de un objeto con la precisión necesaria.

383 AIS es un sistema de seguimiento costero de corto alcance que se utiliza actualmente en los buques. Fue desarrollado para proporcionar información de identificación y posicionamiento tanto a buques como a estaciones costeras.

384 Φsat-2 ha sido lanzado en agosto de 2024 a bordo de un SpaceX Falcon 9 con seis aplicaciones de IA.

385 El acrónimo GNSS se refiere a Global Navigation Satellite Systems.

El posicionamiento requiere que la señal se reciba correctamente, no esté alterada ni debilitada para poder recibirse e interpretarse. Actualmente, **la perturbación de la navegación satelital se ha convertido en un objetivo militar** no solo por parte de potencias militares, sino también de grupos terroristas o de la ciberdelincuencia organizada dada su consideración como **tecnología dual** relevante tanto para vehículos no tripulados (UAV, UGV, USV), o dispositivos de internet de las cosas (IoT). La denominada **“guerra electrónica de navegación”** (*Navigation Warfare, NAVWAR*) representa un dominio crítico dentro del espectro más amplio de la *Guerra Electrónica* (EW)

Un aspecto singular de NAVWAR es su **dilema de doble uso**. Las mismas capacidades que permiten conducir las operaciones militares podrían degradar las operaciones de las fuerzas amigas y dañar los sistemas civiles. La información puede ser alterada de forma intencionada empleando diversos métodos. Los más empleados son las **interferencias** (*“jamming”*) y la **suplantación** (*“spoofing”*).

- **GPS JAMMING (INTERFERENCIA)**. Ataque basado en enviar una señal que impide al UAV el cálculo de su posición real. Se basa en que la transmisión de una señal de potencia relativamente baja puede anular las señales GNSS mediante interferencias.
- **GPS SPOOFING (SUPLANTACIÓN)**. Ataque significativo mediante el envío de señales falsas a cualquier sistema inteligente que utilice señal GNSS para posicionamiento y navegación. Se basa en enviar una señal errónea intencionada al receptor del sistema para generar un cálculo erróneo de la posición con el fin de hacer creer al objeto que está en otra posición.

Las técnicas empleadas contra ataques del tipo **suplantación**, sobre todo, a la señal GPS sobre sistemas no tripulados se basan en el análisis de la señal de reloj con efecto Doppler y mecanismos de cifrado. Se trata de sistemas complejos que reducen la precisión de la posición al emplear muchos sensores mecánicos que acumulan errores y suelen generar múltiples alarmas de falsos positivos. Frente a estas limitaciones, **el uso de IA ofrece muchos mejores resultados** y se ha convertido en una herramienta indispensable para detectar si la señal de navegación ha sido alterada o permitir la navegación sin ella.

Panella (2024) describe diversas técnicas de navegación basadas en el uso de la IA. Algunas de ellas son las siguientes:

Integración de datos con IA en sistemas de navegación

Los **sistemas de navegación basados en IA** requieren la fusión de datos de varios sensores a bordo y de algoritmos de aprendizaje automático (ML). Al integrar información de

unidades de medición inercial (IMU), cámaras, radares, LIDAR³⁸⁶ y otras fuentes de datos ambientales como barómetros y magnetómetros, **la IA permite obtener una comprensión integral del entorno de la aeronave** (Aftatah y Zebbara, 2024). Estos sistemas de navegación basados en IA procesan constantemente datos de sensores, identifican patrones, toman decisiones en tiempo real y se ajustan a las condiciones cambiantes, todo ello sin depender de la entrada de satélites.

Los modelos de aprendizaje automático se entrenan con amplios conjuntos de datos de dinámica de vuelo, condiciones ambientales y posibles escenarios de navegación, lo que **permite a la IA “aprender” a interpretar los datos de los sensores** para garantizar un vuelo estable, seguro y preciso. Además, las redes de aprendizaje profundo permiten que los sistemas de navegación basados en IA predigan y reconozcan desafíos en tiempo real como obstáculos, cambios climáticos repentinos o interferencias hostiles. Estos sistemas pueden ajustar dinámicamente las trayectorias de vuelo y optimizar la eficiencia del combustible, el éxito de la misión y la seguridad general.

Sistemas de navegación inercial y navegación basada en IA

Un componente clave de la navegación basada en IA en entornos sin posibilidad de usar GNSS es la integración de sistemas de **navegación inercial (INS)**. El INS utiliza acelerómetros y giróscopos para calcular la posición de la aeronave mediante el seguimiento de la velocidad, la aceleración y la orientación. Sin embargo, los sistemas INS tradicionales son propensos a desviarse con el tiempo. Los sistemas de navegación basados en IA pueden mitigar esta deriva, ya que la IA monitoriza continuamente los errores acumulados y los recalibra para mantener un posicionamiento preciso.

Navegación visual e integración de IA

Al aprovechar las técnicas de visión artificial, los sistemas de IA utilizan cámaras o radares tipo LIDAR para detectar puntos de referencia, características del terreno y estructuras artificiales hechas por el hombre (p.ej. edificios, puentes, trincheras). Estas señales visuales permiten a la aeronave establecer su posición en relación con el entorno, lo que permite la navegación sin señales GNSS.

Capacidades autónomas y seguridad en la navegación basada en IA

A medida que las capacidades de la navegación basada en IA continúan evolucionando, la seguridad sigue siendo una prioridad absoluta. Los sistemas de navegación basados en

³⁸⁶ Se trata de una técnica de teledetección activa que utiliza un sensor embarcado en diferentes tipos de plataformas que emite pulsos de luz ininterrumpidamente y capta sus retornos, también denominados ecos o rebotes. Midiendo el tiempo que tarda en regresar ese pulso de luz, se puede calcular la distancia recorrida y, de esa forma, obtener la información tridimensional de los elementos.

IA pueden permitir que las aeronaves no tripuladas operen con una mínima intervención humana, incluso en entornos complejos donde las señales GNSS no son fiables o no están disponibles. Los algoritmos de IA supervisan el estado de los sensores, empleando técnicas de mantenimiento predictivo para evitar posibles fallos de funcionamiento del sistema.

A pesar de estos avances persisten **limitaciones frente a ataques combinados de interferencia y suplantación**: se ha probado en contextos concretos no generalizables en los que persisten altas tasas de falsos positivos y se requiere su validación frente a todo tipo de señal GNSS. Por estos motivos, se han desarrollado métodos para **rastrear la posición de aeronaves incluso cuando no puedan transmitir su posición GPS** utilizando solo su **dirección de aeronave de 24 bits** transmitida y la hora de recepción de equipos espaciales como cargas útiles.

Uso de relojes atómicos para PNT

Otro elemento necesario es la mejora de la precisión de la sincronización en sistemas de posicionamiento, navegación y control de tiempo (PNT). En este sentido, la **incorporación de relojes atómicos en satélites** representa un avance crucial para garantizar una sincronización ultra precisa y confiable.

Estos relojes, basados en **fenómenos cuánticos**, permiten medir el tiempo con una exactitud sin precedentes, lo que resulta esencial en operaciones que demandan alta precisión y robustez, como las maniobras tácticas militares, las telecomunicaciones críticas y la vigilancia en el espacio (véase el Anexo 3).

El **sistema de navegación Galileo** ofrece, desde enero de 2023, una **precisión** horizontal de hasta 20 cm y 40 cm en vertical, convirtiéndose en la primera constelación de navegación por satélite en ofrecer esta precisión de forma gratuita las 24 horas del día en la mayor parte del planeta en condiciones nominales. Galileo usa un sistema de tiempo (*Galileo System Time, GST*), mantenido por un conjunto de relojes atómicos ultra precisos con una exactitud de nanosegundos.

5.5.2.4 Ajustes de la órbita para evitar colisiones

La acumulación de desechos espaciales con más de 500.000 piezas de desechos espaciales más grandes que una canica, y millones de fragmentos más pequeños flotando en la órbita de la Tierra plantea un problema crítico, que podría **inutilizar ciertas órbitas y aumentar riesgos de colisión** (Shah, 2024); problema que se hace más crítico con el continuo lanzamiento de nuevos satélites, y el paso a una situación de no operatividad, pero aún en órbita de otros muchos.

Uno de los aspectos más preocupantes derivados del problema de los desechos espaciales es la posibilidad de que se desarrolle el denominado **síndrome de Kessler**, una cascada

de colisiones que se perpetúa a sí misma y genera más y más desechos. El consiguiente bucle de retroalimentación podría eventualmente hacer que ciertas regiones orbitales sean demasiado peligrosas para las operaciones de satélites, haciendo que grandes **franjas del espacio orbital de la Tierra sean inutilizables en el futuro**.

Tradicionalmente, **la vigilancia de los desechos o escombros espaciales se ha basado en radares y telescopios ópticos** para detectar y rastrear objetos en órbita. Estos métodos tienen limitaciones en términos de precisión, cobertura y procesamiento de datos en tiempo real. La creación de **modelos de IA basados en datos de código abierto para rastrear multitud de objetos en la órbita terrestre** de forma automática permite detectar **maniobras de satélites** que pueden evitar colisiones entre objetos espaciales o detectar el lanzamiento de misiles desde el espacio.

La IA tiene la capacidad potencial de transformar el **mapeo de desechos espaciales** de varias maneras **mejorando la velocidad y precisión de detección, y automatizando el proceso**. Los algoritmos de IA pueden procesar grandes cantidades de datos recopilados de satélites, sensores terrestres y telescopios mucho más rápido y con mayor precisión que los analistas humanos. Estos algoritmos son capaces de identificar objetos pequeños, predecir sus trayectorias y detectar posibles colisiones, proporcionando información crítica para evitar futuros accidentes espaciales. Concretamente, se ha empleado la IA en los siguientes casos:

- **Seguimiento impulsado por IA.** Los sistemas impulsados por IA están revolucionando el seguimiento de escombros mediante el análisis de grandes conjuntos de datos en tiempo real. Los **algoritmos de aprendizaje automático** predicen su movimiento, priorizan los objetivos de alto riesgo y proporcionan información procesable para las misiones de remoción de estos. Esto mejora la eficiencia y reduce los riesgos de colisión, lo que hace que la gestión orbital sea más precisa.
- **Sistemas autónomos de captura.** Las naves espaciales guiadas por IA equipadas con **brazos robóticos o remolcadores** pueden identificar y capturar basuras de forma autónoma. Mediante el uso de la visión artificial, estos sistemas se adaptan al movimiento impredecible de los residuos, lo que permite una eliminación precisa con una mínima intervención humana. Este enfoque ya se está probando en proyectos como la misión *ClearSpace-1* de la ESA³⁸⁷.
- **Láseres terrestres o espaciales guiados por IA.** Su función es **empujar suavemente pequeños escombros hacia las rutas de reentrada en la atmósfera** terrestre sin provocar una fragmentación. Algunas ideas para el futuro incluyen enjambres de satélites impulsados por IA que trabajan en colaboración para rastrear, capturar y transportar los escombros.

387 https://www.esa.int/Space_Safety/ClearSpace-1

- **Prevención mediante predicción.** La IA también es vital para prevenir nuevos desechos. Al predecir las colisiones de satélites y optimizar la eliminación al final de su vida útil, los operadores pueden mitigar los riesgos. El diseño impulsado por la IA garantiza que las futuras naves espaciales se construyan teniendo en cuenta la sostenibilidad.

5.5.2.5 Mantenimiento predictivo de satélites

El **uso de la IA para facilitar el mantenimiento preventivo** es bien conocido en múltiples aplicaciones en sectores industriales. Era lógico que, tras su progresiva maduración tecnológica, también se usase en el sector del espacio. Ello ha implicado adaptar la tecnología a su ejecución en satélites o naves espaciales combinado con el uso de modelos digitales del objeto espacial. Para ello, el mantenimiento predictivo se beneficia de los avances en **simulación** combinados con el uso de interfaces de **realidad virtual (RV)** y **realidad aumentada (RA)** en las interfaces del modelo con el operador.

La IA está desempeñando un papel cada vez más importante en el **software de simulación militar**. Los algoritmos de IA pueden crear entornos de formación dinámicos y receptivos que se adaptan a las acciones de los alumnos, proporcionando una experiencia más personalizada. Esta tecnología permite la simulación de tácticas y comportamientos enemigos, haciendo que los escenarios sean más desafiantes y realistas.

Un ordenador especializado (*Hewlett Packard Enterprise (HPE) Spaceborne Computer-2*) fue lanzado en febrero de 2021 a la ISS con el fin de proporcionar la **infraestructura para llevar a cabo experimentos avanzados** empleando soluciones basadas en IA y aprendizaje automático en el espacio. El ordenador está vinculado a la nube *Azure de Microsoft* a través de las estaciones terrestres de la NASA y HPE y permite procesar datos en órbita y **enviar a una estación terrena solo la información relevante**, con lo que se reducen los tiempos de transmisión de datos.

5.5.3 Optimización de comunicaciones militares espaciales

Con el desarrollo y despliegue de **constelaciones de satélites de comunicaciones en órbitas bajas**, empieza a tener relevancia el uso de la IA para la **optimización del rendimiento del diseño de constelaciones de satélites**. En el futuro el diseño de la órbita de los satélites deberá satisfacer demandas regionales diferenciadas, aprovechando el uso de algoritmos de IA basados en el aprendizaje por refuerzo y en el aprendizaje profundo para automatizar los necesarios ajustes orbitales.

Mediante el ajuste de las capas orbitales y las densidades de los satélites e incorporando en el diseño la distribución de las estaciones terrenas y datos de densidad de población, **la IA permite optimizar la utilización de los recursos existentes sin aumentar el número total de satélites**.

5.5.3.1. Caso de Starlink

La **constelación de banda ancha comercial** más desarrollada actualmente es la desplegada por la empresa **SpaceX** denominada **Starlink**.³⁸⁸ Su ritmo de lanzamiento es muy rápido (los primeros 60 satélites fueron lanzados en mayo de 2019) y en agosto de 2025 está formada por 8.094 satélites en órbita, de los cuales 8,075 estaban en funcionamiento. En julio de 2025 Starlink había superado los seis millones de clientes en 140 países

SpaceX espera llegar a tener **hasta 42.000 satélites operativos en su constelación**. Como es habitual, estos satélites han evolucionado. El despliegue de la constelación se está realizando mediante **lanzamientos simultáneos de decenas de satélites**. La **versión más moderna del satélite Starlink es la V2** que está operativa desde 2025 con una capacidad de datos cuatro veces mayor que sus predecesores, y con la capacidad de proporcionar servicios directamente a dispositivos celulares (Pultarova, 2025).

El desarrollo es continuo y acelerado. SpaceX ya ha anunciado el satélite **Starlink V3** que estará optimizado para el lanzamiento mediante el vehículo *Starship* de SpaceX. Cada lanzamiento Starlink V3 en Starship está planeado para añadir 60 Tbps de capacidad a la red *Starlink*, más de 20 veces la capacidad añadida con cada lanzamiento V2 Mini empleando un Falcon 9. Cada satélite **Starlink V3** permitirá alcanzar 1 Tbps de velocidad de bajada y 160 Gbps de capacidad de subida, lo que es más de 10 veces la capacidad de bajada y 24 veces la capacidad de subida de los satélites *Starlink V2 Mini*³⁸⁹.

Starlink es una **tecnología inherentemente dual** que se ha convertido en una herramienta fundamental: su uso no se restringe al ámbito civil, sino que también **se ha extendido al ámbito militar** como ha ocurrido en Ucrania tras la invasión de Rusia en 2022³⁹⁰. El acuerdo para la implementación de su uso fue extremadamente **eficiente** (el acuerdo inicial de *Starlink* se hizo en *Twitter*, y solo necesitó dos días para que el envío inicial del hardware llegara a Ucrania). Sin embargo, **la gobernanza de su uso no ha sido sencilla** por el control de la red y la prohibición del uso en determinadas zonas como ha sido el caso de Crimea (Bojor *et al.*, 2024). Últimamente, su uso como elemento de la negociación con Estados Unidos en marzo de 2025 para presionar al gobierno de Ucrania a aceptar las condiciones de un alto el fuego con Rusia le ha conferido una relevancia geopolítica mayor.

388 Un satélite de Starlink orbita a unos 550 Km de la Tierra y tiene una vida útil de aproximadamente cinco años. Las velocidades de descarga para los usuarios de Starlink están entre 25 y 220 Mbps, y las velocidades de carga entre 5 y 20 Mbps.

389 https://www.reddit.com/r/spacex/comments/1hqxsib/starlink_v3_specifications_and_a_starlink_v2_mini/?tl=es-es

390 El gobierno ucraniano solicitó terminales Starlink el 26 de febrero de 2022, solo dos días después de que comenzara la invasión, y las primeras llegaron al país el 28 de febrero. A principios de abril de 2022, SpaceX y la Agencia de Estados Unidos para el Desarrollo Internacional anunciaron que habían entregado conjuntamente unos 5.000 terminales Starlink a Ucrania, y que SpaceX había proporcionado directamente más de 3.000 de ellos. El número ha crecido desde entonces hasta los 25.000.

Más específicamente para su uso en el ámbito militar, SpaceX ha presentado un nuevo servicio denominado **Starshield**, una **red satelital segura que se basa en la tecnología de Starlink**, pero diferente de la empleada para servicios comerciales. **Starshield pretende ser más resistente** a ataques cibernéticos sofisticados³⁹¹.

Con el incremento masivo (decenas de miles) del número de satélites en una constelación, la **optimización de las órbitas** se ha convertido en un problema imposible de resolver sin el uso de técnicas de IA. Recientemente se ha empezado a evaluar el uso de aprendizaje profundo para **optimizar el diseño de las mejores órbitas para una constelación de satélites LEO** (del tipo de Starlink) con el fin de mejorar la cobertura en regiones polares o remotas (Shang, 2025). El aprendizaje profundo por refuerzo se aplica para optimizar los parámetros de la órbita, y ajustar la densidad de despliegue de satélites para mejorar el rendimiento de la cobertura y la utilización de recursos en áreas prioritarias.

5.5.3.2. Caso de IRIS² de la UE

La UE no dispone por el momento de una constelación de satélites para proporcionar servicios comerciales seguros de Internet³⁹². **Eutelsat** (fusionada con la británica *OneWeb*) se ha convertido en la **única constelación de satélites operativa de cobertura mundial junto con Starlink**. *Eutelsat* dispone de 630 satélites en la órbita baja terrestre que son suficientes para prestar un servicio similar en Europa³⁹³.

La iniciativa de la UE para el **desarrollo de la constelación de satélites IRIS²** (*Infrastructure for Resilience, Interconnectivity and Security by Satellite*) aborda los desafíos a largo plazo de la seguridad, la protección y la resiliencia de la UE al ofrecer **servicios de conectividad mejorados a los usuarios gubernamentales**³⁹⁴. La *Regulación* del Parlamento Europeo y del Consejo de IRIS² fue aprobada en marzo de 2023³⁹⁵.

391 SpaceX también está construyendo una red de cientos de satélites espía bajo un contrato clasificado con la Oficina Nacional de Reconocimiento (NRO), una agencia de inteligencia que gestiona satélites espía. La red está siendo construida por la unidad de negocio Starshield de SpaceX en virtud de un contrato de 1.800 millones de dólares firmado en 2021 con NRO. <https://www.reuters.com/technology/space/musks-spacex-is-building-spy-satellite-network-us-intelligence-agency-sources-2024-03-16/>

392 Airbus, Thales y Leonardo están explorando planes para establecer una empresa conjunta europea en el sector satelital, con el objetivo de desafiar la red Starlink con el “Proyecto Bromo” (en honor a un volcán indonesio). La iniciativa busca crear una compañía de satélites europea independiente siguiendo el modelo del fabricante de misiles MBDA, propiedad conjunta de Airbus, Leonardo y BAE Systems. <https://dig.watch/updates/european-space-companies-launch-satellite-initiative-to-compete-with-starlink>

393 Existen diferencias en la velocidad. Starlink promete banda ancha de hasta 200 megabits por segundo, mientras que la de Eutelsat es de 150. También se diferencian en el precio. Los terminales OneWeb cuestan cerca de 10.000 euros, a los que hay que añadir el precio de suscripción mensual. Mientras que Starlink cobra, según su web, un pago único de a partir de 349 euros con una suscripción mensual desde 29 a 40 euros, según el uso. https://www.elconfidencial.com/tecnologia/novaceno/2025-03-05/starlink-elon-musk-guerra-ucrania-rusia-eeuu-europa-internet-satelite_4079269/

394 https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en

395 Regulation (EU) 2023/588 of the European Parliament and of the Council of 15 March 2023 establishing the Union Secure Connectivity Programme for the period 2023-2027 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2023.079.01.0001.01.ENG&toc=OJ%3AL%3A2023%3A079%3ATOC

La nueva **constelación multi-orbital** estará formada por **290 satélites** y combinará los beneficios ofrecidos por los satélites de órbita terrestre media (MEO) y de órbita terrestre baja (LEO). Se basa en una infraestructura espacial con tres capas: MEO, a 8000km, y High-LEO, a 1200km, enfocadas a dar servicios de comunicaciones seguras de banda ancha en banda Ka militar; y la capa Low-LEO por debajo de los 750 km de altitud y de índole demostrativa, liderada por HISPASAT y concebida para incluir cargas de pago gubernamentales alojadas ("*hosted – payloads*"), que se beneficien del perímetro de seguridad de IRIS2, e interconectadas con el resto del sistema³⁹⁶.

Para aplicaciones de defensa, **IRIS² ofrecería conectividad de baja latencia y alta velocidad, lo que permitiría operaciones de combate colaborativas**. Sistemas como aviones de combate, fragatas, drones, satélites de reconocimiento, tropas terrestres y centros de mando podrían comunicarse en tiempo real sin restricciones de distancia. También puede servir como piedra angular para programas importantes como el *Future Combat Air System (FCAS)*, que integra cazas de próxima generación, drones de apoyo y una nube de combate.

Además, la red de 290 satélites actuará como relés de datos, lo que permitiría **transmitir imágenes de observación satelital a nivel mundial en tiempo real**. Esta arquitectura distribuida proporciona **resistencia frente a las amenazas antisatélite**. Por ejemplo, un misil dirigido contra un satélite tendría un impacto limitado, ya que los 289 satélites restantes seguirían funcionando.

Mientras tanto, **OneWeb** también sigue desarrollándose y en diciembre de 2024 Airbus Defence and Space se ha adjudicado un contrato con Eutelsat para construir la **ampliación de su constelación de órbita baja (LEO) OneWeb** con un total de 100 satélites, cuya entrega está prevista a partir de finales de 2026, garantizando la continuidad y la mejora del servicio para los clientes actuales y futuros. Los nuevos satélites permitirán la integración 5G en tierra, y garantizarán una **arquitectura tecnológica compatible con la constelación multiórbita IRIS²** que entrará en servicio en 2030³⁹⁷.

Es previsible que, al final de la presente década, las aplicaciones civiles deberían evolucionar hacia **receptores multimodo compatibles con varias constelaciones** (por ejemplo, *Starlink*, *OneWeb*, *Kuiper*) en terminales de usuario, como se ha visto en los sistemas GNSS para el mercado de la navegación satelital. Este proceso, sin embargo, parecía ser muy lento y **dependiente de la consolidación del mercado de comunicaciones basadas en constelaciones de satelitales**, y de desarrollar una competencia real entre operadores satelitales.

396 Se espera que la constelación aproveche la Infraestructura Europea de Comunicación Cuántica (EuroQCI), lanzada en 2019 con la participación de los 27 países de la UE. EuroQCI tiene como objetivo crear una red de comunicación cuántica segura a escala europea.

397 <https://www.airbus.com/sites/g/files/jlcbta136/files/2024-12/ES-Airbus-SpS-Press-Release-Airbus-awarded-Eutelsat-contract-to-build-Oneweb-low-orbit-constellation-extension.pdf>

Sin embargo, el proceso en el medio de conflictos militares se acelera. El operador móvil más grande de Ucrania, *Kyivstar*, comenzó a probar **servicios de mensajería satelital de servicio directo a celular (DTC) con Starlink** en julio de 2025³⁹⁸. Los teléfonos móviles con redes 4G o LTE se conectarán directamente a los satélites Starlink en órbita para que puedan enviar y recibir mensajes de texto. La eventual red, que se lanzará a mediados de 2026, dará a los ucranianos acceso al servicio celular en las zonas montañosas y rurales del país.

Este acuerdo puede ser un movimiento coherente para Ucrania a pesar de la **profundización de la dependencia con Starlink**, quien ha amenazado en el pasado con cerrar los servicios en el país. Pero para el gobierno de Ucrania *“la soberanía en este punto se convierte en una segunda prioridad... La prioridad número uno es ganar la guerra”*.

5.5.4 Simulación basada en IA e interoperabilidad de datos espaciales

El uso de la IA **está transformando el campo del modelado y la simulación**. Con herramientas de IA es posible crear **simulaciones más realistas en entornos sintéticos**, con “adversarios ficticios” y entornos que pueden adaptarse en tiempo real a las acciones del usuario, mejorando la predicción de comportamientos y resultados. Las simulaciones basadas en IA permiten practicar, ganar experiencia y para mejorar las habilidades del personal militar en un entorno seguro y controlado de toma de decisiones.

El uso de técnicas de modelado y simulación (M&S) está surgiendo en todo tipo de sectores, civiles y militares, y no es exclusivo del espacio. También el **uso de los gemelos digitales en los sistemas de simulación guarda estrecha relación con la IA** al permitir crear representaciones virtuales de operaciones y equipos reales. Esta funcionalidad facilitará un análisis detallado de tácticas y una evaluación continua del rendimiento, tanto a nivel individual como grupal, con retroalimentación en tiempo real.

En el ámbito de la OTAN la **conexión de los sistemas de mando y control C2 con los sistemas de simulación permite mejorar la preparación de los operadores** en el apoyo a las operaciones al permitir un mayor realismo y eficacia general, una disminución de los costes y riesgos, y una reducción del tiempo de preparación y respuesta. Un ámbito de creciente interés es el uso de la IA para **automatizar operaciones espaciales**. En el caso de los Estados Unidos el desarrollo del sistema experimental de mando y control en satélites **R2C2** (*Rapid and Resilient Command and Control*) permite automatizar algunas funciones de los operadores de satélite.

La **OTAN** ha establecido diversos *estándares* (conocidos como *STANAG*) para asegurar la **interoperabilidad de los sistemas de mando y control** en relación con otros tipos de

398 <https://www.euronews.com/next/2025/07/16/does-ukraines-first-in-europe-internet-deal-with-starlink-mean-more-dependence-on-elon-mus>

sistemas. Concretamente, facilitar la **interoperabilidad de los sistemas de Modelado y Simulación (M&S)** mediante arquitecturas de alto nivel (HLA, IEEE 1516) o la norma IEEE1278 que definen la **Simulación Interactiva Distribuida (DIS)** y que se recoge asimismo en el STANAG 4603.

5.5.5 Plataformas pseudo satelitales a gran altitud

Una tendencia que está adquiriendo gran importancia es el empleo en el ámbito de la defensa de las denominadas **“Plataformas a gran altitud” no tripuladas** (situadas en la estratosfera a una distancia de 18 Km a 22 Km de la superficie terrestre, superior a un avión, pero inferior a un satélite en órbita baja) reconocidas con las siglas de **High Altitude Platform Systems (HAPS)** o, de manera informal como **“pseudo satélites”**.

Al reducir la altitud a la superficie de la Tierra se consiguen menores latencias, y una menor potencia de señal en emisión y recepción, elementos básicos para múltiples **comunicaciones de banda ancha con terminales de usuario sencillos** y, especialmente, permitiría incorporar 6G al final de la presente década. Las HAPS tienen una superficie de cobertura mucho mayor que las estaciones de base terrestres y están mucho más cerca que los satélites de los usuarios terrestres (Abbasi *et al.*, 2024).

El **uso principal de las HAPS en el sector de la defensa** es el de apoyar las comunicaciones incrementando las tasas de transferencia de datos (incluyendo funciones de relé), y proporcionando un componente adicional dentro de redes integradas y servicios en la nube con reducción de costes frente a sistemas convencionales de comunicaciones satelitales LEO o GEO. También se espera que tenga utilidad en el sector de la seguridad como ha indicado *Frontex (European Border and Coast Guard Agency)* en 2023, en combinación con satélites.

La IA se utiliza cada vez más para **optimizar los pseudo satélites a gran altitud (HAPS)** para diversas aplicaciones: de planificación de la misión y navegación; en telecomunicaciones para mejorar la cobertura 5G de baja latencia y servicios de IoT mediante la optimización de las arquitecturas de red; en gestión de emergencias: mediante el análisis de datos históricos para la previsión y respuesta a desastres naturales; en la automatización de vuelos impulsada por IA mejora la navegación, la eficiencia operativa y la adaptabilidad a los cambios ambientales; y en la recopilación de datos en tiempo real para la gestión de desastres, la observación de la Tierra y otras aplicaciones críticas.

Se espera que en los próximos años **el uso de la IA integrado en plataformas HAPS crecerá de la mano del desarrollo y despliegue de 6G** (Abbasi *et al.*, 2024) en los que la gestión de recursos de comunicaciones se convierte en un problema complejo.

5.5.6 Gemelos digitales de sistemas espaciales

El concepto de **tecnología de gemelos digitales** fue propuesto inicialmente por la NASA en 2002. **Un gemelo digital es una réplica virtual de un sistema físico que refleja su comportamiento y características en tiempo real.** Combina datos de varias fuentes con información y visualizaciones sobre el comportamiento (Liu *et al.*, 2024).

El uso de gemelos digitales basados en modelos de datos y algoritmos de simulación basados en IA están suponiendo una revolución en la denominada **“ingeniería digital”** que permite **acelerar el desarrollo de sistemas complejos** en todos los dominios. Esta mejora también sucede en el dominio espacial. Cuando el gemelo digital interacciona con otras partes físicas en tiempo real se puede mejorar la comprensión del fenómeno y obtener datos para mejorar y aprender de ello.

Nos encontramos todavía en un momento en el que el uso de **gemelos digitales complejos ciber-físicos** (no solo modelos de datos sin conexión con entidades físicas) posee un nivel de madurez no muy elevado por lo que la experimentación y la obtención de conjuntos de datos fiables y robustos es esencial. Sin embargo, muchas agencias espaciales han comenzado a exigir en los contratos con empresas proveedoras la **entrega de un modelo digital para facilitar su operación y mantenimiento posterior**. Un ejemplo es la adjudicación por parte del Departamento de Defensa de Estados Unidos a **Sedaro Corporation** un contrato SBIR para **implementar la plataforma de gemelos digitales Sedaro**³⁹⁹.

5.5.7 Robótica espacial potenciada por la IA

En las últimas dos décadas **la IA ha permitido dar un impulso a la robótica** permitiendo que **sistemas robóticos** ya sean robots antropomórficos colaborando con humanos (*co-bots*), vehículos robotizados (*rovers*) o brazos robóticos en sistemas fijos como se hace en la industria sean **capaces de tomar decisiones de forma más inteligente en función de la información recibida en tiempo real del entorno**.

En el sector espacial el uso de la **robótica espacial inteligente** ha cobrado impulso tanto en sistemas de exploración de otros objetos espaciales (la Luna, planetas, asteroides, etc.) como para los propios satélites o naves espaciales. **La robótica espacial implica el diseño y la fabricación de robots adaptados para operar en el entorno del espacio ultraterrestre** y satisfacer diversas funciones en misiones espaciales. Puede tratarse de *rovers* (móviles) o fijos en la superficie de un planeta o luna, o en naves espaciales orbitando la Tierra u otros objetos espaciales (Zhihong *et al.*, 2022).

399 <https://www.sda.mil/>

A diferencia de las generaciones anteriores **los robots impulsados por IA apoyados por visión por computadora pueden evaluar su entorno y tomar decisiones de forma autónoma**. Con esa capacidad se adaptan a condiciones impredecibles o desconocidas durante las misiones, ofreciendo mayor autonomía para operar de forma independiente cuando no hay comunicación con la Tierra o las latencias son muy elevadas para ser efectivas⁴⁰⁰.

La incorporación de **sistemas de IA permite a los robots espaciales realizar tareas muy diversas** como la recolección de muestras, el ensamblaje de estructuras y la navegación por terrenos complejos con una mínima intervención humana. A través del aprendizaje automático, los robots refinan continuamente sus movimientos para una mayor precisión. Además, la IA avanzada permite a estos robots crear mapas en 3D, identificar obstáculos y planificar rutas eficientes, lo que los hace esenciales para la exploración planetaria.

Un ámbito específico de interés de la NASA es que las actividades de construcción en la Luna y Marte pasen progresivamente del diseño teórico a la **creación de infraestructuras reales**. La combinación de la robótica impulsada por la IA que utiliza la impresión 3D y las operaciones autónomas de abastecimiento de materiales construirá los fundamentos básicos de la infraestructura extraterrestre. La NASA tiene como objetivo **enviar robots autónomos para construir hábitats espaciales de forma autónoma sin supervisión humana a partir de 2028**, aunque estos programas pueden ralentizarse por problemas presupuestarios.

Los rovers de Marte de la NASA, *Curiosity* y *Perseverance*, ejemplifican esta tecnología mediante el **uso de IA para navegar y analizar muestras de forma autónoma**, mientras que el helicóptero *Ingenuity* impulsado por IA de *Perseverance* amplía la exploración con estudios aéreos de áreas inaccesibles para los rovers. Concretamente, el *Mars Rover Perseverance* utiliza la IA para navegar de forma autónoma por la superficie marciana, identificar sitios prometedores para la exploración, analizar rocas, y evitar peligros

El instrumento más avanzado con IA a bordo del *Mars Rover Perseverance* es el **Planetary Instrument for X-ray Lithochemistry (PIXL)**. La IA ayuda a **PIXL** de dos maneras. En primer lugar, permite colocar el instrumento justo una vez que el instrumento está en las proximidades de un objetivo rocoso. Situado en el extremo del **brazo robótico del Perseverance**, la cámara de **PIXL** verifica repetidamente la distancia entre el instrumento y la roca objetivo para ayudar con el posicionamiento. La figura 5.38 permite ver el instrumento **PIXL** y el análisis generado de una roca.

400 <https://nstxl.org/ai-driven-advancements-in-space/>

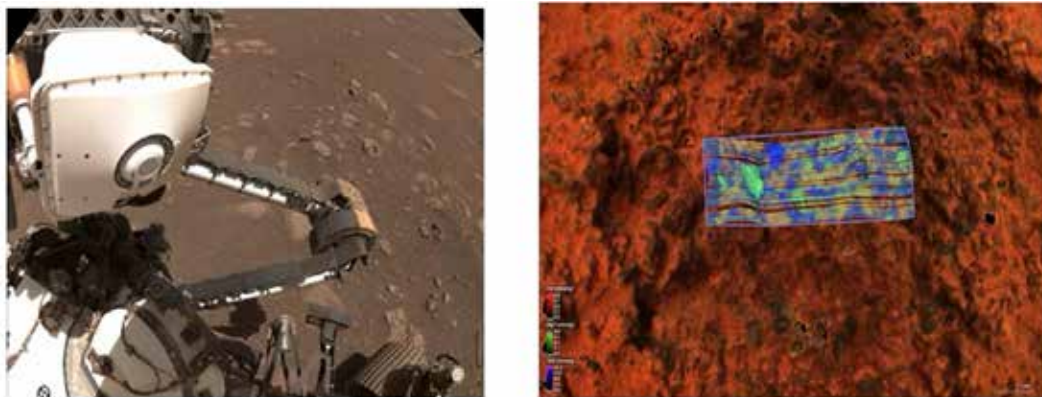


Figura 5.38. Izquierda: Instrumento PIXL del Mars Rover Perseverance y Derecha: Imagen de una roca de Marte creada usando PIXL, que determina su composición mineral con rayos X. Fuente: <https://www.nasa.gov/missions/mars-2020-perseverance/perseverance-rover/heres-how-ai-is-changing-nasas-mars-rover-science/>

Es indudable que estas experiencias robóticas de la NASA como las indicadas están asociadas a un uso científico, civil y no militar, del espacio. Sin embargo, también se han empezado a desarrollar otros **sistemas robóticos espaciales con fines duales** o militares contando con la financiación de agencias de I+D de defensa.

Uno de estos desarrollos es el llevado a cabo por el **NRL** (*U.S. Naval Research Laboratory*) del *Naval Center for Space Technology* de Estados Unidos financiado por DARPA. En 2024 se ha completado el **desarrollo de un sistema robótico para una nave espacial calificado para dar servicio a satélites en órbita** (Pasquini, 2024) denominado “*Robotic Servicing of Geosynchronous Satellites Integrated Robotic Payload*”. La figura 5.39 permite ver el sistema en desarrollo.



Figura 5.39. Sistema robótico de NRL. Fuente: <https://www.defense.gov/News/News-Stories/Article/Article/3966145/naval-research-lab-completes-development-of-satellite-servicing-robotics/>

Si bien es cierto que muchos de los sistemas robóticos espaciales en desarrollo son experimentales, no hay que olvidar que **el desarrollo se va a acelerar**. NASA, junto con organizaciones espaciales privadas, utilizará 10.000 millones de dólares de su presupuesto en 2025 para **impulsar el desarrollo espacial basado en IA e iniciar la exploración espacial asistida por máquinas**⁴⁰¹.

5.5.8. Situación de Europa en el uso de la IA espacial en defensa

Las capacidades europeas en el desarrollo de aplicaciones de IA en el sector espacial de la defensa tienen luces y sombras. Son muchos los países europeos que participan en el sector espacial (tanto de la UE como también, principalmente, el RU) y se ha incrementado el número de empresas start-ups con productos disruptivos de doble uso para el diseño de plataformas satelitales, cargas útiles y servicios ligados (p.ej. procesamiento de imágenes satelitales y computación en el borde). Sin embargo, Europa no posee todavía capacidades de lanzamiento recuperable y depende de empresas de Estados Unidos para ello (Loizou e Ippolito, 2024).

Uno de los sistemas duales exitosos ha sido el desarrollo por la UE durante las últimas dos décadas del sistema de navegación **Galileo**. Específicamente relevantes en el contexto de uso dual son los servicios derivados del uso de la señal gubernamental **PRS** (*Public Regulated Service*) para administraciones públicas y aplicaciones sensibles como defensa, seguridad y emergencias. Este servicio **utiliza la IA** para gestionar datos complejos, optimizar la navegación y proteger contra interferencias o ciberataques.

Asimismo, **la señal PRS ayuda a gestionar datos GNSS fusionados con sensores inerciales y otros sistemas**, optimizando la precisión y resistencia frente a interferencias como las de interferencia y suplantación de la señal satelital. Además, se utiliza en la monitorización y análisis de señales para garantizar la autenticidad y protección de datos cifrados, esenciales para aplicaciones militares y de defensa garantizando la autenticidad y seguridad de las señales. Concretamente: 1) el uso de modelos predictivos para la monitorización y predicción de actividad ionosférica, mejorando la precisión en condiciones adversas, y 2) el procesamiento avanzado de señales mediante técnicas como modulación **BOC** (*Binary Offset Carrier*), que optimiza la robustez y eficiencia espectral del sistema.

La IA mejora la **interoperabilidad del servicio PRS de Galileo** con otros sistemas de navegación satelital **GNSS** al optimizar la integración de datos y mejorar la resiliencia del sistema. Empleando técnicas de **aprendizaje automático se pueden fusionar señales GNSS de múltiples constelaciones** (Galileo, GPS, GLONASS) **y sensores adicionales**, garantizando precisión y robustez incluso en condiciones adversas. Además, la IA facilita la detección de

401 <https://ai-techpark.com/ai-robotics-space-exploration-2025/>

interferencias y la autenticación de señales, fortaleciendo la cooperación entre sistemas globales para aplicaciones críticas como defensa y transporte.

También se emplean **algoritmos de IA para la explotación de datos** del sistema de uso dual de observación de la Tierra denominado **Copérnico**, de los diversos satélites de comunicaciones en órbitas geoestacionarias de los países de la UE junto a las múltiples aplicaciones desarrolladas por la ESA en el programa **ARTES** (*Advanced Research in Telecommunications Systems*) (ARTES, 2024), y la obtención de información de lanzadores de la UE con los cohetes **Ariane 6**. Este uso se incrementará en los próximos años con el desarrollo y despliegue de la constelación de satélites **IRIS²** en órbitas combinadas LEO y MEO mencionado anteriormente.

Un problema que aún sigue pendiente para extraer todas las ventajas del uso de la IA es la **estandarización de los datos y metadatos** lo que limita la colaboración efectiva en aplicaciones de defensa y seguridad en las que participan diversos países aliados⁴⁰². Para ello, sería necesario **Actualizar y promover el uso formatos interoperables como RINEX** (*Receiver Independent Exchange*)⁴⁰³.

En el contexto del **diseño digital** es destacable el esfuerzo de la ESA para experimentar el uso de modelos digitales basados en IA para acelerar el desarrollo de satélites. Concretamente, el programa de **diseño disruptivo de sistemas de comunicación satelital con diseño generativo** (*Disruptive satcom Systems Design with Digital Generative Design*) financiado por la ESA (ARTES, 2024) pretende **experimentar el uso de las técnicas de IA generativa** dentro del dominio de las comunicaciones por satélite.

Estas tecnologías de IA, aunque prometedoras, presentan una **curva de aprendizaje compleja** y con incertidumbres con respecto a su aplicabilidad y efectividad en el diseño de satélites de comunicaciones para que las soluciones generadas por IA no solo sean innovadoras, sino también prácticas, fabricables y que cumplan con los estándares de la industria. Además, el éxito de la IA generativa depende en gran medida de la disponibilidad y la calidad de los datos.

Se pueden citar algunas empresas españolas proveedoras de servicios espaciales.

Deimos Space⁴⁰⁴ es una empresa española con capacidades de uso de IA en el sector espacial. Como ejemplo, puede mencionarse su participación en el proyecto CISERES de

402 <https://www.ftidefense.com/news/accelerating-data-management-decision-chain-military-space-operations>

403 Se trata de un formato ya antiguo (1989) de archivos de texto que almacena, de forma estandarizada, información del cálculo de magnitudes como la posición y las velocidades a partir de una serie de mediciones a los satélites de las diferentes constelaciones GNSS. Este formato también permite el intercambio y procesamiento de datos independientemente de la marca, modelo o característica del receptor GNSS o sistema de procesamiento. El formato se ha ido actualizando periódicamente y la última versión (4.01) es de 2021 en la que se ha incluido más metadatos de las señales GNSS para poder automatizar el análisis de la información. <https://gisresources.com/from-rinex-4-0-a-guide-to-gnss-data/>

404 Fue fundada en 2001 con sede en España y subsidiarias en Portugal, Italia, Rumanía y Reino Unido. Desde el 1 de noviembre de 2024, Deimos fue adquirida por Indra y se fusionó con Indra Espacio.

la ESA⁴⁰⁵; se trata de una pequeña misión satelital liderada y cofinanciada por Deimos, diseñada para mejorar significativamente los tiempos de respuesta a las crisis utilizando procesamiento de imágenes satelitales a bordo e IA predictiva. Con ello, el tiempo necesario para compartir datos podría reducirse a menos de un minuto reduciendo megabytes de datos a unos pocos kilobytes.

Otro ejemplo de capacidades españolas es la empresa **PLD Space**⁴⁰⁶ pionera y referente en Europa en el desarrollo de cohetes reutilizables, con el desarrollo de la familia de vehículos de lanzamiento **MIURA** y la cápsula tripulada LINCE. Colabora con *Deimos Space* para el desarrollo del sistema de Guiado, Navegación y Control del nuevo cohete MIURA 5, GMV en robótica y GNC entre otros.

También es relevante el **uso progresivo de la IA en grandes empresas con participación española**. Un ejemplo destacado del uso de la IA en el sector espacial es el uso del aprendizaje por refuerzo (*reinforcement learning, RL*) considerado por la empresa **Airbus** como la de mayor potencial, pues permite mejor escalabilidad y generalización, toma de decisiones en tiempo real con comportamiento adaptativo, posibilidad de hibridar RL con otros métodos.

Seguidamente, se describen algunos **proyectos emblemáticos** que ponen de manifiesto las capacidades tecnológicas españolas en el espacio relacionados con la IA: **El satélite de observación PAZ y su programa sucesor PAZ-2** y los dos satélites de comunicaciones del programa **SpainSat NG**.

El satélite **PAZ**, operado por *Hisdesat*, es el primer satélite radar español en observación de la Tierra, incluido en el **Programa Nacional de Observación de la Tierra por Satélite (PNOTS)**⁴⁰⁷. PAZ cubre las necesidades de **observación en seguridad y defensa** y otras de carácter civil, pudiendo tomar más de 100 imágenes diarias de hasta 25 cm de resolución, tanto diurnas como nocturnas, y con independencia de las condiciones meteorológicas⁴⁰⁸.

Permite la **observación del territorio para múltiples aplicaciones de carácter dual**: control fronterizo, inteligencia, control medioambiental, protección de los recursos naturales, operaciones militares, verificación de tratados internacionales, vigilancia de la superficie terrestre, urbanismo, planificación de infraestructuras, evaluación de catástrofes naturales y cartografía de alta resolución, entre otras.

405 https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Ciseres_AI-powered_satellites_for_rapid_disaster_response

406 La empresa fue fundada en 2011 por dos emprendedores, en Elche (Alicante), y en febrero de 2025 ya cuenta con más de 300 empleados. <https://www.pldspace.com/es/nosotros>

407 Se lanzó el 22 de febrero de 2018 a bordo de un cohete Falcon 9, desde la Base Aérea de Vandenberg, California <https://www.aee.gob.es/Actividades/Nacionales/PAZ.html>

408 Paz cubre un área de más de 300.000 kilómetros cuadrados al día, da quince vueltas diarias a la Tierra, a una altura de 514 kilómetros.

España ha puesto en marcha un nuevo **programa PAZ-2** de observación de la Tierra de interés militar tipo radar SAR con dos satélites que sustituirá al PAZ actual⁴⁰⁹. Se tratará de dos satélites con una resolución de imágenes de 25 x 25 cm y una imagen de 500 Km de tamaño. Al basarse en imagen radar de apertura sintética (SAR) podrá observar de día y de noche y descargar las imágenes en la banda K militar con un ancho de banda de 1,2 HGz. Los satélites PAZ-2 están previstos que sean lanzados en 2028 y no entren en servicio hasta diciembre de 2031 el primero y agosto de 2032 el segundo⁴¹⁰.

Se espera que España pueda alcanzar un **65% de tecnología nacional** en el desarrollo del programa PAZ-2. En la figura 5.40 puede verse una infografía de uno de los futuros satélites.



Figura 5.40. Infografía de un satélite del programa PAZ-2. Fuente: <https://www.infoespacial.com/texto-diario/mostrar/4900392/satelites-observacion-hisdesat-ultima-detalles-firmar-programa-paz-ii-junto-ministerio-defensa>

El **diseño de un nuevo sistema de satélites militares de nueva generación**⁴¹¹ denominado **Spainsat NG**⁴¹² arrancó en 2019 con un coste estimado total que se acercará a los 2.000 millones de euros con un metaobjetivo de **incrementar la soberanía tecnológica española en defensa**⁴¹³ y con los siguientes objetivos:

- Asegurar el **mando y control** efectivos en operaciones de las Fuerzas Armadas más allá de la línea de visualización en 2/3 de la Tierra.

409 <https://www.defensa.com/espana/defensa-pone-marcha-programa-paz-ii-observacion-tierra-valorado>

410 El acuerdo para la construcción se ha firmado el 9 de julio de 2025 entre Hisdesat y Airbus. <https://www.avionrevue.com/espacio/hisdesat-y-airbus-firman-el-acuerdo-para-la-fabricacion-de-los-satelites-del-programa-paz-2/>

411 Actualmente, las Fuerzas Armadas cuentan con dos satélites militares lanzados a principios del siglo actual en la fase final de su vida útil: Spainsat y XTAR-EUR.

412 <https://www.hisdesat.es/c-seguras/programa-spainsat-ng/>

413 Más del 40% de los satélites será desarrollado por la industria nacional, liderada por un consorcio de cuatro co-contratistas (las filiales francesa y española de las empresas europeas Airbus D&S y Thales Alenia Space), siendo Airbus DS España la contratista principal e integradora de la carga útil de banda X y TAS España la contratista principal e integradora de las cargas útiles de bandas Ka militar y UHF, actuando Airbus DS Toulouse como el líder del consorcio.

- Garantizar la capacidad de **comunicación en teatros de operaciones carentes de infraestructura** en los que España tiene o podrá tener tropas desplegadas.
- Desarrollar **comunicaciones satelitales en movimiento**, con mayor capacidad y seguridad.
- Liberar el potencial de la **red central de combate**.

El sistema completo de **Spainsat NG** está compuesto por una pareja de satélites **geoestacionarios** junto a su componente de control y seguimiento en tierra. El lanzamiento del primero de los satélites, el **Spainsat NG 1**, se ha realizado con éxito el 30 de enero de 2025 desde Cabo Cañaveral en Florida utilizando un Falcon-9 de Space X⁴¹⁴ (véase figura 5.41). El lanzamiento del segundo satélite **Spainsat NG 2** está previsto para octubre de 2025 (ventana de lanzamiento del 22 al 29 de octubre).



Figura 5.41. Despegue del satélite SpainSat NG I en Cabo Cañaveral el 30 de enero de 2025. Fuente: <https://www.infoespacial.com/texto-diario/mostrar/5242241/hisdesat-anuncia-lanzamiento-spainsat-ng-2-realizara-octubre>

Desde el punto de vista tecnológico los satélites *SpainSat NG* cuentan con propulsión iónica, chips diseñados específicamente, y un sistema de antenas muy avanzados de banda X con 16 haces independientes que se pueden orientar electrónicamente controladas por software (también tiene antenas en las bandas UHF y Ka). Eso permite modificar su tamaño y su forma para apuntar dónde sea necesario y reducir interferencias (*anti-jamming*) y de suplantación (*spoofing*) de acuerdo con los estándares de la OTAN. Asimismo, cuenta con protección ante radiación nuclear.

414 Se ha integrado en un cohete Falcon 9 de Space X lanzado desde Cabo Cañaveral en Florida.

El **desarrollo de aplicaciones y servicios** de uso militar sobre estos nuevos satélites incorpora tecnologías de vanguardia, integrando la IA con tecnologías de big data y de internet de las cosas, con el fin de garantizar prestaciones adaptadas a las necesidades militares actuales. Está previsto que ambos satélites den servicio de comunicaciones no solo a las Fuerzas Armadas españolas, sino también formarán parte de *Govsatcom* para dar servicio a la Comisión Europea, y también a la OTAN.

5.5.9 Apoyo a nuevas empresas de base tecnológica en el sector espacial

En muchos casos la innovación en el espacio se basa en sistemas con tecnologías desarrolladas por empresas consolidadas del sector espacial. Sin embargo, ha crecido el **interés en la creación de nuevas empresas de base tecnológica europeas con productos disruptivos** basados en tecnologías emergentes.

Estas startups suelen enfrentarse a barreras de entrada elevadas con reticencias de los fondos de inversión convencionales para asumir riesgos elevados, y, al menos, en las primeras fases desde su creación requieren apoyo público especializado para poder consolidar su oferta y escalar. Con este motivo, la Comisión Europea puso en marcha en 2022 un conjunto de iniciativas destinadas a **mejorar las condiciones financieras para las empresas startups europeas del sector espacial**.

La **Iniciativa de Emprendimiento Espacial CASSINI**⁴¹⁵, apoyada por el *Fondo Europeo de Inversiones* (FEI), es una de estas iniciativas que se suma al apoyo financiero a las empresas del denominado “Nuevo Espacio” (*New Space*) que ofrece el *Consejo Europeo de Innovación* (EIC). Para ello cuenta con el programa de aceleración denominado “*CASSINI Business Accelerator*”. Concretamente, el *Emerging Technologies Challenge* premia empresas con soluciones disruptivas que combinen los datos espaciales de la UE con tecnologías profundas como la Inteligencia Artificial (IA), las tecnologías cuánticas, la cadena de bloques, la realidad extendida o el metaverso.

También la ESA ha realizado desde hace años un esfuerzo en apoyar nuevas empresas. La *Oficina del Programa de Transferencia de Tecnología* (TTPO) de la ESA⁴¹⁶ apoya a emprendedores con ideas innovadoras que empleen tecnología espacial o desarrollen aplicaciones para crear nuevos productos y servicios en entornos no espaciales a través de los *Business Incubation Centres* (BIC). Se presta apoyo a empresas con productos disruptivos empleando tecnologías emergentes como la IA o las tecnologías cuánticas.

415 El Mecanismo de Inversión Cassini apoya con 1.000 millones de euros en inversiones para fondos de capital riesgo interesados en invertir en empresas del sector espacial con sede en la UE. <https://www.cassini.eu/cassini-initiative>

416 Technology Transfer Programme Office (ESA) https://www.esa.int/Enabling_Support/Space_Engineering_Technology/Technology_Business_Opportunities/Technology_Transfer_Programme

5.5.10 Competitividad europea en el contexto del sector espacial

Como ya se ha indicado en un capítulo precedente, en 2024 la Comisión Europea encargó a Mario Draghi un informe sobre la competitividad europea que presentó en septiembre de 2024 (Draghi, 2024). En el informe se reconoce que **el sector de la defensa es un motor clave de innovación para toda la economía**. Además, para Draghi los programas de doble uso no están suficientemente desarrollados en la UE.

En relación con el sector del “espacio” Draghi asume que *“la UE ha desarrollado un sector espacial de clase mundial, a pesar de niveles mucho más bajos de financiación, pero ahora está comenzando a perder terreno.”* Para Draghi los **activos espaciales son clave para las operaciones militares** (incluidas las de vigilancia e inteligencia) por lo que es necesario incrementar la coordinación y las sinergias entre las actividades espaciales y militares que, desde su punto de vista, no se aprovechan plenamente en la UE.

Desde el punto de vista del esfuerzo necesario, el informe reconoce que, si bien todos los Estados miembros de la UE asumen el espacio como un ámbito estratégico, su nivel de urgencia para financiar actuaciones, y sus estrategias para proteger los activos espaciales son muy variadas. Solo recientemente, con la adopción de la *Estrategia Espacial de la UE para la Seguridad y la Defensa* de marzo de 2023 (JOIN, 2023), la UE ha comenzado a **desarrollar sinergias entre el espacio y la defensa** para: i) aprovechar el uso del espacio en apoyo de las operaciones de seguridad y defensa (también en el ámbito de la vigilancia); y ii) aumentar el nivel de protección de los bienes espaciales.

Es destacable la propuesta de **explotar mejor las sinergias entre las políticas industriales de espacio y defensa** que, como se ha presentado en el presente documento, tienen muchos puntos en común. Específicamente, dice que *“los activos espaciales deben ser reconocidos como infraestructuras críticas de seguridad y se les debe conceder el nivel de protección pertinente”*.

5.6 Un marco de uso en defensa de la IA en rápida evolución

5.6.1. Avance sin consenso

La experiencia acumulada con el proceso de digitalización y la transición hacia un campo de batalla inteligente demuestra las **necesidades de cambios profundos de doctrina militar implicados**. Los diferentes aspectos tratados en este capítulo dan cuenta de los rápidos avances generados por la adopción de la IA en defensa alimentados por conflictos militares de alta intensidad. También, es relevante la existencia de diversos condicionantes para la extensión de su uso.

Es obvio que el **empleo de la IA en áreas sensibles** como son las de defensa y seguridad con el posible impacto en vidas humanas derivadas de su uso requiere que la tecnología

alcance el máximo nivel de madurez, y que la **“explicabilidad”** de las decisiones tomadas por un sistema automático, elemento esencial en la toma de decisiones para su aceptación por las Fuerzas Armadas, avance rápidamente.

Otro condicionante básico para su adopción es el de la **calidad de los datos disponibles**. Si el uso masivo de conjuntos de datos en tiempo real es esencial en todos los sectores para entrenar algoritmos que permitan detectar patrones, predecir amenazas, apoyar la toma de decisiones o alimentar análisis predictivos, **en el ámbito de la defensa y seguridad tiene una relevancia aún mayor**.

También para lograr un uso real en defensa, la capacidad de **anticipar comportamientos y situaciones que se puedan dar en el campo de batalla** requiere procesar grandes volúmenes de datos históricos, lo que, a su vez, obliga a disponer de modelos de lenguaje específicos entrenados para sistemas de defensa. Sin embargo, **la obtención de datos etiquetados y relevantes** que permitan entrenar a los algoritmos requiere obtenerlos de operaciones reales en el campo de batalla; **el uso de datos sintéticos no es suficiente**.

En el ámbito del uso de la IA en el sector espacial de defensa, el **procesamiento automatizado de datos geoespaciales es un factor crítico**. Se requiere procesar grandes cantidades de datos en tiempo real, con resoluciones muy elevadas para detectar cambios en el terreno o movimientos del enemigo o generar alertas cuando ocurren eventos en ubicaciones específicas mediante un análisis inteligente de imágenes espaciales, que ayuden a la toma de decisiones inmediata como se ha indicado en secciones anteriores.

Finalmente, la **interoperabilidad entre los sistemas militares de mando y control, nube de combate o simulación** empleados por distintas fuerzas armadas, así como con plataformas aliadas o de coalición en un **contexto de operación multidominio que incluye obligatoriamente el sector espacial** es una tendencia que supone un reto para los sistemas automatizados de toma de decisiones basado en IA. Reto que, sin embargo, ha adquirido una relevancia muy elevada y en el que los esfuerzos actuales en IA se concretarán en **sistemas interoperables muy potentes al final de la presente década**.

5.6.2 Consecuencias para España

Referido exclusivamente al caso español es evidente que la necesidad de incrementar el gasto en defensa hasta alcanzar el 2,1% del PIB como compromiso ya acordado⁴¹⁷, obligará a realizar inversiones en las que la IA será un elemento clave.

417 Aunque el acuerdo en la reunión del Consejo Atlántico de la OTAN en junio de 2025 es alcanzar el 5% en 2035, el compromiso del gobierno español es del 2,1%. Para comprender el esfuerzo presupuestario que significa, baste indicar que, si alcanzar el 2% del PIB supone unos 33.000 millones de euros, llegar al 3% supondría un incremento del presupuesto anual hasta unos 50.000 millones de euros.

Del documento denominado **Plan Industrial y Tecnológico para la Seguridad y la Defensa** (Ejercicio 2025) del gobierno español de abril de 2025 (Gobierno de España, 2025) con una dotación total de 10.470 millones de euros se puede leer: *“El Gobierno de España planea mantener la inversión en seguridad y defensa en el 2% del PIB mientras dure la actual coyuntura internacional y hasta que la UE alcance los objetivos de autonomía industrial y seguridad recogidos en su Libro blanco de defensa. Una pieza clave para proyectar esta continuidad de forma eficiente y ordenada serán los llamados Programas Especiales de Modernización (PEMs). El Plan contempla la puesta en marcha de 31 nuevos PEMs, que se unirán a los más de 50 en curso, y que movilizarán unos 3.807 millones de euros del total en su primer año, con una duración aproximada de, al menos, cinco años, hasta 2030 (Gobierno de España, 2025)”*.

Del *Plan* español mencionado pueden destacarse algunas actuaciones que implican el uso de la IA. Más concretamente en el Plan aprobado se incluye:

- Bajo la responsabilidad del CESTIC el desarrollo de modelos de ciberseguridad y ciberinteligencia mediante un laboratorio de supercomputación y se empleará IA para reforzar la ciberseguridad. Integración de IA en la plataforma del Sistema de Seguridad Nacional, mejora de la analítica de datos para crisis.
- Bajo la responsabilidad de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales (SETID) se pretende impulsar la actividad en IoT, cuántica e IA para ciberseguridad en defensa y uso dual, refuerzo del SOC 5G, colaboración con universidades y apoyo a empresas para aumentar la participación en programas internacionales.
- Como parte del PEM y en el epígrafe de *Conectividad Multidisciplinar* se aborda el desarrollo de un Sistema de comunicaciones para las misiones militares para proporcionar al mando el conocimiento de la situación en un tiempo útil para contribuir en el proceso de toma de decisiones, transmisión de órdenes y control de la misión.
- Bajo Conectividad Multidisciplinar en Seguridad Aérea del PEM se pretende disponer de un sistema tripulado remotamente para misiones de inteligencia, vigilancia y reconocimiento a nivel táctico, así como modernizar los 18 sistemas actuales del ET a un único sistema, permitiendo el control de la batalla aérea en tiempo real.
- También se incluyen las primeras partidas para el desarrollo del Sistema Espacial de Observación de la Tierra (SEOT) denominado PAZ II formado por dos nuevos satélites de tecnología Radar de Apertura Sintética (SAR).

Ante el anuncio del Plan, **Tedae** (*Asociación Española de Empresas Tecnológicas de Defensa, Seguridad, Aeronáutica Espacio*) indica la necesidad de *“una planificación*

*presupuestaria estable y sostenida que permita a las empresas desarrollar todo su potencial*⁴¹⁸.

También **el Grupo de trabajo considera que esa estabilidad y sostenibilidad es una condición necesaria**, aun aceptando la necesidad de dotar al proceso de planificación de la flexibilidad necesaria para aprovechar los avances científicos y tecnológicos de la IA que se han indicado en el capítulo 3 del presente informe.

5.7 Conclusiones

La visión ofrecida en este capítulo 5 sobre el uso real y efectivo actual de la IA por las fuerzas armadas, y las previsiones de su uso en los programas de desarrollo en marcha para los próximos años, marca un escenario en el que **su uso se va a acelerar pasando rápidamente de una fase de experimentación en conflictos bélicos reales a otra de adopción generalizada**.

Contribuye a esta aceleración el **deterioro de la situación geopolítica internacional** y la necesidad de asegurar la supremacía en caso de potencial conflicto; objetivos para los que el despliegue y uso de tecnologías de IA en operaciones militares asume un papel relevante. Todos los países observan con detenimiento su uso en Ucrania, Gaza, Sudán, etc. para aprender de experiencias reales.

A pesar de que el uso de la IA puede penetrar en múltiples áreas de la defensa, el presente capítulo se ha centrado en **tres temas seleccionados** que, en nuestra opinión, tienen el máximo interés y describen de una manera suficientemente amplia la evolución de la IA en defensa:

1. el primero ha abordado la visión del GT hacia un **campo de batalla inteligente** en el que los sistemas de mando y control multidominio, las nubes de combate, y las armas autónomas van a hacer un uso masivo de la tecnología de IA;
2. el segundo tema ha tratado de la relevancia de la **IA en la guerra híbrida y cognitiva** cuya expansión ha sido y creemos que seguirá siendo muy rápida como consecuencia de las capacidades que ofrece la IA;
3. finalmente, en el tercer tema se aborda el uso de la **IA en el sector espacial de la defensa**; se trata de un sector inherentemente dual y competido que se configura como un nuevo escenario de confrontación entre grandes potencias y parte esencial de las operaciones multidominio.

418 <https://www.infodefensa.com/texto-diario/mostrar/5267500/tedae-valora-positivamente-nuevo-plan-industrial-tecnologico-seguridad-defensa>

Hubiera sido posible abordar en detalle otros aspectos del uso de la IA en defensa solamente esbozados en el capítulo como es la **“guerra electrónica”** o, incluso, profundizar en algunos de los temas tratados brevemente como es el uso de la IA en los **“sistemas integrados de mando y control”** o de **“nube táctica de combate”**. Tampoco se han descrito otros usos más convencionales de la IA como los de su aplicación en defensa para el apoyo logístico, el mantenimiento predictivo, o para la formación y entrenamiento, áreas en las que, a pesar de las peculiaridades existentes en defensa, no difieren en demasía de su uso en aplicaciones civiles.

Creemos, sin embargo, que con los temas seleccionados basta para caracterizar el uso y evolución de la IA en el ámbito de la defensa. Como ya se ha indicado, algunos aspectos de uso tienen relevancia desde la **dimensión ética y regulatoria** que se ha abordado en el siguiente capítulo.

Con todo ello, pueden extraerse las siguientes **conclusiones**:

- **El uso de la IA desde la dimensión táctica y operativa militar como tecnología dual de carácter habilitador se está acelerando** y forma parte, en mayor o menor medida, de, prácticamente, todos los sistemas de armas y equipos militares. Creemos que de su introducción efectiva en las fuerzas armadas dependerá conseguir o no una superioridad en el combate en el denominado *“campo de batalla inteligente”* cuya transición desde el *campo de batalla digital* es innegable, aunque paulatino.
- **El desarrollo tecnológico asociado a la IA capacita el desarrollo y uso de sistemas autónomos de creciente complejidad** que ayudan a la toma de decisiones a diferentes niveles y, en el caso de sistemas autónomos de armas letales, ejecuten las acciones decididas con menor intervención del operador humano. Este hecho plantea la necesidad de determinar cómo usar estos sistemas inteligentes desde el punto de vista personal y colectivo, táctico y estratégico, y cuáles deberían ser las limitaciones a su uso, y asegurar su cumplimiento.
- El uso de la IA **tiene una importancia decisiva en la guerra híbrida y cognitiva** que se ha expandido fuertemente en los últimos años. En este ámbito, el uso de la IA se verá potenciado por su convergencia con otros dominios científicos y tecnológicos como es el de la neurotecnología, el de la psicología, el de la ciberseguridad, y el de las redes sociales. Todos ellos configuran un espacio de actuación complejo en el que el *“campo de batalla se traslada a la mente”*.
- **El espacio exterior próximo a nuestro planeta se configura como un dominio de actuación**, progresivamente integrado con los demás, en el que la proliferación de objetos y la necesidad de tomar decisiones en tiempo real obliga a incrementar la capacidad de procesamiento a bordo y la delegación de decisiones a algoritmos de IA.

- En el futuro, la **confluencia de la IA con las tecnologías cuánticas**, confluencia aún incipiente, pero en la que se está experimentando tiene el potencial de cambiar las reglas de juego. No creemos que eso se produzca en esta década, pero sí en la próxima. El Anexo 3 resume la situación actual.

La expansión del uso de la IA en defensa tiene que encontrar **respuestas a algunas preguntas abiertas cruciales** que incrementen la confianza en su uso por las Fuerzas Armadas, y para las que todavía no hay una solución técnica completa. Entre ellas, se han identificado las siguientes relacionadas con la confianza como elemento clave de la expansión del uso de la IA en defensa:

1. ¿Quién almacena los datos clasificados de interés de IA en Defensa?

La respuesta obvia serían las propias Fuerzas Armadas en centros de datos específicos. El problema es que el “interés” también se encuentra en otros muchos desperdigados en múltiples entidades públicas y privadas. Muchos datos tienen un interés dual.

2. ¿Cómo puede afectar el envenenamiento de datos empleados en el entrenamiento de un modelo de IA?

Se trata de un problema serio puesto que la validación de los datos en tiempo real puede ser difícil. Si sobre ellos se toman decisiones de forma autónoma el problema de falta de confianza se traslada al uso posterior durante la extracción de inferencias.

3. ¿Cómo puede ser atacado un sistema en la fase de aplicación/inferencia?

La ciberseguridad de los sistemas militares es un problema al que se le está prestando mucha atención, pero que en el caso de sistemas autónomos o SALA puede tener graves consecuencias.

4. ¿Qué desafío imponen las “alucinaciones” y la “caja negra” de un sistema IA para llevar a cabo misiones críticas?

El problema de las alucinaciones o la imposibilidad de conocer las razones de un algoritmo de IA para proporcionar una determinada respuesta (p.ej. al solicitar asistencia en la toma de decisiones a una aplicación basada en un SML o LLM) constituye una barrera para la expansión de la IA en aplicaciones de defensa.

En definitiva, nos encontramos con la adopción de soluciones basadas en la IA en un momento crucial de una **revolución tecnológica en la manera de conducir las operaciones militares** del que dependerá la evolución de la propia sociedad. Se trata de un proceso que implica no solo continuar el desarrollo tecnológico para madurar las tecnologías de IA, sino que también conlleva múltiples consideraciones éticas y regulatorias que se abordarán en el siguiente capítulo.

Capítulo 6

CAPÍTULO 6.

DIMENSIÓN ÉTICA Y REGULATORIA DE LA IA EN DEFENSA

6.1 Contexto del marco ético de la IA en defensa

6.1.1 Perspectiva histórica de la ética militar

El ámbito de la ética²⁴⁷ **militar** tiene un recorrido de siglos de historia. Se trata con la ética militar de ofrecer una perspectiva especializada, pero no aislada de consideraciones éticas más generales, derivada de las capacidades que hacen del ser humano un “sujeto ético”²⁴⁸.

El objetivo específico de la ética militar es determinar los criterios y condiciones que hacen que la guerra, aceptando la violencia como componente esencial de su naturaleza y asumiendo el uso de la fuerza con efectos letales sobre las personas, **sea legítima en su inicio, desarrollo y consecuencias** (Moliner, 2020, 2021).

La teoría asociada a la **guerra justa** se puede remontar a las primeras civilizaciones con normas aplicables²⁴⁹, aunque son autores occidentales de raíces cristianas como *San Agustín* y *Santo Tomás de Aquino* (origen del concepto de “legítima defensa”) los que la desarrollan con más intensidad; ellos sirvieron de base al trabajo de **Francisco de Vitoria** que puede considerarse el “*padre de los derechos humanos*” (Baqués 2024).

El concepto de guerra justa presupone que **existen usos legítimos de la guerra**, pero también establece **límites morales a la hora de librarla**²⁵⁰. Para ello se distingue entre los siguientes conceptos²⁵¹:

- a. *Ius ad bellum* (justificaciones morales para ir a la guerra) requiere que la causa de la guerra sea justa; que la autoridad correcta tome la decisión; que la decisión se tome con la intención correcta de lograr la paz; que la guerra sea un último recurso; que el mal general de la guerra no supere al bien.

247 Según el Diccionario de la Lengua Española la ética es el conjunto de normas morales que rigen la conducta de la persona en cualquier ámbito de la vida.

248 “La curiosidad, emociones, sentimientos, sentido común, la capacidad de llevar a cabo juicios y tener conciencia moral son, de momento, capacidades humanas que nos convierten en seres irremplazables, en sujetos éticos” (alocución de J.A. Moliner al GT en abril de 2025).

249 En Moliner (2024) se encuentran algunas referencias a conductas en la guerra en el “código de Hammurabi” compilado hacia el año 1780 a. C., y que es el más antiguo conjunto de normas legales escritas de las que hay constancia.

250 Para Francisco de Vitoria (Baqués, 2024) “no constituye en ningún caso una justa causa para la guerra el alegato de la diversidad de religión, el deseo de ensanchar el propio territorio o la gloria y el provecho particular del príncipe”.

251 <https://es.carnegiecouncil.org/explore-engage/key-terms/just-war>

- b. *Ius in bello* (principios morales a seguir durante la guerra) rige el trato a los prisioneros, exige la protección de los civiles y prohíbe el uso desproporcionado de la fuerza. Este concepto está directamente relacionado con el *Derecho Internacional Humanitario* en el que se plasma jurídicamente.
- c. *Ius post bellum*, que denota la justicia después de la guerra. El concepto ha sido propuesto para designar el marco normativo de la transición del conflicto armado a una paz sostenible, recogiendo la creciente influencia del derecho internacional en procesos de transición (Rojas-Orozco, 2021).

La teoría de la guerra justa tiene también una dimensión relacionada con la **forma de llevarla a cabo**, y esa forma está directamente ligada a la tecnología empleada. Puede afirmarse que todas las guerras, aun en el sentido de “*guerra justa*” evocado anteriormente, emplean la **tecnología** para lograr sus fines. Sobre la tecnología disponible en cada época histórica se construyen los sistemas de armas, de organización de las unidades militares y de inteligencia sobre los que se diseñan las tácticas y estrategias empleadas en las operaciones militares para lograr la superioridad y, también las “*ordenanzas militares*” adaptadas a la tecnología en uso. Todas ellas intervienen en la visión que se ofrecerá en este capítulo.

Como indica Moliner (2020) en su tesis doctoral (enfatizado propio): “*Si aceptamos el derecho de nuestras sociedades a la defensa militar, sustentada en todos los supuestos de legalidad y legitimidad, como un servicio público, que contribuye a la salvaguardia de los valores e intereses de un sistema político que promueve la libertad, la dignidad del ser humano (con su sentido moral) y los principios democráticos, el apoyo que recibe de la tecnología la defensa militar en la búsqueda de la disuasión y superioridad, hace que esa tecnología se deba poner, en nuestras sociedades, al servicio de consideraciones éticas*”.

Desde el punto de vista ético, una primera **tecnología militar con consideraciones éticas relevantes** fue la introducción del uso del “arco” y la “flecha” como arma contra otros seres humanos (fuera de su uso para la caza en búsqueda de alimento o defensa frente a ataques de animales) que permiten lograr un **efecto letal “a distancia”** sin ni siquiera tener contacto, algunas veces, ni visual, con el enemigo; de hecho, se intenta matar a una persona desconocida a la que no se ve. La historia de los **intentos de impedir el uso de la ballesta** explícita como la sociedad (en este caso, la iglesia) intentó establecer restricciones a su uso²⁵².

252 Es interesante referirse en este punto a los intentos de prohibición de la ballesta por parte de la iglesia católica. El intento de prohibición tuvo lugar en 1139, en el Segundo Concilio de Letrán, cuando estas armas eran todavía una novedad en la batalla, aunque no se limitó sólo a las ballestas. El canon 29 del concilio dice: «*El uso del arte mortífero y odioso a ojos de Dios de los ballesteros y arqueros contra cristianos católicos queda, en adelante, prohibido bajo anatema*». La referencia a los arqueros es probable que surgiera con el “arco largo” inglés de efectos también notables. Unos años más tarde, en 1143, el Papa Inocencio II confirmó nuevamente este hecho, amenazando a los ballesteros, fabricantes y comerciantes de esta arma con la excomunión y la maldición. Ninguna de estas prohibiciones surtió efecto. En 1630, el Papa Urbano VIII prohibió su uso entre los cristianos, permitiendo únicamente el uso de la ballesta en la guerra contra los «Infieles». Esta distinción introduce otro elemento de carácter ético perturbador: no se trata de consideraciones sobre el arma en sí misma, sino contra quién se utiliza.

Este proceso de distanciamiento ha continuado en la historia de la humanidad y ahora es omnipresente con armas mucho más mortíferas en la que **el ataque contra un objetivo humano predeterminado se realiza con operadores humanos situados a kilómetros de distancia** como ocurre con los drones con visión en primera persona pilotados remotamente.

Para muchos autores, si la **pólvora** (elemento desencadenante del desarrollo de las armas de fuego) originó la primera revolución militar, y la **tecnología nuclear** (en su vertiente militar del armamento nuclear) la segunda, la aparición de los **sistemas de armas letales autónomos (SALA)**²⁵³ suponen la tercera. Actualmente, la tecnología más relevante en este contexto de discusión ética del uso es la irrupción de la inteligencia artificial en su relación directa con los **sistemas de armas letales autónomos** que será el foco del presente capítulo.

No es extraño, por este motivo, que los **aspectos éticos del uso de la IA en el ámbito militar** hayan constituido una preocupación recurrente en gobiernos, instituciones multilaterales, entidades nacionales y ciudadanos asumiendo hace décadas desde la hipótesis de disponer de **sistemas capaces de tomar decisiones sin contar con la supervisión humana directa** o, al menos, sin la necesidad técnica de hacerlo para lograr su objetivo. Son precisamente **consideraciones éticas y no técnicas** las que han centrado la discusión sobre el papel que debe jugar el ser humano y los algoritmos de IA en el uso de este tipo de armamento.

Es relevante indicar que **todo comandante militar tiene la obligación ética de disminuir el riesgo de los soldados a sus órdenes** y a ello contribuyen los SALA empleados en todo tipo de operaciones: inteligencia, vigilancia y reconocimiento, desminado, combate en áreas urbanas, interdicción aérea, guerra submarina, evacuación de heridos del frente de batalla, etc. También los sistemas autónomos y robóticos guiados por la IA aumentan su eficacia y evitan situaciones de riesgo excesivo para el combatiente al **no estar sujetos a emociones como la ira o el miedo ni reducir el estado de alerta debido al cansancio o la fatiga**²⁵⁴.

Se ha aducido repetidas veces en relación con el uso de la IA y su empleo en los SALA el riesgo de que el alejamiento del campo de batalla del combatiente tanto desde la perspectiva física como psicológica podría contribuir a un **relajamiento de las restricciones para entrar en combate y a una reducción de la contención ética** para evitar riesgos innecesarios a los no combatientes. El problema se ha planteado expresamente en el caso de los **operadores de drones de ataque** (Moliner, 2018).

253 Se utilizará en el capítulo el término SALA y no el inglés de LAWS (*Lethal Autonomous Weapon System*).

254 En la evacuación de heridos en el campo de batalla, los robots militares, especialmente los vehículos terrestres no tripulados (UGV), están ganando terreno a medida que la tecnología madura (más flexibles y con mayor autonomía). Estos robots pueden identificar y transportar a los heridos a zonas seguras, reduciendo el riesgo para los soldados y personal médico. Además, los drones ambulancia, como el “Grille”, están siendo desarrollados para una evacuación más rápida y eficiente, incluso bajo fuego. La mayor parte de los robots terrestres empleados por Ucrania (47%) realizan misiones logísticas y de evacuación, mientras que sólo el 12% se envían al combate <https://legrandcontinent.eu/es/2025/07/11/en-tierra-el-ejercito-ucraniano-se-robotiza-para-compensar-su-desventaja-numerica/>

Si la **IA empleada en sistemas de armas con capacidad letal** son y serán capaces de ejecutar operaciones menos costosas, menos indiscriminadas y destructivas y con menos bajas propias, aspectos que no están totalmente asentados, el problema que podría surgir es el quebrantamiento del **principio de último recurso de la Guerra Justa**. Se reduce, así, el coste para los responsables políticos de decidir el desencadenamiento de la guerra, pues habría *menos bajas humanas*²⁵⁵; sin embargo, **se aumenta la posibilidad de embarcarse en guerras con causas menos justas y legítimas o incluso ilegales y totalmente ilegítimas**. El riesgo se multiplica al incrementarse el número de conflictos militares entre bandos que posean un número relevante de sistemas de armas autónomas o semiautónomas.

Este problema también surge cuando el combate no se dirime entre sistemas autónomos, sino que uno de ellos inflige daños a seres humanos desde el punto de vista de una **asimetría tecnológica entre los medios a disposición del atacante y del defensor**, afectando, expresamente, a civiles o a combatientes pobremente armados. En la historia de la humanidad esta asimetría tecnológica ha ocurrido repetidas veces planteando problemas morales en su uso como fue el caso del *arco largo inglés* en la batalla de Crécy contra los franceses en 1346 durante la Guerra de los Cien años (Cartwright, 2020), o más recientemente con el uso de la **ametralladora**²⁵⁶.

En el fondo, desde finales del siglo XX existía el convencimiento compartido por muchos expertos de que era necesario **establecer límites al uso de la IA en el ámbito militar para evitar peligros futuros**, aunque no se supiese cómo hacerlo ni tampoco hasta qué punto la tecnología iba a evolucionar. De hecho, las discusiones en el plano teórico se adelantaron en el tiempo a la disponibilidad real de tecnologías de IA suficientemente maduras para su utilización efectiva en armas autónomas en el campo de batalla; situación que solo ha empezado a ocurrir en el siglo XXI con la **convergencia de la IA con la microelectrónica, la robótica, los sensores, y las comunicaciones de banda ancha**.

Con el desarrollo de la IA en convergencia con las tecnologías indicadas, la atención en la última década se ha centrado en los **aspectos éticos derivados del uso de los SALA** (Moliner, 2024; González, 2022) que parecía el caso más evidente y peligroso y en el que empiezan a acumularse evidencias de su uso en combate, aunque no pueda hablarse de sistemas totalmente autónomos²⁵⁷. Todavía, la mayor parte de ellos están pilotados remotamente, aunque sus capacidades de decisión autónoma se desconocen realmente con fuentes abiertas.

255 La hipótesis de que el uso de sistemas militares basados en IA conduzca a conflictos militares con menores bajas es discutible. Si bien, en un escenario simétrico, puede alejar a los combatientes, también amplía el “espacio de contacto”, y en conflictos en zonas urbanas hace casi imposible distinguir entre combatientes y no combatientes.

256 La primera demostración del poder asimétrico de las ametralladoras se produjo a mediados de la década de 1890, en Sudán. Durante una rebelión unos pocos soldados ingleses abatieron con ametralladoras a 15.000 sudaneses armados con lanzas y mosquetes. <https://www.desenfunda.com/pt/blog/como-funciona-una-ametralladora-y-su-historia/?srsltid=AfmBOoqG1uNlx9pNxd8meDokl-nl96Y7LPSNEfj4kJu9vH2Q18wHhZ>

257 La primera incidencia registrada de un arma autónoma fue en la segunda guerra civil libia. Según un informe del Panel de Expertos sobre Libia del Consejo de Seguridad de la ONU, en 2020, un dron Kargu-2 del Gobierno de Acuerdo Nacional

Desde los años ochenta del siglo pasado ya se hablaba del riesgo de la emergencia de **“robots asesinos”** (*killer robots*), sin que existieran todavía. Sin embargo, múltiples novelas y películas de ciencia-ficción elucubraban sobre un futuro presentado al espectador como “técnicamente creíble” ante el que la humanidad se encontraría en un riesgo existencial por no poder controlar su comportamiento. En McCormic (2014) puede leerse un conjunto de eventos históricos de sistemas “autónomos” militares con un avance progresivo de su nivel de autonomía e inteligencia. Ahora, estamos más cerca de que su grado de inteligencia permita descartar al ser humano en su operación²⁵⁸.

La preocupación del uso de los SALA y la necesidad de proceder a su regulación procedía del **cambio del juicio dirigido por humanos al asistido por IA** que podría *“erosionar la capacidad de los mandos militares para asumir plenamente la responsabilidad moral de sus decisiones, comprometiendo en última instancia las virtudes militares que, como el coraje, la responsabilidad y el deber, están fundamentalmente arraigadas en el juicio y la toma de decisiones humanos”*.

En nuestra opinión, el uso de la IA para la automatización de la toma de decisiones en el ámbito militar **no es un problema radicalmente diferente desde el punto de vista técnico al encontrado en otros contextos como es el judicial o el médico** en los que también se ha ensayado el uso de sistemas de IA delegando en ellos funciones con efectos sobre las personas.

En los casos citados los sistemas basados en IA han demostrado su capacidad de **ayuda al humano en mejorar su actividad**, aunque el marco legislativo debe adaptarse para consolidar el papel del sistema de IA en una función de “apoyo al ser humano”, aunque con una función mucho más compleja que la que las ayudas mecánicas y de cálculo ofrecían previamente. Lo que diferencia claramente el uso de la IA para apoyar la toma de decisión en el ámbito militar radica en los potenciales efectos letales que pueden tener sobre las personas.

Esta evolución se ha concretado en los últimos años en el uso de los denominados **“agentes inteligentes”** (IA específicas o estrechas desarrolladas para una determinada aplicación) que asumen funciones que, hasta hace poco tiempo, se ejecutaban únicamente por seres humanos. En poco tiempo, el **juez**, el **médico** o el **profesor**, por citar tres profesiones, se verán **ayudados en el desarrollo de sus actividades por agentes inteligentes**; con ellos, mejorarán su proceso de toma de decisiones (más rápidamente, accediendo a más datos almacenados o en tiempo real, asegurando el cumplimiento de determinados prerrequisitos legales o técnicos, etc.). Los datos de evolución del mercado de agentes inteligentes permi-

persiguió y atacó a las fuerzas leales al mariscal de campo Ilibio Jalifa Hafter, cuando estaban en retirada (<https://elpais.com/opinion/2025-03-24/esas-tecnologias-son-letales.htm>)

258 Recuérdense los 10 niveles de automatización descritos en el capítulo 5 y las consecuencias cuando se supera el nivel 7 y el ser humano empieza a quedar “fuera del bucle” de decisión.

ten estimar que **su uso se extenderá en muy poco tiempo en todos los sectores, incluido el de defensa**²⁵⁹. El siguiente paso, la adopción de **sistemas multiagentes inteligentes** que se comunican entre sí, intercambian datos, y realizan tareas entre ellos para apoyar al ser humano en la realización de tareas más complejas, forma parte del desarrollo actual de la IA.

En esta misma línea de pensamiento, disponer de **agentes inteligentes militares** que ayuden al responsable militar (p. ej. el comandante de un sistema de mando y control) será una realidad con la que ya se está experimentando; y no tardarán en hacerse más ubicuos en todas las unidades militares e, incluso, desplegando agentes inteligentes a nivel individual. Algunos de estos agentes, integrados en **sistemas multiagentes, pueden formar parte de armas autónomas letales de mayor eficiencia** o como base para el uso de otras armas convencionales, formando parte de cadenas letales, y elevando la preocupación del control de su uso.

El **Comité Internacional de la Cruz Roja** (CICR, 2022) exponía esta preocupación afirmando: *“los sistemas de armas autónomas son todas las armas que seleccionan objetivos y les aplican la fuerza sin intervención humana. Cuando alguien activa un arma autónoma, no sabe exactamente a qué personas u objetos atacará, ni tampoco sabe con precisión dónde ni cuándo se producirá ese ataque*²⁶⁰. *Esto se debe a que las armas autónomas se activan mediante sensores y software que comparan aquello que los propios sensores detectan en el entorno con un “perfil de objetivo”. Por ejemplo, podrían activarse por la forma de un vehículo militar o el movimiento de una persona. El vehículo o la víctima son los desencadenantes del ataque, no el usuario”*.

También para el **CICR** el uso de sistemas de aprendizaje automático aplicado a las armas autónomas es un tema delicado: *“si se permitiera que el sistema “aprendiera” a identificar objetivos mientras se utiliza, ¿cómo podrían los usuarios de armas autónomas tener una certeza razonable de que el ataque se mantendrá dentro de los límites de lo jurídicamente permitido en conflictos bélicos?”*²⁶¹

Desde un punto de vista positivo, como señala Moliner (2023a) *“hay quien sustenta que el desarrollo de la IA podría llegar a mimetizar la mente humana casi de forma antropomórfica, incluyendo el replicar la conciencia del ser humano o el emitir juicios sobre lo que es ético. Ello permitiría que los SALA dirigidos por la IA, al no estar influidos por emociones humanas propias de la guerra como el temor, la ira o la venganza, actuarían de forma mucho más*

259 Se estima que el mercado de agentes de IA crezca de 7.840 millones de dólares en 2025 a 52.620 millones para 2030 con una CAGR del 46.3% <https://www.marketsandmarkets.com/Market-Reports/ai-agents-market-15761548.html>

260 El que esta apreciación sea cierta o no en un caso concreto depende del nivel de automatización del SALA y el papel que juega el humano en la decisión. En muchos casos, las coordenadas del objetivo y el momento del ataque sí son controlados por el operador humano. Esta reflexión lleva a considerar que no todas las decisiones tienen el mismo valor desde el punto de vista de sus consecuencias éticas, y algunas deben reservarse al ser humano.

261 <https://www.icrc.org/es/document/preguntas-y-respuestas-sobre-armas-autonomas>

moral en combate y no cometerían violaciones o actos punibles en conflictos y guerras (enfático propio). En todo caso, en 2025 estamos desde el punto de vista tecnológico, muy alejados de este supuesto, pero en un contexto de fuerte aceleración del desarrollo tecnológico.

La **posición formal de las Naciones Unidas** manifestada desde 2018 por su secretario general António Guterres ha sido la de que los SALA son ***“políticamente inaceptables y moralmente repugnantes”***, por lo que se ha pedido que se prohíban en virtud del derecho internacional. En la ***Nueva Agenda para la Paz de 2023***, se reiteró este llamamiento, recomendando que los Estados acuerden, para 2026, *“un instrumento jurídicamente vinculante que prohíba los sistemas de armas autónomas letales que funcionen sin control o supervisión humana, y que no puedan utilizarse de conformidad con el derecho internacional humanitario, y que regule todos los demás tipos de sistemas de armas autónomas”*.

También se señaló que, *“en ausencia de normas multilaterales específicas, el diseño, el desarrollo y la utilización de estos sistemas planteaban problemas humanitarios, jurídicos, de seguridad y éticos y planteaban una amenaza directa a los derechos humanos y las libertades fundamentales”*²⁶². Es interesante en este último punto indicar que para las Naciones Unidas **no se trata únicamente de regular el uso de estos sistemas sino también de impedir su diseño y desarrollo**. Se trata de aplicar en este contexto un principio de *“no proliferación”* sobradamente conocido en el caso de las armas nucleares.

No en todos los sistemas de armas autónomas letales el rol del ser humano es igual, como tampoco lo es su uso. Esto lleva a plantearse preguntas cómo: ¿Debería distinguirse entre un uso **defensivo** y otro **ofensivo** a la hora de limitar el uso de los SALA?²⁶³ En el supuesto de una respuesta afirmativa ¿Quiere decir que su desarrollo debe ser lícito y el esfuerzo debe focalizarse en la **regulación de su uso** a efectos de determinar responsabilidades? No existe todavía una regulación aceptada.

Aunque no exista una definición totalmente consensuada del término SALA se utilizará como base los trabajos de la *Convención sobre prohibiciones o restricciones del empleo de ciertas armas convencionales que puedan considerarse excesivamente nocivas o de efectos indiscriminados* de 2023²⁶⁴.

262 <https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/>

263 El empleo de sistemas de defensa aérea autónomos empleando sistemas de IA que permiten identificar un objeto que se aproxima como enemigo con alta probabilidad (usando firma radioeléctrica, térmica, sonora, etc.), y lanzar automáticamente un misil para neutralizar la amenaza se está aceptando sin suscitar problemas éticos significativos. La base es reducir o eliminar bajas civiles que se producirían en caso de no hacerlo.

264 [https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_\(2023\)/CCW_GGE1_2023_CRP.1_0.pdf](https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_CRP.1_0.pdf)

En un documento de 2023 elaborado por un grupo de expertos de las Naciones Unidas (CCW/GGE.1/2023/WP.4)²⁶⁵ se refería a las SALA en el siguiente contexto: *“Reconociendo que la investigación y el desarrollo de nuevas tecnologías en la esfera de la inteligencia artificial están progresando a un ritmo acelerado, lo que podría permitir la adquisición de armas nuevas y más sofisticadas con funciones autónomas, incluidos los **sistemas de armas que, una vez activados, pueden identificar, seleccionar y atacar objetivos con fuerza letal sin necesidad de que un operador intervenga más** (“sistemas de armas autónomos” a los efectos del presente proyecto de artículos y sin perjuicio de cualesquiera otros entendimientos de este o términos similares para otros fines)”*.

Es interesante comparar con la definición que China había propuesto en 2022 también en el contexto de las Naciones Unidas (CCW/GGE.1/2022/WP.6) **distinguendo entre “sistemas de armas autónomas aceptables e inaceptables”**. La postura de China se concretaba en los siguientes elementos:

*“Las características básicas de los **Sistemas de Armas Autónomas Inaceptables** deben incluir, entre otras, las siguientes: En primer lugar, la letalidad, es decir, la carga útil letal suficiente (carga) y los medios. En segundo lugar, la autonomía, es decir, la ausencia de intervención y control humano durante todo el proceso de ejecución de una tarea. En tercer lugar, la imposibilidad de terminación, lo que significa que una vez iniciada, no hay forma de terminar la operación. En cuarto lugar, el asesinato indiscriminado, lo que significa que el dispositivo ejecutará la misión de matar y mutilar independientemente de las condiciones, escenarios y objetivos. En quinto lugar, la evolución, es decir, que, a través de la interacción con el entorno, el dispositivo puede aprender de forma autónoma, expandir sus funciones y capacidades en un grado que supera las expectativas humanas.*

Por otro lado: *“Los **Sistemas de Armas Autónomos Aceptables** podrían tener un alto grado de autonomía, pero siempre están bajo control humano. Significa que pueden ser utilizados de manera segura, creíble, fiable y manejable, que pueden ser suspendidos por los seres humanos en cualquier momento y que cumplen con los principios básicos del derecho internacional humanitario en las operaciones militares, como la distinción, la proporcionalidad y la precaución”*.

Es relevante señalar la publicación en julio de 2024 de la **compilación consolidada de las propuestas realizadas** por muchos países a las Naciones Unidas sobre los **“Sistemas de armas autónomos letales”**²⁶⁶. El Informe del Secretario General indica en la Introducción que: *“En el párrafo 2 de su resolución 78/241 sobre los sistemas de armas autónomos letales, la Asamblea General solicitó al Secretario General que recabara las opiniones de los Estados Miembros y los Estados observadores sobre los sistemas de armas autónomos*

265 El grupo incluía representantes de Australia, Canadá, Japón, la República de Corea, El Reino Unido y los Estados Unidos.

266 https://digitallibrary.un.org/record/4059475/files/A_79_88-ES.pdf

letales, entre otras sobre las formas de abordar las dificultades y preocupaciones conexas que planteaban esos sistemas desde las perspectivas humanitaria, jurídica, tecnológica, ética y de seguridad y sobre el papel de los seres humanos en el uso de la fuerza”²⁶⁷.

Las casi 200 páginas del informe y **la variedad de las opiniones manifestadas por los países no auguran un proceso sencillo para alcanzar un acuerdo en 2026 como se desea**; todo ello sin entrar siquiera a debatir la capacidad real de las Naciones Unidas para forzar su cumplimiento en el caso de que se llegase a ello.

Solamente a título de ejemplo el documento indica que, en sus aportaciones, los Estados se refirieron alternativamente a los “*sistemas de armas autónomos*” y a los “*sistemas de armas autónomos letales*”. El documento indica: “*Algunos Estados consideraron que la palabra “letal” era una referencia importante a la capacidad de un sistema para aplicar fuerza letal. Otros opinaron que la letalidad de un sistema de armas dependía de su uso más que de su diseño. Varios Estados argumentaron en contra del uso de la palabra “letal”, al afirmar que carecía de base en el derecho internacional humanitario y señalar, entre otras cosas, que la letalidad era un efecto de la forma en que se utilizaba un arma. Asimismo, se señaló que el uso no letal de la fuerza también podía dar lugar a violaciones del derecho internacional humanitario*”.

Adicionalmente, debe tenerse en cuenta que **el análisis ético del uso militar de la IA no debe circunscribirse al empleo de las armas autónomas letales**. Actualmente, la discusión abarca también el uso de algoritmos de IA en las plataformas de decisión, en la selección automática de objetivos, en la delegación de competencias en equipos híbridos humano-robot, y en todos los aspectos relacionados con la *guerra cognitiva* en los que se pretende interferir o modular el comportamiento del ser humano, sin que pueda considerarse todo ello un arma cinética convencional. Las diferencias en la determinación del responsable directo o no de las consecuencias derivadas de su uso es relevante en un caso u otro. En otras palabras, **no se trata solo de analizar el uso ético de la funcionalidad de un arma, sino el papel que juega en una cadena que culmina en el ataque a un objetivo**.

Actualmente, el uso militar más relevante y extendido de la IA es la adopción de **Sistemas de Apoyo a la Decisión** (*Decision Support System, DSS*)²⁶⁸, muchos de ellos basados en datos capturados y analizados en tiempo real. Su utilidad para procesar grandes cantidades de datos, imposibles de manejar por su volumen por operadores humanos, corre el riesgo de eclipsar las virtudes militares mencionadas anteriormente. Al asumir una mayor carga

267 Resolución aprobada por la Asamblea General el 22 de diciembre de 2023. Para más detalles consultar <https://undocs.org/es/A/RES/78/241>

268 Existen otros sistemas de IA empleados en las Fuerzas Armadas para la realización de funciones similares a las encontradas en el uso civil como son los de gestión logística inteligente, mantenimiento preventivo, entrenamiento, o uso de gemelos digitales para el desarrollo de productos. En estos casos, no se plantean debates sobre los aspectos éticos asociados.

cognitiva en las operaciones militares, **un DSS basado en IA podría diluir el elemento humano de la toma de decisiones morales y éticas.**

En todo caso, la importancia de estos sistemas para incrementar la eficiencia es evidente y ha servido, desde una posición simplista, para justificar su uso. *Tal Mimran*, profesor de la Universidad Hebrea de Jerusalén, decía: *“En 2015 se necesitaba un equipo de alrededor de 20 oficiales de inteligencia para trabajar durante unos 250 días para reunir entre 200 y 250 objetivos. Hoy, la IA lo hace en una semana”* (Sherhan, 2024). En el futuro, lo podrá hacer en minutos.

En nuestra opinión un planteamiento de prohibición total no es realista y **el análisis ético debe realizarse con mucho mayor detalle en función de las diferencias entre los posibles casos de uso.** Desde el punto de vista ético, cabría preguntarse qué ocurre si la IA no estuviese directamente ligada al arma en sí, sino a la identificación de un objetivo que predetermina la víctima sobre la que actuar con un armamento convencional ¿Cómo asegurar que la elección se hace correctamente? ¿Con qué criterios se aceptarían márgenes de error? ¿Quién asume las responsabilidades en los siguientes eslabones de la cadena?

Todas estas preguntas llevan a la necesidad de disponer de una **gobernanza del uso de la IA** que determine las autoridades responsables y los procedimientos a emplear aceptando la idea de **“control humano significativo” (CHS)** sobre el uso de la IA. Los tres requisitos exigidos por el supuesto de un CHS en el informe elaborado por la ONG británica *Article 36*²⁶⁹ eran (Moliner, 2024):

1. *Información: un operador humano, y otros responsables por el planeamiento del ataque, necesitan tener adecuada información contextual sobre el área objetivo de un ataque, información sobre los objetivos de la misión, e información sobre los efectos inmediatos y a largo plazo del arma que se derivarán de un ataque en ese contexto.*
2. *Acción: el inicio del ataque debería requerir una acción positiva por un operador humano.*
3. *Rendición de cuentas [accountability]: aquellos responsables de evaluar la información y ejecutar el ataque necesitan responsabilizarse de los resultados del ataque.*

Desde una perspectiva civil la figura 6.1 (Zaidan e Ibrahim, 2024) considera la **necesidad de disponer de una organización internacional responsable de regular la IA** cubriendo sus diversas competencias, como la elaboración de normas, la aplicación y la supervisión. También incluye la representación de los diferentes actores involucrados en el proceso

²⁶⁹ La primera vez que apareció el concepto de Control Humano Significativo fue en abril de 2013 en un informe de la Organización No Gubernamental británica *Article 36* (*Article 36*, 2013) haciendo referencia al artículo 36 del I Protocolo Adicional de 1977 a las Convenciones de Ginebra de 1949.

regulatorio, principalmente los Estados, otras organizaciones internacionales, empresas privadas y la sociedad civil. Cabe mencionar que algunos autores suman a esta clasificación otros actores como el “mercado” y la “comunidad académica”.



Figura 6.1 Regulación de la IA. Fuente: Adaptada y completada de Zaidan e Ibrahim (2024). <https://www.nature.com/articles/s41599-024-03560-x>

De este esquema también se desprenden las dificultades existentes para llegar a un acuerdo general puesto que a la **inexistencia de una entidad regulatoria común** (las *Naciones Unidas* no tienen esa función aceptada globalmente ni tampoco dispone de medios para ejercerla) se une las diferentes posiciones mantenidas por el resto de las partes interesadas; fundamentalmente, las **posiciones de los Estados**, influidos por la sociedad civil en su respectivo contexto nacional, y las **posiciones de las organizaciones internacionales**; también deben tenerse en cuenta las **posiciones de las empresas** con la necesidad de cumplir las legislaciones nacionales y, al mismo tiempo, maximizar sus beneficios con usuarios ubicados en todo el mundo.

6.1.2 Interacción entre el marco ético y el regulatorio de la IA militar

Los análisis en el marco ético en el dominio militar no permiten establecer los procedimientos aceptables o no del uso de la IA si no van acompañados de una **regulación específica de la que emanen directrices operativas**. El punto de vista adoptado en la elaboración del presente capítulo es la de que **el marco ético y regulatorio están estrechamente ligados y deben considerarse conjuntamente**.

La IA debe abordarse en el ámbito jurídico con un marco ético y regulatorio equilibrado. Las normas jurídicas deben proporcionar orientación dentro de un marco ético sin los avances tecnológicos. La colaboración internacional y la participación de las partes interesadas son esenciales en este proceso. Además, se debe adoptar un **enfoque interdisciplinar**, con la

colaboración entre expertos en tecnología, derecho, ética y economía para garantizar la implementación efectiva de los marcos de IA. ¿Es eso posible en el ámbito del uso militar de la IA?

La complejidad del problema puede verse en la figura 6.2 en la que se han representado todos los elementos implicados. En la parte superior se indican los elementos que configuran el **marco ético** del uso de la IA y en la parte inferior los relativos al **marco legislativo y regulatorio**. Ambos se ven condicionados por el dominio militar y tecnológico.



Figura 6.2. Relaciones entre el marco ético y el regulatorio. Fuente: elaboración propia

Como se indica en la figura 6.2 **no son marcos disjuntos** y evolucionan en la medida en la que lo hacen los valores compartidos de la sociedad en la que se aplican, y de la experiencia de su aplicación en diferentes casos de uso. Esta evolución condicionada por la de los valores sociales explica también cómo las regulaciones nacionales divergen y explica la dificultad de encontrar una posición común.

Finalmente, se ha indicado en la figura 6.2 la **especial relevancia de los sistemas de armas autónomas letales** (y su papel en una cadena de fines letales) sobre los que gira gran parte de la discusión ética y regulatoria de la IA en todos los países, multitud de organismos internacionales y, expresamente, en las Naciones Unidas, como se ha mencionado anteriormente.

Téngase en cuenta que **el marco legal relativo a la IA es más amplio que el considerado bajo la óptica de su uso en defensa**. La IA introduce varias cuestiones jurídicas clave, en particular en los siguientes ámbitos²⁷⁰ (algunos de ellos también son compartidos en el con-

270 <https://www.narterlaw.com/en/artificial-intelligence-and-law-ethical-and-regulatory-framework/#:~:text=AI%20must%20be%20approached%20in,are%20essential%20in%20this%20process.>

texto de las fuerzas armadas o para la industria de defensa, pero que no se van a abordar en el presente documento al no ser específicos del uso militar):

1. **Responsabilidad legal:** ¿Quién será responsable cuando los sistemas de IA cometan errores? ¿Cómo se estructurará la responsabilidad entre fabricantes, desarrolladores y usuarios?²⁷¹
2. **Derechos de propiedad intelectual:** ¿Cómo deben gestionarse los derechos de propiedad intelectual de los contenidos generados por la IA? El estatus de las obras artísticas, los escritos o las innovaciones tecnológicas producidas por la IA sigue siendo objeto de debate²⁷².
3. **Trabajo y derechos humanos:** ¿Cómo se abordará el impacto de la IA en la mano de obra y los derechos laborales? A medida que aumente la automatización, ¿qué soluciones se encontrarán para abordar los problemas relacionados con la seguridad laboral y los derechos sociales?²⁷³
4. **Derecho penal e IA:** ¿Quién debe ser considerado responsable de los delitos cometidos a través de sistemas de IA? ¿Cómo deben determinarse las repercusiones jurídicas de los daños causados por los sistemas habilitados para IA?²⁷⁴

Seguidamente, se aborda la **situación actual del debate sobre el uso responsable de la IA en el ámbito de la defensa**. Posteriormente, se analizará cómo ese debate ha derivado en directrices o regulaciones específicas. A continuación, se analizarán los posibles enfoques existentes para disponer de una **regulación específica del uso de la IA en el ámbito militar** como reclaman las Naciones Unidas, y las posibilidades de que eso ocurra en un contexto de aceleración del desarrollo tecnológico en el que es difícil evitar la obsolescencia del proceso regulador.

Finalmente, se extraen unas **conclusiones** volviendo a considerar un contexto de aceleración del desarrollo tecnológico relacionado con la IA y, en especial, el ámbito de su **convergencia con la neurotecnología** en el que los aspectos éticos y regulatorios cobran un interés manifiesto; más aún cuando se combinan con su uso en el ámbito de la defensa.

271 Esta pregunta y la dificultad de disponer de una respuesta legislativa tiene vigencia hoy día en el despliegue de vehículos autónomos (no sólo de armas) cuyo uso es dual (civil y militar).

272 Téngase en cuenta que en muchos casos de desarrollos tecnológicos militares no se emplean patentes (compromiso entre protección legal y difusión de conocimiento), sino que se recurre al secreto industrial.

273 La aplicabilidad de los derechos sociales y de seguridad laboral no son directamente aplicables al personal de las fuerzas armadas en la ejecución de su misión en combate.

274 En este sentido, ¿Es necesario adaptar el marco jurídico militar al uso de los SALA?

6.2 Uso responsable de la IA en el ámbito militar

6.2.1 Marco jurídico

Ante la ausencia de un marco jurídico específico, se considera que **el tratamiento de la IA en el ámbito militar deber estar subordinado al derecho internacional**. En la compilación efectuada por las Naciones Unidas, *“los Estados señalaron que la elección de armas, medios y métodos de guerra, incluidos los sistemas de armas autónomos letales, debía cumplir el derecho internacional, especialmente el **derecho internacional humanitario**”*.

El **Derecho Internacional Humanitario (DIH)** se considera una parte del *Derecho Internacional (DI)* aplicado a conflictos armados, que no deberían existir si el Derecho fuese respetado. Su objetivo principal es **garantizar un mínimo de humanidad en una situación inhumana**. Esto tiñe inevitablemente sus fuentes, normas y principios de interpretación agregándoles no solo dificultad, sino motivando la crítica de aquellos que cuestionan la existencia misma del *Derecho Internacional Humanitario* (Salmón, 2004).

También las respuestas de los Estados en la respuesta ante la consulta de las Naciones Unidas mencionada anteriormente subrayaron la importancia de los **principios de distinción, proporcionalidad, necesidad militar y precauciones en el ataque**, así como la exigencia de evitar daños superfluos o sufrimientos innecesarios en el uso de la IA. Más concretamente²⁷⁵:

1. Distinción. Se refiere a obligar a los Estados a distinguir entre civiles y combatientes en el contexto de los conflictos armados.
2. Proporcionalidad. Se refiere a la prohibición de ataques contra objetivos militares que “se prevea que causarán incidentalmente muertos o heridos entre la población civil, daños a bienes de carácter civil, o una combinación de ambas cosas, que sean excesivos en relación con la ventaja militar concreta y directa prevista”.
3. Necesidad militar. Se refiere a permitir medidas que sean realmente necesarias para lograr un propósito militar legítimo y que no estén prohibidas por el derecho internacional humanitario. En el caso de un conflicto armado, el único propósito militar legítimo es debilitar la capacidad militar de las demás partes en el conflicto.

275 El Comité Internacional de la Cruz Roja ha expandido estos principios a los diez siguientes: 1) Principio de humanidad, 2) Principio de igualdad entre los beligerantes, 3) Principio de necesidad militar, 4) Principio de no discriminación, 5) Principio del derecho de Ginebra, 6) Principio de inmunidad, 7) Principio de prioridad humanitaria, 8) Distinción, 9) Proporcionalidad, 10) Limitación de la acción hostil.

<https://www2.cruzroja.es/documents/5640665/691578756/PRINCIPIOS.pdf/9483f93c-748a-27dc-9096-1cf4d8a98061?t=1627896739666>

4. Precauciones en el ataque. Se refiere a la necesidad de reducir riesgos en vidas humanas si se pueden utilizar sistemas robotizados. Un caso simple es el uso de un robot inteligente para desactivación de explosivos, en vez de arriesgar la vida de un especialista humano.

La evolución tan rápida de la tecnología hace prácticamente imposible que un marco regulatorio por detallado que sea pueda anticipar todos los casos de uso y los problemas éticos y regulatorios asociados²⁷⁶. Por este motivo, es muy relevante la necesidad de permitir la **experimentación de la regulación en entornos controlados**, incluyendo el uso de sistemas que permitan simular diferentes escenarios de aplicación de la regulación y analizar su utilidad real²⁷⁷.

6.2.2 IA Responsable en el Ámbito Militar (REAIM)

Las cumbres entre Estados denominadas “**IA Responsable en el Ámbito Militar (REAIM)**” son ilustrativas del **interés en establecer límites éticos al uso de la IA**, aunque no supongan la creación de un marco legislativo y se muevan en el espacio de la “voluntariedad” de acción basada en la discusión y la experiencia.

Como resultado de dichas reuniones han surgido varios documentos, incluida la *Declaración Política de REAIM de 2023* (Steene and Jenks, 2023) sobre el *Uso Militar Responsable de la Inteligencia Artificial y la Autonomía*, y el documento final de la *Cumbre REAIM* celebrada en Corea del Sur en septiembre de 2024²⁷⁸ que respalda la **puesta en marcha de un plan de acción**.

La **Declaración de REAIM 2023** comprende un conjunto de **directrices jurídicamente no vinculantes que describen las mejores prácticas para el uso responsable de la IA en defensa**. Entre ellas, garantizar que los sistemas de IA militar sean auditables, tengan usos explícitos y bien definidos, estén sujetos a pruebas y evaluaciones rigurosas a lo largo de su ciclo de vida, y que las aplicaciones con consecuencias relevantes se sometan a una revisión de alto nivel y puedan ser desactivadas si demuestran un comportamiento no deseado.

El **documento final de la segunda Cumbre REAIM** celebrada en Corea del Sur en septiembre de 2024²⁷⁹ se apoya en la declaración anterior y respalda la puesta en marcha de un **plan de acción**²⁸⁰. Está previsto celebrar la tercera edición de REAIM en España en el segundo semestre de 2025 en La Coruña tras alguna reunión previa preparatoria coincidiendo con la

276 El ejemplo de la regulación de la IA por la UE en la que hubo que abordar la IA generativa durante el proceso de negociación del reglamento es un caso claro de cómo la rapidez de cambios tecnológicos significativos afecta al proceso regulatorio.

277 La idea de la creación de espacios de experimentación regulatoria (*regulatory sandboxes*) se está aplicando por la Comisión Europea en diversos ámbitos de la regulación digital.

278 https://overseas.mofa.go.kr/eng/brd/m_5676/view.do?seq=322676

279 La segunda Cumbre REAIM se celebró en Seúl en septiembre de 2024 y fue acogida por la República de Corea junto con los Países Bajos, Singapur, Kenia y el Reino Unido. https://overseas.mofa.go.kr/eng/brd/m_5676/view.do?seq=322676

280 Government of the Republic of Korea, REAIM Blueprint to Action, 10 September 2024. <https://thereadable.co/reaim-blueprint-for-responsible-ai-use-military/>

Cumbre de la OTAN celebrada en el mes de junio de 2025²⁸¹. **La implementación exitosa del Plan de Acción supondría un salto esencial.** En todo caso, se trata aún de pasos iniciales, y nada asegura que, en caso de conflicto militar agudo, se vayan a seguir por los contendientes cuando su supervivencia esté en juego (aduciendo la situación de “riesgo existencial”).

Paoli y Afina (2025) argumentan que para facilitar la aplicación de Plan de Acción de REAIM: *“Los Estados podrían considerar la posibilidad de **diferenciar el uso de la IA por parte de las fuerzas militares en la conducción de hostilidades** (conflictos armados internacionales y conflictos armados no internacionales) **del uso de la IA por parte de las fuerzas militares en otros tipos de operaciones**, como el mantenimiento de la paz, la respuesta a emergencias o el socorro en casos de desastre, y el **apoyo a la seguridad nacional y la seguridad pública** (apoyo a las fuerzas del orden, seguridad fronteriza, lucha contra la piratería, protección de infraestructuras críticas, etc.).”*

Este enfoque implicaría **aceptar la existencia de diversos marcos regulatorios** aplicables en función de las competencias y tipo de uso por los responsables en cada caso. No será fácil llegar a una implementación efectiva de un marco regulatorio común en esos términos.

6.2.2.1 Posición española

España ha contribuido a la consulta de las Naciones Unidas sobre las armas autónomas letales. Concretamente, España, junto a otros países europeos (Finlandia, Francia, Alemania, Italia, Países Bajos, Noruega y Suecia) había propuesto ya en 2022 (CCW/GGE.1/2022/WP.7) para la consideración del Grupo de Expertos Gubernamentales las siguientes propuestas con respecto a un **posible marco normativo y operacional sobre las tecnologías emergentes en la esfera de los sistemas de armas autónomas letales**:

“Los Estados deben comprometerse a:

- *Prohibir los sistemas de armas letales totalmente autónomos que operen completamente fuera del control humano y de una cadena de mando responsable, así como;*
- *Reglamentar otros sistemas de armas letales que gocen de autonomía a fin de garantizar el cumplimiento de las normas y principios del derecho internacional humanitario, preservando la responsabilidad humana y la rendición de cuentas, asegurando un control humano adecuado e implementando medidas de mitigación de riesgos”.*

En el contexto nacional relativo a la aplicación de la IA en defensa es destacable la Resolución 11197/2023 de 29 de junio, de la Secretaría de Estado de Defensa, por la que se aprueba

281 <https://hcass.nl/event/gc-reaim-symposium-next-steps-for-responsible-practice/>

la **Estrategia de desarrollo, implantación y uso de la Inteligencia Artificial en el Ministerio de Defensa** (MINDEF, 2023). La Estrategia establece y determina:

- a. *El contexto y la visión estratégica para el desarrollo, la implantación y el uso de la IA en el MDEF.*
- b. *Los principios de desarrollo, implantación y uso responsable de la IA en el ámbito de la Defensa.*
- c. *Las Líneas de Acción Estratégicas que deben guiar la adopción de la IA en el MDEF.*
- d. *Las posibles áreas de aplicación y casos de usos actuales y futuros de esta tecnología para los cometidos del MDEF, dentro de los cuales tendrán prioridad los que tengan relación directa con el desempeño de las misiones y cometidos de las Fuerzas Armadas.*
- e. *Una estructura de dirección y coordinación para el desarrollo, implantación y uso de aplicaciones basadas en IA en el MDEF.*
- f. *Los mecanismos de coordinación entre todos los Centros o Unidades del MDEF con competencias en el desarrollo, implantación, y uso de soluciones basadas en IA.*

La Estrategia del Ministerio de Defensa señala que la IA **afecta de modo transversal a todas las actividades militares desarrolladas por las Fuerzas Armadas** en apoyo de sus tareas principales, defensa colectiva, gestión de crisis y seguridad cooperativa. Asimismo, se indica que *“su uso estará siempre de acuerdo con la legislación nacional e internacional, los principios de uso ético de la IA y dirigida a su área de aplicabilidad”*.

De acuerdo con la citada Estrategia, los principios que regirán su desarrollo, implantación y uso son los siguientes:

- a. **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.*
- b. **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.*
- c. **Inteligibilidad y trazabilidad:** *las aplicaciones de IA serán comprensibles y transparentes para el personal relevante, incluyendo el uso de metodologías, fuentes y procedimientos auditables.*
- d. **Fiabilidad y transparencia:** *las aplicaciones de IA estarán dirigidas a casos de uso explícitos, bien definidos y acotados y se proporcionará información para fomentar una comprensión general de estas aplicaciones por todas las partes interesadas. La seguridad,*

la protección y la solidez de estas capacidades estarán sujetas a pruebas y garantías dentro de esos casos de uso a lo largo de todo su ciclo de vida.

- e. **Gobernabilidad:** *las aplicaciones de IA se desarrollarán y utilizarán de acuerdo con sus funciones previstas en el diseño, asegurando la capacidad de detectar y evitar consecuencias no intencionadas. Se habilitarán mecanismos de desconexión o desactivación cuando se reconozcan comportamientos no previstos o indeseados.*
- f. **Mitigación del sesgo:** *se tomarán todas las medidas necesarias para minimizar errores y orientaciones subjetivas en el desarrollo y uso de aplicaciones de IA.*
- g. **Privacidad:** *el desarrollo, la implantación y el uso de aplicaciones basadas en IA deben respetar la privacidad de las personas, desde el diseño y durante todo el ciclo de vida.*

La Estrategia española no es muy explícita desde el punto de vista ético, limitándose a decir: *“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”*. En definitiva, conduce al establecimiento de directrices posteriores.

El **marco de aplicación de la IA en la industria de defensa española** se ve apoyado por otras regulaciones nacionales como el Real Decreto 817/2023, de 8 de noviembre del Ministerio de Asuntos Digitales y Transformación Digital que establece un *entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial*²⁸². Se pretendía con ello, alinearse con lo que meses después (en mayo de 2024) sería la Regulación de la IA (AI Act) de la UE.

6.3 Regulación dual de la IA

6.3.1 Evolución de la regulación civil a la militar de la IA

El **cambio de actitud a favor de la necesidad de disponer de una regulación de la IA** empieza a calar desde 2018 en gobiernos y organizaciones que han mantenido históricamente una actitud más orientada a la *“autorregulación”* y el uso de *“directrices voluntarias”* por parte de los actores implicados. En todo caso, el foco de estos esfuerzos se centra en el uso de la IA en aplicaciones civiles.

282 <https://www.boe.es/eli/es/rd/2023/11/08/817>

Para tener una idea de los movimientos generados en este sentido, sólo en 2023 y 2024 se han realizado muchos esfuerzos diferentes por parte de organismos multilaterales para promover una **gobernanza global de la IA** que permita establecer las reglas de uso más allá de lo que un país pueda acordar independientemente. Se citan seguidamente algunos de ellos, aunque sea necesario adoptar una actitud cautelosa sobre su posible éxito: el **proceso de IA de Hiroshima**, las posiciones de la **OCDE**, el esfuerzo de las **Naciones Unidas**, y las regulaciones abordadas a **nivel nacional** por diversos países.

En mayo de 2023, el **G-7** lanzó el **“Proceso de IA de Hiroshima”**²⁸³ (G7, 2023) un foro dedicado a armonizar la gobernanza de la IA con un conjunto de directrices de obligado cumplimiento para los países firmantes. En octubre de 2023 su **“declaración”** (*código de conducta internacional*) fue ratificado por los 7 países del G7 (Alemania, Canadá, Estados Unidos, Francia, Italia, Japón y el Reino Unido). El objetivo de los once “principios rectores” establecidos finalmente por el G7 es *“promover una IA segura y digna de confianza en todo el mundo y proporcionar orientación voluntaria para las acciones de las organizaciones que desarrollen los sistemas de IA más avanzados, incluidos los modelos fundacionales y la IA generativa”*.

Los trabajos del G7 han influido en las posiciones de Estados Unidos y en las de la UE. También en la UE la presidenta de la Comisión Europea ha instado a las empresas a comprometerse a cumplir el código de conducta del G7 de inmediato. *“Hago un llamamiento a los desarrolladores de IA para que firmen e implementen este código de conducta lo antes posible”*.

Otro ejemplo de esfuerzos a nivel internacional es el realizado por la OCDE. La primera recomendación del Consejo de la **OCDE** sobre IA data de mayo de 2019; desde entonces, ha mantenido un interés creciente actuando de secretariado para el **GPAI** (*Global Partnership for AI*)²⁸⁴. En junio de 2023, la **OCDE** publica el informe sobre la IA en relación con la investigación (OCDE, 2023a) adoptando una **posición positiva al desarrollo abierto de la IA**. En julio de 2023, la OCDE publica su informe sobre el impacto de la IA sobre el empleo (OECD, 2023b). Con estas resoluciones, **la OCDE ha instado a los gobiernos a adoptar políticas que garanticen el uso confiable de la IA y la capacitación adecuada de los trabajadores durante el periodo de transición**.

En **julio de 2023**, la **ONU**, a través del secretario general, Antonio Guterres, pidió el establecimiento de un **organismo de control regulador global de la IA** (ONU, 2023). Su objetivo político es claro: *“Insto al Consejo a que aborde esta tecnología con un sentido de urgencia, una lente global y una mentalidad de alumno”*.

283 Hiroshima Process International Code of Conduct for Organisations Developing Advanced AI Systems <https://digital-strategy.ec.europa.eu/en/library/hiroshima-process-international-code-conduct-advanced-ai-systems>

284 Concretamente, la OCDE facilitará las sinergias entre el trabajo científico y técnico de GPAI y el liderazgo internacional en políticas de IA proporcionado por la OCDE, fortaleciendo la base de evidencia para políticas dirigidas a una IA responsable. <https://www.gpai.ai/about/>

En **marzo de 2024** la *Asamblea General de las Naciones Unidas* aprobó por unanimidad la primera resolución para la regulación internacional de la inteligencia artificial (IA), primer fruto de la llamada “conversación global” sobre esta tecnología. El texto, titulado “*Aprovechar las oportunidades de una IA segura y confiable para un desarrollo sostenible*”, fue iniciativa de Estados Unidos y “copatrocinado” o respaldado por más de 120 Estados miembros²⁸⁵.

En **diciembre de 2024**, el *Consejo de Seguridad* de la ONU debatió el **uso de la IA en los conflictos**. El secretario general de la ONU, António Guterres, señaló que los conflictos recientes se han convertido esencialmente en campos de pruebas para las aplicaciones militares de IA, con algoritmos utilizados en la toma de decisiones de vida o muerte. Advirtió que “*la inteligencia artificial sin supervisión humana dejaría al mundo ciego, y tal vez en ningún lugar más peligroso e imprudente que la paz y la seguridad mundiales*”.

No está claro hasta dónde puede llegar las Naciones Unidas en su esfuerzo de establecer un marco de uso de la IA aceptado globalmente. El llamamiento sobre la urgente necesidad de una **cooperación global para reducir la fragmentación de la gobernanza de la IA** se encontrará con posiciones divergentes entre países en un momento de alta conflictividad como el actual, y en el que la fortaleza tecnológica de los países en este ámbito es claramente asimétrica²⁸⁶. Además, el poder ejecutivo de las Naciones Unidas es muy limitado e impide, en la práctica, forzar el cumplimiento de sus resoluciones cuando están implicados los intereses de las grandes potencias.

En un ámbito separado del de las Naciones Unidas, y con ánimo de agrupar no solo las perspectivas de los estados miembros de las Naciones Unidas, sino también las de otros actores relevantes como las grandes empresas se han celebrado tres **cumbres de seguridad en IA** (*AI Safety Summit*) en los años 2023, 2024 y 2025.

- En noviembre de 2023, organizada por el gobierno del Reino Unido, se celebra la **1ª Cumbre de la Seguridad en IA**²⁸⁷ cuya Declaración Final (*Bletchley Declaration*)²⁸⁸, aunque sea muy vaga, demuestra un interés creciente en abordar colectivamente (participaron 27 países y múltiples organizaciones y empresas) los riesgos derivados del uso de la IA.
- La **2ª Cumbre** se ha celebrado en Seúl (Corea del Sur) en mayo de 2024 organizada conjuntamente por el Reino Unido y Corea del Sur, con el objetivo de mantener abierto el debate. El número de participantes creció significativamente frente a la 1ª Cumbre. China fue también invitada al debate ministerial. Es destacable que en esta segunda edición

285 <https://news.un.org/es/story/2024/03/1528511>

286 Algunos miembros de las Naciones Unidas, en particular Rusia, advirtieron contra la imposición de normas occidentales.

287 Los documentos de la Cumbre pueden encontrarse en: <https://www.gov.uk/government/topical-events/ai-safety-summit-2023>

288 <https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023>

el ámbito de discusión, además de reforzar los compromisos internacionales para un desarrollo “seguro” de la IA se amplió para **incorporar “innovación” e “inclusividad”**.

- La **3ª Cumbre** se celebró en París (Francia) en febrero de 2025. Para concluir el evento, 60 actores firmaron una *“Declaración sobre Inteligencia Artificial Inclusiva y Sostenible para las Personas y el Planeta”*, con el objetivo de alinear el desarrollo de la IA con el progreso hacia los Objetivos de Desarrollo Sostenible (ODS).

Sin embargo, en esta última ocasión, **dos grandes potencias en IA como Estados Unidos y el Reino Unido se negaron a firmar la declaración** de París. La postura crítica de la nueva administración de Estados Unidos se manifestó en contra de la *“excesiva regulación de la IA”* y abogó por un enfoque de *“no intervención”*. También el Reino Unido, por boca de su primer ministro, indicó que *“la iniciativa no era del interés del país”*. Estos desaires sugieren cambios drásticos en la narrativa sobre la seguridad de la IA y la gobernanza internacional de la IA, y anuncian dificultades mayores para lograr un consenso global (Torchio y Tassin, 2025).

Posiblemente, el interés de Francia como país anfitrión en **ampliar el marco de discusión de la reunión desde la seguridad estricta de la IA al análisis de los riesgos y oportunidades del desarrollo de la IA en otros ámbitos**, como el cambio climático y el uso de la energía diluyó la discusión e impidió una clara continuidad con el trabajo y las declaraciones acordadas en las cumbres anteriores. Esta situación arroja dudas sobre la continuidad de las Cumbres de Seguridad en IA con la estructura actual.

En definitiva, no es evidente pensar que los **esfuerzos voluntaristas** de organismos como el G7, la OCDE, o la ONU, o los resultados de cumbres como las organizadas por el gobierno del Reino Unido en 2023, Corea del Sur en 2024 y Francia en 2025 sean capaces de poner en marcha una gobernanza efectiva de la IA a tiempo en un momento en una fase en la que **el desarrollo de modelos y aplicaciones de IA se ha acelerado en todos los dominios**, y su uso militar también se acelera como se ha visto en el capítulo anterior.

Aunque no deben despreciarse estos esfuerzos, **ninguna de estas iniciativas tiene capacidad operativa real para obligar a los actores implicados**, y menos aún al sector empresarial, a cumplirlos, pero sí tienen una función relevante de *“foro de debate”* que, en el mejor de los casos, facilitarán la consecución de **acuerdos políticos muy generales de los que puedan derivarse regulaciones nacionales o entre diversos países** como podría ser el caso de los Estados miembros de la UE.

Otro enfoque regulatorio complementario al multilateral, y aprovechando las discusiones y regulaciones de estos es el realizado por muchos países para dotarse de **regulaciones nacionales específicas**. En este caso la ventaja es que los gobiernos sí disponen de las competencias necesarias desde el punto de vista legislativo y los medios para obligar a su cumplimiento, adaptándose a las peculiaridades de cada país. Por el contrario, el principal

problema es que su marco de aplicación queda reducido al ámbito de un único país, y su impacto real para controlar el desarrollo de la IA a nivel global es débil; sin embargo, lo que sí pueden ofrecer es un **marco de aplicación más seguro para el usuario final en ese país determinado**, aunque sea a costa de impedir el uso de determinados sistemas o de ralentizar el proceso innovador comparado con otros países.

Desde el punto de vista nacional, **las posiciones de los países sobre la necesidad y el tipo de regulación sobre la IA que sería necesaria son muy distintas**. Hay países avanzados tecnológicamente que prefieren no tener una legislación específica para IA como India o Singapur, o limitarse a disponer de unas “*directrices voluntarias*” como es el caso de Japón o, en cierta manera, de Estados Unidos y Corea del Sur apoyado en algunos aspectos legislativos más generales. Esa posición contrasta con la de otras potencias tecnológicas como China y la UE que ya disponen de legislaciones específicas de IA, aun a riesgo de que la obsolescencia tecnológica y la falta de flexibilidad en su aplicación y evolución o las restricciones, reales o percibidas, a la innovación las haga poco útiles a medio plazo y estén obligadas a llevar a cabo un proceso continuo de adaptación.

Finalmente, merece resaltarse el esfuerzo del Gobierno del **Reino Unido** que publicó su *Libro Blanco sobre la IA* el 29 de marzo de 2023, en el que expone sus propuestas para regular el uso de la IA en el Reino Unido. En lugar de introducir una nueva legislación de gran alcance para regular la IA, el Gobierno del Reino Unido se ha centrado en **establecer expectativas para el desarrollo y el uso de la IA junto con el empoderamiento de los reguladores existentes**, como la *Oficina del comisionado de Información* (ICO), la *Autoridad de Conducta Financiera* (FCA) y la *Autoridad de Competencia y Mercados* (CMA), para que emitan directrices y regulen el uso de la IA dentro de sus competencias.

6.3.2 Regulación de la IA en la UE

Un caso particular es el de la **UE** dado que su regulación sobre la IA afecta a 27 Estados miembros y **la UE ha dedicado desde hace años un gran esfuerzo en dotarse de un marco regulatorio consistente y avanzado pensando en reducir los riesgos ante el ciudadano europeo**. Su importancia deriva también de que la potencia reguladora de la UE suele tener reflejo en la adoptada por otros países como ha ocurrido en los ámbitos digitales y medioambientales en competencia con otras potencias (Bradford, 2024).

El debate sobre lo que la UE debería hacer en el ámbito de la IA arrancó en abril de 2018 con una “*Comunicación*”²⁸⁹ de la Comisión Europea titulada “*Inteligencia Artificial para Europa*” a la que siguió otra comunicación en diciembre del mismo año sobre un “*Plan coordinado para la Inteligencia Artificial*”. Con ellas la Comisión Europea quiso enmarcar un **debate co-**

²⁸⁹ Las “Comunicaciones” son documentos de debate y reflexión para las instituciones comunitarias y todos los agentes europeos, pero sin efectos jurídicos.

lectivo sobre la IA que era necesario para conseguir una posición común aceptable por todas las instituciones comunitarias sobre el desarrollo e impacto de una tecnología emergente.

Este proceso regulatorio de la UE ha tenido un gran **impacto en el ámbito digital** con una multiplicidad de reglamentos como se indica en la figura 6.3 lo que ha conducido también a múltiples adaptaciones legislativas en los Estados miembros. Algunas de estas regulaciones tardan años en aplicarse totalmente y, cuando han entrado plenamente en vigor, han conducido a la **imposición de sanciones económicas a algunas grandes empresas** con reacciones políticas en contra de la regulación por parte de los gobiernos de los países en los que se encuentran sus matrices²⁹⁰.



Figura 6.3. Regulación digital de la UE. Fuente: elaboración propia

El siguiente año, en abril de 2019, la Comisión Europea quiso focalizar la discusión en *“la construcción de confianza en una inteligencia artificial centrada en el ser humano”*, seguida por otra comunicación en 2020 denominada *“Inteligencia Artificial: Un enfoque europeo para la excelencia y la confianza”* apoyada por un grupo de expertos que, en 2019, publicó un documento titulado *“Directrices éticas para una IA confiable”* (Comisión Europea, 2019). Con todo ello la UE pretendía enmarcar la discusión en un problema básico del uso de la IA en la sociedad: **incrementar la confianza del ciudadano en los algoritmos de IA empleados en las múltiples aplicaciones digitales** que se expandían aceleradamente en todos los ámbitos de su vida personal y profesional.

El Parlamento Europeo creó en 2018 un **Comité Especial sobre Inteligencia Artificial en la Era Digital (AIDA)**²⁹¹, aunque la IA militar no fue su foco. El informe realizado reconoce que la IA sirve como una tecnología de doble uso con aplicaciones tanto civiles como militares.

²⁹⁰ En el caso de grandes empresas de Estados Unidos ha afectado a las relaciones con la UE dada la intervención directa del gobierno de Estados Unidos en contra de las sanciones a sus grandes empresas digitales.

²⁹¹ [https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/729381/EPRS_ATA\(2022\)729381_ES.pdf&ved=2ahUKewiUhrPoqtKNAXU0KvsDHUQ_HqAQFnoECCAQAQ&usg=AOvVaw32kHwnThj1nbJcHLgyf0g](https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/729381/EPRS_ATA(2022)729381_ES.pdf&ved=2ahUKewiUhrPoqtKNAXU0KvsDHUQ_HqAQFnoECCAQAQ&usg=AOvVaw32kHwnThj1nbJcHLgyf0g)

Hace hincapié en la necesidad de contar con directrices éticas y de gobernanza claras para garantizar un uso responsable de la IA en los sectores de la seguridad y la defensa.

En octubre de 2020, también el **Parlamento Europeo** empieza a preocuparse por los aspectos éticos derivados del uso de la IA con la adopción de un texto titulado *“Marco de aspectos éticos de la inteligencia artificial, robótica y tecnologías relacionadas”*. En ese documento **el Parlamento reconoce el papel dual de la IA** señalando que *“las tecnologías de IA son, en esencia, de uso dual, y el desarrollo de la IA en actividades relacionadas con la defensa se beneficia de intercambios entre tecnologías militares y civiles”*. El informe puso de manifiesto la **preocupación por la posibilidad de que la UE vaya a la zaga de otras potencias mundiales en el desarrollo de la IA, incluidas las aplicaciones militares**, y subraya la importancia de la soberanía tecnológica europea. También analiza el papel de la IA en la mejora de la ciberseguridad y la lucha contra las amenazas híbridas, e insta a la UE a desarrollar medidas sólidas de ciberseguridad impulsadas por la IA.

Tras todos los trabajos, documentos y deliberaciones previas mencionadas, la Comisión Europea publicó en abril de 2021 su *“Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen Normas Armonizadas en Materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y se Modifican Determinados Actos Legislativos de la Unión”*.

El texto de la Comisión propuso un marco reglamentario sobre inteligencia artificial con los siguientes objetivos específicos:

- Garantizar que los sistemas de IA introducidos y usados en el mercado de la UE sean seguros y respeten la legislación vigente en materia de derechos fundamentales y valores de la Unión;
- Garantizar la seguridad jurídica para facilitar la inversión e innovación en IA;
- Mejorar la gobernanza y la aplicación efectiva de la legislación vigente en materia de derechos fundamentales y los requisitos de seguridad aplicables a los sistemas de IA;
- Facilitar el desarrollo de un mercado único para hacer un uso legal, seguro y fiable de las aplicaciones de IA y evitar la fragmentación del mercado.

La UE asumió como un elemento básico de este Reglamento el *“principio de precaución”* de las administraciones públicas en relación con la IA apoyado en un grupo de prohibiciones a diferentes niveles para proteger al usuario. La propuesta clasifica el uso de la IA en función de los **niveles de riesgo para el usuario: inaceptable, alto, limitado, y mínimo**. Se utiliza un enfoque de riesgos inspirados en el empleado para la regulación de los dispositivos médicos.

La **clasificación como alto riesgo** conlleva el análisis del potencial lesivo en la salud y la seguridad o los derechos fundamentales de las personas, y las finalidades para las que se contempla su uso. De acuerdo con el Reglamento, estos sistemas estarán sujetos a obligaciones estrictas antes de que puedan comercializarse. Los sistemas de IA considerados de alto riesgo en el Reglamento europeo abarcan las tecnologías de IA empleadas en:

- Infraestructuras críticas (por ejemplo, transportes), que pueden poner en peligro la vida y la salud de los ciudadanos;
- Formación educativa o profesional, que pueden determinar el acceso a la educación y la carrera profesional de una persona;
- Componentes de seguridad de los productos (p.ej. aplicación de IA en cirugía asistida por robots);
- Empleo, gestión de trabajadores y acceso al trabajo por cuenta propia (p.ej. programas informáticos de clasificación de currículos personales);
- Servicios públicos y privados esenciales (p.ej. sistemas de calificación crediticia que priven a los ciudadanos de la oportunidad de obtener un préstamo);
- Aplicación de las leyes, que pueden interferir con los derechos fundamentales de las personas (p.ej. evaluación de la fiabilidad de las pruebas);
- Gestión de la migración, el asilo y el control de las fronteras (p.ej. comprobación de documentos);
- Administración de justicia y procesos democráticos.

Como ejemplo de aplicación, se limitan aquellas prácticas que tienen un gran *“potencial para manipular a las personas mediante técnicas subliminales que trasciendan su consciencia o que aprovechan las vulnerabilidades de grupos vulnerables concretos, como los menores o las personas con discapacidad, para alterar de manera sustancial su comportamiento de un modo que es probable que les provoque perjuicios físicos o psicológicos a ellos o a otras personas”*.

La propuesta prohíbe igualmente que las autoridades *“realicen calificación social basada en IA con fines generales”*. Por último, también se prohíbe, salvo excepciones limitadas, el *“uso de sistemas de identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley”*.

A raíz de ello, el Parlamento Europeo aprobó el 3 de mayo de 2022 una **Resolución sobre la inteligencia artificial en la era digital** (2020/2266(INI)).

Finalmente, tras un largo proceso de discusión con diferencias de partida entre los Estados miembros, el Consejo de la Unión Europea aprobó el **Reglamento de IA** de la UE que fue publicado el 13 de junio de 2024 (UE, 2024). Una vez aprobada, la Ley de IA está sujeta a un **período de implementación de dos años** durante el cual deberán establecerse sus estructuras de gobernanza, por ejemplo, la *Oficina Europea de Inteligencia Artificial*, antes de aplicarse a todos los proveedores de IA a finales de 2025 o comienzos de 2026 como pronto. No parece sencillo que, ante la presión de grandes empresas europeas, se acuerde una moratoria²⁹² que, por ahora, es rechazada por la Comisión Europea..

En resumen, **la Ley de IA comenzó a prepararse en 2018, la propuesta de Reglamento data de 2021 y, tras su aprobación, entrará completamente en vigor en 2026, o más tarde**. La consecuencia es que todo el proceso legislativo supondrá muchos años de elaboración e implementación completa en los que la tecnología evolucionará profundamente (ya hubo que acomodar en el texto del Reglamento aprobado provisiones sobre la IA generativa que no se consideraron en la propuesta inicial).

La pregunta abierta es si la UE será capaz de **adaptar paulatinamente el Reglamento de IA** para cubrir una evolución tecnológica tan rápida y proporcionar un marco legislativo sólido y estable que proporcione garantías jurídicas a las empresas, sirva para proteger al ciudadano, y promueva la innovación. En nuestra opinión, solo será posible si se **acorta sustancialmente el ciclo legislativo** sin perder por ello capacidad de debate en profundidad. De hecho, este es uno de los objetivos identificados por la Comisión Europea.

6.3.3 Pasos hacia una regulación de la IA en el ámbito militar

La **progresiva introducción de la IA en el campo de batalla** como se ha descrito en el capítulo 5 de este informe plantea varias preocupaciones éticas importantes para las que no existe un consenso a nivel internacional. Lo que es evidente es que el desarrollo tecnológico de la IA avanza muy deprisa, así como su uso en aplicaciones militares, mientras que las discusiones sobre su regulación global no lo hacen a ese ritmo.

Algunos de los problemas en el ámbito militar son técnicamente similares a los encontrados en aplicaciones civiles, aunque sus consecuencias sean diferentes. Uno de ellos es **determinar quién es el responsable cuando los sistemas de IA toman decisiones autónomas**. También en el ámbito civil si un sistema de IA causa daños no intencionados, la asignación de responsabilidades se convierte en un reto como conocen bien las autoridades y com-

²⁹² En julio de 2025 los responsables de 44 grandes empresas europeas solicitaron por carta a la Comisión Europea una moratoria de dos años sobre la aplicación de la Ley de Inteligencia Artificial, que empieza a entrar en vigor el 1 de agosto de 2025. Los firmantes advierten de que el actual marco normativo es confuso, redundante y amenaza con lastrar la competitividad tecnológica e industrial del continente, en un momento clave para la carrera global por el liderazgo en inteligencia artificial, donde Estados Unidos y China tienen una posición de liderazgo. <https://www.ft.com/content/a825759e-aec8-4184-bc73-f604f169204c>

pañías de seguros con las aceptaciones para la circulación de vehículos autónomos en las ciudades o carreteras. En el caso de la IA faltan datos y experiencia.

En el ámbito de la defensa este problema ha sido fuente de preocupaciones sobre la asunción de **responsabilidad en las operaciones militares**, aunque se trate únicamente de emplear la IA para la determinación automática de objetivos. Los problemas planteados en Gaza por el uso por parte de Israel de una herramienta como *Lavender* en la que se acepta que un porcentaje de los objetivos seleccionados tenían “*conexiones débiles*” fue ampliamente criticado (Abraham, 2024)²⁹³. *Lavender* no es, en realidad, un sistema de armas, pero puede formar parte de una cadena de acción (*killer chain*) en la que la información generada puede utilizarse de forma letal o no por otros sistemas autónomos o por humanos empleando armas convencionales.

Otra consideración clave es el **cumplimiento del derecho internacional**. Esto se relaciona con la adhesión de los sistemas de IA a principios como la **distinción** (garantizar que los combatientes y los civiles estén debidamente diferenciados) y la **proporcionalidad** (garantizar que las acciones militares sean proporcionales a la amenaza). Garantizar que los sistemas de IA puedan seguir efectivamente estos principios es esencial para garantizar el cumplimiento del derecho internacional. Por lo tanto, **sigue siendo fundamental en el uso de la IA en conflictos militares asegurar que el sistema es acorde con el Derecho Internacional Humanitario**. El problema es que la información necesaria para atestiguarlo depende de la voluntad de los bandos en conflicto para proporcionarlos en un contexto de transparencia que, en el caso de conflictos militares, no existe.

El debate radica en si se debe permitir que los robots tomen decisiones autónomas sobre vidas humanas o si los humanos deben conservar la autoridad final en la toma de decisiones (al menos, desde el punto de vista del *Control Humano Significativo*²⁹⁴). La postura generalizada es que, si bien la IA puede mejorar la velocidad y la precisión de la toma de decisiones, “*mantener el juicio humano en el proceso de toma de decisiones es esencial para garantizar que se mantengan los estándares éticos*” (Clapp, 2025).

En este marco de discusión, se ha planteado por diversos autores que el **uso de robots autónomos en combate no es ético** por dos razones conceptuales principales:

- En primer lugar, los robots reducen los riesgos hasta tal punto que las guerras futuras pueden ser más frecuentes, ya que las muertes humanas a menudo sirven como elemento

293 “Lavender”, es un sistema de recomendación de IA diseñado para utilizar algoritmos para identificar a miembros de Hamas como objetivos. Se combina en su uso con otro (Where’s Daddy?) que rastrea a los objetivos geográficamente para que puedan ser seguidos hasta sus residencias familiares antes de ser atacados. <https://theconversation.com/gaza-war-israel-using-ai-to-identify-human-targets-raising-fears-that-innocents-are-being-caught-in-the-net-227422>

294 el Control Humano Significativo (CHS) se refiere, de forma genérica, a la posibilidad de que el ser humano, es decir su operador, lo gobierne en todo momento y mantenga en su empleo la capacidad humana de proporcionarle inputs, derivados de su propio juicio y que le permitan retener un dominio legal y éticamente aceptable de las funciones críticas que se le encomienda ejecutar (Moliner, 2024).

disuasorio al ejercer presión política sobre los gobiernos. Al reducir los riesgos para las propias tropas de un Estado, estos sistemas también pueden reducir la barrera política para el despliegue o el uso de la fuerza y aumentar la probabilidad de una escalada del conflicto debido a interacciones rápidas dirigidas por máquinas.

- En segundo lugar, los robots no pueden distinguir de forma fiable entre combatientes y no combatientes, lo que potencialmente puede aumentar el riesgo de víctimas civiles. Por otro lado, los soldados robóticos podrían reducir las bajas humanas al retirar a los soldados de la línea de contacto del campo de batalla y facilitar el cumplimiento de las doctrinas militares sin interferencias emocionales.

Los problemas teóricos mencionados son rebatibles. Como ya se ha indicado en el capítulo 5 la experiencia en una guerra como la de Ucrania en la que los drones con diferentes grados de autonomía forman parte habitual del campo de batalla junto a sistemas de armas convencionales, no se produce ninguna reducción en el número de bajas²⁹⁵. Sí es verdad que no es fácil distinguir entre combatientes y no combatientes, pero ese problema no es exclusivo del uso de los “robots” y se ha convertido en un problema general con todos los sistemas de armas con efectos a distancia o cuando civiles aportan información que puede tener un valor militar.

Este es el caso de las aplicaciones desarrolladas en Ucrania en las que “civiles” pueden emplear una aplicación denominada **ePPO** descargada en su teléfono móvil (véase figura 6.4) por la que cualquier persona puede actuar como un “combatiente” proporcionando información de un objetivo (existen 200.000 usuarios activos): 1) El usuario selecciona el tipo de amenaza y envía una alerta, 2) En 2-7 segundos, el informe con la ubicación GPS aparece en los mapas digitales de las fuerzas aéreas AD y 3) Los algoritmos de IA ayudan a predecir la trayectoria del objeto (Azarkhina, 2025).



Figura 6.4. Aplicación ePPO. Fuente: Azarkhina, 2025.

²⁹⁵ De hecho, se trata de un conflicto militar de alta intensidad que, a pesar de usarse centenares de miles de drones en ambos bandos, el número de bajas supera el 1.400.000 personas (Jones y McCabe, 2025).

La discusión ética reside en que con el uso de este tipo de aplicaciones la distinción entre combatientes o no se hace más difícil y puede justificar el bombardeo de zonas civiles porque no actúa como tales, aunque no se conozca por parte de los atacantes quienes han hecho uso de la aplicación y quien no. Obviamente, el argumento contrario es que no se hace más que apoyar la defensa de vidas humanas; **si no hubiese ataques a zonas civiles, la aplicación no tendría utilidad.**

También se han expresado reservas sobre el aumento del uso militar de la IA derivadas del **peligro de no controlar las emociones en el campo de batalla** (Wilson, 2025) que pueden agravar situaciones, asesinatos por venganza o el incumplimiento de órdenes legítimas. Otros investigadores opinan que sistemas de IA pueden ser una mejor alternativa porque las emociones humanas “*negativas*” son reemplazadas por un “*campo de batalla más humano*”. Dudamos que esa hipótesis sea real porque el uso de sistemas de IA va a coexistir con otros convencionales, posiblemente para siempre.

En definitiva, si bien las opiniones entre expertos siguen divididas, **el uso de robots en combate es probablemente inevitable**, como lo es la adopción de aplicaciones específicas de IA, y sobre esa hipótesis debe plantearse la futura regulación de su uso en defensa.

6.4 Regulación de IA en defensa

6.4.1 Visiones diferentes

El rápido avance de la IA militar se ha intensificado, y los debates internacionales destacan la **falta de un marco unificado para garantizar el cumplimiento de los marcos legales establecidos que rigen los conflictos armados**. Esto incluye la defensa de principios como la distinción, la proporcionalidad y la necesidad de proteger a los no combatientes y prevenir daños excesivos.

Sin embargo, existe una limitación básica si el punto de partida es el de las regulaciones para usos civiles de la IA como es el caso de la UE. En la cumbre de IA de París de febrero de 2025, el vicepresidente de Estados Unidos, JD Vance, abogó por un enfoque más flexible y favorable a la innovación para la regulación de la IA y criticó el enfoque europeo. De hecho, la decisión de hacerlo o no “*se ha convertido en un tema geopolítico candente*”.

Visión de los Estados Unidos

En los últimos años, el **Departamento de Defensa** de los Estados Unidos (DoD) ha desarrollado un marco ético para abordar los problemas relacionados con la IA y la automatización. Algunos hitos son los siguientes²⁹⁶:

²⁹⁶ <https://blog.palantir.com/ai-automation-and-the-ethics-of-modern-warfare-df1f0b212397>

- En **octubre de 2019**, la *Junta de Innovación de Defensa* publicó el documento técnico de los **Principios de Ética de la IA**. El documento agrupa los resultados de un estudio destinado a abordar la cuestión de por qué se necesita una articulación ética de la IA militar. La Junta propuso cinco principios y doce recomendaciones concretas, aunque no vinculantes, para introducir esos principios en la práctica del DoD, cubriendo las principales áreas de capacidades de IA responsable, equitativa, trazable, confiable y gobernable.
- En **febrero de 2020** el DoD adopta los **Principios Éticos para la IA**²⁹⁷. Se trataba de recomendaciones para guiar las pruebas, el despliegue y el escalado de las capacidades habilitadas para la IA en todo el Departamento de Defensa.
- En **marzo de 2020** el DoD integra los Principios Éticos para la IA en los **programas de adquisición y creación de prototipos comerciales**²⁹⁸. Iniciada a través de la Unidad de Innovación de Defensa (DIU), una organización del DoD centrada en el despliegue y la ampliación de la tecnología comercial en todo el ejército de los EE. UU., la iniciativa refleja los esfuerzos para poner en práctica los principios de IA propuestos dentro de los programas de adquisición comercial.
- En **mayo de 2021** el subsecretario de Defensa publica un memorándum en el que pide la **“Implementación de una IA responsable en el Departamento de Defensa”**²⁹⁹ como un “enfoque holístico, integrado y disciplinado del Departamento de Defensa para la IA responsable (RAI)” de acuerdo con seis principios fundamentales: Gobernanza de la RAI, Confianza de los combatientes, Ciclo de vida de productos y adquisiciones de IA, Validación de requisitos, ecosistema de IA responsable y fuerza laboral de IA.
- En **noviembre de 2021** el DoD publica **“Directrices de IA responsable en la práctica”** de DIU (Dunnmon et al., 2021) con el que los principios éticos de la IA se desarrollan aún más. La publicación consta de preguntas específicas que deben abordarse en cada fase del ciclo de vida de la IA (planificación, desarrollo e implementación) para ayudar a garantizar que los programas de IA se alineen con los Principios Éticos para la IA del DoD. El documento sirve como “punto de partida para definir un proceso mediante el cual los Principios Éticos del Departamento de Defensa para la IA pueden ponerse en práctica en los programas de adquisición”.
- En **junio de 2022** el DoD publica su **Estrategia de Inteligencia Artificial Responsable y Vía de Implementación**³⁰⁰. El documento esboza un camino para poner en práctica los

297 <https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/>

298 <https://www.diu.mil/responsible-ai-guidelines>

299 <https://media.defense.gov/2021/May/27/2002730593/-1/-1/0/IMPLEMENTING-RESPONSIBLE-ARTIFICIAL-INTELLIGENCE-IN-THE-DEPARTMENT-OF-DEFENSE.PDF>

300 <https://media.defense.gov/2022/Jun/22/2003022604/-1/-1/0/Department-of-Defense-Responsible-Artificial-Intelligence-Strategy-and-Implementation-Pathway.PDF>

principios éticos de IA del DoD y avanzar en la IA Responsable (RAI) a través de seis líneas de esfuerzo que incluyen la modernización de las estructuras de gobernanza, el logro de niveles estándar de competencia tecnológica, y cultivar niveles adecuados de cuidado y mitigación de riesgos en los ciclos de vida de los productos y adquisiciones de IA.

- En **enero de 2023** el DoD actualiza la Directiva 3000.09 de 2012 **“Autonomía en los sistemas de armas”**³⁰¹ con especificaciones adicionales del proceso que debería seguirse si el DoD llegara a desplegar sistemas de armas autónomos fuera de los contextos muy limitados de defensa no letal o estática, *“a bordo y/o en red de instalaciones, plataformas, y vehículos o embarcaciones no tripulados, incluida la garantía de coherencia con los Principios Éticos de la IA del DoD y el Derecho de la Guerra”*.

Durante la Administración *Biden*, Estados Unidos adoptó una postura proactiva a la hora de establecer principios éticos para el uso de la IA en defensa, haciendo hincapié en principios clave como la **responsabilidad**, la **equidad**, la **trazabilidad**, la **fiabilidad** y la **governabilidad**.

En este contexto, el Departamento de Defensa (DOD) elaboró una propuesta de estrategia y una ruta de implementación de **Inteligencia Artificial Responsable (RAI)**, que proporciona pautas de gobernanza, capacitación para el personal de defensa y protocolos de gestión del ciclo de vida para sistemas de IA. La postura de Estados Unidos influyó en las declaraciones de las cumbres REAIM mencionadas anteriormente.

Para garantizar la seguridad y el cumplimiento del derecho internacional, el DoD ha desarrollado marcos de prueba y evaluación que tienen como objetivo salvaguardar los sistemas de IA de la manipulación de adversarios y evaluar su fiabilidad en contextos operativos. También elaboró un **Código de Conducta no vinculante para los Sistemas de Armas Autónomos Letales** para fomentar el comportamiento responsable y el cumplimiento de las normas legales, pero se opuso a cualquier prohibición preventiva de los SALA.

En febrero de 2023, durante la Cumbre de REAIM in La Haya, la **Declaración Política de los Estados Unidos sobre el Uso Militar Responsable de la Inteligencia Artificial y la Autonomía**³⁰² proporcionó un marco normativo para guiar el desarrollo, el despliegue y el uso éticos y responsables de la IA en entornos militares.

La Declaración hace hincapié en el cumplimiento del derecho internacional, en particular del derecho internacional humanitario, y subraya la importancia de mantener la responsabilidad humana en las operaciones militares habilitadas por la IA. La Declaración se describe como un conjunto de **directrices jurídicamente no vinculantes que describen las mejores prácticas para el uso responsable de la IA en un contexto de defensa**. Esto

301 <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf>

302 <https://www.state.gov/declaracion-politica-sobre-uso-responsable-de-inteligencia-artificial-y-autonomia-en-el-ambito-militar>

incluye garantizar que los sistemas de IA militar sean auditables, tengan usos explícitos y bien definidos, estén sujetos a pruebas y evaluaciones rigurosas a lo largo de su ciclo de vida, y que las aplicaciones de altas consecuencias se sometan a una revisión de alto nivel y puedan ser desactivadas si demuestran un comportamiento no deseado.

Sin embargo, la **“Orden Ejecutiva sobre Inteligencia Artificial” de la Administración Biden ha sido revocada por la de Trump mediante otra Orden Ejecutiva**. En la firmada por Trump se pretende incrementar el liderazgo de Estados Unidos en IA considerando que la anterior imponía restricciones a la innovación. La nueva directiva ordena la creación de un plan de acción de IA para reforzar el dominio de Estados Unidos en este campo, incluida la seguridad nacional³⁰³.

Visión de la OTAN

La **Estrategia de IA de la OTAN** de 2021 estableció una Visión Estratégica, con cuatro Objetivos y seis Resultados. En el marco de la Estrategia de IA, los Aliados respaldaron seis **Principios de Uso Responsable (PRU)** de la IA en la Defensa, a saber, Legalidad, Responsabilidad y Rendición de Cuentas, Explicabilidad y Trazabilidad, Confiabilidad, Gobernabilidad y Mitigación de Sesgos.

Posteriormente, la OTAN ha publicado la **estrategia revisada de IA en 2024**³⁰⁴, que establece estándares para el uso responsable, la protección contra la explotación adversaria y la adopción acelerada de la IA en operaciones militares. Esta estrategia actualizada se basa en la versión de 2021 e incorpora los avances recientes en IA, como la IA generativa y las herramientas de gestión de la información impulsadas por la IA. Los objetivos de la Estrategia de IA de la OTAN son:

- a. *Proporcionar una base para que la OTAN y los Aliados lideren con el ejemplo y fomenten el desarrollo y el uso de la IA de manera responsable para los fines de defensa y seguridad de los Aliados;*
- b. *Acelerar e incorporar la adopción de la IA en el desarrollo y la disponibilidad de capacidades, mejorando la interoperabilidad como elemento clave dentro de la Alianza, incluso mediante la presentación de casos de uso de IA;*
- c. *Proteger y supervisar nuestras tecnologías de IA, gestionar los riesgos relacionados y proteger nuestra capacidad de innovación, abordando las consideraciones de la política de seguridad, como la puesta en marcha de nuestras PRU; y*
- d. *Identificar y protegerse contra las amenazas del uso de la IA por el adversario.*

303 <https://apnews.com/article/trump-inteligencia-artificial-decreto-2cc5bc1fbaf87460dabe787738663d36>

304 https://www.nato.int/cps/ua/natohq/official_texts_227237.htm

Las prioridades clave incluyen la aplicación de los **Principios de Uso Responsable** de la OTAN, la mejora de la interoperabilidad de los sistemas de IA en toda la Alianza, la integración de la IA con otras tecnologías disruptivas emergentes y el fortalecimiento del ecosistema de IA de la OTAN.

6.4.2. Empleo de las reglas de enfrentamiento (ROE) para el uso de la IA

Un enfoque que ha tomado predicamento en los últimos años es el de aprovechar las **reglas de enfrentamiento** (*rules of engagement, ROE*) bien conocidas en el ámbito militar como marco de referencia para determinar **cómo usar la IA en operaciones militares**.

Según el *Manual de Reglas de Enfrentamiento de San Remo* de junio de 1994³⁰⁵, las ROE son “una combinación de requisitos de política militar y política [que] **deben estar limitados por los parámetros legales internacionales y nacionales existentes**”. Más concretamente (Kwick et al., 2025): “Las ROE son un instrumento utilizado por los comandantes militares para regular la conducta, en particular el uso de la fuerza, del personal bajo su mando. Son, en esencia, normas que rigen el uso de la fuerza y las acciones que pueden (potencialmente) influir o regular la escalada del uso de la fuerza o de las hostilidades en la zona de operaciones”.

Más específicamente, las ROE proporcionan autorización y/o límites para “el uso de la fuerza, el posicionamiento y la posición de las fuerzas, y el empleo de ciertas capacidades específicas”. Suelen contener elementos básicos, como instrucciones generales para el comandante y cuestiones políticas y jurídicas generales relacionadas con la operación. Con ellas, las fuerzas armadas pueden **traducir los objetivos estratégicos políticos y militares y los requisitos legales internacionales en contextos operativos**. Las reglas de enfrentamiento también pueden indicar qué comandantes de la cadena de mando son responsables de autorizar acciones específicas³⁰⁶.

Vestner (2024) propuso que las **reglas de enfrentamiento** pueden servir como **marco para regular el uso de aplicaciones militares de la IA**, sobre la base de un análisis de los instrumentos básicos para la preparación y realización de operaciones militares con IA. La publicación argumenta que las ROE responden bien a las necesidades regulatorias de la IA, en particular porque “representan un marco holístico, específico y concreto, pero flexible”. En el futuro, las ROE pueden ser especialmente útiles para regular la formación de equipos humanos y máquinas y el control humano de los sistemas de IA.

Si bien las ROE siguen siendo fundamentales para las operaciones militares, expertos reunidos en un taller en *La Haya* debatieron si el ROE tradicional podía servir como un instrumento

³⁰⁵Es aplicable a los conflictos armados en el mar <https://international-review.icrc.org/sites/default/files/S0250569X0002481Xa.pdf>

³⁰⁶ En el caso de la OTAN, su comité Militar elaboró el documento MC-362 en el que define las ROE como: “directivas dirigidas a las fuerzas militares (incluidos los soldados), en las que se definen las circunstancias, las condiciones, el grado y los procedimientos para el empleo de la fuerza o de acciones que podrían considerarse como provocaciones”. Disponible en línea: <https://www.legaltoday.com/practica-juridica/derecho-penal/penal/reglas-de-enfrentamiento-roe-2008-05-12/>

eficaz para generar instrucciones específicas de la IA; en segundo lugar, cómo las autoridades responsables de emitir estas directivas militares interpretarían y traducirían elementos técnicos y operativos complejos en directrices claras y viables para las fuerzas armadas. Como resultado, los expertos coincidieron en que **la complejidad y la imprevisibilidad inherentes a la IA pueden requerir un nuevo enfoque, uno que exija directivas flexibles y específicas del contexto capaces de abordar los desafíos específicos de la IA** (Kwick et al., 2025).

6.4.3. Posición de las empresas privadas del sector de la defensa

Parece una contradicción mutuamente excluyente conciliar el desarrollo de herramientas software que preserven principios éticos y, a la vez, proporcionen la máxima eficacia a las fuerzas armadas, incluso con problemas éticos asociados si su función es letal, que aseguren la supervivencia y la victoria frente al enemigo.

Este dilema se ha trasladado a las **empresas de defensa** que desarrollan este tipo de sistemas. Shoeni y Vestner (2023) argumentan: *“La industria de defensa desarrolla, produce y vende armas que causan un gran daño. Opera en la intersección de los sectores público y privado, con una mayor dependencia de las empresas tecnológicas. Aunque estas empresas existen principalmente para servir a sus Estados anfitriones, interactúan habitualmente con sistemas legales extranjeros y diversas culturas. Este contexto crea desafíos éticos únicos”*.

No es extraño por ello que algunas de estas empresas hayan definido públicamente su **posición institucional en contratos relacionados con la defensa**, incluso cambiando la posición en el transcurso del tiempo. Esta situación ha conducido, a veces, a problemas de posicionamiento ante la plantilla (p.ej. con opiniones en contra de ingenieros directamente implicados en el desarrollo de sistemas de armas) que pueden aducir conflictos éticos cuando sus deberes profesionales confrontan con sus creencias personales o valores relacionados con la defensa³⁰⁷. Dos casos significativos son los de las empresas **Palantir** y **Alphabet**, ambas con sede en Estados Unidos que mantienen posiciones institucionales sobre este tema.

Palantir, una empresa de defensa en Estados Unidos, aboga públicamente (Palantir, 2023) por un compromiso de la entidad que *“refuerce las aplicaciones responsables y defendibles, apoye las misiones críticas de inteligencia a través de tecnología construida para proteger la privacidad y las libertades civiles, acepte y respalde el doble compromiso de proteger y preservar los imperativos éticos y, al mismo tiempo, brinde a los combatientes las mejores herramientas para ejecutar los objetivos de su misión”*.

Alphabet, empresa matriz de *Google*, ha reescrito sus directrices sobre cómo utilizará la IA, eliminando una sección que anteriormente descartaba las aplicaciones que *“probablemente*

307 La posición habitual es que los ingenieros de la industria de defensa no están directamente involucrados en el combate y no están sujetos a las reglas de la guerra. Sus obligaciones éticas se basan en sus responsabilidades profesionales, no en las de un soldado.

causaran daño” (en el desarrollo de armas o sistemas de vigilancia). Google defendió el cambio, argumentando que las empresas y los gobiernos democráticos necesitaban trabajar juntos en una IA que *“apoye la seguridad nacional”*. El hecho de que Alphabet levante una prohibición ya antigua sobre el uso de IA para desarrollar armas y herramientas de vigilancia es “muy preocupante”, desde la posición de grupos de derechos humanos como *“Humans Rights Watch”*³⁰⁸ (Hooker y Wallace, 2025).

Los problemas éticos ligados al desarrollo de sistemas militares se han planteado de manera más concreta no referidos a la industria de defensa convencional en la que tanto la empresa en su creación como sus empleados en el proceso de contratación han aceptado la actividad ligada al desarrollo de armas o sistemas militares, sino en otras **empresas digitales focalizadas en IA**. Estas empresas digitales han desarrollado históricamente sistemas civiles, pero, al tratarse de tecnologías duales, han empezado a conseguir contratos para el desarrollo de sistemas de defensa adaptando sus productos del mercado civil a requisitos militares. Para algunos de sus empleados eso suponía un **cambio sustancial sobrevenido en las condiciones del entorno de trabajo** preexistente con la que manifestaban su desacuerdo.

Un caso conocido en este sentido es el de *Google* y su participación en el proyecto ***Maven***³⁰⁹ que provocó una **carta abierta a la dirección en contra de esa participación** por parte de más de 3.600 empleados y otros firmantes hasta llegar a totalizar 6.300 en 2018. En el texto, se indicaba: *“Creemos que Google no debería participar en el negocio de la guerra. Por ello, pedimos que se cancele el Proyecto Maven y que Google escriba, haga pública y ponga en vigor una política clara que establezca que ni Google ni sus contratistas construirán jamás tecnología de uso bélico”*. La empresa, por su parte aducía que *“Google trabaja en una parte que específicamente tiene fines no ofensivos y que utiliza un software de reconocimiento de código abierto disponible para cualquier cliente de Google Cloud”*.

Finalmente, *Google* abandonó el proyecto en 2019³¹⁰, aunque su puesto fue ocupado por otras empresas del sector como *Microsoft*. Tras el ataque a Israel por parte de Hamas, **el Departamento de Defensa decidió implementar los algoritmos de IA desarrollados por el Proyecto Maven** que ha seguido su desarrollo.

Otro ejemplo de controversia tuvo lugar en febrero de 2019 cuando más de 200 empleados de *Microsoft* exigieron que la empresa cancelara un contrato de 480 millones de dólares con el Ejército de los Estados Unidos para abastecer a soldados con más de 100.000 gafas

308 El grupo de derechos humanos criticó la medida, señalando que podría “complicar la rendición de cuentas” en las decisiones militares que tienen implicaciones de vida o muerte.

309 Maven es un programa piloto para acelerar la aplicación militar de la inteligencia artificial. Pretende ayudar a procesar de forma eficiente las grabaciones de video que diariamente recolectan los drones utilizados por las fuerzas militares estadounidenses, detectando vehículos y otros objetos, haciendo seguimiento de sus movimientos y proveyendo los resultados de su análisis al Departamento de Defensa.

310 <https://www.bbc.com/mundo/noticias-44355550>

de realidad aumentada con tecnología “HoloLens”.³¹¹. La respuesta de Microsoft fue: “*no vamos a retener tecnología a instituciones que hemos elegido democráticamente para que protejan nuestras libertades*” (Riley y Burke, 2019). Es evidente que la mayor percepción del riesgo por la población laboral puede hacer modificar las reticencias de la misma forma que ha ocurrido en el pasado, y se imponga una visión compartida de “defensa del país” (el caso de Ucrania es paradigmático). En todo caso, no parece que este tipo de casos se haya extendido.

6.5 Necesidad de regulación del uso militar de la IA en la UE

La Regulación de **Inteligencia Artificial (AI Act) de la UE, excluye explícitamente de su ámbito de aplicación la seguridad nacional, la defensa y los fines militares**. La ley se centra exclusivamente en la IA comercial, excluyendo las aplicaciones militares y los servicios de seguridad nacional. De hecho, durante las negociaciones, algunos Estados miembros, en particular Francia, presionaron para que se establecieran **exenciones para preservar la autonomía estratégica de Europa**, garantizando restricciones mínimas a la IA en defensa y seguridad.

Si bien el Reglamento europeo no regula directamente la IA militar, sí puede **influir en la política de IA de defensa**, particularmente en tecnologías de doble uso como es el desarrollo de los drones o el uso de servicios digitales potenciados por la IA. El Reglamento aprobado introduce una **clasificación basada en el riesgo para las aplicaciones de IA**, imponiendo obligaciones de cumplimiento a los proveedores que, desde el punto de vista conceptual, podría trasladarse al ámbito militar.

El “*enfoque centrado en el ser humano*” de la ley podría dar forma a futuros debates sobre los SALA dentro de la política de defensa de la UE. En todo caso, dado que la ley de IA establece claramente que uno de sus objetivos es **garantizar la soberanía tecnológica y la autonomía estratégica de la Unión**, podría indicar que no se desea un enfoque restrictivo del desarrollo de esta tecnología en el sector militar; el objetivo a largo plazo sería asegurar que estos sistemas se desarrollaran en la UE y bajo sus condiciones de uso.

En el fondo, el problema reside en admitir la dificultad de que la Regulación de IA aprobada por la UE pueda adaptarse para el uso militar. De hecho, **la UE debería crear un marco para la IA responsable en defensa, utilizando como modelo la clasificación de riesgos de la Ley de IA**. Un marco unificado demostraría el liderazgo de la UE en la gobernanza de la IA, abordando los riesgos y garantizando el uso responsable de la IA tanto en el ámbito militar como en el civil.

311 La licitación indicaba que se necesitaba una pantalla montada en el casco capaz de proporcionar visión nocturna, la búsqueda sigilosa de armas y la capacidad de reconocer amenazas automáticamente <https://www.tni.org/en/article/militarising-big-tech?translation=es>

La posición inicial de las empresas europeas del sector de la defensa es considerar que los incrementos presupuestarios acordados en la UE suponen el incremento de puestos de trabajo, y oportunidades para la mejora de condiciones laborales. Sin embargo, la posición de algunos sindicatos ha sido la de que la reconversión de industrias europeas (p.ej. la del automóvil) para incrementar la producción militar, supone una transformación del mercado laboral que no favorece a los trabajadores. Estas posiciones han llevado a una movilización activa y organizada en diversos países de la UE que, por ahora, no se ha extendido ni ha cambiado las posiciones de los gobiernos ni de los sectores empresariales.³¹²

La necesidad de una **regulación más estricta de la IA militar por parte de la UE**, a pesar de que la Ley de IA la exime de la supervisión está justificada por preocupaciones de seguridad nacional, pero plantea la **urgencia en establecer marcos de gobernanza globales**, dado el potencial de doble uso de la IA tanto en aplicaciones civiles como militares.

Además, **la posición pragmática de que la IA militar debería regularse únicamente a nivel nacional se está debilitando**. Dado que estas tecnologías tienen implicaciones transfronterizas y que los países de la UE ya colaboran en iniciativas de defensa, es necesario un enfoque regulador coordinado. Muchos analistas señalan que, si la Ley de IA actual podría poner trabas al proceso de innovación debido a un **exceso de regulación, ampliar la Ley al ámbito militar conllevaría el mismo problema** con el agravante de poner en riesgo la superioridad militar que podría concederse a potenciales enemigos con regulaciones de uso militar de la IA menos estrictas.

El **Parlamento Europeo** ha sido un actor clave en el debate sobre la IA militar, abordando la cuestión desde el principio. Ha adoptado dos tipos de resoluciones principales: una centrada en los sistemas SALA, y otra que abarca tanto la IA militar como las armas letales autónomas. En resumen, **el Parlamento está abierto al uso militar de la IA y reconoce la importancia estratégica y el potencial de la IA para proteger a los soldados y a los civiles** con tres principios clave para la IA militar: (1) mantener la participación humana en el mando y el control, (2) garantizar la responsabilidad legal de las personas y los Estados, y (3) abogar por la gobernanza internacional de la IA a través de las Naciones Unidas, incluidas las regulaciones de exportación.

En cuanto a los SALA, el Parlamento ha instado sistemáticamente al Consejo a **impedir el desarrollo y el uso de SALA que operan sin un control humano significativo y a presionar para que se prohíban en todo el mundo**. En concreto, quiere que el Consejo participe en las negociaciones de la ONU en el marco de la *Convención sobre Ciertas Armas Convencionales* para regular la IA militar y prohibir las armas “totalmente autónomas”.

³¹² Por ejemplo, en Italia se convocó una huelga de transportes en junio de 2025 con el lema “Bajad las armas, subid los salarios”. <https://www.swissinfo.ch/spa/italia-afronta-una-huelga-general-de-transportes-contra-la-precariidad-y-el-rearme/89544692>

La Resolución de 2021 hace hincapié en la **necesidad de que la UE desarrolle un marco global para regular las tecnologías de IA, garantizando que se ajusten al Derecho internacional y defiendan los derechos fundamentales**. Destaca la importancia de las directrices éticas, la transparencia y la rendición de cuentas en el despliegue de la IA, especialmente en los ámbitos que afectan a la administración pública y a las operaciones militares. El Parlamento pide la cooperación de los Estados miembros para establecer normas y prácticas comunes para el uso de la IA, promoviendo la innovación y salvaguardando al mismo tiempo los principios éticos y las normas jurídicas.

6.5.1 Avances en la regulación para el uso de sistemas de armas inteligentes

En relación con los **aspectos éticos ligados al uso de SALA** (Moliner, 2024 o González, 2022) la organización no gubernamental británica “**Article 36**” indicaba ya en 2013 que deberían cumplirse un conjunto de condiciones para que existiera un **control humano como se ha indicado** previamente en este capítulo.

Como Moliner (2024) indica: *“Se presenta, así, el problema de la responsabilidad legal y moral de quién toma la decisión: ¿el diseñador, los desarrolladores, el hardware, los algoritmos de IA, el comandante de la operación, los operadores, la propia máquina dotada de entidad jurídica?”* Es la traslación al dominio militar de preguntas que ya se están haciendo en el ámbito civil para la incorporación de vehículos autónomos en las ciudades y carreteras y que, de hecho, condicionan su despliegue real.

Creemos que **las condiciones establecidas para el CHS siguen siendo válidas en términos generales**, pero debe reconocerse que son difíciles de acomodar con la realidad militar como el caso del empleo de los enjambres de drones indican. Es interesante indicar que en el **debate sobre los aspectos éticos ligados a los SALA** (generalmente, a favor de su prohibición) hay posiciones que quieren distinguir entre los empleados para **defenderse** (p.ej. sistemas automáticos contra el ataque de drones) de los de **ataque**; incluso, se considera que SALA “*bien diseñados*” pueden ayudar a reducir las bajas civiles y militares al ser más precisos en la identificación del objetivo y estar menos sesgados por razones ideológicas (Verbruggen, 2023).

Para otros analistas, la **lejanía del operador humano del objetivo** (como sucede en drones letales operados remotamente) hace más sencilla en términos morales la decisión de dar la orden para disparar. Además, La combinación de la disminución del riesgo para los soldados y la distancia física del campo de batalla hace que **la discriminación entre combatientes y no combatientes sea más difícil**. Todo ello va a obligar a la **incorporación de los requisitos éticos en el ciclo de vida del sistema**, desde el proceso de diseño hasta el uso final, implicando a todos los actores relevantes (Moliner, 2024). La combinación de la comprensión ética de los humanos y las rápidas capacidades analíticas de la IA puede acelerar el proceso de toma de decisiones (SDI, 2024).

Se conoce que, al menos, Estados Unidos, Reino Unido, Israel, China, Corea del Sur, Irán, Italia, Francia, India, Pakistán, Rusia, Turquía, Australia y Polonia han fabricado drones militares inteligentes operativos. En los últimos años **estos países están invirtiendo fuertemente en el desarrollo de SALA** con una gama cada vez mayor de tamaños, capacidades, y nivel de inteligencia. Algunos otros países, como Ucrania, azuzados por la necesidad, están consiguiendo en poco tiempo la experiencia, los datos y la capacidad para convertirse en un actor relevante en el futuro del empleo táctico de drones, incluso con acciones tácticas innovadoras como los ataques con drones a aeropuertos rusos a mucha distancia del frente transportados y camuflados en camiones realizados el 1 de junio de 2025 en la denominada “Operación Telaraña”³¹³.

Aunque diversos informes recientes indican que tanto Rusia como Ucrania están encontrando **dificultades relevantes para conseguir una operación ideal de drones autónomos integrados con el resto de las fuerzas armadas**, conseguirlo es, en nuestra opinión, una cuestión de tiempo. Los algoritmos de enjambre mejorarán rápidamente y la inteligencia en los procesadores a bordo de mucha mayor potencia y bajo consumo para incrementar la autonomía permitirán su integración en sistemas autónomos. A ello se añade el desarrollo de sistemas de mando y control multidominio potenciados por motores de decisión sobre IA.

En el capítulo 5 se ha comentado el caso de un ataque ucraniano en el frente de Járkov exclusivamente con drones aéreos y UGV (terrestres) en julio de 2025 que había producido la rendición de un número indeterminado de soldados rusos ante drones por primera vez en la historia. Retomamos este caso en el presente capítulo desde el punto de vista del **vacío legal existente**; la Convención de Ginebra no establece cómo y en qué condiciones se pueden rendir combatientes a máquinas para la aplicación del concepto de “*prisionero de guerra*”. En el caso mencionado, los drones “escortaron” a los soldados rendidos hacia la zona en la que se encontraban las fuerzas ucranianas; a partir de ese momento, todo normal. Debe recordarse que los drones y UGVs ucranianos estaban tripulados remotamente.

Sin embargo, por establecer una situación ficticia, podría pensarse en qué pasaría si alguno de los soldados rendidos huyera antes de llegar al destino: ¿podría un dron perseguirle y neutralizarle siguiendo el entrenamiento de sus algoritmos de IA?, ¿quién sería el responsable? Tal y como Wallace et al. (2025) han analizado como “rendición habilitada tecnológicamente” es necesario disponer de una interpretación adaptativa de las leyes del conflicto armado, y asegurar que esa interpretación es igual por los bandos en conflicto.

313 Parece que los ataques sobre cuatro aeropuertos militares rusos han destruido más de 40 aviones, incluyendo los bombarderos estratégicos con capacidad nuclear Tu-95 y Tu-22M3, así como los aviones de alerta temprana A-50. Según fuentes del Servicio de Seguridad de Ucrania (SBU), la “Operación Telaraña” tardó un año y medio en organizarse. Primero se introdujeron de contrabando 117 drones FPV en Rusia, seguidos posteriormente por cabinas móviles de madera. Una vez en territorio ruso, los drones se ocultaron bajo los techos de estas cabinas instaladas en camiones. En el momento del ataque, los techos se abrieron a distancia, lo que permitió que los drones despegaran y atacaran las bases aéreas cercanas; probablemente, empleando IA para reconocer los objetivos. <https://www.bbc.com/mundo/articles/c331jz5kj82o>

Dado que **el número de países que se han dotado de este tipo de sistemas** en sus arsenales mediante su adquisición en los mercados internacionales **crece de forma continua**, en pocos años será un armamento incorporado habitualmente en los ejércitos de todos los países. Obviamente, su número y capacidades (inteligencia, tamaño, autonomía, velocidad, armamento, cargas de pago, etc.) y, por supuesto, el coste, diferirá fuertemente de unos a otros. Si este supuesto de **mejoras técnicas, de crecientes inversiones y de adopción generalizada por los ejércitos** se cumple, el marco ético y regulatorio correspondiente adaptado a ese escenario debería estar acordado al final de esta década. No será sencillo.

En la última **Resolución de la Asamblea General de Naciones Unidas** el 24 diciembre de 2024 sobre este tema (UN, 2024) se expresa la aplicabilidad del marco actual a la IA en el ámbito militar: *Afirma que el derecho internacional, incluida la Carta de las Naciones Unidas, el derecho internacional humanitario y el derecho internacional de los derechos humanos, se aplica a las cuestiones regidas por él que se producen en todas las etapas del ciclo de vida de la inteligencia artificial, incluidos los sistemas habilitados por la inteligencia artificial, en el ámbito militar;*

La **pregunta abierta a la sociedad** (sobre todo, a la occidental a la que pertenecemos) es conocer hasta qué punto está dispuesta a **renunciar a derechos democráticos en la defensa contra una guerra cognitiva potenciada por la IA** que es cada vez más visible, y cómo encontrar el equilibrio en una situación marcada por el desarrollo de la IA a un ritmo muy rápido que hace obsoletos en poco tiempo los marcos regulatorios existentes. **Encontrar ese equilibrio no es sencillo**, y el debate se prolongará en el tiempo.

6.5.2 La ética militar entre la IA y la neurotecnología (NT)

El cerebro juega un papel fundamental para el ser humano al ser el órgano básico para conocer **lo que ocurre en el cuerpo humano y en el entorno exterior y cómo responder a ello**. Su importancia deriva de que la mayor parte de los avances ligados al aumento de capacidades humanas está relacionada directa o indirectamente con el cerebro y la tecnología básica para modificar su acción es la **neurotecnología**.

En la última década se ha prestado **considerable atención al análisis de los temas éticos asociados al uso de la neurotecnología** en el ámbito médico y fuera de él en el ámbito civil desde comienzos de este siglo (León, 2024); mucho menos esfuerzo se ha focalizado en las consecuencias de su uso en defensa para las que la tecnología era inmadura y las cuestiones éticas tenían un claro interés conceptual, pero muy alejadas de la práctica y la experiencia como ya se expuso en el capítulo 5.

Su importancia, sin embargo, ha crecido en los últimos años desde dos perspectivas complementarias: la utilización de la neurotecnología como parte del objetivo de **aumento de**

capacidades humanas hacia un “soldado potenciado”, y desde el objetivo de la guerra cognitiva en la que sea posible **actuar sobre el cerebro.**

En ambos casos, **el objetivo es la mente humana,** ya sea para mejorar sus prestaciones o para interferir en su funcionamiento. El **desarrollo paralelo de la IA y la neurotecnología así como su posible uso en defensa** está íntimamente entrelazada dando origen al concepto de un nuevo tipo de guerra que se ha denominado *“neuro-cognitive warfare”* (McCreight, 2023) (McCreight, 2024).

Desde el punto de vista técnico, los algoritmos de aprendizaje automático junto al desarrollo de implantes cerebrales han sido fundamentales para el **aumento constante del conocimiento sobre la estructura y el funcionamiento del cerebro.** Principalmente, estas tecnologías han facilitado el procesamiento de grandes conjuntos de datos y la identificación de patrones discretos dentro de extensos **conjuntos de neurodatos** complejos. Los algoritmos de IA también son indispensables para la conexión en tiempo real de los patrones de actividad extraídos de los neurodatos con los comandos operativos deseados; ellos se han constituido en un factor clave para el desarrollo y uso de interfaces cerebrales inteligentes.

En este contexto de desarrollo acelerado de la neurotecnología y su consideración como tecnología de uso dual, surge el deseo de conocer los **aspectos éticos y regulatorios** de la misma, asociados a su posible uso en aplicaciones de defensa.

6.5.3 Aspectos éticos y regulatorios asociados a la neurotecnología

A nivel normativo, la **convergencia entre la IA y la neurotecnología** implica que también deben tenerse en cuenta las preocupaciones éticas y legales relacionadas con el procesamiento de la IA. Aunque el cerebro actúa en la percepción sensorial y la motora, el debate ético actual se concentra con mayor intensidad, en el **desarrollo y uso de las tecnologías de aumento cognitivo y social.**

Aunque la lista de posibles preocupaciones éticas es muy elevada, existen dos específicamente relacionadas con el ámbito de la neurotecnología que son muy relevantes: la **privacidad mental** y el **libre albedrío o agencia humana.**

La **“privacidad mental”** se refiere a la **aceptación de que el contenido de la mente de una persona solo es conocido conscientemente por esa persona.** Con el nivel de madurez tecnológica alcanzado actualmente **nadie** puede acceder a ese contenido, a menos que la persona decida compartirla con otros ya sea hablando, escribiendo, dibujando o utilizando el lenguaje corporal para expresarla y comunicarla a otros³¹⁴. De hecho, esta es la **base de**

³¹⁴ Obviamente, bajo coacción, física o psicológica (o bajo los efectos de ciertos fármacos para reducir la voluntad) se puede forzar a un individuo a dar una información no deseada a otros, pero, incluso en estos casos, esta información es percibida

la interacción social en la especie humana: el cerebro humano coordina la respuesta del sistema sensorial para comunicarse con otros seres vivos (no solo con otros seres humanos) dentro de los límites de las capacidades posibles para el ser humano.

Con los avances científicos y tecnológicos en el ámbito de la neurotecnología, **la presunción de la privacidad mental ya no es necesariamente cierta**. La neurotecnología permite actualmente registrar y transmitir datos relacionados con la actividad cerebral, e interpretarlos sin mediar una comunicación sensorial con el emisor.

Es habitual en la práctica médica que, empleando sistemas tecnológicos comunes, **parte de los datos generados por el sistema nervioso de una persona pueden ser obtenidos incluso sin el control consciente de esa persona**. Si estos datos se reducen al conocimiento y monitorización de determinadas variables fisiológicas (p.ej. el análisis de la información contenida en un electroencefalograma) o la determinación de las zonas activadas del cerebro³¹⁵ (p.ej. mediante un sistema de magnetoencefalografía) no existe un problema real de privacidad, suponiendo el consentimiento previo de esa persona (paciente), puesto que **esa información no es suficiente para conocer en qué está pensando ni cómo modificar ese pensamiento**.

El problema ético surge cuando el desarrollo tecnológico pueda hacer factible que una persona sometida a un proceso de neuromonitorización y neuroestimulación **revele de forma no intencionada o no consciente (sin saberlo o sin querer hacerlo) datos de su actividad cerebral relacionado con su pensamiento**; es decir, conocer lo que realmente está pensando, sin utilizar su sistema sensorial, y con ello sea posible obtener información a través de la neurotecnología que de otro modo no facilitaría vulnerando el supuesto de privacidad mental³¹⁶. Problema ético más agudo en el caso de que se pudiera modificar externamente sus recuerdos o modificar su forma de pensar.

En resumen, el concepto de **privacidad mental** con problemas éticos relevantes derivados del uso de la tecnología debe circunscribirse al caso de la **obtención de datos referidos a los pensamientos del individuo y no solo a condiciones fisiológicas del cerebro** como ya se hace rutinariamente en la práctica médica.

por otros individuos una vez se haya transformado en forma sensorial (p.ej. mediante el lenguaje hablado, gráfico o corporal). Estos casos son moral y éticamente inaceptables y regulados en las legislaciones penales internacionales.

315 Mediante otros tipos de análisis cerebral como los que se realizan con técnicas de magnetoencefalografía o resonancia magnética nuclear.

316 En sentido estricto, no es raro en entornos médicos (p.ej. durante una intervención quirúrgica) monitorizar las condiciones fisiológicas de un paciente, incluso de su estado mental (p.ej. mediante la obtención continua del electroencefalograma), sin que el paciente esté consciente; pero eso no permite conocer la información almacenada en su memoria. También empiezan a aparecer sistemas de monitorización del estado de coma (desde superficial a profundo) lo que obliga también a obtener datos de la actividad cerebral.

Este problema ético adquiere mayor relevancia cuando, además, esta información puede tener un **valor comercial**³¹⁷ o cuando se integran datos cerebrales con otros tipos de datos sensibles, como la relación con otras enfermedades (p.ej. el VIH), el uso de drogas, las mutaciones genéticas con implicaciones clínicas, el historial de abortos y la actividad en línea. Compartir estos datos podría plantear riesgos tanto de re-identificación como de uso indebido de información altamente privada.

La **iniciativa BRAIN** denomina **neuroética** al campo que estudia las implicaciones éticas, legales y sociales de la neurociencia. En el taller del “*Neuroethics Working Group*” de la iniciativa BRAIN en septiembre de 2023 (NEWG, 2023) el trabajo se focalizó en dos aspectos: (1) explorar formas significativas de **categorizar los datos del cerebro humano** según los riesgos potenciales del intercambio de datos, y (2) considerar las diferencias resultantes en la **forma en que los investigadores deben tratar y usar esos datos**.

El segundo problema ético es el denominado de “**agencia humana**” o “**libre albedrío**” que se refiere a la **libertad y autonomía de una persona**. Dado que la neurotecnología en combinación con diversos fármacos puede emplearse para “*estimular el cerebro de una persona*”, es posible **influir en su comportamiento, pensamientos, emociones o recuerdos**, tanto para incrementar como para inhibir algunas capacidades cerebrales, y generar con ello efectos perniciosos o sesgados³¹⁸.

Además, dada la madurez relativa de la neurotecnología persisten **dificultades para predecir y evitar efectos indeseados**, así como la dificultad de establecer sólidas relaciones causa-efecto para poder emplearlas de forma segura, con efectos persistentes tras reducir o eliminar la intervención. En todo caso, es muy previsible que la combinación de la neurotecnología con los avances en IA durante la presente década permitirá **acelerar el desarrollo de dispositivos de neuroestimulación inteligentes** que exacerbarán estos retos éticos y hará aún más urgente encontrar un consenso entre todos los actores relevantes.

Aunque existen numerosas referencias en los tratados internacionales sobre la libertad de pensamiento y creencias, no es evidente que las provisiones legislativas actuales sean suficientes y puedan aplicarse adecuadamente al uso de la neurotecnología; sencillamente, **fueron ideadas sin tener en cuenta el desarrollo de la neurotecnología** y hasta donde podría llegar. Como es habitual, los avances de la tecnología llevan al marco regulatorio a sus límites y provocan una adaptación o reinterpretación continua con el riesgo de la dificultad de generalizarse la interpretación para todos los casos y países.

317 Además de su aplicación médica, los datos neuronales son cada vez más solicitados en el mercado de consumo para fenotipado digital, información emocional, neurojuegos, y neuromarketing.

318 Puede no requerirse una técnica de estimulación directa. Este es el caso resultante de la exposición a algunos juegos digitales aditivos o de sofisticadas técnicas de neuromarketing. Por lo tanto, los problemas derivados en determinadas personas, como los niños, han motivado la creación de regulaciones específicas para proteger a los niños de los efectos de esos juegos, aunque no exista una interacción directa con el cerebro humano.

La relación de la neurotecnología con la IA es creciente puesto que tanto para el análisis de grandes volúmenes de datos neuronales, ahora disponibles y almacenados, como en su procesamiento posterior se emplean herramientas de IA. También el uso de **gemelos digitales de partes pequeñas del cerebro** (no se dispone aún de tecnología suficiente como para generar un modelo digital preciso de todo el cerebro) está desarrollándose rápidamente con el objetivo de **conocer de forma anticipada el efecto sobre el cerebro de drogas** o de **técnicas de estimulación profunda** y acelerar con ello el desarrollo de fármacos o terapias para enfermedades neurodegenerativas.

La discusión sobre la regulación en neurotecnología, igual que ocurre con otros ámbitos tecnológicos de rápido desarrollo como es el caso de la inteligencia artificial, ha estado ligado a la búsqueda del **equilibrio entre la seguridad y la innovación**. Nos encontramos en un típico contexto del denominado *dilema de Collingridge*³¹⁹ en la que una legislación preventiva inhibirá la evolución de la tecnología, y otra laxa creará situaciones de difícil retorno. La solución habitual basada en un **uso responsable del principio de precaución** no es sencilla de aplicar cuando el conocimiento sobre la tecnología y sus impactos no son bien conocidos y coexisten en la sociedad visiones tecno-optimistas y tecno-pesimistas que dificultan la obtención de un acuerdo regulatorio global.

Las Naciones Unidas han expresado la necesidad de **actualizar el marco de la “Declaración Universal de Derechos Humanos” para incluir la neurotecnología** como un tema clave: *“En 2023, conmemoraremos el setenta y cinco Aniversario de la Declaración Universal de Derechos Humanos y los treinta años desde la aprobación de la Declaración de Viena y el Programa de Acción sobre los derechos humanos. Según se acerca este hito, ha llegado el momento de valorar lo conseguido, rejuvenecer o compartir valores y actualizar nuestro pensamiento sobre los derechos humanos. Deberá considerarse, por ejemplo, actualizar o clarificar nuestra aplicación de los marcos y estándares para abordar temas en la frontera del conocimiento e impedir daños para las personas en los espacios digitales y tecnológicos, incluyendo los que afectan a la libertad de expresión, discursos de odio, privacidad, el derecho a olvidar y la neurotecnología”*.

Tras dos años de trabajo del *Comité Internacional de Bioética* (CIB), la UNESCO publicó en diciembre de 2021 el **“Informe sobre las cuestiones éticas de la neurotecnología”** (UNESCO, 2021). En el informe se indica que *“las crecientes posibilidades neurotecnológicas de modificar el cerebro y, en consecuencia, la mente, de forma invasiva y omnipresente, plantean cuestiones relativas a la integridad mental. El imperativo de salvaguardar la dignidad humana exige la protección de la integridad del cuerpo, que puede ser vulnerada mediante la alteración, modificación y/o manipulación neurotecnológica”* (UNESCO, 2023).

319 Fue propuesto por David Collingridge en 1980, profesor de la Universidad de Aston (Reino Unido), en un libro llamado *The Social Control of Technology*. En sus propias palabras: “Cuando el cambio es fácil, su necesidad no puede ser anticipada; cuando la necesidad de cambio es aparente, el cambio ya se ha vuelto caro, difícil y laborioso”.

Asimismo, en el informe citado de la UNESCO se indica que **la neurotecnología también podría alterar la identidad personal**. Por ejemplo, mediante técnicas de modificación de la memoria, si madurasen suficientemente en el futuro, los individuos podrían optar por alterar el contenido de un recuerdo y, por tanto, cambiar su identidad personal. La estimulación cerebral profunda, que permite a las personas recuperar la autonomía de movimientos, también puede suponer una amenaza para su auténtico yo, ya que la mente puede desorientarse por la presencia activa de un dispositivo técnico³²⁰.

Independiente, pero relacionado con el anterior, se encuentra la **“Recomendación de la UNESCO sobre la ética de la IA”** que incluye una disposición que establece que *“Las cuestiones éticas relacionadas con los sistemas impulsados por IA para neurotecnologías e interfaces cerebro-computadora deben considerarse para preservar la dignidad y la autonomía humanas.”*

Las modificaciones cognitivas derivadas del uso de técnicas de neuroestimulación profunda han derivado en un amplio debate sobre los **“neuroderechos”** que, algunos países, como Chile (Ruiz *et al.*, 2024) han pretendido incorporar a su legislación³²¹. Los neuroderechos se han definido (Yuste *et al.*, 2021) como *“un nuevo marco jurídico internacional y de derechos humanos [...] que pueda entenderse como un nuevo conjunto de derechos humanos para el cerebro”*.

El término **“neuroderechos”** incluye (lista no exhaustiva) los derechos a la identidad personal, el libre albedrío, la privacidad mental, la igualdad de acceso a las tecnologías de mejora cognitiva, y la protección contra el sesgo algorítmico. El concepto ha sido desarrollado por la plataforma *Neuro Rights Initiative*, liderada por la Universidad de Columbia en Nueva York e impulsada por una comunidad internacional de neurocientíficos³²². No obstante, muchos de estos problemas, acelerados por la convergencia entre la inteligencia artificial y el mejor conocimiento del cerebro humano, requieren un acuerdo detallado a nivel global que es inexistente en la actualidad.

Desde un enfoque de **neuroética aplicada a la actividad científica** la iniciativa **BRAIN** en Estados Unidos ha decidido prestar un interés específico a los aspectos éticos que deberían guiar a los investigadores y a las agencias financiadoras de sus proyectos: *“Aunque la investigación del cerebro implica cuestiones éticas que son comunes a otras áreas de la ciencia biomédica, también implica consideraciones éticas especiales. Debido a que el cerebro da lugar a la conciencia, a nuestros pensamientos más íntimos y a nuestras necesidades humanas más básicas, los estudios mecanicistas del cerebro ya han dado lugar a nuevas cuestiones sociales y éticas”*. En este contexto, la iniciativa BRAIN ha propuesto un **conjunto**

320 La aplicación de neurotecnologías como los neurodispositivos y las interfaces cerebro-ordenador a niños y adolescentes, que se encuentran aún en pleno desarrollo, puede dificultar la distinción entre los rasgos de carácter y comportamiento atribuibles al neurodispositivo y la maduración “normal” del cerebro.

321 También son destacables: la Carta de Derechos Digitales de España, la Carta para el desarrollo responsable de las neurotecnologías de Francia y el informe sobre la regulación de la neurotecnología del Regulatory Horizons Council del Reino Unido.

322 <https://neurorightsfoundation.org/>

de directrices en el que enmarca las condiciones éticas para llevar a cabo una actividad investigadora en neurotecnología³²³.

En otro ámbito de trabajo sobre la ética de la neurotecnología se ha prestado atención al **problema de la consciencia** y su relación con diversos aspectos científico-técnicos relacionados. Tres aspectos de avances disruptivos aún inmaduros han merecido la atención por las consecuencias ético-legales que pueden tener si se siguen desarrollando y llegan a resultados operativos³²⁴. Algunas preguntas relacionadas son las siguientes:

- **Muerte encefálica:** ¿Es la muerte encefálica equivalente a la muerte de una persona? ¿Debería utilizarse la muerte encefálica o la muerte cardíaca como criterio legal para considerar a una persona fallecida? ¿Es éticamente permisible preservar el cerebro aislado de una persona muerta con la esperanza de revivir la consciencia de la persona en el futuro?
- **Organoides cerebrales** (pequeños agregados de neuronas creados en laboratorio que imitan la estructura y función del cerebro): ¿Pueden los organoides cerebrales albergar consciencia? Y, si es así, ¿Debería ser permisible el uso de organoides cerebrales con fines de investigación?
- **Consciencia en otros seres vivos:** ¿Qué posición moral debe concederse a otros seres, especialmente a los animales superiores, teniendo en cuenta la naturaleza de su consciencia? ¿Cómo afectaría este estatus a la investigación con animales y a los derechos de los animales?

Diversos estudios han expresado reservas sobre los riesgos del aumento del uso militar de la IA derivadas del peligro de **perturbar el control de las “emociones” en el campo de batalla** (Wilson, 2025); **el desarrollo de técnicas de IA combinadas con las de neurotecnología** pueden agravar respuestas ante una provocación, asesinatos por venganza, o favorecer el incumplimiento de órdenes legítimas. Sin embargo, otros investigadores opinan que sistemas de IA pueden ser una mejor alternativa porque las emociones humanas “negativas” son reemplazadas por un “campo de batalla más humano”.

No existe actualmente un consenso en el mundo científico sobre la mejor forma de abordar estos problemas ni, por supuesto, un marco legal específico aplicable. La fase en la que nos encontramos es la de la percepción del problema y la determinación de las condiciones en las que la investigación puede proseguir. En lo que sí hay consenso es en **exigir la voluntariedad en la participación en experimentos**. Concretamente, la neurotecnología y la neurofarmacología no deben utilizarse sin el **consentimiento informado**, así como una supervisión sobre el uso de innovaciones que puedan dañar a las personas y reducir su

323 El programa de neuroética de la Iniciativa BRAIN de los NIH identifica cuestiones éticas relevantes, organiza talleres y gestiona el Neuroethics Working Group (NEWG) presentado anteriormente. <https://braininitiative.nih.gov/about/neuroethics-working-group>

324 <https://www.britannica.com/topic/neuroethics>

función cognitiva, temporal o permanentemente e, incluso, abordar el **daño psicológico** que pueda producirse como resultado del uso de la neurotecnología como un arma. Todavía es pronto para saber las consecuencias que puede tener en el ámbito de la sanidad militar, aunque sí se han empezado a analizar posible usos para el tratamiento de traumas generados del combate.

6.6 Riesgos éticos en el ámbito militar derivados del uso de la IA en la guerra cognitiva

RAND (Black et al., 2024) considera que la **“gobernanza de la IA en el ámbito de la defensa” es un problema perverso (“wicked problem”)** para el que solo existen soluciones parciales a algunos de los problemas planteados.

La **gobernanza de la IA en la guerra cognitiva** es un problema perverso de este estilo. La creciente relevancia de las noticias falsas en sociedades digitalizadas, y la sensación de que no es fácil conocer si una información es verdadera o no, se ha convertido en un problema de índole social para la población que ha empezado a **exigir actuaciones por parte de los gobiernos para frenar su extensión**. Estos, a su vez, han comenzado a responder con las herramientas habituales a su alcance: incremento de las prohibiciones en los procesos de difusión con mecanismos de censura previa, endurecimiento de las penas en el ámbito judicial, y algunas actuaciones de intervención de medios de comunicación.

El informe de la IE elaborado por Pujol y Xuan (2024) propone tres conjuntos de recomendaciones *“con el fin de proteger el orden liberal internacional de los riesgos de la guerra cognitiva y sus tecnologías emergentes”*:

- *Intensificar los esfuerzos para comprender y crear conciencia sobre los mecanismos y las implicaciones de la guerra cognitiva en los sectores académico, industrial y de defensa para preparar eficazmente a los ciudadanos y a los responsables políticos.*
- *Desarrollar un marco de gobernanza integral para la guerra cognitiva y sus tecnologías emergentes, determinando cómo o en qué casos se aplica el derecho internacional existente, y estableciendo mecanismos claros para la atribución y la rendición de cuentas.*
- *Amplificar la colaboración entre las diversas partes interesadas para capitalizar el potencial de las tecnologías emergentes para abordar las vulnerabilidades de las democracias liberales y protegerlas de los riesgos de la guerra cognitiva”.*

La **pregunta abierta a la sociedad** (sobre todo, a la occidental a la que pertenecemos) es conocer hasta qué punto está dispuesta a **renunciar a derechos democráticos en la defensa contra una guerra cognitiva potenciada por la IA** que es cada vez más visible, y cómo encon-

trar el equilibrio en una situación marcada por el desarrollo de la IA a un ritmo muy rápido que hace obsoleto los marcos regulatorios existentes. **Encontrar ese equilibrio no es sencillo.**

En un contexto más amplio que el de la guerra cognitiva, aunque forma parte de ello, eventos mencionados previamente como las cumbres de la **IA Responsable en el Ámbito Militar** (REAIM), por ejemplo, son ilustrativos del interés de establecer límites éticos al uso de la IA. En todo caso, son aún pasos iniciales.

Hay autores que, desde la perspectiva legal (Wanyana, 2025), preconizan la urgente necesidad de claridad sobre qué tipo de acciones en el ámbito cognitivo constituyen un **uso prohibido de la fuerza** en virtud del Artículo 2(4) de la Carta de las Naciones Unidas, tradicionalmente, interpretado como ataques militares que involucran fuerza física, pero claramente ambiguo en este contexto de guerra cognitiva; y, en el caso de que se proceda a ello, **determinar el umbral** que deben cumplir dichas acciones para que se puedan considerar como fuerza prohibida. Debe tenerse en cuenta que el uso de determinadas armas puede crear **secuelas no letales** y no a corto plazo, pero que invalidan al soldado para su función durante periodos prolongados.

Otro artículo clave de la **Carta de las Naciones Unidas** en este contexto es el Artículo 51 calificando a un *“ataque armado como uso de la fuerza que implique destrucción sustancial de la propiedad, pérdida de vidas o lesiones”*. Desde esta perspectiva las operaciones cognitivas que causan daño físico a las personas y a la propiedad se considerarían como *fuerza prohibida*.

Si la interpretación de guerra cognitiva, y su consiguiente clasificación, fuese la de simples operaciones encubiertas o conflictos por debajo del umbral de un conflicto armado debido a su naturaleza no cinética con efectos psicológicos y no físicos, se estaría olvidando el cambio profundo que se está produciendo acelerado por el uso de la tecnología. **Su capacidad de movilización de la población y acelerador de “conflictos cinéticos” le confiere una relevancia mayor.** Como indica Wanyana (2025) *“El umbral combinado de gravedad e intención también es crítico para determinar cuándo se puede emplear una respuesta militar en defensa propia contra un ataque cognitivo ofensivo.”*

El **desarrollo del marco ético para la guerra cognitiva está en sus inicios.** Su desarrollo requiere que todos los actores implicados, incluyendo los ciudadanos, participen en un **diálogo continuo** para abordar los desafíos y oportunidades emergentes que presenta la guerra cognitiva potenciada por la IA, y acordar un marco de actuación flexible y adaptado a la evolución de la tecnología.

6.7 Conclusiones y previsible evolución

En un documento sobre los “Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R) del *Centro Conjunto de Desarrollo de Conceptos* del CESEDEN (Gómez de

Ágreda, 2020) se decía: *“No es una guerra nueva, ni es más o menos violenta por el hecho de que las máquinas la ejecuten o ayuden a hacerlo. La guerra es un fenómeno humano y son los hombres los que la llevan a cabo. Tampoco es un mero cambio de herramientas, de armas con las que pelear. La guerra es un acto político y social que muta con la política y la sociedad que la llevan a término. La tecnología permite adaptar los instrumentos a las necesidades de la guerra, pero también condiciona el entorno social que da lugar a la misma. Entender la guerra implica entender a la sociedad que la hace. La inteligencia artificial cambia ambas y lo hace a un ritmo exponencial”*.

El debate sobre la **posibilidad de desarrollar regulaciones específicas sobre el uso de la IA en el dominio militar** ha sido especialmente complejo como demuestra el caso de la regulación de la IA por la Unión Europea. El recurso al empleo de **“directrices voluntarias”** ampliamente aceptadas por los países es una vía alternativa con esfuerzos como **REAIM**. Sin embargo, nada asegura que en el caso de un conflicto militar real se vayan a cumplir. La necesidad de asegurar la superioridad en el caso de que el adversario las emplee cuando está en riesgo la propia supervivencia hace difícil su aplicación.

La opción de aplicar al caso de los SALA el mismo tipo de control preventivo que se hace con las armas nucleares, o las de destrucción masiva como químicas o biológicas no parece sencillo. La trazabilidad de sistemas software de IA y el análisis de su funcionalidad es mucho más complejo que en el caso de material radioactivo. Además, están sometidos a frecuentes cambios y modificaciones basadas en la experiencia de su uso o como resultado del reentrenamiento de los algoritmos de IA con nuevos datos. **Estos cambios pueden ser realizados tanto por los fabricantes iniciales como, en algunos casos, por los usuarios**. Este hecho invalida un proceso de *“validación previa del sistema de IA”* por el fabricante.

Mientras que el desarrollo de la tecnología de IA y su aplicación en defensa se acelera, la discusión sigue abierta por las Naciones Unidas. En la Resolución de diciembre de 2024 (UN, 2024) se acuerda incluir en el programa provisional de su octogésimo período de sesiones, en relación con el tema titulado *“Desarme general y completo”*, un subtema titulado *“La inteligencia artificial en el ámbito militar y sus consecuencias para la paz y la seguridad internacionales”*.

La visión de las Naciones Unidas es **ampliar el ámbito de discusión más allá de las armas letales**³²⁵. Concretamente, ha solicitado contribuciones (UN, 2024) *“sobre las oportunidades y los desafíos que plantea para la paz y la seguridad internacionales la aplicación de la inteligencia artificial en el ámbito militar, con especial atención a esferas distintas de los sistemas de armas autónomas letales”*. Entre ellas, podrían considerarse las de mando y control, gestión de la información, logística o entrenamiento (Paoli y Afina, 2025).

³²⁵ Hasta enero de 2023, los debates multilaterales sobre la IA en el ámbito militar se limitaban al mandato del Grupo de Expertos Gubernamentales de las Altas Partes Contratantes de la Convención sobre Ciertas Armas Convencionales en relación con las tecnologías emergentes en el ámbito de los SALA.

Desde el punto de vista tecnológico, si se llegase a un estado de madurez de las tecnologías ligadas a la robótica inteligente es posible pensar en **enfrentamientos entre robots**³²⁶. En estos casos, vale preguntarse ¿cuál sería el marco ético de este enfrentamiento? ¿Cómo cubriría las ROE estos casos?

La **evolución convergente de la IA con la robótica y la neurotecnología** puede hacer factible, a partir de la próxima década, que el ser humano disponga de tecnologías con las que podrá incrementar significativamente sus capacidades sensoriales, motoras, cognitivas y sociales. Será con ello la única especie que no solo ha podido transformar el planeta Tierra, y con ello lo ha puesto en peligro, sino que dispondrá de tecnologías suficientes como para **decidir si quiere transformarse conscientemente a sí mismo y preservarse colectivamente como especie**.

En ese contexto, se suscita algunas preguntas abiertas de relevancia ética: ¿tenemos derecho a modificar la especie humana o solo a restituir capacidades? ¿quién tiene/tendrá derecho a ser “mejorado”? ¿debemos permitir que estas mejoras sean transmisibles a las siguientes generaciones?, ¿combatiremos con soldados mejorados?, ¿debemos prepararnos para el caso en que otros adversarios sí lo hagan? Ante ello, la humanidad, a través de sus gobiernos convenientemente informados por la ciencia y la tecnología, **debe decidir si quiere hacerlo, y, en su caso, cómo, abordando los riesgos inherentes a ello**.

326 No estamos tan lejos de ello, aunque sea en situaciones individuales. El caso de que un vehículo autónomo terrestre o marítimo se enfrente a un dron aéreo autónomo en Ucrania es un escenario que puede producirse este mismo año.

Capítulo 7

CAPÍTULO 7.

VALORACIÓN DE LA SOBERANÍA TECNOLÓGICA DE LA UE EN IA DESDE LA PERSPECTIVA DE LA DEFENSA

7.1 Contexto

En los capítulos precedentes del informe se ha presentado un **panorama de la situación de la IA en defensa desde cuatro dimensiones complementarias**: 1) el desarrollo científico-tecnológico de la IA, 2) la situación del mercado de IA y el impacto socioeconómico de la industria de la defensa, 3) el uso actual y previsible de la IA en las operaciones militares con énfasis en la evolución hacia un campo de batalla inteligente, el uso de la IA en la guerra híbrida y en el sector espacial de la defensa y, finalmente, 4) los aspectos éticos y regulatorios que conciernen al uso militar de la IA.

No se ha pretendido con ello analizar expresamente la **situación actual de la autonomía estratégica de la UE**, ni su posición relativa con respecto a otras potencias tecnológicas. Sin embargo, sí se han desgranado a lo largo del informe algunos ejemplos de la aplicación de la IA en el contexto europeo de la defensa, con datos sobre el peso de su industria de defensa en el desarrollo de productos y servicios específicos basados en el uso de la IA. También se ha abordado el **marco regulatorio europeo aplicable a la IA** comparándolo con los que se encuentran en otros países o se promueven desde diferentes organismos.

Sin embargo, la UE es consciente de que debe **incrementar su autonomía estratégica** para ser capaz, en la medida de lo posible, de tomar decisiones propias sin depender de otros países basándose en el papel habilitador resultante de la mejora de su soberanía tecnológica. Por este motivo, conocer el **nivel de soberanía tecnológica de la UE en IA actual y el que sería alcanzable desde una postura realista** se ha convertido en un elemento básico de la definición de la política europea.

El objetivo concreto del capítulo 7 es analizar el **nivel de soberanía tecnológica en IA de la UE desde la perspectiva de la defensa europea en 2025 y su evolución en el horizonte de 2030**, aun aceptando que perseguir un modelo autárquico no es posible ni deseable. Se pretende, asimismo, desde una postura realista, analizar cómo la UE puede **mejorar su posición relativa** frente a otras potencias tecnológicas con las que colabora o compite durante la presente década para poder jugar un papel relevante en el contexto mundial, así como las posibilidades reales de **reducir las dependencias críticas** con respecto a otros Proveedores de la cadena de valor de IA fuera de la Unión.

El análisis se realiza en 2025, un año en el que la UE, tras los debates surgidos en 2024 con informes como los generados por *Enrico Letta*, *Mario Draghi*, *Sauli Niinistö* y *Manuel Heitor*,

ha comenzado el debate político y presupuestario con el Consejo y el Parlamento Europeos sobre El nuevo marco **financiero plurianual para el periodo 2028-2034**. El documento publicado por la Comisión Europea el 16 de julio de 2025 supone el arranque de un **proceso de negociación** de más de dos años que debe culminar antes de diciembre de 2027.

El marco financiero se complementa de otros dos documentos no oficiales todavía (en estado borrador) que son esenciales para el objeto del presente informe: los borradores de regulaciones para el nuevo programa marco de investigación e innovación denominado **Horizonte Europa 2028-2034**, y el del nuevo **Fondo Europeo de Competitividad** para al mismo periodo. En conjunto, y en el marco presupuestario de las perspectivas financieras que se aprueben, permitirá debatir y acordar definir el grado en el que la UE podrá conseguir la soberanía tecnológica deseada en IA y los recursos necesarios para ello.

7.2 Posicionamiento geopolítico de la UE

7.2.1. La UE en el contexto de la rivalidad tecnológica global

La **pugna sistémica** que marca la relación entre *Estados Unidos* y *China* se ha convertido en la cuestión fundamental que modula la geopolítica actual de la tecnología, pero, sobre todo, condicionará progresivamente la evolución del resto de la presente década y, probablemente, de la próxima con impactos relevantes en todos los países desarrollados. Dentro de esta dinámica de confrontación multidimensional, la **rivalidad en términos de innovación tecnológica** se ha convertido en un aspecto crucial del que la UE no puede sustraerse ni permanecer al margen porque su seguridad colectiva y su papel global futuro depende de ello.

La **dualidad de la tecnología** y la intensificación de la pugna entre las dos potencias citadas implica que el incremento de la **seguridad colectiva**, entendida en sentido amplio, desde la energética a la agroalimentaria, el control de los datos, hasta la de defensa y seguridad, se ha convertido en un elemento clave, mientras que el aspecto económico, considerado aisladamente, pasa a un segundo plano (Choi, 2022) o se subordina al concepto de “*seguridad económica*”.

Este concepto de seguridad ha pasado de una perspectiva ligada a las personas a una visión mucho más amplia y colectiva en la UE formulada en 2023 por el Comité Internacional de la Cruz Roja⁴¹⁹ como “*un marco común destinado a lograr la seguridad económica mediante la promoción de la base económica y la competitividad de la UE, mediante la protección*

419 El Comité Internacional de la Cruz Roja (CICR) definió en 2015 la seguridad económica como la condición de aquellas personas, hogares o comunidades que son capaces de satisfacer sus necesidades esenciales y de solventar los gastos ineludibles de forma sostenible, conforme a los requerimientos fisiológicos, el medio ambiente y las pautas culturales propias de cada lugar (<https://www.icrc.org/es/document/que-es-la-seguridad-economica>). Sin embargo, en el contexto de la política de la UE tiene un significado más amplio.

frente a los riesgos, y mediante la creación de asociaciones con el mayor número posible de países, a fin de abordar preocupaciones e intereses comunes”⁴²⁰.

Si bien la **existencia de un cambio geopolítico es aceptada en toda la UE, la percepción del riesgo y la seguridad por parte de gobiernos y población no es uniforme en todos los Estados miembros**. Este hecho condiciona las decisiones que puede adoptarse en todos los planos, condicionando la evolución de los presupuestos generales y los de defensa, en particular, en los contextos nacionales y comunitarios. En muchos casos, estos riesgos a nivel nacional están asociados a la evolución histórica del país, su posicionamiento geográfico, y el papel que juega o desea jugar en la escena mundial.

En un reciente trabajo de Wolf *et al.* (2025) se analiza la **relación entre los presupuestos dedicados a defensa por los Estados miembros de la UE en relación con la distancia geográfica de su capital a Moscú**. La figura 7.1. refleja esta situación en la que los Estados miembros difieren claramente en sus prioridades y presupuestos de defensa en función de las visiones nacionales y preocupaciones geográficas de cada uno en un contexto en el que la guerra de Ucrania y el cambio de posición de Estados Unidos está tensando el tablero geopolítico europeo.

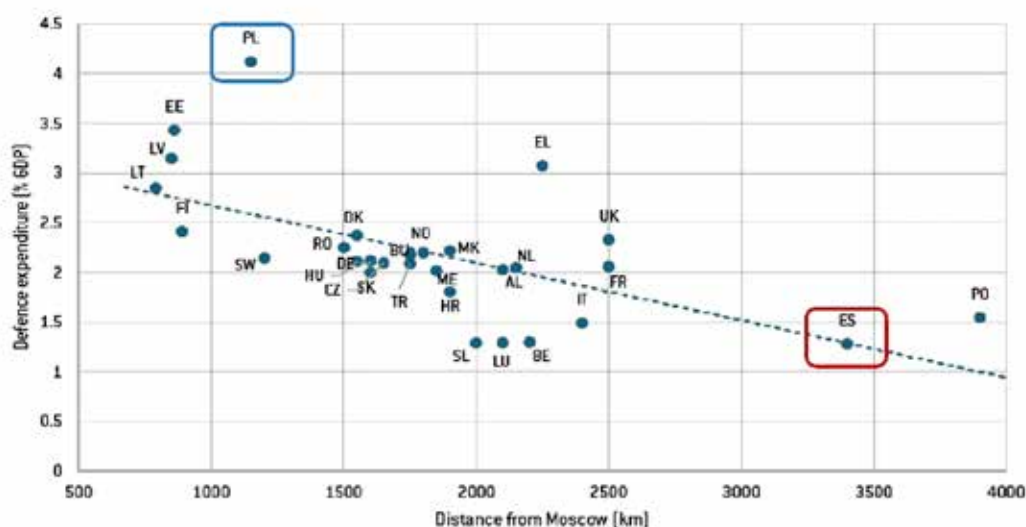


Figura 7.1. Relación entre gastos de defensa en relación con el PIB y distancia a Moscú. Fuente: Wolf et al. (2025)

Obsérvese la diferente percepción existente en **Polonia** o **España** en la relación entre el gasto en defensa con respecto al PIB y la distancia respectiva a Moscú. En el caso de España refleja una posición muy alejada todavía en 2024 del objetivo político en la OTAN de

420 https://ec.europa.eu/commission/presscorner/detail/es/ip_23_3358

alcanzar un mínimo de gasto en defensa del 2% del PIB y mucho más lejos si se considera el acordado de un 5% en 2035 en la última Cumbre de la OTAN.

El criterio del **gasto en defensa** y su evolución es relevante, pero no es el único factor para determinar el papel que un país determinado puede jugar en las relaciones internacionales. Es muy relevante también determinar la **capacidad tecnológica** de sus fuerzas armadas, el tipo de armamento desplegado⁴²¹, y su complementariedad o superioridad con respecto al de los de otros países, aliados o no, en función de sus intereses y riesgos. **No es lo mismo disponer de recursos para adquirir equipos militares que para disponer de capacidades industriales para su desarrollo.**

El **cambio radical en el panorama tecnológico** acelerado en la última década, en gran parte motivado por la relevancia adquirida por las tecnologías duales, ha desestabilizado las relaciones internacionales en general, pero, sobre todo, ha afectado a la **estructura de las cadenas de suministro mundial**. Se asume, por tanto, la **imposibilidad de basar las decisiones nacionales en una autarquía tecnológica** que ni siquiera Estados Unidos posee; por este motivo, asegurar la provisión de componentes y sistemas tecnológicos desde otros países “aliados” cuando no se puede disponer de ellos a nivel nacional se ha convertido en un factor fundamental de la **seguridad económica colectiva**.

Las cadenas de valor global han evolucionado durante las tres últimas décadas desde una **fase optimista de expansión de la globalización** regida por la eficiencia económica y la aplicación de reglas comerciales aceptadas por todos los países, a otras más realistas en las que era necesario **asegurar la resiliencia de las cadenas globales frente a potenciales disrupciones** por encima de todo, aunque ello implicase aceptar una menor eficiencia económica en el flujo de datos y productos físicos.

La consecuencia derivada de esta evolución y la imposibilidad de adoptar un enfoque autárquico es la **necesidad de confiar en aliados con los que se puedan establecer relaciones de confianza a largo plazo** para la provisión de materias primas, componentes y productos críticos. En la práctica, esta evolución puede suponer cambios bruscos o paulatinos de los proveedores y, por tanto, la aparición de **inestabilidades de suministros derivadas de condicionantes geopolíticos**.

Como ejemplo de estos cambios, las decisiones tomadas por Estados Unidos y otros países con el establecimiento de **sanciones, aranceles o restricciones a la importación o exportación** aplicados a componentes o productos tecnológicos sobre otros países, entre ellos a la propia UE, van a acelerar estos cambios y forzar la **transformación de las cadenas de**

421 Considérese como ejemplo, la existencia o no de armamento nuclear en el arsenal de una determinada nación como base para su posicionamiento frente a otros.

provisión⁴²². En el momento en el que se redacta este capítulo del informe las discusiones entre Estados Unidos y la UE sobre los aranceles de importación aplicados a múltiples productos han alcanzado un acuerdo político, pero no es factible aún conocer cómo se estabilizarán. Situación similar de incertidumbre sucede con otros muchos países.

Es en este contexto geopolítico altamente cambiante en el que debe analizarse el papel que juega la IA como factor relevante del **proceso de digitalización**, y la forma en la que la UE puede **mejorar su soberanía tecnológica**.

El **proceso de digitalización progresivo** descrito en el capítulo 2 no sólo afecta a los sectores socioeconómicos civiles, sino que **se extiende también al ámbito de la defensa**. Frente a este panorama, la **debilidad competitiva de la UE frente a otras grandes potencias en el control de las tecnologías digitales, y, en especial, de la IA**, configura el punto de partida del análisis realizado en este capítulo.

7.2.2. Evolución de los esfuerzos europeos hacia una mayor soberanía tecnológica

Durante 2024 se han presentado un conjunto de informes complementarios encargados por la Comisión Europea y respondidos desde diversas instituciones de la UE para debatir **la forma de posicionar mejor a la Unión en el mundo desde la perspectiva de la innovación, la competitividad y la defensa**, aspectos estrechamente interrelacionados. Los múltiples debates suscitados desde entidades públicas y privadas muestran la relevancia del problema, y las dificultades en obtener un consenso global.

Los informes preparados a petición de la Comisión Europea por **Enrico Letta** (2024) focalizado en la necesidad de profundizar en el mercado único europeo, el de **Mario Draghi** (2024) centrado en la competitividad europea, y el de **Sauli Niinistö** (2024) enfocado en la necesidad de tener una UE preparada para abordar mayores riesgos, son especialmente relevantes para entender la situación y los desafíos a los que se enfrenta la UE. A ellos puede sumarse el de **Manuel Heitor** (2024) orientado hacia la necesidad de profundizar en las políticas de investigación e innovación como base para la discusión sobre la estructura y prioridades del siguiente programa marco europeo en el contexto del propuesto “**Fondo Europeo de Competitividad**” de la UE, y las actuaciones específicas sobre IA en su consideración de tecnología dual que debe adoptar la UE ⁴²³.

422 Como ejemplo de ello, puede mencionarse la decisión tomada por Apple en abril de 2025, presionado por los factores geopolíticos indicados, de desplazar la producción de sus productos fabricados en China a India o a Vietnam (parcialmente desde 2022) o aumentar su producción en estos países, lo que, a su vez, obliga a moverse a algunos de sus proveedores críticos. Todo ello sucede al mismo tiempo que anuncia el incremento de sus inversiones en Estados Unidos. No está claro si el Gobierno de Estados Unidos aceptará esos cambios de país de origen de la producción. <https://es.euronews.com/business/2025/04/25/apple-planea-trasladar-a-la-india-el-ensamblaje-del-iphone-en-un-golpe-a-china>

423 La Comisión Europea ha presentado el Plan de Acción «Continente de IA» para convertir los puntos fuertes de la UE, como el talento y las industrias tradicionales, en aceleradores de la IA. El ambicioso objetivo es que la UE pueda ser un líder mundial en IA y promover el desarrollo y el despliegue de soluciones de IA que beneficien a la sociedad y a la economía. https://commission.europa.eu/topics/eu-competitiveness/ai-continent_es

Concretamente, el denominado **“Informe Draghi”** (Draghi, 2024) describe los **retos a los que se enfrentan la industria y las empresas de la UE para ser competitivas**. En él se esboza cómo Europa ya no podrá depender de muchos de los factores que han respaldado su crecimiento en el pasado, se establece un diagnóstico claro y se ofrecen recomendaciones concretas para situar a Europa en una trayectoria diferente.

Incluso, en el caso de que la UE esté dispuesta a financiar de varias formas una **mayor inversión en defensa de forma urgente**, no será suficiente; como dice Draghi, *“Junto con la urgente necesidad de aumentar la inversión global en defensa, existen razones de peso para reforzar la cooperación y la puesta en común de recursos para la investigación y el desarrollo en materia de defensa a nivel de la UE”*. Claro mensaje para el siguiente marco financiero plurianual.

El **contexto estratégico de la UE** en la que se han indicado algunos de los elementos clave derivados del informe presentado por Draghi (2024) se describe en la figura 7.2. La conjunción de todos ellos conduce a la necesidad de abordar unos desafíos de seguridad que requieren una **respuesta estratégica urgente para que la UE pueda decidir su propio futuro**.



Figura 7.2. Contexto geoestratégico de la UE. Fuente: Elaboración propia a partir del informe de Draghi (2024)

Además de la relevancia para la UE de otras **grandes potencias** como son *Estados Unidos* o *China*, también *Rusia* ocupa un lugar destacado por su implicación en el deterioro de la seguridad europea tras su invasión de Ucrania en 2022. Igualmente, aparecen **otras áreas geográficas de conflicto** de relevancia para Europa como son el Ártico con intereses geopolíticos de muchos países acelerados por su progresivo deshielo, el Norte de África (con riesgos sistémicos en Libia y en los países del Sahel), Oriente Medio y Africa Oriental

(con conflictos militares abiertos en Israel, Gaza, Siria, Líbano, Yemen o Sudán), y sin un ámbito geográfico definido, la creciente amenaza de guerra híbrida en toda la Unión como ya se ha expuesto en el capítulo 5 de este informe.

La figura 7.3 elaborada a partir del informe de *Mario Draghi* indica cómo **el fortalecimiento de la defensa y seguridad europea debe implicar decisiones y puesta en marcha de actuaciones de forma coordinada en muchas políticas públicas diferentes**. Entre ellas, se pueden mencionar las políticas de investigación e innovación, las financieras, las industriales y comerciales, o las de relaciones internacionales; todas ellas deberán estar acompañadas de los **cambios legislativos y procedimentales necesarios** (p.ej. hacia la simplificación y la reducción de la fragmentación) que deben asumirse en el marco comunitario y en los Estados miembros.



Figura 7.3. Áreas de fortalecimiento de la defensa y seguridad europea. Fuente: elaboración propia

En todas estas actuaciones, subyace la necesidad de **mejorar la soberanía tecnológica de la UE**. Aunque no se trata exclusivamente de una necesidad focalizada expresamente en la IA, ni únicamente en el sector de la defensa, su influencia y relevancia como **tecnología habilitadora de carácter dual** es evidente en la tercera fase del proceso de digitalización en la que nos encontramos. Este hecho se ejemplifica en el control político del desarrollo de chips específicos relacionados con el uso eficiente de la IA, así como en la captura y gestión de grandes volúmenes de datos o la expansión de la IA generativa a través de servicios en la nube.

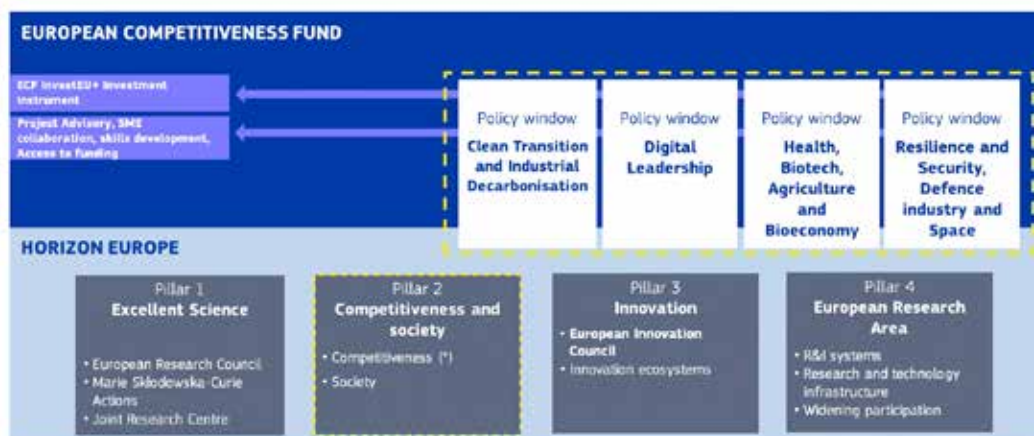
El 16 de julio de 2025 ha supuesto el **arranque del proceso de negociación en la UE del nuevo marco financiero plurianual para el periodo 2028-2034**⁴²⁴ y la difusión no oficial de los borradores de los reglamentos del **programa marco de investigación e innovación Horizonte Europa** y del **Fondo Europeo de Competitividad** para el mismo periodo 2028-

424 https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1847

2034; ambos reglamentos, aun siendo independientes, han sido concebidos para facilitar y coordinar su ejecución con los Estados miembros incrementando la flexibilidad de gestión.

La propuesta presentada por la Comisión Europea del denominado **Marco Financiero Plurianual (MFP)** (Comisión Europea, 2025e, 2025f) supone casi 2 billones de euros, o el **1,26 % de la renta nacional bruta media de la UE entre 2028 y 2034** (ligero incremento frente al 1,13% actual dadas las reticencias de varios Estados miembros en incrementarlo sustancialmente⁴²⁵).

La Comisión Europea mantiene la postura de que estos presupuestos son los necesarios para apoyar la ambición de Europa de ser independiente, segura, y próspera durante la próxima década. Por este motivo, entre las partidas más relevantes para el presente informe deben destacarse los **175.000 millones de euros asignados al programa Horizonte Europa 2028-2034** (frente a los 100.000 millones del actual) y los **409.000 millones del nuevo Fondo Europeo de Competitividad** que invertirá en tecnologías estratégicas tal y como se recomendaba en los informes de *Enrico Letta* y *Mario Draghi* en 2024⁴²⁶. El **Fondo Europeo de Competitividad** se concentrará en cuatro áreas prioritarias: 1) Transición limpia y descarbonización; 2) transición digital; 3) salud, biotecnología, agricultura y bioeconomía; y 4) **defensa y espacio** con una asignación inicial de **131.000 millones** lo que supone multiplicar por cinco los recursos disponibles en el marco financiero plurianual actual (2021-2027). La figura 7.4 resume esquemáticamente la estructura propuesta por la Comisión Europea con la interacción prevista entre el HE 2028-2034 y el resto de los componentes del Fondo Europeo de Competitividad.



(*) Collaborative R&I consistent with activities in the Competitiveness Fund

Figura 7.4. Estructura del Fondo Europeo de Competitividad. Fuente: Comisión Europea (2025e)

425 Debe tenerse en cuenta que a partir de 2028 la UE deberá comenzar a pagar unos 25.000 millones de euros relativos a los compromisos derivadas de los intereses de los préstamos de Next Generation EU creado tras el COVID-19 por lo que el volumen disponible del presupuesto 2028-2034 será muy aproximado al actual. Aun así, algunos Estados miembros ya han manifestado su oposición a cualquier incremento presupuestario lo que augura un complejo proceso de negociación.

426 Por el contrario, la Política Agraria Común (PAC) ve reducido su futuro presupuesto en un 25%.

Es pronto para conocer cómo la IA se verá reflejada en los próximos programas, pero **dado su carácter dual tendrá un peso destacable en la prioridad de transición digital, y en la de defensa y espacio**. Seguro que, desde el punto de vista de aplicaciones de usuario, también tendrá relevancia en las otras dos prioridades (sobre todo en salud, y en la gestión inteligente de redes de energía).

La Comisión Europea propone que los Estados miembros y las regiones tengan la posibilidad de apoyar con carácter voluntario y en función de las necesidades y prioridades regionales **proyectos relacionados con la defensa en sus planes de asociación nacionales y regionales**. El presupuesto previsto para el capítulo de **movilidad militar**, parte del instrumento “*Conectar Europa*”⁴²⁷ se multiplicará por diez respecto a las cantidades disponibles actualmente. Apoyará las inversiones en **infraestructuras de doble uso** junto con las civiles y contribuirá a dar un gran impulso al desarrollo de la ciberseguridad, la infraestructura y la defensa en general.

En resumen, los próximos dos años serán muy intensos en un **proceso negociador entre los 27 Estados miembros en el Consejo y el Parlamento Europeo** en el que, a buen seguro, las presiones y posturas encontradas, como ocurre habitualmente, harán difícil llegar a un consenso antes de diciembre de 2027. Pero como siempre, se llegará. Lo que no es tan evidente es cómo la evolución de la situación geopolítica durante más de dos años afectará a los objetivos de que la UE recupere una posición clave.

7.3 Análisis de la soberanía tecnológica en IA de la UE

El análisis de la situación de soberanía tecnológica para una determinada tecnología depende de muchas variables. Puede hacerse empleando un **modelo en diferentes niveles** como el que se indica en la figura 7.5. La figura representa el **grado de autosuficiencia tecnológica** alcanzable (del 0 al 100%) en diversos ámbitos de intervención política en tres niveles diferenciados (León, 2023).

Obviamente, la situación es muy distinta en un momento dado entre diferentes países para cada tecnología. Por este motivo, el esquema de la figura 7.5 **no debe interpretarse como una visión estática de la situación de soberanía tecnológica**. No solo debido a que la tecnología evoluciona dinámicamente, sino porque también lo hace el posicionamiento relativo de cada país frente a ella condicionando sus regulaciones y el marco de alianzas internacionales.

El **primer nivel** se relaciona con el acceso a recursos naturales y las infraestructuras de procesamiento y transporte de materiales, productos y datos. El **segundo nivel** se relacio-

⁴²⁷ Está destinado a financiar redes de transporte y energía más ecológicas y más sostenibles, así como la transición digital con 33.700 millones de euros de 2021 a 2027. https://ec.europa.eu/commission/presscorner/detail/es/ip_21_1109

na con las capacidades de investigación e innovación y recursos humanos formados para ello, y también con las de fabricación de componentes y sistemas industriales. Finalmente, el **tercer nivel** está relacionado con la estructura del mercado, el marco regulatorio y los principios y valores compartidos.



Figura 7.5. Niveles de soberanía tecnológica. Fuente: León (2023).

La figura 7.5 **no se refiere a ninguna tecnología ni a ningún país específico**. Si se centrara en el caso de la UE, pueden indicarse algunas dificultades genéricas europeas en el **primer nivel** relativas al acceso a recursos naturales con dependencias que afectan a muchas tecnologías y sectores industriales. Como ejemplo, algunos datos de la situación de dependencia de la UE en 2023 son los siguientes:

- El 63% del **cobalto** procede del Congo, y el 60% se refina en China.
- El 97% del **magnesio** procede de China.
- El 71% de **platino** procede de Suráfrica.
- El 98% del **boro** procede de Turquía.
- El 94% de las importaciones de la UE de **tierras raras** procedían de China, Malasia y Rusia.
- El 100% de las **tierras raras para imanes** se refinan en China.

Además, existe una fuerte dependencia europea de China en importaciones de **magnesio**, **germanio** y **galio** que, actualmente, están sometidas a limitaciones de exportación por parte del gobierno de China con repercusiones en el ámbito de la IA (p.ej. en el desarrollo de chips de IA, en los centros de proceso de datos, o en múltiples sistemas militares) y a múltiples productos manufacturados. Sin embargo, en el ámbito de los **servicios digitales**

avanzados, la dependencia europea es, sobre todo, con Estados Unidos y en la falta de cables de datos submarinos cuya propiedad sea de empresas o entidades europeas.

Dados los objetivos de este capítulo, resulta apropiado aplicar el modelo precedente como **marco de reflexión** para valorar la situación actual de la soberanía en IA de la UE. Desde una **perspectiva cualitativa** elaborada por el Grupo de Trabajo, la figura 7.8 ejemplifica la situación de dependencia de la UE en relación con la IA⁴²⁸.



Figura 7.6. Valoración cualitativa de la soberanía tecnológica de la UE en IA.
Fuente: elaboración propia

Obsérvese que, en la situación descrita para la IA en la UE, su **grado de soberanía tecnológica cualitativa** indicado en la figura 7.6 **es mejorable** si se actúa con decisión y voluntad política sobre los elementos indicados en cada uno de los niveles. Brevemente:

- El **acceso a recursos naturales** está condicionado por la necesidad de disponer de semiconductores empleados en IA, y se dispone de fuentes de energía a costes competitivos para alimentar los centros de datos empleados en el entrenamiento de algoritmos de IA o para la extracción de inferencias.

Mejorar esta situación implicaría poner en marcha actuaciones para **reducir las dependencias europeas en algunas materias primas**; proceso que ya ha iniciado la UE identificando las más críticas y modificando las regulaciones para facilitar su extracción (p.ej. con el litio o las tierras raras) simplificando y acelerando los informes medioambientales. De todas formas, la relevancia de este factor en el caso concreto de la IA es menor que

428 La figura se refiere en términos generales y no expresamente en el uso militar de la IA.

en otras tecnologías más ligadas al desarrollo de sistemas hardware o baterías eléctricas por citar dos ejemplos.

Otra cosa distinta es la **resiliencia del suministro energético**, factor básico para la ubicación de los centros de proceso de datos y la atracción de inversiones fuera de la UE. Ambos factores condicionan el flujo de información necesaria para los sistemas de IA y su control en la propia UE.

- Las **infraestructuras de procesamiento y transporte** de las materias primas o de componentes necesarios para el desarrollo y uso de sistemas de IA obligan a la UE a asegurar el suministro desde países lejanos; en gran medida, de Estados Unidos y Asia (China, India, Corea del Sur, Vietnam, Taiwán, Malasia, Japón) a través de rutas de aprovisionamiento no aseguradas desde zonas conflictivas en muchos casos. Tanto los dispositivos semiconductores como muchos sistemas electrónicos empleados en sistemas de IA proceden de **proveedores especializados fuera de la UE**.

Mejorar la situación europea actual obliga a la diversificación de proveedores en países amigos o su acercamiento físico a la UE en condiciones que faciliten la provisión en situaciones de riesgo. Estas medidas se deben complementar con otras orientadas a la generación de acopios de **reservas estratégicas de algunos componentes esenciales** que aseguren la provisión y mantenimiento de los sistemas de IA como, de hecho, ya realiza China en relación con algunas GPUs de *Nvidia* motivados por las sanciones impuestas por Estados Unidos.

Asimismo, también es necesario que la UE asegure el **flujo de datos mediante cables submarinos o redes satelitales**. En relación con los cables de datos de alta capacidad, cuyo uso para el acceso a aplicaciones de IA ha incrementado su relevancia, la situación europea es de **debilidad** puesto que la mayor parte es propiedad de grandes empresas digitales no europeas y su seguridad (p.ej. en el Mar Báltico) se ha convertido en un problema político relevante como parte de la guerra híbrida en la que la UE se encuentra sumida.

- La **fabricación de componentes y sistemas de IA** está condicionada en la UE por la inexistencia de grandes fundiciones (*foundries*) para la fabricación de circuitos integrados para IA, aunque sí es buena en el desarrollo de máquinas de *fotolitografía extrema* (EUV) de muy alta resolución⁴²⁹ capaces de fabricar muchos tipos de chips, entre ellos los de IA, dado su carácter de proceso dual.

También es necesario mejorar la soberanía tecnológica europea en el caso de los **supercomputadores y los grandes centros de datos para IA**: no basta con disponer de ellos,

⁴²⁹ En realidad, se trata de un proceso dual, agnóstico frente al uso último (civil o militar) de los chips que se fabriquen con esa tecnología.

sino que deberían construirse en base a incrementar al máximo posible la tecnología europea. Asociado a ello se encuentra la necesidad de poner en marcha y controlar la operación de los denominados “*espacios compartidos de datos europeos*”.

La situación actual mejorará cuando las **foundries** previstas en Alemania de TSMC e Intel (en este caso, parece difícil confirmar la inversión) y las inversiones en otros países europeos como Francia se pongan en funcionamiento durante la segunda mitad de esta década. Muy probablemente, algunos de los chips fabricados estarán asociados a *aceleradores de IA* y a su integración en supercomputadores especializados que maximicen el uso de tecnologías europeas. En el caso de España, sí se ha confirmado la instalación en Málaga de un centro piloto de IMEC (centro de investigación piloto radicado en Bélgica).

- Las **actividades de investigación, innovación y formación** de recursos humanos en IA que ya realiza la UE son destacables y han crecido frente a las existentes al comienzo de la presente década.

Sin embargo, no se trata solo de mejorar los indicadores frente a los de la propia UE, sino de hacerlo más rápido que otros competidores para reducir la distancia existente. En este sentido, diversas áreas de los niveles (*stack*) desde el hardware a las aplicaciones de IA son claramente deficitarias en relación con las inversiones o personal especializado, y la transferencia de ese conocimiento hacia la industria es mejorable. Tampoco ayuda la fragmentación del mercado europeo.

En nuestra opinión, la UE tiene que realizar un **mayor esfuerzo para consolidar su ecosistema de innovación en IA con una visión paneuropea** y romper con los silos existentes nacionales y regionales. Además, no solo debe incrementar el esfuerzo en la formación de más recursos humanos en tecnologías de IA para reducir el déficit actual y previsto, sino también retenerlos en la UE y explotar las oportunidades para atraer investigadores a la UE⁴³⁰.

Al respecto, es destacable como **Ucrania se ha convertido en un laboratorio vivo** en el que sistemas de defensa habilitados para IA están madurando rápidamente con reiterados procesos de experimentación y evaluación de su eficacia táctica y operacional llevados a cabo de forma constante y rápida sobre el terreno (Goncharuk, 2024). Los procesos de simplificación administrativa que la Comisión Europea está dispuesta a poner en marcha

430 En este sentido, la oportunidad derivada de los problemas sufridos por investigadores sin nacionalidad de Estados Unidos está siendo aprovechada por varios Estados miembros de la UE con el lanzamiento de programas específicos. También la Comisión Europea ha puesto en marcha un proyecto piloto que forma parte de un paquete de 500 millones de euros para 2025-2027 y de la iniciativa más amplia “Elige Europa” para hacer de Europa un “imán para los investigadores”, presentada en mayo de 2025. La iniciativa se centra en tres objetivos: mantener la ciencia libre y abierta, invertir en talento y acelerar la innovación en Europa. A través del Consejo Europeo de Investigación (CEI), los investigadores que se trasladan a Europa ya reciben un complemento más allá de su subvención, que recientemente se ha duplicado. Además, unas nuevas «super subvenciones» de siete años en el marco del CEI ofrecerán apoyo a largo plazo a los mejores talentos.
https://ec.europa.eu/commission/presscorner/detail/es/ip_25_1146

en el ámbito de la defensa deberán acercar a la UE a ese modelo, de forma compatible con el necesario control del uso de los recursos públicos.

- La **estructura del mercado de IA europeo** presenta una fuerte dependencia de grandes empresas y plataformas de IA no europeas que ofrecen productos y servicios de IA en la nube, con pocos startups de IA de alta valoración (unicornios) sitios en la UE.

La necesidad de consolidar el **mercado de la IA europea** en base a adquisiciones y fusiones de empresas para estar en condiciones de competir mejor en los mercados internacionales y reducir la fragmentación actual se configura como un factor de principal importancia. No es un proceso sencillo porque las presiones de los gobiernos para disponer de “campeones nacionales” digitales y específicamente, en el sector de la defensa son fuertes, a pesar de los esfuerzos de la UE, partiendo de que las regulaciones europeas actuales para la fusión de empresas no lo facilitan.

Por otro lado, a pesar del **crecimiento de los fondos de capital riesgo de IA**, y el surgimiento de startups con productos y servicios disruptivos en IA, no se están generando empresas europeas que crezcan lo suficiente frente a lo que ocurre en otras zonas geográficas, y persiste el riesgo de que continúen sus procesos de escalada en Estados Unidos. Desde el punto de vista de la defensa la valoración del mercado debería ser una cuestión accesoria frente a la de favorecer el desarrollo de capacidades en la UE y su posicionamiento internacional.

- La UE está orgullosa de disponer de un **marco regulatorio avanzado de IA**, aún en proceso de plena implementación como se ha visto en el capítulo 6, acompañado de otras regulaciones en el ámbito digital sobre el mercado, servicios digitales o datos que, conjuntamente, proporcionan un marco de seguridad para el ciudadano europeo. Debe recordarse, como se ha indicado en el capítulo previo, que se trata de un marco regulatorio para el desarrollo y uso de la IA en aplicaciones civiles.

Desde el punto de vista de la soberanía tecnológica europea se trata de una **buena situación de partida** comparada que, sin embargo, presenta **dos debilidades**: 1) la necesidad de **conciliar regulación e innovación** en iguales o mejores condiciones que las existentes en otros países, equilibrio que ha sido puesto en duda por grandes empresas digitales; y 2) la necesidad de que un modelo de **regulación de IA basado en la reducción de riesgos pueda evolucionar al ritmo que lo hace la tecnología de IA y sea mimetizado en otros países**. Ninguno de los dos aspectos está firmemente asentado.

- Finalmente, un elemento clave del nivel 3 que ha influido en la regulación y en la evolución del propio mercado es la existencia de un **conjunto de principios y valores compartidos en relación con la tecnología en la sociedad y, expresamente, en aqué-**

Ilas de alto impacto social como es la IA con los que la UE desea verse reflejada en el mundo. En este punto, el enfoque de la UE con respecto a la inteligencia artificial se centra en la excelencia y la confianza, con el objetivo de impulsar la investigación y la capacidad industrial, garantizando al mismo tiempo la seguridad y los derechos fundamentales⁴³¹.

Estos valores y principios no son, necesariamente, compartidos en todos los países, y eso implica dificultades en las relaciones tecnológicas internacionales en las que **la UE deberá demostrar, a la vez, firmeza y pragmatismo** desde la previa construcción de posiciones comunes entre todos los Estados miembros.

El análisis realizado en las páginas anteriores sobre la situación de la soberanía tecnológica europea en IA no se refiere expresamente al uso de la IA en defensa, aunque muchas de las valoraciones realizadas sí sean aplicables. No se olvide que se trata de una tecnología habilitadora de carácter dual. La **diferencia al aplicarse a la situación en defensa con respecto al uso civil de la IA** es que los condicionantes geopolíticos para determinar la procedencia de componentes y sistemas e, incluso, su uso posterior una vez adquiridos, son mucho más relevantes, y la necesidad de interoperabilidad con sistemas de otros países (p.ej. en el contexto de la OTAN) mucho más apremiantes; en este caso, no son solo las reglas del mercado las que aplican.

La figura 7.7 ofrece una visión específica de las **capas técnicas del desarrollo y operación de sistemas de IA** que complementa el modelo de soberanía tecnológica en niveles presentado en la figura 7.6 desarrollado anteriormente. En este caso, el propósito es analizar la **situación actual de la soberanía tecnológica de la IA en el ámbito de la defensa** en cada una de las capas.

Las capas tecnológicas elegidas van desde el **hardware de computación especializado de IA (N1)**, apoyado, a su vez, por redes de comunicaciones de gran ancho de banda, a las **plataformas software para el acceso a la ejecución de modelos (N2)**, basado en grandes centros de datos y servicios digitales en la nube de banda ancha, a los **modelos de datos fundacionales (N3)**, algunos abiertos y otros propietarios, pero pocos desarrollados en la UE, a los **modelos de datos en dominios concretos** (salud, educación, finanzas, defensa, etc.) **(N4)** y, finalmente, el desarrollo y despliegue de **aplicaciones finales (N5)**.

Se han incluido a la derecha de la figura algunas consideraciones y ejemplos representativos en cada uno de los niveles aplicados al sector de la defensa.

431 <https://digital-strategy.ec.europa.eu/es/policies/european-approach-artificial-intelligence>



Figura 7.7. Consideraciones de soberanía tecnológica de IA en defensa en un modelo en niveles. Fuente: elaboración propia

La **valoración cualitativa de soberanía tecnológica** europea desarrollado en la elaboración de este informe es que la UE tiene un problema grave en los tres primeros niveles, y su situación es mejor en los dos últimos. El esfuerzo indicado en las cifras presentadas anteriormente sobre el nuevo marco financiero para el periodo 2028-2034 no permiten conocer como los recursos se asignarán a la mejora de la posición europea en IA.

En la Comunicación de la Comisión Europea de abril de 2025 titulada **“IA Continent Action Plan”** (Comisión Europea, 2025d), se adopta un tono optimista en el que nada está perdido: *“La carrera global por el liderazgo en IA está lejos de terminar. Los avances continúan redefiniendo los límites de lo que es posible. Desde los modelos de base de vanguardia hasta las aplicaciones especializadas de IA, el panorama de la IA en la UE sigue siendo dinámico, impulsado por la investigación, las tecnologías emergentes y un próspero ecosistema de empresas emergentes y en expansión”*.

La Comisión Europea propone un **Plan de Acción**⁴³² para mejorar la posición de la UE en IA basado en actuaciones sobre cinco elementos: infraestructura de computación, datos, formación, desarrollo de algoritmos y adopción, y simplificación regulatoria (Comisión Europea, 2025c, 2025d).

432 https://commission.europa.eu/document/download/f633985c-440a-4285-95c3-9fe16fd0fc65_en?prefLang=es

- Infraestructura de computación.

Se basa en el despliegue y escalado de **factorías de IA** en múltiples países europeos. Las iniciales son las representadas en la figura 7.8 Muchas de ellas se basan en los centros de supercomputación más importantes para asegurar la capacidad de procesamiento necesario con inversiones para optimizar la ejecución de modelos de IA. La idea es que dispongan de un mínimo de 100.000 procesadores avanzados de IA (aunque no sean europeos).

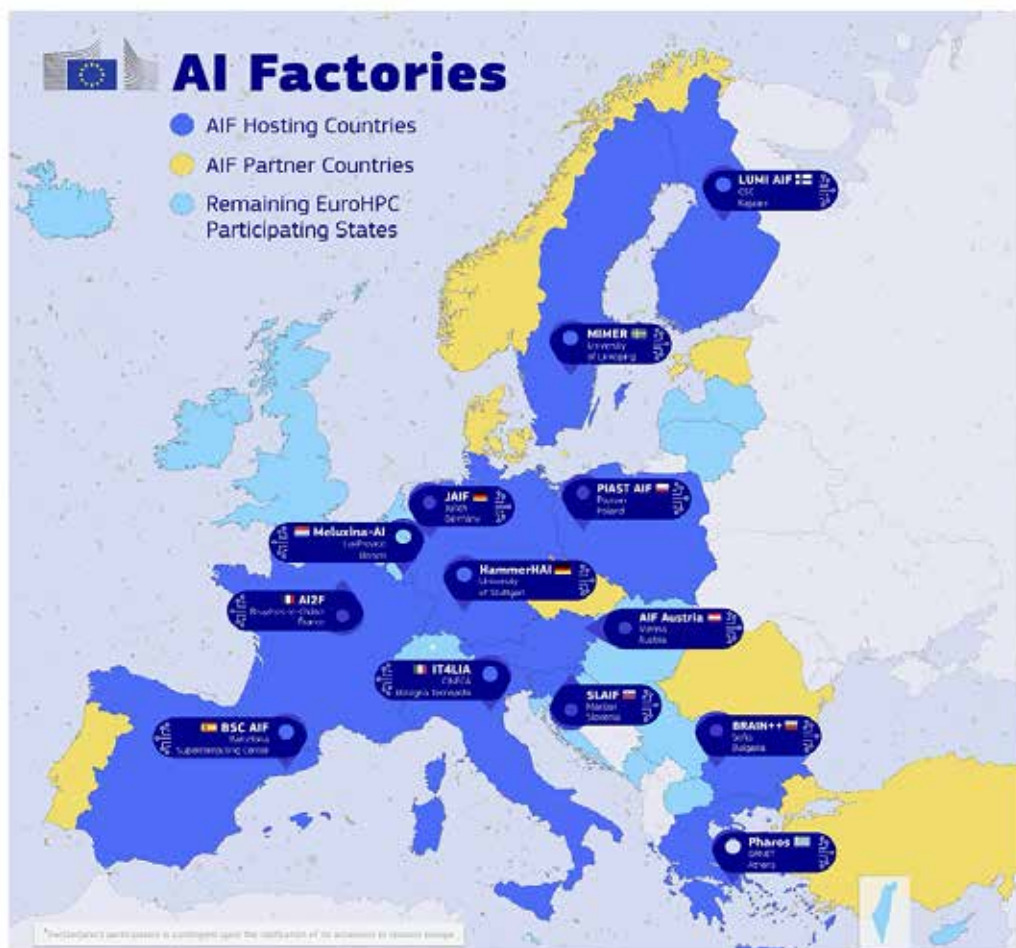


Figura 7.8. Factorías de IA en la UE. Fuente Comisión Europea (2025)

Se pretende que las **“Factorías de IA”** diseminadas por diferentes Estados miembros estén focalizadas en **sectores prioritarios**. La Tabla 7.2 (Comisión Europea, 2025d) indica la temática y países de las iniciadas en 2025.

Key Sectors	AT	BG	DE	EL	ES	FI	FR	IT	LU	PL	SE	SI
Health & Life Sciences	●		●	●	●	●	●	●		●	●	●
Technology & Digital		●		●	●	●	●	●	●	●	●	●
Environment & Sustainability		●	●	●	●		●	●	●	●	●	●
Education & Culture	●	●	●	●	●		●	●			●	●
Manufacturing & Engineering	●	●	●			●	●				●	●
Finance & Business	●		●		●		●	●	●		●	
Agriculture & Food	●				●		●	●			●	●
Cybersecurity & Dual use							●	●	●			
Space & Aerospace		●					●		●	●		
Public Sector	●		●		●					●		

Tabla 7.1 Factorías de IA. Fuente: Comisión Europea, 2025d

Por su interés para **España** es relevante indicar que el **BSC** (*Barcelona Supercomputing Centre*) alojará una de las *Factorías de IA* aprovechando las capacidades disponibles de computación de altas prestaciones (HPC) del *Mare Nostrum 5*. Concretamente (Comisión Europea, 2025d):

*“La **BSC AI Factory** proporcionará a los usuarios el desarrollo y la operación de un conjunto completo de servicios de computación de alto valor orientados a la IA y otros servicios con soporte especializado. MareNostrum 5 se actualizará para incorporar las arquitecturas de computación orientadas a la IA más recientes, especialmente diseñadas para flujos de trabajo de IA como el entrenamiento y la inferencia de LLM, incluyendo un sistema de almacenamiento diseñado para cargas de trabajo de IA, conectado al almacenamiento masivo de MareNostrum 5. Incluirá capacidades avanzadas de computación de IA con un software de IA dedicado y especializado y un extenso repositorio de datos. La BSC AI Factory se complementará con el establecimiento de una plataforma única y experimental optimizada para la IA para probar nuevas tecnologías informáticas a medida que lleguen al mercado.”*

Debe tenerse en cuenta que el **BSC** también se está posicionando en el ámbito de la **computación cuántica** (véase Anexo 3) con recursos nacionales y europeos y, por tanto, estará en una buena posición de partida ante la convergencia entre la IA y las tecnologías cuánticas que se producirá en los próximos años.

En la actualidad, la UE está retrasada respecto a los *Estados Unidos* y *China* en cuanto a la capacidad disponible de los centros de datos, ya que depende en gran medida de las infraestructuras instaladas y controladas por otras regiones del mundo, a las que los usuarios de la UE acceden a través de la nube. La *Ley de Desarrollo de la Nube y la IA* que la UE ha previsto presentar a finales de 2025 o comienzos del 2026 abordará estos obstáculos, con vistas a **triplicar la capacidad de los centros de datos de la UE en los próximos cinco a siete años** y llevarla a un nivel que satisfaga las necesidades de las empresas y las administraciones públicas de la UE para 2035.

No obstante, las inversiones en infraestructura de las factorías de IA propuestas por la UE requerirían un **presupuesto mucho mayor del previsto en el Plan de Acción** si se desea generar un impacto real frente a las previsiones de Estados Unidos y China⁴³³. Todo dependerá hasta 2034 del margen de maniobra que pueda tener la Comisión en las nuevas perspectivas financieras que empiezan a discutirse y los recursos que asignen a ello los Estados miembros.

- Datos.

Como ya se ha indicado en el presente informe, **el acceso a datos fiables y bien organizados es esencial** para que la UE pueda aprovechar todo el potencial de la IA. La *Comisión Europea* propondrá en el segundo semestre de 2025 una nueva **Estrategia de Datos de la Unión** para poner a disposición de empresas e investigadores públicos más datos en apoyo del desarrollo y la innovación de la IA.

Una herramienta importante en este contexto serán los **Data Labs**, ligado a las factorías de IA. Estos laboratorios de datos **reunirán y federarán datos de diferentes fábricas de IA que cubren los mismos sectores**. Además, se conectarán a los correspondientes *Espacios Comunes Europeos de Datos* y pondrán estos datos a disposición de los desarrolladores de IA en condiciones adecuadas; supondrá la disponibilidad de grandes volúmenes de datos de alta calidad en los sectores de la salud, la energía u otros. Para facilitar ese acceso, la Comisión ha iniciado el desarrollo de **Simpl**, un software compartido en la nube para facilitar la gestión y conexión de los espacios de datos⁴³⁴

Consciente de que el entrenamiento de modelos de IA se realizar predominantemente en inglés, la Comisión ha promovido en marzo de 2025 la **Alianza para las Tecnologías Lingüísticas (ALT-EDIC)** como un esfuerzo a gran escala para poner en común los datos lingüísticos de la UE. Se basará en un repositorio exhaustivo de recursos lingüísticos de alta calidad con el fin de colmar la brecha en los datos multilingües y preservar la diversidad lingüística y cultural de Europa.

- Formación.

La **Hoja de ruta para 2030 sobre el futuro de la educación y las competencias digitales** y su iniciativa sobre la IA en la educación apoyarán el desarrollo de la alfabetización en materia de IA en la educación, en particular, mediante especialistas en IA de la UE y mejorar y reciclar adecuadamente las capacidades de los trabajadores y ciudadanos de la UE en el uso

433 Las inversiones previstas en factorías de IA por parte de la UE no parece que pueden competir globalmente. Meta ya dispone en un solo centro de datos de los 100.000 chips de IA que contendrán en conjunto las cuatro factorías que empezará a desplegar la UE a finales de 2025 (García-García, 2025)

434 Simpl es una plataforma de middleware de código abierto, inteligente y segura que admite el acceso a los datos y la interoperabilidad entre los espacios de datos europeos. <https://digital-strategy.ec.europa.eu/es/policies/simpl>

de la IA. Una acción fundamental en este contexto será la puesta en marcha de la **AI Skills Academy** una ventanilla única que proporcionará educación y formación sobre competencias relacionadas con el desarrollo y el despliegue de la IA, y en particular la IA generativa.

Para complementar los programas educativos existentes la Comisión apoyará **el aumento de la oferta general de titulaciones** (grados, másteres y programas de doctorado) de la UE en tecnologías clave, incluida la IA.

- Desarrollo de algoritmos y adopción.

La **Estrategia de Aplicación de la IA** se centrará en los sectores industriales europeos clave en los que la UE tiene un fuerte liderazgo. Estos sectores tienen el mayor potencial sin explotar en cuanto a la adopción de la IA e incluyen, entre otros, la fabricación avanzada; aeroespacial; **seguridad y defensa**; agroalimentario; investigación en energía y fusión; medio ambiente y clima; movilidad y automoción; farmacéutico; biotecnología; diseño de materiales avanzados; robótica; comunicaciones electrónicas; Industrias culturales y creativas; y ciencia.

Además, el **sector público** será uno de los principales impulsores estratégicos de la estrategia. La Estrategia garantizará que la IA se utilice para mejorar la calidad y la eficiencia de los servicios públicos, en ámbitos como la asistencia sanitaria, la justicia, la educación y la administración pública

La red de **centros europeos de innovación digital** (*European Digital Innovation Hubs*) presentes en todos los Estados miembros de la UE y en otros diez países europeos, incluidos los países candidatos, desempeñará un papel clave para **apoyar la integración efectiva de la IA**, que abarca el 85 % de las regiones europeas. Tienen como objetivo garantizar el éxito de la transformación digital de las pymes, las empresas de mediana capitalización y las organizaciones del sector público. En su segunda fase, a partir de diciembre de 2025, se convertirán en **Centros de Experiencia para la IA**.

- Simplificación regulatoria.

La Comisión Europea es consciente de que tiene que facilitar a los actores del ecosistema de IA el cumplimiento de la regulación de IA. Para ello ha puesto en marcha una **Oficina de Apoyo** (*AI Act Service Desk*) como punto central de información.

Esta medida se acompañará con la puesta en marcha de diversos **espacios de prueba de regulación** ("*regulatory sandboxes*") con el fin de ensayar la implementación de normas, estándares y directrices de aplicación de la Ley de IA. En todo caso, será necesario recabar información de la experiencia en la implementación para acordar nuevos cambios, si fuera necesario.

Las actuaciones indicadas no están específicamente orientadas específicamente a aplicaciones en el sector de la defensa, aunque **dado el carácter dual de la IA las actuaciones en varias de las “factorías de IA” impactan potencialmente en la industria de defensa europea.**

Desde el punto de vista de la **industria de defensa europea** la mejora de la soberanía tecnológica debe concentrarse en sistemas que incorporan la IA como parte de equipos militares de los tipos analizados en el capítulo 5 con la vista puesta en su desarrollo en los Estados miembros de la UE; si fuera posible, con modelos de desarrollo y adquisición comunes. La siguiente tabla 7.2. pretende focalizar la **situación de la soberanía tecnológica (ST) de la UE en cada una de las capas anteriores centradas en el uso militar de la IA** indicando su previsible evolución hasta 2030 y las limitaciones o dificultades existentes para que la mejora de la soberanía tecnológica sea una realidad.

Nivel relativo a la IA	ST de la UE en IA para defensa 2025	ST de la UE en IA para defensa 2030	Limitaciones o dificultades de la UE para mejorar su ST en IA
Hardware de computación especializado en IA (p.ej. GPUs o chips neuromórficos).	No se dispone de fabricantes europeos de chips de IA ni tampoco se dispone de líderes de herramientas automatizadas de diseño, aunque sí existen capacidades de diseño de chips.	La situación de la UE mejorará con la puesta en marcha de fundiciones en las que parte de la producción puede destinarse a chips de defensa.	La sostenibilidad de las foundries europeas no va a depender únicamente del mercado de defensa, pequeño en volumen total sino del total en semiconductores de la UE. El riesgo es que los mercados se constituyan en bloques cerrados.
Plataformas software de IA para decisiones automatizadas y gestión de datos.	Actualmente, solo se dispone de sistemas parciales y se recurre a servicios en la nube proporcionados por grandes empresas.	Interés en disponer de sistemas propios para la gestión de conjuntos de datos controlados en defensa (p.ej. en sistemas de mando y control C2).	Los compromisos de incremento de los recursos en defensa pueden permitir el desarrollo de sistemas específicos para defensa compartidos por varios países. El caso de la nube de combate o un sistema de C2 es uno de ellos.
Modelos de datos para IA	El uso de grandes modelos de datos LLM fundacionales está en manos de grandes empresas digitales no europeas. Algunas empresas europeas han generado modelos específicos sobre LLM abiertos.	La tendencia en la UE es disponer de modelos de datos más pequeños y adaptados a tareas concretas en defensa. Mistral podría generar esos modelos en colaboración con otras empresas.	No existe un programa paneuropeo para la generación de un LLM para defensa, y su uso en las fuerzas armadas está en una fase de experiencias controladas para evaluar ventajas e inconvenientes.
Modelos y datos contextuales para IA	La necesidad de disponer de sistemas de mando y control multidominio obliga a integrar datos de múltiples sensores.	Al final de la década se dispondrá de espacios de datos adaptados, al menos, para cubrir a las necesidades de defensa de algunos Estados miembros.	Los espacios de datos militares interoperables y compartidos no existen todavía, pero la UE puede trabajar en esa línea adoptando modelos de datos interoperables.

Nivel relativo a la IA	ST de la UE en IA para defensa 2025	ST de la UE en IA para defensa 2030	Limitaciones o dificultades de la UE para mejorar su ST en IA
Aplicaciones finales basadas en IA	La UE posee capacidades para el desarrollo de aplicaciones finales de IA, aunque no se hayan impuesto en los mercados mundiales. En el caso de defensa se integran en las plataformas militares como parte de su arquitectura.	Todos los proyectos de europeos de desarrollo de nuevas plataformas o sistemas de armas autónomos dispondrán de aplicaciones de IA generativa para la interfaz con los operadores, módulos de aprendizaje automático y gestión inteligente de datos.	Los costes de desarrollo de aplicaciones complejas para defensa deben tener un mercado más amplio que el derivado de su uso específico en un producto concreto.

Tabla 7.2 Valoración de la soberanía tecnológica europea en IA para la defensa. Fuente: elaboración propia.

De todos los elementos indicados en la tabla 7.2 la **influencia de la geopolítica es clara sobre los semiconductores empleados en la UE para la IA** y merece una atención específica. Posteriormente, también se analizará esta soberanía en el caso de plataformas digitales en la nube. A ello se destinarán los siguientes apartados.

7.4 Geopolítica y semiconductores para IA

7.4.1 Situación de la UE en el mercado mundial de semiconductores

En la fabricación de semiconductores, para disponer de un nodo de proceso de última generación se requieren inversiones de gran magnitud recurrentes cada cinco años como máximo y no de una sola vez en el momento inicial. De ello se desprende como aspecto crítico que **abordar posibles soluciones requieren adoptar una perspectiva multinacional y no únicamente nacional**. La complejidad de la toma de decisión, por tanto, es evidente.

Asimismo, el **diseño de chips es un proceso complejo** que requiere ingenieros y científicos altamente cualificados, tecnología avanzada y propiedad intelectual (licencias) para crear diseños para obtener el rendimiento y la funcionalidad del chip. Teniendo en cuenta los diferentes segmentos de la cadena de valor, la **innovación en el diseño de chips es crucial** para los futuros avances en la tecnología de semiconductores (SIA, 2022).

Aunque las estimaciones varían de unos informes a otros, existe un consenso entre las consultoras tecnológicas internacionales de que **la demanda de circuitos integrados lógicos avanzados crecerá rápidamente en los próximos años impulsada principalmente por la IA, la informática de alto rendimiento y las comunicaciones inalámbricas**. Del mismo modo, los nodos tecnológicos maduros seguirán teniendo demanda en algunos sectores industriales, aunque a un nivel mucho más bajo.

Estados Unidos tiene una sólida posición de liderazgo en el diseño de circuitos integrados, lo que aumenta su capacidad para dar forma a las normas técnicas, mejora la seguridad nacional al depender menos de diseños realizados en otros países, y proporciona beneficios indirectos a los fabricantes de equipos originales (OEM) en industrias que van desde la tecnología de la información y las telecomunicaciones hasta el transporte y la energía. En relación con las **herramientas de diseño automatizadas** las empresas estadounidenses *Cadence Design Systems* y *Synopsis*, así como *Siemens EDA* (antigua *Mentor Graphics*), representan el 70% de las ventas mundiales.

En el contexto indicado, la UE ha dependido en exceso de la **subcontratación de una parte importante del diseño y la fabricación de semiconductores** en las últimas décadas (Bloomberg, 2021). En consecuencia, y de acuerdo con el Consejo de la UE (2022), **la UE tiene capacidades limitadas tanto en el diseño como en la fabricación de productos microelectrónicos**, lo que le sitúa como un actor secundario en la fabricación a nivel global.

Esta debilidad también ha afectado a la **disponibilidad de capital humano**. Las empresas europeas están especialmente preocupadas por atraer talento, tanto especialistas como personas con habilidades básicas y conocimientos de ingeniería. Ello ha obligado a la UE a financiar **programas específicos para atraer a Europa a investigadores de otros países** en áreas STEM, sobre todo de Estados Unidos, intentando revertir el conocido problema de “brain drain” que se ha desarrollado durante décadas.

Un punto débil de la UE es que los **chips lógicos avanzados** sólo representan el 8% de la demanda total europea (Dachs, 2023; CE, 2021a), lo cual se explica porque la demanda de la UE está impulsada principalmente por sectores como la automoción y la electrónica industrial, que requieren circuitos integrados diferentes y menos exigentes que los utilizados en nodos de proceso más avanzados de 2-5 nm. También debe considerarse la demanda limitada de chips integrada en productos de alta tecnología para el usuario final en sectores como el aeroespacial, el de defensa o el de equipos médicos.

También **la UE va a la zaga de Estados Unidos, Taiwán y Corea en esfuerzos de I+D sobre semiconductores**. El gasto de capital (CapEx) europeo en semiconductores representa sólo el 3-4% del gasto mundial de la industria (ASML, 2022). Además, la UE tiene previsto invertir (según lo acordado en la *Ley del Chip*) sólo una fracción de lo que China y Estados Unidos tienen previsto invertir en los próximos años.

En 2021 **Europa representaba menos del 1% del total mundial de sedes de empresas de chips sin fábrica**, en contraste con el 68% de Estados Unidos y el 21% de Taiwán. De hecho, el diseño lo realizan principalmente las empresas integradas de diseño y fabricación (IDM) y está vinculado a los mercados de mayor volumen. Una proporción significativa de chips utiliza actualmente propiedad intelectual de origen estadounidense para su

diseño. En consecuencia, **la cuota europea de *fabless* ha disminuido del 4% en 2010 a menos del 1% en 2022.**

La cuota de mercado, por sectores, de los dispositivos semiconductores para los **usuarios finales de la UE** en 2023⁴³⁵ refleja la siguiente distribución: automoción 39 %, industrial 23 %, comunicación 12 %, consumidor 7 %, e informática 1,4 %. Como se puede ver, la **brecha existente entre los sectores de la automoción y otros sectores** utilizando las cuotas de mercado como aproximación son elevadas, y no es precisamente el sector de la automoción el más relevante desde el punto de vista de la IA. La cuota de la UE en informática, estrechamente relacionada con la IA, es muy pequeña.

7.4.2 Uso de hardware abierto en el ámbito militar

Frente a la situación descrita en la sección anterior, muchas empresas han empezado a prestar atención al **empleo de chips basados en arquitecturas abiertas como RISC-V** con crecimientos estimados del mercado muy elevados para afrontar los costes y los problemas de suministro que han comenzado a surgir. Es decir que la utilización de GPUs basadas en tecnología propietaria no es la única estrategia que el sector privado está encarando para gestionar sus necesidades.

El interés de la UE y de otros países por emplear **soluciones de hardware abierto como RISC-V** se explica por su potencial de revolucionar los dominios de la propiedad intelectual (PI) y de las empresas de diseño sin fabricación (*fabless*). Las inversiones en RISC-V han crecido rápidamente en los últimos tres años. La utilización de hardware y software de código abierto ofrece posibilidades para aplicaciones basadas en núcleos, como **procesadores, procesadores gráficos, procesadores de imágenes, aceleradores para IA/ML, procesadores de seguridad y procesadores de gestión de energía**. Además, facilita la portabilidad entre sistemas y software.

El uso de **código abierto puede ayudar a preservar la soberanía** cuando la concesión de licencias de PI a terceros países no comunitarios es la única alternativa. Sin embargo, se necesita una masa crítica de contribuyentes europeos a los proyectos de código abierto. En el caso europeo, pero no de la UE, debe considerarse que el gran competidor en términos de PI para el diseño de chips es **Arm**, empresa británica, pero controlada en un 90% por el conglomerado japonés **Softbank**.

Es significativo que *Meta* prosigue en su estrategia de independencia en hardware con el desarrollo de su **primer chip de inteligencia artificial (IA) basado en RISC-V** diseñado específicamente para el entrenamiento de modelos avanzados. La compañía ha trabajado

435 <https://www.consilium.europa.eu/es/policies/eu-chips-industry/#0>

junto con *Broadcom* en el diseño de este acelerador personalizado, fabricado por *TSMC*, con el objetivo de **reducir su dependencia de las unidades de procesamiento gráfico (GPU) de Nvidia**, como las H100, H200, B100 y B200⁴³⁶.

Además de las grandes empresas, está emergiendo un conjunto de **start-ups especializadas** que impulsan el desarrollo de las opciones no propietarias que por ahora se utilizan para acelerar los modelos de recomendación, tanto en inferencia como en entrenamiento. Las potencialidades de este estándar abierto no se agotan ahí, sino que se extienden a que surjan nuevos actores en el desarrollo de herramientas, de software, de periféricos, así como de otros conjuntos de instrucciones (ISA) propietarias.

En este marco de aceleración de **vías alternativas** que ofrezcan soluciones a un escenario que exhibe desde su configuración inicial signos de complejidad, la UE lanzó en 2018 el proyecto de desarrollo de un **Procesador Europeo** (*European Processor Initiative -EPI*) con el objetivo de desarrollar un procesador con propiedad intelectual (IP) completamente europeo basado en RISC-V con arquitectura EPAC para un chip acelerador.

Basado en la experiencia obtenida debe mencionarse el esfuerzo europeo para **expandir el uso de RISC-V** bajo control en la UE con el lanzamiento del proyecto **DARE** (*Digital Autonomy with RISC-V in Europe*)⁴³⁷ coordinado por el BSC y financiado por el EuroHPC Joint Undertaking⁴³⁸. Su objetivo es servir de base para **computación de altas prestaciones e IA (acelerador de inferencias)**. En la figura 7.9. puede verse la estructura del proyecto que ha arrancado en 2025. Obsérvese que se diseñarán tres chips, uno de ellos (*Axelera AI*) es el **acelerador de inferencias para aplicaciones de IA**.

436 <https://revistacloud.com/meta-prueba-su-primer-chip-de-ia-basado-en-risc-v-para-entrenamiento-de-modelos/>

437 <https://dare-riscv.eu/home/>

438 Los Estados miembros de la UE aportan 120 millones de euros, y EuroHPC JU otros 120 millones de euros.

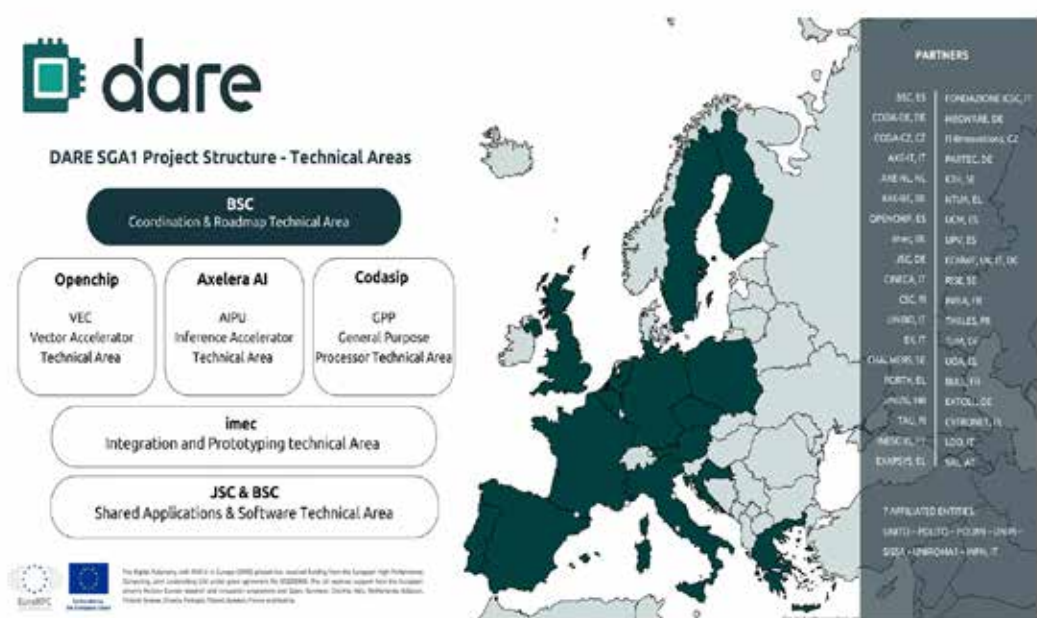


Figura 7.9 Proyecto Dare. Fuente: <https://dare-riscv.eu/home/>

Para entender su **relevancia en términos de soberanía tecnológica europea**, debe tenerse en cuenta que la mayoría de los sistemas HPC en Europa se basan en motores de Intel, AMD y Nvidia, todos con sede en los Estados Unidos. El cambio al RISC-V ISA no solo permite a Europa reducir potencialmente sus costes de creación de chips en el ámbito de la HPC y la IA, sino que también permite a Europa adelantarse a una situación que le permita mejorar su posición relativa.

7.4.3 Geopolítica de la fabricación de semiconductores

La **cadena de valor de los semiconductores presenta múltiples puntos de fricción** cuyo control o bloqueo se ha convertido en un elemento clave de las estrategias de las potencias tecnológicas. Desde el acceso a materias primas, a máquinas de fabricación, al software de diseño, o a las rutas de aprovisionamiento, todos ellos se han convertido en potenciales cuellos de botella, y origen de conflictos entre países.

Uno de los puntos clave de interés geopolítico se sitúa en la fase de **fabricación o fundición de chips**. Se basa en un gran número de complejos procesos avanzados de fabricación, con sistemas de fotolitografía muy costosos que representan aproximadamente una cuarta parte del valor añadido de los semiconductores, pero **casi dos tercios del gasto en capital físico** (OCDE, 2023b).

Durante las últimas décadas, la mayoría de las inversiones en nuevas instalaciones de producción de chips se han realizado en Asia. Aproximadamente **el 75% de la capacidad mundial de fabricación de semiconductores se concentra en Asia Oriental y China**. Los volúmenes de inversión que requieren las fábricas de última generación para mantener unas instalaciones tecnológicamente avanzadas conocidas como **salas blancas** podrían explicarlo. Las **salas blancas** deben mantener un nivel extremo de limpieza y control térmico y están equipadas con maquinaria compleja para la producción de chips. Posteriormente, se requiere también disponer de **capacidades de pruebas y encapsulado** de dispositivos en un chip.

Para tener una idea de los niveles de riesgo, la configuración actual de la cadena de valor global de semiconductores tiene más de **50 puntos potenciales únicos de fallo**, lo que equivale a más del 65% del valor del mercado mundial vulnerable a interrupciones o shocks ocasionados por diversos motivos (desde el crecimiento de la demanda, los largos ciclos de fabricación, la inflexibilidad del suministro, hasta las tensiones geopolíticas). **Esta situación no afecta únicamente a la UE** sino también a los Estados Unidos y a otras potencias occidentales con lo que resulta evidente que **la cadena de suministro dista mucho de ser resiliente** (EMI, 2023).

La suposición de que toda la discusión geopolítica de los semiconductores gira en torno a la seguridad del suministro y la resiliencia de las cadenas de valor actuales ignora la **dinámica cambiante de la política y la economía internacionales, que ya están remodelando las reglas del juego**. El mundo se está alejando del libre comercio, por lo que no se puede dar por sentado un suministro seguro de chips producidos en Asia (Dachs, 2023; Mariotti, 2022). En esta industria, los retos y las oportunidades varían de un segmento a otro, al igual que su impacto en otras tecnologías emergentes. La evolución tecnológica actual del sector demuestra que el diseño y la fabricación son componentes esenciales de la producción de chips avanzados o de gama alta.

Un punto esencial para la UE se refiere a las **condiciones en las cuales las empresas de fabricación** (como TSMC, Samsung, o Intel) **deciden instalarse en el territorio comunitario**. En el caso de TSMC⁴³⁹, Alemania ha aceptado que los costos de los chips fabricados en Dresde sean entre un 20-30% más caros que los mismos producidos en Taiwán, y con una muy limitada transferencia de conocimiento hacia los ecosistemas locales europeos. Esta situación tiene un doble impacto. Por un lado, es esperable que afecte a la competitividad de las firmas europeas usuarias. Por otro lado, pone en evidencia los mayores costes europeos de seguir esta alternativa para incrementar el nivel de soberanía tecnológica, a pesar de que su efecto en la **mejora de la resiliencia** de la provisión de semiconductores es innegable. Se trata, por tanto, de **encontrar el equilibrio entre coste y resiliencia**.

⁴³⁹ La empresa creada se denomina ESMC. TSMC tiene una participación mayoritaria (70%) en ESMC, junto con las empresas alemanas Bosch e Infineon y la neerlandesa NXP.

A partir de los datos empleados en este estudio y el análisis cualitativo correspondiente, **el desarrollo de chips europeos dependerá de las capacidades de I+D y de acuerdos estables con fundiciones situadas en otras partes para garantizar la producción de los chips diseñados**. Asimismo, las instalaciones de fabricación de la UE dependen del rendimiento relativo con respecto a los procesos de nodos más avanzados implementados por fundiciones no europeas.

La limitada participación de las empresas de la UE en el diseño de chips lógicos avanzados y segmentos de memoria no significa que el bloque carezca de capacidades de I+D. Institutos punteros como el **IMEC** en Bélgica (y próximamente con infraestructuras en Málaga, España) que también posee capacidades de fabricación en líneas piloto, el **CEA-Leti** en Francia y el instituto **Fraunhofer** en Alemania han realizado importantes investigaciones en el campo de los semiconductores y han contribuido a crear robustos ecosistemas de innovación.

Muchos avances tecnológicos han sido el resultado de **colaboraciones entre empresas, universidades e instituciones de investigación** que aúnan conjuntamente fondos y esfuerzos apoyados por programas comunitarios como el actual *Horizonte Europa 2021-2027*. Se trata de actores clave en el desarrollo de la propiedad intelectual europea, la acogida de líneas piloto y la contribución al desarrollo de competencias y a la formación (CE, 2022).

Sin embargo, a pesar de las intenciones formuladas en el ámbito de la política europea con la aprobación de la Ley Chip, la situación es compleja ya que, en los últimos veinte años, la evolución de la cadena de valor de los semiconductores ha creado barreras de entrada difíciles de superar (Kleinhans, 2021). Ricart y Álvarez-Aragonés (2024) señalan **dos puntos débiles de la UE** que podrían, de persistir en el tiempo, dejar al bloque fuera de las tres grandes potencias mundiales: **el número reducido de grandes empresas y start-ups de IA Generativa y el moderado volumen de capital riesgo europeo que invierte en ellas**. En este sentido, la debilidad relativa de sus activos y competencias que impactan sobre su nivel de ciencia y tecnología podría socavar los cimientos de su capacidad efectiva para incidir tanto en los debates en los foros internacionales como en el establecimiento de los marcos regulatorios de la IA.

7.4.4 Soberanía tecnológica europea en semiconductores para la defensa

Dado que **la tecnología de semiconductores es dual**, nada impide que los esfuerzos de mejora de la soberanía tecnológica en semiconductores puedan beneficiar a su aplicación en defensa, incluidos los chips pensados para IA como GPUs y aceleradores de inferencias, pero también otros más especializados como chips neuromórficos.

En el caso concreto de su uso militar existen **dos aspectos relevantes** que influyen en la toma de decisiones: un **volumen de mercado limitado** en términos de número de chips,

mucho menor que el existente en el mercado civil, y **consideraciones de costes menos relevantes** que los que se aplican para aplicaciones civiles con chips integrados en millones de productos. Fabricar “*pequeñas cantidades*” requiere infraestructuras menores, aunque la complejidad del diseño no disminuya. Ello ha permitido pensar en líneas de fabricación de chips de IA especializadas en defensa.

También RISC-V se puede utilizar para aplicaciones militares. En sus inicios DARPA estuvo ligada a la iniciativa de RISC-V pensando en que sería una alternativa de menor coste para el desarrollo de sistemas militares y aeroespaciales. Por ejemplo, el *Laboratorio de Propulsión a Chorro (JPL)* de la NASA seleccionó semiconductores que utilizan la arquitectura RISC-V para su proyecto de misión espacial autónoma.

La relevancia de utilizar una arquitectura abierta como RISC-V fue reconocida rápidamente por países como *China* que la vio como una **estrategia válida para evitar la dependencia de tecnologías de Estados Unidos y otros países que se sumaron a sus sanciones**. Como ejemplo de este posicionamiento, entre los 15 organismos que más patentes han registrado sobre RISC-V se encuentran dos centros chinos que se encargan de desarrollos militares⁴⁴⁰.

Dos ejemplos de **uso militar en China de RISC-V** son radares y sistemas de previsión de ciberataques⁴⁴¹. El *Instituto del Software en la Academia China de Ciencias (CAS)* anunció en 2021 un chip RISC-V destinado a evitar cierto tipo de ciberataques. La Universidad de *Beihang* diseñó en 2022 un chip RISC-V que procesa señales de radar. También China anunció en 2024 la creación del **chip criptográfico E450R** por la empresa *Unisoc* basado en RISC-V⁴⁴². El *Instituto de Tecnología de Computación del CAS*, uno de los vetados por las sanciones de Estados Unidos, presentó en mayo de 2023 la segunda generación de sus chips RISC-V “*Xiangshan*” de alto rendimiento para PCs, pero además a él se sumó la presentación del sistema operativo “*Aolai*” específicamente diseñado para gestionar dichos procesadores. En nuestra opinión, la distancia de China con Estados Unidos se va acortando.

Desde el **punto de vista europeo** los esfuerzos de investigación procedentes de universidades o centros de investigación europeos son también aplicables al desarrollo de tecnologías duales habilitadoras como **diseño de chips de IA con aplicaciones en defensa** (sobre todo, en TRLs medios). Sin embargo, para que esta potencialidad se manifieste es necesario incrementar la financiación específica y la colaboración con la industria para asegurar la transferencia de conocimiento hacia la **provisión de sistemas europeos para las fuerzas armadas europeas** o, en un contexto de internacionalización, para otros países aliados en los mercados internacionales.

440 Este posicionamiento de China provocó algunas reacciones en Estados Unidos para impedir su acceso, más allá de las restricciones de fabricación con trabas a empresas americanas y con estándares diferentes. No creemos que esta postura se pueda mantener. <https://itif.org/publications/2024/07/19/the-us-china-tech-conflict-fractures-global-technical-standards/>

441 <https://tecnologiaconjuancho.com/china-impulsa-risc-v-independencia-tecnologica/>

442 <https://www.xataka.com/empresas-y-economia/china-tiene-su-propio-chip-seguridad-risc-v-sus-creadores-no-tiene-rival>

Los **incrementos presupuestarios** en la UE derivados de los compromisos de defensa en los presupuestos nacionales de los Estados miembros, los créditos proporcionados por el programa **SAFE** de la UE, si los Estados miembros los solicitan, y las discusiones en torno al futuro *“Fondo de Competitividad”* pueden permitir a la UE dar un **salto cualitativo en sus capacidades de desarrollo de chips para sistemas de defensa** que reduzcan a medio plazo la dependencia actual.

Finalmente, las Fuerzas Armadas de los Estados miembros deberán **desarrollar capacidades de prueba y despliegue efectivo de sistemas de IA** en unidades operativas y disponer de suficiente personal especializado en áreas concretas de la IA (p.ej. para el establecimiento de requisitos y el desarrollo de LLM específicos).

7.5 Geopolítica y plataformas digitales para la IA en defensa

Un ámbito estrechamente relacionado con la soberanía tecnológica europea en IA es el de las **plataformas digitales para proporcionar servicios de IA**. Su uso se ha extendido a todos los sectores socioeconómicos, aunque el interés en esta sección se centra en el desarrollo y adopción de **plataformas con arquitecturas software adaptadas a aplicaciones de defensa**.

De forma análoga a lo ocurrido con las plataformas dominantes en otros **dominios civiles** proporcionados por grandes empresas (*Airbnb, Facebook, Amazon, Android*, plataformas de redes sociales, etc.) que han incorporado servicios innovadores con motores de IA, y acceso a través de la nube, también ocurre en el sector de la defensa. La extensión de este enfoque puede **modificar el modelo tradicional de contratación de defensa y reemplazarlo con un enfoque más “ágil” y competitivo** de innovación tecnológica.

El problema es que su adopción también generará dependencias de otros proveedores. Existen opiniones (Hoijtink y van der Kist, 2025) de que **la adopción del “modelo de plataforma” en defensa probablemente conducirá a nuevos monopolios y dependencias**, que serán difíciles de revertir una vez que las plataformas de software que ejecutan el hardware y las operaciones militares estén en manos de solo un puñado de empresas de tecnología de defensa, en su mayoría no europeas. Resolverlo no es ajeno, por tanto, a la transformación de la fragmentación actual en un verdadero **sector industrial de defensa europeo**.

El desarrollo de **plataformas de software para el procesamiento, clasificación y análisis de datos militares obtenidos en tiempo real de múltiples sensores** sobre los que se puedan generar servicios específicos como muchos agentes inteligentes empleados en sistemas de mando y control o logística militar es una necesidad creciente en defensa. La clave es disponer de una plataforma para la gestión inteligente de la enorme cantidad de datos organizativos con otros en tiempo real generados por sensores incorporados en equipos militares, transferidos a través de dispositivos en red y almacenados en diferentes bases de datos.

Una de las plataformas específicas de defensa más empleadas es la proporcionada por la empresa estadounidense **Palantir**, denominada **AIP**⁴⁴³. Su objetivo es permitir a las organizaciones de defensa que la utilicen emplear LLMs e IA avanzada para misiones críticas, de manera segura empleando una red privada. **AIP** aprovecha datos organizativos junto con interfaces hombre-máquina para una toma de decisiones inteligente y rápida, mediante herramientas de IA con barreras de seguridad e impulsadas por principios de uso centralizado responsables.

Es destacable en términos de dependencia tecnológica europea el hecho de que el *Mando Aliado de Operaciones (ACO)* de la OTAN haya adquirido en marzo de 2025 el sistema **Palantir Maven Smart System NATO (MSS NATO)**, que será empleado para mejorar diversos aspectos de las operaciones militares de la Alianza⁴⁴⁴. Como indica la nota de prensa de la OTAN: “Al proporcionar una capacidad de combate común habilitada por datos a la Alianza, a través de una amplia gama de aplicaciones de IA, desde grandes modelos de lenguaje (LLM) hasta aprendizaje generativo y automático, MSS NATO mejora la fusión de inteligencia y la selección de objetivos, el conocimiento y la planificación del espacio de batalla y la aceleración en la toma de decisiones.”

No es evidente hasta qué punto esta decisión **condicionará las decisiones futuras de adquisición de plataformas de IA en los países europeos pertenecientes a la OTAN**. Si no se acuerda de manera urgente un desarrollo europeo propio, la soberanía tecnológica europea en este ámbito puede verse comprometida perpetuando la dependencia de Estados Unidos.

Otro ejemplo de desarrollo en este ámbito es el de la empresa **Anduril** con su plataforma **Lattice**⁴⁴⁵. Se trata de una **plataforma dual de software abierto** capaz de ser utilizada para aplicaciones civiles y de defensa. Está diseñada para ser independiente de los sensores, las redes y los sistemas. **Lattice** toma datos de sensores y sistemas dispares y distribuidos y los traslada a una **única capa de integración**. En esta capa de integración se utilizan técnicas de IA, aprendizaje automático y procesamiento de sensores/datos para filtrar información de alto valor para los usuarios. Los usuarios reaccionan a los datos asignando tareas a otros sistemas, como sensores, vehículos u otros activos **dentro de la propia plataforma** a modo de agentes inteligentes.

Una de las áreas de aplicación militar más relevante de este tipo de plataformas es en los **sistemas de mando y control**. El *Joint All-Domain Command and Control (JADC2)* es un ejemplo de prioridades para el Departamento de Defensa de Estados Unidos. **Lattice** se ha acercado a los requisitos de **JADC2** mediante la creación de un **sistema operativo abierto**

443 <https://www.palantir.com/platforms/aip/defense/>

444 <https://www.ncia.nato.int/newsroom/news/nato-acquires-ai-enabled-warfighting-system>

445 <https://www.anduril.com/article/anduril-s-lattice-a-trusted-dual-use-commercial-and-military-platform-for-public-safety-security/>

para la defensa que sea simple, escalable, extensible y, en última instancia, aproveche la IA para acelerar la decisión en cadenas de mando complejas. En este posicionamiento de la industria de defensa de Estados Unidos en Defensa es sintomático dar cuenta de los acuerdos alcanzados con otras empresas de IA como *OpenAI* y *Meta* lo que augura una aceleración en la disponibilidad y despliegue de esos sistemas⁴⁴⁶.

Los dos casos mencionados de *Palantir* y *Anduril* se corresponden con productos de empresas no europeas con lo que los ejércitos de los Estados miembros de la UE que las adoptan podrían, trabajando con el fabricante, adaptar la plataforma a sus necesidades, pero **no evitarían la dependencia de ellos**. La existencia de plataformas de este estilo desarrolladas completamente en la UE sería la mejor **garantía de asegurar su soberanía tecnológica**, pero ello implica un esfuerzo importante y continuado que requeriría adoptar **visiones paneuropeas** con la asignación de recursos comunitarios.

No creemos que un objetivo tan ambicioso pueda abordarse fácilmente por empresas europeas de forma aislada y, en el mejor de los casos, llevará tiempo conseguir plataformas de IA con prestaciones similares a las que ofrecen otras empresas occidentales no europeas como las indicadas que, a su vez, **seguirán evolucionando muy rápidamente**⁴⁴⁷.

Tampoco ayuda a conseguirlo la **fragmentación en el desarrollo de sistemas de defensa** con objetivos similares en varios Estados miembros de la UE alimentados por proyectos, programas y presupuestos decididos de manera independiente. La voluntad política de la *Comisión Europea* de actuar sobre el mercado europeo de defensa para reducir paulatinamente su fragmentación que se deriva del programa REARM y el instrumento SAFE deberían continuarse en el periodo 2028-2034 con recursos comunitarios adicionales cuyo acceso esté condicionado a compras mancomunadas entre Estados miembros.

7.6 Desafíos para el futuro

El presente capítulo ha pretendido ofrecer una valoración global de la situación de la UE en relación con su soberanía tecnológica en IA aplicada al sector de la defensa. La valoración global indica una **debilidad derivada de la fragmentación de las adquisiciones en cada**

446 OpenAI ha firmado un acuerdo con Anduril para combinar los modelos de OpenAI con el hardware y software de Anduril para detectar y derribar drones. Meta, en colaboración con la startup militar Scale AI, está promocionando su modelo de lenguaje grande, Llama, para la planificación y la toma de decisiones militares (Hoijsink y Kist, 2025).

447 Como un ejemplo reciente, Scale AI, junto con sus socios tecnológicos Anduril y Microsoft, desarrollará e implementará soluciones impulsadas por IA y flujos de trabajo de agentes personalizados que se entregarán inicialmente al Comando Indo-Pacífico y al Comando Europeo, según un comunicado de Scale AI en mayo de 2025. Este anuncio significa la primera incursión del Pentágono en la integración de agentes de IA en y a través de flujos de trabajo militares para proporcionar sistemas avanzados de apoyo a la toma de decisiones. <https://www.nationaldefensemagazine.org/articles/2025/4/5/pentagon-ready-to-let-ai-make-some-decision>

Estado miembro y la ausencia de grandes empresas digitales y de defensa europeas con énfasis en la IA.

La situación de partida no es buena. La UE y sus Estados miembros asignan 14.400 millones de euros anuales a la I+D militar, comparado con los 130.000 millones de euros que gasta Estados Unidos, diez veces más, y Google gasta casi diez veces más que el presupuesto combinado de I+D de los 27 Estados miembros de la UE (Clapp, 2025).

Revertir esta situación va a requerir recursos y tiempo, pero, sobre todo, la **decisión política** de hacerlo de manera sostenida durante largos periodos. La **oportunidad** derivada del proceso de negociación de del nuevo marco financiero plurianual de la Unión no puede desaprovecharse por el Consejo y el Parlamento Europeo para dar un salto cualitativo relevante en el posicionamiento europeo en IA.

Una estrategia de innovación destinada a lograr la soberanía tecnológica en IA debería considerar la posibilidad de basarse en la **creación de competencias transversales** para tener éxito. Ello supone abordar simultáneamente la priorización de proyectos de I+D con recursos abundantes en el contexto europeo que empleen IA, disponer de infraestructuras y herramientas software para diseño y fabricación de procesadores, sensores y plataformas inteligentes, asegurar la disponibilidad de recursos humanos especializados, y **mantener a largo plazo la voluntad política de mejorar la soberanía tecnológica.**

Creemos **que la UE deberá hacer un esfuerzo en los próximos años para disponer lo antes posible de alternativas tecnológicas europeas** de altas prestaciones y eficientes que aborden desde el desarrollo de dispositivos semiconductores clásicos (CPU, GPU, FPGA, ASIC, memorias y arquitecturas abiertas RISC-V) a otros de computación neuromórfica, pensando en la ejecución de algoritmos de IA, el desarrollo de LLMs “europeos”, la disponibilidad de plataformas de toma de decisión y su **integración en múltiples sistemas militares.**

La oportunidad de aprovechar los crecientes recursos procedentes de la UE asignados a la **industria de defensa** en el presupuesto comunitario que empieza a negociarse, así como la priorización hacia un mayor esfuerzo en el desarrollo de tecnologías duales como la IA puede servir de base **para condicionar a los Estados miembros, últimos responsables de las adquisiciones militares, a adquirir sistemas y plataformas militares europeas.**

De todas formas, las inversiones privadas de empresas digitales y/o de defensa europeas en el desarrollo de plataformas de IA como las indicadas deben considerar una estrategia de acceso a un **mercado dual, militar y civil que es global.** Únicamente de esta forma podrán **recuperar la inversión** que supone su desarrollo, a pesar del apoyo público comunitario o de los Estados miembros que consigan.

Competir a nivel global también implica que los mercados de defensa sean abiertos, dentro de la UE y fuera, y ello chocará con las ideas de imponer restricciones a las empresas no europeas para penetrar en el mercado de la Unión. Creemos que la existencia de **acuerdos equilibrados con presencia de empresas de defensa no europeas con capacidades de I+D instaladas en la UE** para realizar parte de sus desarrollos junto a empresas europeas sería una estrategia posible⁴⁴⁸. Su implementación dependerá de las condiciones que se establezcan en los futuros programas de la UE como el *HE 2028-2034* y el *Fondo de Competitividad* referidos a la participación de entidades de terceros países en proyectos colaborativos.

En el horizonte de 2030, las sinergias de la IA con otras tecnologías habilitadoras emergentes, entre ellas las **tecnologías cuánticas** y la **neurotecnología**, abren un amplio abanico de posibilidades que la UE debería estar dispuesta a aprovechar desde ahora para poder asegurar un **nivel de soberanía tecnológica de la UE suficiente** en dos campos emergentes muy relevantes.

El **Anexo 3** de este informe presenta la visión de los autores sobre la **convergencia futura de las tecnologías cuánticas (en computación, comunicaciones y sensórica) con la IA**, y su posible aplicación militar en la denominada “**guerra cuántica inteligente**” que ya se otea en el horizonte de la próxima década.

En todo caso, **la UE tiene que replantearse su estrategia de socios internacionales en el desarrollo de la IA**. La política seguida de cooperación con Estados Unidos en el *Consejo de Comercio y Tecnología entre la UE y Estados Unidos* en el que la IA constituía un elemento clave de la agenda de trabajo y permitió alinear sus posturas en el G7, G20 o en la OCDE (García-García, 2025) **se ha paralizado en 2025**⁴⁴⁹. Con ello, también las dos partes se han alejado en la búsqueda de una vía de “acuerdo regulatorio” por lo que el futuro del **impacto de la Regulación de IA de la UE en otros países es reducido**.

Más allá de Estados Unidos, la UE tiene que ver si otros **foros de cooperación tecnológica** establecidos con *Japón, Corea del Sur, India y Canadá* (adicionales a los acuerdos existentes con el *Reino Unido, Noruega, Suiza, Israel o Turquía*) que ya participan en los programas marco de investigación e innovación)⁴⁵⁰ pueden servir de **marco para acuerdos futuros en el ámbito de la IA** que combinen aspectos tecnológicos y regulatorios comunes aprovechando sus discrepancias con Estados Unidos. La cooperación con *China* tampoco parece sencilla para la UE en las condiciones geopolíticas actuales, salvo en acuerdos puntuales desde una visión muy pragmática.

448 Como ejemplo, Palantir posee equipos de investigación y desarrollo en el Reino Unido y en Francia.

449 Creado en 2021, ha sido paralizado por la Administración Trump y no ha habido reuniones en el primer semestre de 2025. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_es

450 La cooperación tecnológica con Israel está en proceso de discusión en el escenario de la guerra en Gaza. Algunos países como España han reducido esa cooperación tecnológica en sistemas de defensa.

Trasladar esta situación de **cooperación internacional en la IA en defensa** ligada al incremento de la soberanía tecnológica de la UE en ese ámbito es aún más arriesgado dadas las incertidumbres actuales. **La UE necesita tiempo y no solo recursos económicos para desarrollar sus propios sistemas avanzados de IA en defensa.**

Si las condiciones geopolíticas se complicasen y hubiese que disponer de sistemas inteligentes avanzados para los ejércitos europeos con urgencia, la UE se vería en la tesitura de adquirir muchos de ellos a Estados Unidos e **incrementar su dependencia tecnológica con esa potencia.** Confiamos en que ello no se haga **relegando iniciativas paneuropeas** porque como Ucrania enseña, ambas cosas son posibles.

Capítulo 8

CAPÍTULO 8.

CONCLUSIONES Y RECOMENDACIONES

8.1 Contexto

El presente capítulo del informe pretende extraer del análisis efectuado en los capítulos anteriores un **conjunto limitado de las conclusiones más relevantes obtenidas** del informe realizado sobre el **uso de la inteligencia artificial (IA) en defensa**.

Para cumplir el objetivo, el Grupo de Trabajo (GT) ha realizado un esfuerzo para **seleccionar y reducir estas conclusiones** en función de dos criterios: por un lado, aquéllas que reflejen mejor la **situación europea** desde la perspectiva de defensa y, por el otro, trasladando al **contexto español** aquéllas consideradas más relevantes o con mayor impacto previsible en España.

Esta decisión se ha adoptado aun teniendo en cuenta que el informe contiene información de la situación y uso de la IA en aplicaciones militares que son válidas en otros entornos geográficos. Además, otros muchos aspectos de interés particular permanecen en el contenido de los diferentes capítulos del informe.

Asimismo, a partir de las conclusiones de este capítulo, se ha extraído **un conjunto reducido de recomendaciones de actuación** con el objetivo y pretensión de que sean útiles e implementables para mejorar el posicionamiento de la Unión Europea en el uso avanzado de la IA en el ámbito de la defensa y su posible traslación a la situación del sector de la defensa española y su mejora en los próximos años.

Los autores son conscientes de que **disponer de la capacidad para hacer realidad en el ámbito de la defensa las recomendaciones propuestas es un proceso complejo** que requiere una **voluntad política**, un **esfuerzo de inversión** continuado en el tiempo, y una **participación** de diversos tipos de actores a diferentes niveles de la sociedad para que puedan llevarse a cabo.

Con objeto de facilitar la toma de decisión sobre la puesta en marcha de las recomendaciones identificadas, se ha realizado una **valoración cualitativa de su complejidad, coste, urgencia y ámbito de actuación**, así como un **análisis de sus interdependencias** teniendo como horizonte temporal para cumplir sus objetivos el año 2030.

Muchas de las conclusiones y recomendaciones incluidas en el presente capítulo sobre el uso de la IA pueden tener también **relevancia en otros ámbitos afines a la defensa** como es el de la **seguridad** estrechamente conectado, y parcialmente, en el **industrial**, aunque no hayan constituido el foco principal del informe.

Finalmente, se asume que **la evolución de las tecnologías de IA es muy rápida** como también lo es la forma en la que se adoptan en diversos ámbitos de la defensa; por este motivo, tanto las **conclusiones** como **las recomendaciones de actuación** derivadas deberán **revisarse periódicamente** para asegurar su pertinencia en función de los resultados obtenidos en su puesta en marcha.

8.2 Conclusiones

Seguidamente, se extraen algunas **conclusiones desde la perspectiva de cada una de las dimensiones empleadas en la elaboración del informe**. Posteriormente, se analizarán las **relaciones entre ellas** en el contexto de la Unión Europea (UE), con referencia a España cuando sea apropiado.

8.2.1 Conclusiones sobre la dimensión científico-tecnológica de la IA

La descripción de la **dimensión científico-tecnológica de la IA** en el informe elaborado ha pretendido dar cuenta de una amplia panorámica en la que su desarrollo abarca muchos aspectos. Todos ellos, ya sea de forma directa o indirecta, afectan al sector de la defensa, como corresponde a una **tecnología dual de carácter habilitador**.

Las siguientes **conclusiones** seleccionadas reflejan aquellos **avances o barreras** actuales en el desarrollo de la IA y su evolución a lo largo de la presente década que tienen o tendrán **mayor relevancia en el sector de la defensa**.

1. Con el desarrollo y adopción de sistemas basados en la IA se ha entrado en una **nueva fase del proceso de digitalización de la sociedad** que complementa, se desarrolla y se apoya sobre las anteriores fases desde las últimas décadas del siglo XX con un impacto creciente sobre la sociedad en todos los países.

Se trata de un proceso acelerado y continuado de digitalización **que también afecta al sector de la defensa**, tanto en su adopción por las empresas generadoras de productos y servicios de uso militar en los procesos de desarrollo y fabricación, hasta su utilización final por las propias fuerzas armadas en el ejercicio de sus misiones.

2. **El camino hacia la consecución de una IA general no está claramente definido** ni asumido como un hecho cierto a medio o largo plazo. Persisten diferencias significativas en las opiniones de los expertos sobre si será posible o no su consecución en el futuro.

Probablemente, alcanzar una IA que supere al ser humano en todas las facetas requeriría **avances disruptivos en la tecnología de IA**, no previsibles en este momento. De lo que

sí se dispone es de múltiples y continuadas **mejoras incrementales de los sistemas de IA estrecha**, focalizados en muchos tipos de problemas o dominios de aplicación concretos que se han incorporado en las aplicaciones disponibles actualmente; en muchos de estos ámbitos de aplicación los sistemas de IA existentes ya superan en prestaciones (volumen de datos manejados, velocidad en la toma de decisiones, etc.) al ser humano medio. Este enfoque pragmático es el que se emplea en la aplicación de la IA a problemas específicos de índole militar.

3. La IA actúa como una **tecnología habilitadora de carácter dual** en todos los dominios socioeconómicos, con aportaciones cruzadas entre ellos, pero en el que el volumen de inversiones y el tamaño del sector civil está actuando de motor fundamental para impulsar su desarrollo.

El **impulsor principal del desarrollo científico y tecnológico de la IA** en las últimas dos décadas descansa en las inversiones efectuadas en el sector civil por entidades públicas y privadas. Sin embargo, es en el sector de la defensa, con peculiaridades propias muy relevantes en su adopción, sobre el que se ha focalizado el presente informe, conscientes de que, en muchos casos, se basa en la **adaptación de un producto o servicio en el mercado civil para su uso en el sector de la defensa o viceversa** con el fin de aprovechar el esfuerzo realizado

4. La **progresiva integración de algoritmos de IA** para proporcionar funcionalidades clave de casi todos los productos y servicios empleados por las fuerzas armadas hará que **su uso en defensa será más transparente al usuario final**.

El fenómeno de la **transparencia de la tecnología de IA para el usuario final** no es exclusivo del sector militar, pero en este caso, la integración transparente de la IA en todo tipo de sistemas militares hace que **el usuario final pueda ser menos consciente de sus implicaciones**. Por este motivo, los sistemas de inteligencia artificial aplicados al ámbito militar deben ser capaces de explicar sus conclusiones para asegurar la transparencia, la confianza y la responsabilidad en su uso, especialmente en contextos críticos. Todo ello ha de complementarse con la formación de mandos y personal militar, así como el establecimiento de normas y procedimientos de uso claros y explicables que deben ser prerequisites para su adopción por las fuerzas armadas.

5. La **necesidad de disponer de volúmenes masivos de datos**, estadísticamente significativos y específicos del entorno de trabajo para el entrenamiento de los modelos fundacionales se ha convertido en un **factor esencial dada la relación directa entre la calidad de los datos y la validez de los resultados**, así como entre la cantidad de datos de entrenamiento y las necesidades de cómputo que deben cubrirse mediante hardware especializado.

Existe una relación directa entre la cantidad de datos de entrenamiento y las necesidades de cómputo que deben cubrirse mediante hardware especializado. Este factor **afecta tanto a las técnicas de aprendizaje automático (ML) como a las de aprendizaje profundo (DL)**, incluyendo la IA generativa que se basan en **aprendizaje supervisado**. Otras técnicas como el **aprendizaje por refuerzo** solo se pueden aplicar en entornos muy controlados y sin riesgo, lo que las hace poco utilizables en situaciones de combate, sí siendo válidas para entrenamiento.

6. Los **sistemas multiagentes**, formados por múltiples agentes de IA coordinados entre sí, permiten abordar problemas reales orientados al apoyo al ser humano para el desarrollo de funciones complejas, con lo que se acelerará y extenderá el uso de la IA en la sociedad al resolver problemas reales con ventajas significativas derivadas de su uso.

En el caso de los sistemas de defensa su utilización implicará el **despliegue acelerado de agentes de IA que han de coordinarse en todos los niveles operativos de las Fuerzas Armadas**, lo que conlleva la modificación profunda de muchos de los procesos, tanto tácticos como estratégicos, utilizados actualmente y contribuye a justificar el aparente retraso en su adopción en comparación con los ámbitos civiles (salvo en el caso de conflictos militares de alta Intensidad en el que los riesgos pueden estar subordinados a la supervivencia).

7. La **creciente importancia del hardware especializado para IA**, tanto para el desarrollo de **sensores inteligentes** (p.ej. para computación en el borde) y su interconectividad en las **redes militares de Internet de las cosas** como para el entrenamiento de modelos de IA generativa y la generación de inferencias, ha hecho que su **acceso y control se haya convertido en un factor clave** en la actual batalla geopolítica y tecnológica.

Esta situación implica la necesidad de disponer por parte de la industria, de los conocimientos necesarios para **diseñar y desarrollar circuitos integrados y sensores** avanzados desde la fase de diseño a la de fabricación o, en su defecto, asegurar la existencia de acuerdos estables para su provisión a través de **proveedores confiables** de otros países fuera de la UE, así como disponer por parte de las Fuerzas Armadas de la capacidad para adoptarlos.

8. La fabricación de los modelos más avanzados de las **unidades de procesamiento gráfico (GPUs)** se ha convertido, en el ámbito de la IA, en un **factor crítico para la IA generativa**; su disponibilidad emerge como un **potencial cuello de botella**, y se sitúa en el eje de múltiples restricciones y condicionantes en su exportación para determinados países.

Esta situación se mantendrá en el futuro con mejoras continuadas e incrementales en las prestaciones de los chips procedentes de un número reducido de proveedores que dispongan de las herramientas software adecuadas para la implementación eficiente de los algoritmos de IA en chips especializados (GPUs, FPGAs y ASICs) y de capacidades de fabricación propias o de empresas especializadas. Es probable que al final de la presente década se pueda disponer de una nueva generación de **chips neuromórficos** potentes, con mucho menor consumo, adaptados a la ejecución de algoritmos de redes neuronales.

9. La **IA generativa multimodal** ha madurado muy rápidamente siendo capaz de generar información de datos, texto, voz, imagen o video **muy difícil de distinguir de la realidad**, este hecho genera desinformación y dificultades en su gestión y uso que son críticas en áreas de aplicación de seguridad y defensa.

El uso de la IA generativa multimodal ha crecido rápidamente en sistemas de toma de decisión en el caso de la **guerra híbrida** y en el de la guerra **cognitiva**, adquiriendo una dimensión operativa de gran relevancia. Este uso se produce en un contexto de crecimiento elevado de los **ataques cibernéticos** y del lanzamiento de **campañas de desinformación** provocadas por agentes estatales o paraestatales.

10. Persisten problemas técnicos relevantes en el uso de sistemas de IA derivados del **problema de “caja negra”, de los sesgos y las “alucinaciones” de los algoritmos en los procesos de inferencia** de la inteligencia artificial generativa en aplicaciones derivadas del empleo de modelos grandes de lenguaje (LLM) lo que dificulta su uso en aplicaciones de defensa.

Estos problemas suponen una **barrera para su uso en defensa**, por lo que deberán ser evaluados con criterios objetivos antes de proceder a su adopción en sistemas críticos de decisión en los que es necesario conocer las razones que conduce a una determinada respuesta del sistema de IA militar; sobre todo en aquéllos **con potenciales consecuencias letales**.

11. La necesidad de **reducir los consumos energéticos y computacionales** necesarios para el entrenamiento y para el cálculo de inferencias ha motivado y acelerado los avances actuales para disponer de **modelos de lenguaje (más) pequeños y eficientes** para su uso en dominios concretos, como pueden ser algunos de carácter dual o con restricciones contextuales como los empleados en el espacio.

La proliferación de modelos pequeños de lenguaje puede ofrecer oportunidades de **entrenamiento de modelos con datos de interés militar**. Este proceso implica también la **reducción de las necesidades computacionales y energéticas** de los centros

de procesos de datos relacionados con el entrenamiento de modelos de IA o para la ejecución de algoritmos pre-entrenados en dispositivos finales de usuario.

12. La **integración de la IA con la neurotecnología** es aún incipiente, al tratarse de una tecnología inmadura, pero se producirá durante la próxima década con potenciales disrupciones en la sociedad durante la próxima década y con creciente aplicación en defensa.

La convergencia de la IA con la **neurotecnología** ha avanzado considerablemente, aunque **su uso fuera del ámbito médico es aún limitada**. Su potencial para facilitar el **incremento de las capacidades cognitivas** del ser humano, y su aplicación a personas sanas, le confiere una relevancia potencial en el ámbito de la defensa en el que ya trabajan todas las potencias tecnológicas.

13. La **integración de productos y servicios basados en IA con otras tecnologías**, como las **tecnologías cuánticas**, constituirá la base de la próxima ola de disrupciones tecnológicas en el sector de la defensa.

Dado que algunas de las tecnologías potencialmente implicadas no están **maduras**, será necesario disponer de programas de carácter experimental que permitan **valorar su utilidad potencial**, y, a través de ellos, **acelerar el proceso de maduración** de productos duales emergentes multitecnológicos.

Los tres ámbitos tecnológicos principales de las **tecnologías cuánticas** relacionadas con sistemas de computación, comunicaciones y sensórica basada en principios cuánticos, tienen ritmos de desarrollo diferentes en su adopción en defensa. Esta integración puede llegar a formar parte durante la próxima década de la denominada **“guerra cuántica inteligente”** con el uso combinado de las tecnologías cuánticas con la IA.

8.2.2 Conclusiones sobre la dimensión socioeconómica de la IA

Las siguientes conclusiones sobre la dimensión socioeconómica de la IA reflejan un **mercado creciente y muy dinámico** como parte del proceso de digitalización en el que la UE no posee el liderazgo. Se trata, además, de un **mercado dual** con la entrada de empresas de otros sectores ajenos a la defensa, y de la creación de múltiples startups con tecnologías y soluciones de IA disruptivas.

1. El **mercado global de la IA sigue creciendo** con tasas interanuales (CAGR) muy elevadas; sobre todo, en áreas como las del aprendizaje automático, la IA generativa y los sistemas de agentes inteligentes.

No es extraño, por ello, que el dominio de la IA y su convergencia con otras tecnologías emergentes forme parte de la **batalla por la supremacía tecnológica entre grandes potencias** que destinan recursos crecientes a su desarrollo y despliegue. Estos ritmos de crecimiento para el sector de la defensa son igualmente elevados, impulsados por los crecimientos presupuestarios en defensa y seguridad decididos por muchos países.

2. **El liderazgo en el desarrollo y uso de la IA** con una influencia global en la economía de los países occidentales sigue en manos de **Estados Unidos**, tanto en términos del volumen de mercado alcanzado como en el de la valoración bursátil de sus grandes empresas digitales en todos los eslabones de la cadena de valor.

Esta situación se ve agravada en Europa por el **impacto** para los ciudadanos europeos que ya tienen las grandes **empresas digitales de Estados Unidos en la provisión de servicios en la nube y en redes sociales**. Debe tenerse en cuenta que para sectores donde la dualidad sea un factor clave, es probable que se consolide una **fragmentación del mercado de IA en bloques o áreas de influencia de las grandes potencias**, e incluso de los espacios de datos empleados para el entrenamiento de los modelos cuando primen criterios militares y de seguridad.

3. **China** se ha convertido en muy poco tiempo en uno de los **países líderes en el desarrollo científico y tecnológico de la IA**, ya sea medida en el porcentaje de patentes, en el crecimiento de publicaciones científicas o en el volumen de mercado alcanzado; todo ello, en conjunto, implica la **reducción gradual de su brecha con Estados Unidos**.

China ha podido ya alcanzar a Estados Unidos en varias áreas de aplicación de la IA como son las de **reconocimiento de imágenes** y desarrollo de **modelos de lenguaje eficientes**, apoyado por la emergencia de múltiples startups con enfoques disruptivos, financiadas por fondos gubernamentales. El potencial uso dual de prácticamente todos los productos generados está alineado con el concepto de **fusión militar-civil** preconizado por el gobierno chino desde hace años. Debe tenerse en cuenta que el enfoque/estrategia de China no se orienta hacia el desarrollo del mercado, sino que el foco se sitúa en lograr el objetivo político deseado, a cualquier coste.

4. Las **sanciones y restricciones impuestas a China por Estados Unidos** para la exportación de equipos de fabricación de semiconductores o de circuitos integrados empleados en el entrenamiento de grandes modelos de lenguaje o para la generación de inferencias **ha impulsado y acelerado el desarrollo propio de tecnología de IA en China**.

La respuesta de China a la imposición de sanciones a la exportación e importación de productos tecnológicos ha estimulado el **desarrollo de capacidades nacionales**. Por

este motivo, empresas chinas han conseguido obtener resultados muy apreciables en comunicaciones móviles, entrenamiento de LLMs o sistemas de armas sin necesidad de utilizar las versiones más potentes de los chips de IA o mediante el acopio y adquisición a través de terceros países de estos chips realizado en los dos últimos años.

5. Las empresas del sector de defensa han asumido el **carácter dual de la inteligencia artificial** y están acelerando su inclusión en multitud de productos militares colaborando con empresas digitales, adaptando productos civiles y compitiendo con empresas del resto del mundo.

Las empresas europeas siguen la misma tendencia, aunque creciendo lentamente, y manteniendo la dependencia de componentes y subsistemas básicos de IA con otros países, lo que ha llevado a **replantear el marco de alianzas estratégicas de la UE** con el objetivo de mejorar la resiliencia de su cadena de provisión relacionada con la IA, y apoyar la generación de capacidades propias.

6. La adopción de la IA en el sector de la defensa empieza a extenderse no solo por parte de **grandes empresas digitales** que se aprovechan de la dualidad de uso para su integración en productos y servicios digitales, sino también por el **creciente papel jugado por multitud de empresas startups muy especializadas**.

El surgimiento de **startups con soluciones disruptivas** basadas en el uso de la IA que están siendo experimentadas y probadas por las Fuerzas Armadas de muchos países, junto al mejor acceso a fondos de capital riesgo y de ayudas de las administraciones públicas, está actuando como **factor de aceleración del proceso de innovación dual de la IA**.

7. El esfuerzo en el desarrollo y adopción de IA generativa que lleva a cabo la Unión Europea es creciente, pero no parece ser suficiente para poder asegurar un papel de liderazgo a nivel mundial en los próximos años si no se **aceleran fuertemente las inversiones** y se asegura la disponibilidad de **recursos humanos**.

La UE sigue manteniendo **debilidades significativas en varios niveles de la cadena de valor de la IA**, combinado con otras en el sector de los semiconductores. Además, su esfuerzo inversor global es menor y está fragmentado en los diversos Estados miembros, comparado con las estrategias de sus principales competidores (China y Estados Unidos).

8. La UE no cuenta con **grandes empresas digitales en la generación de productos y servicios basados en IA** que le permitan imponer sus criterios, productos y servicios a usuarios de todo el mundo frente a sus competidores, de mucho mayor tamaño y que están fuertemente apoyadas por sus respectivos gobiernos.

La **debilidad europea actual en la fabricación de semiconductores avanzados** se extiende a la fabricación de **circuitos integrados específicos para IA** (como GPUs, FPGAs y ASICs), a la disponibilidad de **plataformas software en la nube**, y a disponer de **grandes modelos de lenguaje (LLM)** que hayan alcanzado cuotas de mercado significativas a nivel mundial que sirvan de base al desarrollo de aplicaciones finales de usuario.

9. Las **start-ups europeas de IA tienen problemas de financiación para su crecimiento en Europa** y corren el riesgo de que en su proceso de escalado para poder competir en los mercados globales sean adquiridas o controladas por entidades no europeas en sucesivas rondas de inversión

El riesgo más común de las startups europeas en el ámbito de la IA es que sean adquiridas por otras **grandes empresas no europeas** y que migren a Estados Unidos para continuar su proceso de escalada. Además, **dependen en su decisión de futuro de las estrategias de rentabilidad de las inversiones de fondos de inversión especializados**, muchos de ellos no europeos, que han entrado en su capital en diferentes rondas de inversión. Esta situación es especialmente preocupante en aquellas startups que desarrollan productos o servicios para el mercado de defensa.

10. El **valor de los ecosistemas europeos de innovación centrados en la IA existentes** es creciente, con la participación como impulsores de grandes empresas y administraciones públicas comunitarias, nacionales y regionales que asumen la necesidad de incrementar la **interacción estable** entre actores mediante políticas, programas e instrumentos de financiación adecuados.

En el ámbito de la defensa, este proceso es menos evidente por sus connotaciones de seguridad y una mentalidad menos abierta de empresas y administraciones públicas, aunque empiezan a surgir núcleos de ecosistemas innovadores focalizados, apoyados por programas de adquisiciones militares y de I+D **en varios países de la UE**, aunque primando una perspectiva nacional.

11. A pesar de que sigue siendo Estados Unidos el país que posee **los fondos de inversión en defensa** dotados con un volumen mayor de recursos, nuevos **fondos** están creciendo y especializándose en defensa y seguridad en diversos países europeos, tanto en la fase de puesta en marcha como en la fase de escalado de nuevas empresas tecnológicas.

Esta situación también ha empezado a observarse en España, con la creación de fondos de inversión especializados en defensa y seguridad que cuentan con una fuerte **implicación de agencias públicas de financiación junto a capital privado en las rondas iniciales de financiación**. Esta situación se apoya en la presencia de grandes fondos

de inversión corporativos, ya sean nuevos o con la puesta en marcha de vehículos específicos de financiación dual en otros fondos preexistentes.

12. La **industria de defensa española está incorporando la IA** tanto en el proceso de generación de productos mediante el uso de **técnicas de ingeniería digital** centrada en datos y simulación (por ejemplo, con la generación de gemelos digitales) utilizando la IA como un factor esencial para el incremento de la funcionalidad y flexibilidad de sus productos.

El uso acelerado de técnicas de **gestión integrada de datos** y el uso más incipiente de **gemelos digitales** y de **fabricación aditiva 3D**, con objeto de reducir los ciclos de desarrollo y facilitar los de operación y mantenimiento posterior, se ha extendido entre todas las grandes empresas contratistas de programas de defensa.

13. Las **limitaciones de tamaño de la industria de defensa española** pueden impedir jugar un papel de liderazgo mayor en los grandes programas de armamento que se pondrán en marcha en la Unión Europea en relación con la estrategia de fortalecimiento de la industria hacia 2030 (*Readiness 2030*) y los compromisos de inversión adicional de los Estados miembros en adquisiciones de defensa.

Las decisiones adoptadas por la UE y los Estados miembros de **incrementar los recursos para el desarrollo y adquisición de sistemas de defensa** que cubran las brechas identificadas en la UE suponen una oportunidad en los próximos años para **fortalecer la industria de defensa europea y su competitividad en los mercados globales**. Un porcentaje relevante de la **funcionalidad de estos sistemas dependerá de la incorporación de tecnologías de IA**.

14. Desde la perspectiva de la UE, existe una oportunidad para fortalecer el desarrollo de la IA como tecnología dual **priorizando este enfoque en las convocatorias públicas y licitaciones de las administraciones públicas**, cuya normativa debe adaptarse para acelerar el ciclo de innovación.

El inminente comienzo del proceso de elaboración del **nuevo Programa marco de investigación e innovación de la UE** (Horizonte Europa 2028-2034), del programa sucesor del actual **Fondo Europeo de Defensa** como parte del Fondo de Competitividad, o los de la **Agencia de Defensa Europea** o el de la **Agencia Europea del Espacio** constituyen conjuntamente una oportunidad para el desarrollo de productos y servicios inteligentes duales. Ello depende de un incremento significativo de los recursos comunitarios y del fortalecimiento de las sinergias entre ellos y con los Estados miembros con el fin de incrementar la soberanía tecnológica europea en IA.

Debe tenerse en cuenta que el conflicto de Ucrania ha mostrado la **necesidad de facilitar ciclos rápidos de innovación**, como se ha visto en el campo de drones y de ISR. Esta es una capacidad que no puede basarse en convocatorias públicas de los organismos internacionales con los procedimientos existentes en la actualidad, y requiere llevar a cabo **procesos sustanciales de simplificación administrativa y acortamiento de plazos**.

15. El papel de los **estándares y normas industriales** (tanto *de iure* como *de facto*) de productos de IA, así como los procesos de **certificación de sistemas basados en IA**, son elementos clave para conseguir una rápida expansión del mercado de **sistemas inteligentes de defensa interoperables** a nivel internacional.

Todavía nos encontramos en una fase no consolidada en la que no existen muchos estándares específicos relacionados con la IA en el ámbito de la defensa, ni procedentes de organismos internacionales, ni tampoco por parte de la OTAN (STANAGs). En 2024, en la Estrategia de IA revisada de la OTAN, se decidió establecer un *marco común de pruebas, evaluación, verificación y validación de IA (TEV&V)* en toda la Alianza para garantizar la adopción responsable de la IA.

8.2.3 Conclusiones sobre la dimensión táctica, operativa y estratégica del empleo de la IA por las Fuerzas Armadas

El informe realizado ha presentado un panorama en el que **la introducción de la IA en el campo de batalla se acelera alentado por la persistencia de conflictos militares de alta intensidad**. Aunque en este terreno, el uso de información no clasificada puede llevar a engaño sobre el uso y eficiencia real del empleo de la IA por los diferentes ejércitos, sí existen **grandes tendencias** que son las abordadas en el capítulo. De ellas se han extraído las **siguientes conclusiones**.

1. Se está produciendo una **evolución paulatina hacia un campo de batalla inteligente** enmarcado en un **proceso continuo de digitalización** apoyado por la adopción de la IA que seguirá siendo muy rápido e intenso durante toda la presente década.

Esta evolución, sin embargo, está siendo **más lenta en su despliegue en el sector de la defensa que en los ámbitos de uso civil**, dada la relativa **inmadurez** de las tecnologías implicadas como por los riesgos percibidos para poder delegar en ellas funciones críticas, así como por la necesidad de asegurar la **coexistencia** con otros muchos sistemas militares preexistentes.

En todo caso, **el desarrollo de sistemas militares basados en IA sigue alimentando el despliegue de las armas “cinéticas”** que incorporan otras tecnologías críticas, como es el caso de la **robótica** alrededor de sistemas autónomos (p.ej. drones aéreos, terrestres y marítimos).

2. La **búsqueda de la superioridad en las fuerzas de combate** obliga a experimentar con soluciones tecnológicamente inmaduras y acelerar la innovación tecnológica, requiere mantener una estrecha interacción entre las Fuerzas Armadas, las empresas, centros de investigación, y las universidades que permitan su integración en futuras estrategias y tácticas de combate.

Este proceso se ha acelerado en los últimos años mediante el empleo de soluciones de IA en múltiples áreas apoyadas en la **captura y análisis de datos cercana al tiempo real procedentes de múltiples sensores**, así como un uso creciente de **datos sintéticos**. Las experiencias derivadas de ambos bandos en el conflicto de Ucrania señalan las ventajas y las limitaciones en su adopción, así como su relevancia para adaptar tácticas y estrategias de combate y alcanzar la superioridad militar.

3. El uso de **sistemas de IA autónomos o semiautónomos dentro de cadenas de armas letales es tecnológicamente factible**, ya sea en el caso de que su uso esté limitado al proceso de identificación y selección de objetivos como en su neutralización directa o indirecta.

Este uso parece que se acelerará durante la presente década con la emergencia o continuación de **conflictos militares de alta intensidad** en los que el empleo de IA en sistemas autónomos o semiautónomos con niveles de inteligencia crecientes se ha convertido en un **factor clave para asegurar la superioridad en el combate**.

4. La necesidad de contar con **datos de calidad adaptados al dominio de la aplicación, ya sean reales o generados sintéticamente**, y protegidos contra los ciberataques, es un requisito previo para la adopción de la IA en todos los sectores socioeconómicos. En el caso de la defensa, persisten los problemas para disponer de grandes volúmenes de datos obtenidos en condiciones reales, lo que hace aún más necesario el uso de datos generados.

Esta necesidad está siendo impulsada por las administraciones públicas o grupos de empresas, creando los denominados “**espacios de datos compartidos**”. Sin embargo, una barrera para ello en el ámbito de la defensa es que muchos de los conjuntos de datos relevantes para el entrenamiento de sistemas de aprendizaje automático o grandes modelos de lenguaje están **clasificados** y no se comparten fuera de las organizaciones militares. Por este motivo, **el uso de datos sintéticos se ha generalizado**. El problema del *envenenamiento de datos* y las vulnerabilidades en el dominio ciberespacial le añaden una complejidad adicional por sus potenciales efectos.

5. El **papel del ser humano en el bucle o sobre el bucle de decisión** se ha convertido en un factor clave desde el punto de vista técnico y táctico de los sistemas de IA

empleados en defensa, al margen de las **consideraciones éticas** y de la evolución de las **reglas de enfrentamiento** que su uso pueda implicar o motivar.

La aceleración del **desarrollo tecnológico de sistemas de armas letales autónomas (SALA)** permitiría su incorporación acelerada a los ejércitos de todos los Estados miembros lo que, en el caso de suceder, implicará modificaciones profundas en la forma de conducir las operaciones militares y en su impacto en la población.

En este contexto, será cada vez más común que las **plataformas tripuladas** (p.ej. aviones, buques, tanques) vayan acompañadas de **vehículos no tripulados** bajo su control con un nivel creciente de inteligencia para poder llevar a cabo misiones más complejas.

6. En el ámbito **de la guerra electrónica y el control del espacio radioeléctrico** la IA juega un papel creciente. Este control se ha convertido en un factor clave en los conflictos del siglo XXI, motivados por la **expansión de las amenazas, los conflictos y la guerra híbrida** superpuesta a los conflictos militares convencionales.

La creciente complejidad de los **ataques potenciales frente a la información transmitida por el espacio radioeléctrico** en aplicaciones militares (señales de navegación, información de mando y control, datos satelitales, etc.) obliga a desarrollar nuevas técnicas de **guerra electrónica inteligente** más sofisticada y capaz de detectar amenazas en todo el espectro de frecuencias. En este contexto, el uso de la IA es creciente para asegurar el procesamiento de datos en tiempo real imposible de conseguir por operadores humanos, y su posterior interpretación.

7. La **generación automática de campañas de difusión de desinformación y de narrativas** orientadas a entidades o sectores específicos de la población basados en herramientas de IA se han extendido y se encuentran en manos de actores estatales o no estatales como parte de la guerra cognitiva.

Se trata de una situación característica propia de un mundo menos seguro en el que **el dominio de la información y la narrativa es esencial para determinar el curso de las operaciones militares en guerras híbridas y cognitivas**. En especial, el uso de la IA generativa está dando lugar a la emergencia de herramientas de IA especializadas para la generación de contenidos y la difusión dirigida en redes sociales.

8. La UE y sus Estados miembros disponen de sistemas potenciados por IA con herramientas y procedimientos para **detectar y contrarrestar noticias falsas y narrativas intencionadas procedentes de otros países**.

Estas herramientas y procedimientos están ligadas a la necesidad de los gobiernos de **contrarrestar el crecimiento de la injerencia y la manipulación** de otros países:

situación que ha obligado a crear protocolos de respuesta rápida, unidades y procedimientos especializados de intercambio de información entre gobiernos aliados, como ya sucede en el caso de la UE.

9. **El sector espacial se configura como un sector dual** en el que tanto usuarios públicos como privados pueden compartir plataformas satelitales, sistemas de lanzamiento y seguimiento, datos obtenidos, así como disponer de herramientas de IA específicas para su análisis.

Las plataformas satelitales **individuales** o formando parte de **constelaciones** son empleadas en aplicaciones civiles y militares de observación, comunicaciones y navegación. Aunque su estructura puede ser dual, puede requerirse el desarrollo de **cargas útiles especializadas** para cada uno de los dominios.

La profusión del lanzamiento de **satélites para aplicaciones militares** o susceptibles de aplicarse a ellas, como ejemplifica el caso de Starlink en Ucrania, los ha convertido en activos esenciales para todos los gobiernos y, con ello, han adquirido una relevancia estratégica para todos los países que dependen de ellas de forma creciente.

10. **La IA tiene un valor creciente para gestionar eficazmente un dominio espacial más poblado**, en términos de objetos espaciales y fragmentos, sobre todo, en determinadas órbitas bajas, lo que es susceptible de ser empleado como objetivo militar contra activos espaciales de otros países.

El uso de **herramientas de IA para el mejor conocimiento de la situación del dominio espacial** (posición propia y de objetos espaciales cercanos, así como su caracterización) permite disminuir o gestionar los riesgos de **colisión** con restos de satélites o con otros elementos naturales, las **interferencias**, provocadas o no, en la navegación satelital, y la **protección** de los activos espaciales.

11. El desarrollo y adopción de **sistemas hardware de IA especializados en la operación de los activos espaciales** con el objetivo de reducir el consumo y mejorar la flexibilidad, se ha incrementado fuertemente. Esta evolución posibilita disponer de **mayor capacidad de procesamiento a bordo** y la ejecución autónoma de funciones más complejas.

El espacio constituye un **dominio dual de relevancia creciente** en el que la **automatización de operaciones** implica la necesidad de incrementar la capacidad de procesamiento a bordo para la ejecución de algoritmos de IA, el análisis de datos recabados de múltiples sensores y su transferencia a estaciones terrenas. El desarrollo y uso de chips especializados de mayor potencia y bajo consumo es un ámbito de creciente interés.

12. La UE y España se encuentran en una buena posición para la explotación del espacio mediante el **desarrollo de aplicaciones basadas en IA que exploten los datos generados por activos espaciales** y permitan mejorar con ello la soberanía tecnológica europea en la nueva generación de plataformas espaciales.

La experiencia acumulada por la *Agencia Europea del Espacio* y diversas agencias nacionales de espacio en los Estados miembros, junto a una profusión de nuevas empresas del sector espacial con integración de soluciones de IA permitirá mejorar la seguridad europea si se dotan o se les dota de recursos suficientes. España es un jugador relevante en el dominio espacial.

8.2.4 Conclusiones sobre la dimensión ética y regulatoria de la IA

El desarrollo acelerado de soluciones basadas en la IA no ha estado ajeno de **controversias y preocupaciones sobre las consecuencias derivadas de su uso**. Mucho más cuando este uso se produce en el ámbito de la **defensa y seguridad**. La discusión sobre los **aspectos éticos** asociados a un proceso de automatización que relega progresivamente al ser humano de la toma de decisión no está resuelta. Tampoco se dispone de **regulaciones adecuadas para el uso militar de la IA** ni es factible trasladar directamente las existentes en el ámbito civil, teniendo que circunscribirse, por ahora, al uso de directrices voluntarias. Las siguientes conclusiones reflejan el análisis realizado en el informe.

1. **No existe una regulación específica para el uso de la IA en defensa.** Solo existen directrices de desarrollo y uso voluntarias basadas en el **uso responsable de la IA en el ámbito militar** propuestas por diversos organismos, pero sin que se haya llegado a una aceptación global en todos los países.

Esta situación se combina con el hecho de que las regulaciones de IA para aplicaciones civiles tampoco están consensuadas y muchos países tienen enfoques diferentes basados en sus visiones histórico-culturales y su posicionamiento tecnológico en los mercados mundiales. En el caso de la UE se dispone de una *Regulación de IA* aprobada en 2024 que entrará plenamente en vigor en 2026 sin que, por el momento, haya sido adaptada para el desarrollo de sistemas de IA duales ni mimetizada en otros países (ni en otras regiones del globo, ni por agrupaciones multinacionales). Sin embargo, el Reglamento de la UE sobre IA podría utilizarse como base para el desarrollo de sistemas duales de IA.

2. La **disponibilidad creciente de sistemas inteligentes automatizados en niveles elevados que no requieren el concurso de un ser humano** tomando las decisiones necesarias, y que el desarrollo de la IA ya permite, implica asumir **riesgos éticos considerables**, sobre todo, en el caso del uso de **sistemas de armas letales autónomas o semiautónomas (SALA)**.

La UE debería ser consciente de que las normativas de uso de sistemas SALA deben ser consensuadas en lo posible a nivel global, estableciendo limitaciones a su desarrollo y uso. Si ese no es el caso, como sucede en la actualidad, se corre el riesgo de enfrentamientos asimétricos en relación con su utilización, pues pueden llegar no solo a los ejércitos de los Estados, sino a grupos paraestatales cuyas reglas de uso son impredecibles o no están sujetas al cumplimiento de normas internacionales.

3. **El desarrollo de productos basados en tecnologías duales por empresas de sectores ajenos al de la defensa** ha generado problemas derivados de la aceptación de proyectos de potencial utilidad militar por parte de su plantilla técnica, como ya ha ocurrido en el caso de grandes empresas digitales en Estados Unidos, al considerarse que no existía una aceptación previa y se **contravenían sus principios éticos**.

Esta situación puede agravarse en el futuro a medida que aumente el presupuesto y el continuo impulso civil para el desarrollo de la tecnología de IA implique que **más empresas fuera del mundo de la defensa** hasta ahora se involucren en el desarrollo de sistemas de defensa inteligentes.

4. Los problemas éticos de los sistemas militares de apoyo a la decisión basados en IA no pueden analizarse separadamente como sistemas aislados, sino por el **papel que asumen en la integración en cadenas letales ya sean automatizadas o no**.

Este problema ya ha surgido con el uso de herramientas de IA por parte de Israel en Gaza que, aunque no sean en sí mismas armas letales, sí permiten atacar objetivos previamente identificados por la herramienta con un porcentaje de casos erróneos o débilmente conectados.

5. Aunque hayan existido muchos esfuerzos por parte de **organismos internacionales** para conseguir un **uso responsable de la inteligencia artificial**, incluso en aplicaciones duales o estrictamente militares, sus resultados se limitan, por el momento, al objetivo de alcanzar un acuerdo global detallado y efectivo.

No se espera que esos acuerdos vayan más allá de la aprobación de un conjunto de **directrices voluntarias de aplicación** que los países firmantes acepten, pero sin que existan organismos internacionales que aseguren su cumplimiento como sí es el caso de los acuerdos existentes contra la proliferación de las armas nucleares.

6. Encontrar **el equilibrio entre una regulación protectora del usuario y un apoyo a la innovación no es sencillo**, y ese debate sigue abierto en el contexto de la Unión Europea en el proceso de implementación de su regulación de IA, pensada únicamente para aplicaciones civiles y no militares.

La UE deberá adoptar un enfoque flexible durante la puesta en marcha de la Regulación de IA, pero, asegurando interpretaciones coherentes en todos los Estados miembros, y adaptando periódicamente la regulación de IA a la evolución de la tecnología con el fin de asegurar su pertinencia.

7. La **integración progresiva de la inteligencia artificial con la neurotecnología** abre el camino a una nueva fase de los conflictos militares que genera problemas éticos específicos como son los de la **privacidad y de albedrío**, en el contexto de discusión de los **neuro derechos** y su aplicación al ámbito de la defensa.

El ámbito de la **neurotecnología aplicada a la mejora de las capacidades cognitivas humanas**, más allá de los usos médicos, tiene enormes implicaciones éticas en lo que supone alterar las capacidades de la especie humana. **Su desarrollo en el ámbito de la defensa se desarrolla con escasa transparencia** por parte de las potencias más avanzadas conocedoras de su relevancia potencial.

8. Un factor que condicionará el desarrollo y empleo de la IA en operaciones militares es la posible **confrontación militar entre adversarios con marcos éticos y morales diferentes en el uso de sistemas autónomos**.

Este factor puede **condicionar la autolimitación en el uso de determinadas armas inteligentes para no quedar en desventaja frente al adversario** lo que supone que el uso de la IA en estos contextos deberá limitarse, al menos, a llegar a compromisos de **“no primer uso”**, como ya ocurre en determinados países con el empleo de las armas nucleares.

9. Las **tecnologías de aumento de capacidades cognitivas**, más allá de lo que la especie humana permite en su biología, mediante la convergencia entre la neurotecnología con la IA, es un tema aún lejano en términos de adopción masiva, pero que, a la vista de su desarrollo acelerado, implicará un esfuerzo anticipatorio desde el punto de vista ético y regulatorio.

Dados los recientes resultados obtenidos en investigación básica, la **factibilidad tecnológica de la convergencia de la neurotecnología con la IA está más cercana** en el tiempo. También avanza rápidamente la utilización de técnicas de biología sintética sobre el tejido neuronal y su convergencia con la neurotecnología y la IA. Este proceso de **convergencia multitecnológica** obliga a pensar en las **consecuencias éticas y regulatorias derivadas** incluso muchos años por delante a que se hagan realidad.

8.2.5 Conclusiones sobre la soberanía tecnológica europea en IA

Un ámbito el que el informe ha dedicado atención es a la evaluación de la soberanía tecnológica europea en IA empleando diversos modelos. Se ha partido del convencimiento de que **lograr una autonomía estratégica relevante implica conseguir un nivel elevado de soberanía tecnológica**. Sobre esta hipótesis de partida se han desgarnado las siguientes conclusiones.

1. Dada la relevancia estratégica de la tecnología, el objetivo pretendido por la UE de **conseguir su anhelada autonomía estratégica implica incrementar su soberanía tecnológica**.

Este objetivo debe perseguirse, aun aceptando la imposibilidad de lograr una autarquía en ámbitos tecnológicos clave como lo es el de la IA. Para ello será necesario contar con **aliados fiables** para la UE a largo plazo y diversificar los proveedores de productos críticos.

2. Los Estados miembros de la UE dependen de **múltiples sistemas de defensa que incorporan funcionalidades de IA desarrollados localmente o procedentes de otros países cuya transferencia de conocimiento desde el proveedor es parcial**.

El **equipamiento militar** no desarrollado localmente en los países de la UE procede, en gran medida, de **Estados Unidos** y, en menor medida, del Reino Unido, Israel, Turquía, Corea del Sur y Japón. En el caso de los sistemas de armas avanzados, su adquisición suele implicar la **aceptación de condiciones restrictivas** y está sujeta a permisos de uso en diversos casos impuestos por los respectivos proveedores en concierto con los gobiernos de las empresas matrices.

El desarrollo futuro de sistemas de IA militares con un alto grado de soberanía tecnológica europea requerirá **establecer y financiar programas comunes público-privados apoyados en una voluntad política sostenida en el tiempo**, con prioridades acordadas a largo plazo.

Ese será un proceso largo y complejo, puesto que **las competencias en política de defensa recaen en los Estados miembros**, más allá de la coordinación y el uso de recursos relacionados con la **política industrial** que pueda hacerse desde la UE.

3. No será posible alcanzar un nivel suficiente de soberanía tecnológica si la **fragmentación del mercado europeo de defensa** se perpetúa en sistemas de armas que incorporen, de manera relevante, módulos de inteligencia artificial.

La velocidad a la que se está desarrollando la tecnología de IA y su convergencia con otras tecnologías emergentes relacionadas dificulta que la industria de un único Estado miembro de la UE posea todas las capacidades necesarias para un desarrollo autónomo de sistemas militares inteligentes. Por este motivo, **la cooperación tecnológica estable entre los actores de la industria de defensa en un mercado único europeo debe ser un objetivo político prioritario.**

4. Una parte relevante del continuo **incremento de la inversión en sistemas tecnológicos de la defensa** con respecto al PIB, acordado por los Estados miembros de la UE pertenecientes a la OTAN, debe destinarse a inversiones en **sistemas militares inteligentes interoperables**.

El proceso de implementación del acuerdo para aumentar el gasto en defensa en relación con el PIB acordado en la Cumbre de la OTAN de junio de 2025 debería **priorizar el desarrollo de sistemas de IA interoperables** con un mayor esfuerzo de la UE para reducir la dependencia de Estados Unidos

5. Las **startups con productos disruptivos de IA** encuentran problemas para la experimentación de soluciones en estados de madurez bajos (TRL 5-6) junto con las Fuerzas Armadas que aceleren el proceso de innovación y se adapten a los requerimientos de las Fuerzas Armadas de los Estados miembros de la UE.

La solución a estos problemas implica la creación de **instrumentos diferenciados de los sistemas de adquisición pública de tecnología** por parte de las AAPP y las modificaciones regulatorias que sean necesarias por parte de la UE y de sus Estados miembros. Al respecto, las medidas propuestas por el FEI para potenciar el emprendimiento en tecnologías profundas (*deeptech*), y otras políticas de innovación, en especial sobre compra pública innovadora, constituyen aportes concretos en esta perspectiva.

6. La **estrategia de simplificación administrativa** promovida por la UE deberá adaptarse con prontitud con objeto de reducir drásticamente los tiempos de los contratos de adquisición y mantenimiento de nuevos sistemas de armas que impliquen el uso de fondos comunitarios.

Aunque esta situación no sea exclusiva de la IA y afecte a otras tecnologías emergentes, se manifiesta de manera evidente en el desarrollo y adquisición de sistemas autónomos, en los que los avances son muy rápidos, como demuestra la situación en Ucrania.

A la luz de las conclusiones elaboradas tras el análisis de todas las dimensiones del informe, es evidente que **la UE se encuentra en un momento crítico en el que debe actuar con decisión para tomar el control de su propio desarrollo de la IA y asegurar su rápida adopción por parte de sus fuerzas armadas.** Otras grandes potencias tecnológicas con las

que compite han asumido esta realidad y priorizado el desarrollo y uso de la IA conscientes del papel esencial que juega en la búsqueda de la supremacía militar.

8.2.5.1 Escenarios posibles de soberanía tecnológica europea en IA

Identificación de escenarios

A partir de las conclusiones extraídas en la sección anterior, se han identificado y valorado **tres escenarios posibles para la UE en relación con el uso de la IA en defensa en el horizonte de 2030** que se detallan seguidamente. Somos conscientes de que se trata de **escenarios base** para promover la discusión y poder analizar en detalle, si se deseara, la situación existente en el conjunto de la UE o en algunos de los Estados miembros.

Los tres escenarios identificados se han denominado escenario **“optimista”**, escenario **“realista”** y escenario **“pesimista”**. La figura 8.1 indica, de manera sucinta, algunas características que definen cada uno de ellos. Las siguientes subsecciones los describen con un poco más de detalle.



Figura 8.1. Escenarios de la IA en defensa para 2030. Fuente: elaboración propia

Como se ha querido reflejar en la figura 8.1, consideramos que el **escenario realista podría ser alcanzado en 2030** por la UE si se asignasen los recursos necesarios y existiese una voluntad política adecuada mantenida a largo plazo. Contribuirá a ello el convencimiento de los Estados miembros de que **la conflictiva situación mundial obligará a la UE a coordinar mucho mejor sus actuaciones en defensa y hacer más factible los acuerdos** para la consecución de este escenario.

La necesidad de acelerar **la adopción de la IA en defensa no va a ser el eje fundamental, por sí misma, para la toma de decisiones** hacia ninguno de los escenarios. Sin embargo, sí va a **condicionar las prioridades y funcionalidades** de los programas, proyectos de desarrollo y productos que se pongan en marcha y adquieran.

Escenario optimista en 2030

El **escenario optimista** se basa en el supuesto de que **la UE se convierte en una potencia tecnológica mundial, liderando, junto a Estados Unidos y China, el desarrollo y uso de la IA en defensa.**

Este escenario se caracteriza por los siguientes rasgos definitorios:

- Creación de un **mercado único europeo para la defensa** que reduzca significativamente la fragmentación actual y maximice el resultado. Esto hará necesario realizar las modificaciones reglamentarias y consensos interpretativos necesarios en el marco de los Tratados de la UE para dar más responsabilidad a la Comisión Europea en la aplicación de la política de defensa industrial de la UE.
- Consecución de una **soberanía tecnológica elevada en la IA aplicada a la defensa**, desde la obtención de la capacidad de diseño y fabricación de hardware específico de IA, hasta el desarrollo de aplicaciones integradas en sistemas militares reduciendo al máximo las dependencias de proveedores no europeos.
- Puesta en marcha de programas comunitarios de I+D en defensa enfatizando la aplicación de la IA integrados plenamente con los programas nacionales y regionales de los Estados miembros.
- Emergencia de **grandes empresas europeas de IA en defensa** que han llegado a ser líderes mundiales en algunas de las áreas de aplicación.

Escenario realista en 2030

El **escenario realista** se basa en el supuesto de que **la UE se convierte en una potencia tecnológica relevante en el desarrollo y uso de la IA en defensa** con liderazgo en algún área concreta, pero dependiente de otras potencias en el resto de las áreas tecnológicas relevantes en IA.

Este escenario se caracteriza por los siguientes rasgos definitorios:

- La creación de un **mercado único europeo para la defensa** no ha cubierto todos sus objetivos, pero sí se ha producido una mayor sinergia de actuaciones, con la reducción

significativa de la fragmentación actual en algunas áreas prioritarias en las que se han puesto en marcha programas de defensa paneuropeos.

- Se han podido realizar algunas **modificaciones reglamentarias** para facilitar la adopción de acuerdos conjuntos en el ámbito de la defensa empleando esquemas de **cooperaciones reforzadas** coordinadas con la OTAN.
- Consecución de una **soberanía tecnológica limitada en IA aplicada a la defensa** con mejora de las capacidades de diseño de chips específicos de IA y el desarrollo de aplicaciones integradas en sistemas militares, aunque persiste la dependencia de proveedores externos de materias primas, componentes microelectrónicos y en capacidades de fabricación.
- Implementación de **programas comunitarios de I+D en defensa** con recursos limitados que hacen hincapié en la aplicación de la IA y están coordinados con los programas nacionales de los países que lo deseen.
- Fortalecimiento de la cooperación estratégica reforzada entre **grandes empresas nacionales de IA en defensa** para asegurar el liderazgo mundial en algunas de las áreas de aplicación de la IA.

Escenario pesimista en 2030

El **escenario pesimista** se basa en el supuesto de que **la UE no logra convertirse en una potencia tecnológica mundial en el desarrollo y uso de la IA en defensa** consolidándose su dependencia de otros países en varias áreas críticas.

Este escenario pesimista de carácter continuista de la situación actual se caracteriza por los siguientes rasgos definitorios:

- La UE tiene una **soberanía tecnológica limitada en IA para la defensa**, por lo que persiste su dependencia de Estados Unidos en grandes sistemas militares.
- **Los programas de I+D en materia de defensa son básicamente nacionales** con objetivos de independencia tecnológica nacional, aunque hay algunos proyectos cofinanciados con el presupuesto de la UE y contribuciones voluntarias de los Estados miembros.
- **No han surgido grandes empresas europeas con capacidades líderes de IA en defensa**, y la cooperación estratégica entre las empresas pertinentes sigue siendo muy limitada.

La siguiente sección pretende ofrecer, en base a las **conclusiones extraídas**, un conjunto de **recomendaciones de actuación** para que el **escenario realista** presentado pueda ser una realidad en 2030.

8.3 Recomendaciones de actuación

A partir de las conclusiones realizadas se propone un **conjunto reducido de recomendaciones de actuación** para la regulación, desarrollo y uso avanzado de la IA en sistemas de defensa que permitan incrementar su uso responsable **en el contexto europeo y alcanzar el escenario realista esbozado en la sección anterior**. Asimismo, cuando proceda, se analizará su posible adaptación e interés para España.

Aunque se hayan planteado de forma independiente, **las recomendaciones de actuación propuestas en relación con la IA no son totalmente disjuntas**; de hecho, conseguir a través de ellas un impacto elevado en la operatividad de las Fuerzas Armadas de los Estados miembros de la UE y una mejora sustancial de la soberanía tecnológica europea en IA puede requerir la **puesta en marcha simultánea y coordinada de varias de ellas**.

Estas recomendaciones de actuación se orientan tanto a actuaciones de las **Administraciones Públicas** (comunitarias y nacionales) como a la **industria de defensa europea** cuya actividad esté orientada a la generación de productos duales con un uso significativo de la IA dirigido a los mercados de la UE e internacionales.

Se ha pretendido, asimismo, elaborar una **valoración cualitativa** (no es posible realizar una valoración cuantitativa) de cada una de las recomendaciones propuestas en función de **cuatro factores básicos**:

- **Complejidad (baja, media, alta)**. Atiende a la dificultad de poner en marcha la recomendación, dada la necesidad de vencer condicionantes regulatorios, de estructura del mercado de defensa o de posicionamientos políticos.
- **Coste (bajo, medio, alto)**. Se refiere al volumen de inversiones que hay que asignar para poder poner en marcha la recomendación y lograr el impacto deseado
- **Urgencia (baja, media, alta)**. Relativo a la priorización relativa que debe darse a la recomendación para que se logre obtener los efectos deseados antes de 2030.
- **Ámbito (nacional, UE, internacional)**. Se refiere al ámbito de aplicación de la recomendación y sus efectos.

Los autores son conscientes de que el análisis detallado de estas recomendaciones debe implicar a muchos más actores españoles y, en algunas de ellas, europeos. Se trata, por tanto, de un proceso progresivo y paulatino. Con ello, las **recomendaciones de actuación propuestas** son las siguientes:

Recomendación R1. Priorización de la IA en los programas de defensa de I+D y en las adquisiciones militares de los Estados miembros con la visión de facilitar su uso dual.

La UE y los Estados miembros deberán incrementar el esfuerzo para acelerar el doble uso de la inteligencia artificial, estableciendo **prioridades específicas de IA en sus programas de investigación y adquisición públicos y facilitando el uso de sus resultados tanto en mercados civiles como militares.**

Esta recomendación debería considerarse específicamente en el proceso de negociación del **próximo programa marco de investigación e innovación de la UE** (HE 2028-2034) y del futuro **Fondo Europeo de Defensa** (como parte del *Fondo Europeo de Competitividad*), financiados en el Marco Financiero Plurianual (MFF) de la UE para el periodo 2028-2034. Este proceso deberá conseguir también el alineamiento y coordinación con los programas de investigación e innovación nacionales.

Valoración cualitativa:

- Complejidad: **media**. Pueden existir en el proceso negociador sensibilidades diferentes entre los Estados miembros que impliquen dificultades para llegar a un acuerdo del Consejo y Parlamento europeos, o en el ritmo de incremento de los presupuestos de defensa en el marco de los compromisos con la OTAN asumidos por los Estados miembros.
- Coste: **bajo**. La determinación de prioridades no conlleva un gasto en sí mismo ni afecta al volumen total de recursos previstos en los programas mencionados. Sin embargo, sí pueden suponer un **coste de oportunidad** asociado a un riesgo elevado de tener que tomar decisiones de este tipo en un entorno de información reducida y alta incertidumbre, fruto del constante desarrollo de la tecnología.
- Urgencia: **alta**. Aunque el acuerdo debe implementarse para su puesta en marcha en enero de 2028, la propuesta de la Comisión Europea deberá empezarse a discutir en el segundo semestre de 2025.
- Ámbito: **programas comunitarios y nacionales**.

Recomendación R2. Necesidad de crear un marco regulatorio común para el desarrollo y uso de la IA en defensa en consonancia con los principios y valores europeos.

Es necesario establecer lo más rápidamente posible un **marco regulatorio común para el uso de la IA en defensa** partiendo o no de la Regulación de la IA existente actualmente. Aunque las regulaciones o directivas estén legalmente limitadas a los Estados miembros, su uso puede extenderse voluntariamente a otros países aliados.

La adaptación del actual **Reglamento de la UE sobre la IA** para cubrir aspectos de doble uso no está claramente definida. Se trata de un proceso que podría llevarse a cabo de forma

paralela e independiente al impulso de una regulación específica para la IA militar utilizando, en su caso, un modelo de **cooperación reforzada** entre aquellos Estados miembros que lo consideren oportuno o, en su defecto, un conjunto homogéneo y coordinado de directrices de aplicación voluntaria.

Aunque la aplicación de las “regulaciones” (leyes europeas) estén legalmente limitadas a los Estados miembros, su uso puede extenderse voluntariamente, con las adaptaciones que se precisen a otros países alineados con la UE en aspectos de IA.

Valoración cualitativa:

- Complejidad: **alta**. Implica un acuerdo por codecisión (procedimiento ordinario legislativo común) en el caso de la modificación del actual Reglamento de IA. La creación de una nueva regulación limitada a la defensa podría hacerse por acuerdo del Consejo.
- Coste: **bajo**. Se trata de modificaciones regulatorias y no de la puesta en marcha de programas concretos. Los recursos económicos estarían ligados al marco financiero plurianual.
- Urgencia: **alta**. Los procesos de cambio regulatorio son lentos y es necesario definir el marco de actuación lo antes posible.
- Ámbito: **nacional**. Afectaría a todos los Estados miembros, y a la Comisión Europea en el marco de sus competencias.

Recomendación R3. Facilitar la experimentación del uso de la IA en las Fuerzas Armadas de los Estados miembros de la UE para acelerar su adopción.

Es necesario **facilitar la experimentación del uso avanzado de la IA en las Fuerzas Armadas de los Estados miembros** de la UE, de forma que permita evaluar la efectividad y los riesgos que su uso puede conllevar en aplicaciones ligadas a la toma de decisiones.

La experiencia obtenida de la rápida maduración y adopción de tecnologías disruptivas en el campo de batalla de Ucrania permite ver que es posible **reducir drásticamente los tiempos de desarrollo** si la experimentación en condiciones reales o próximas a ello se incorpora efectivamente en el ciclo de vida de su desarrollo y despliegue, y se adapta la normativa vigente para facilitarlo.

Su puesta en marcha puede implicar la **habilitación de espacios físicos y de espacios de datos compartidos** de defensa ubicados en cualquiera de los Estados miembros, pero accesibles a otros en condiciones preestablecidas. Sería posible aprovechar la red de centros de prueba desplegada en los Estados miembros del programa DIANA de la OTAN desplegada en los Estados miembros que tengan relación con la IA, la conectividad, la ejecución de aplicaciones en el borde, y la neurotecnología para crear redes de colaboración en el marco de la OTAN que permitan la experimentación distribuida y a escala de soluciones disruptivas.

Valoración cualitativa:

- Complejidad: **Alta**. La compartición de espacio y datos de manera estable en el ámbito de la defensa requiere llegar a acuerdos no sencillos al tratarse, parcialmente, de información clasificada.
- Coste: **medio-alto**. Dependiente del volumen de datos y de las características del espacio de experimentación que se desee poner en marcha. Puede suponer inversiones en campos de maniobra si se deseara disponer de amplias zonas sensorizadas.
- Urgencia: **media**. Debe tenerse en cuenta que la creación de espacios físicos de datos compartidos no es rápida, puesto que requiere llegar a acuerdos entre países. Por lo tanto, parece oportuno emplear un enfoque progresivo iniciado en algunas de las áreas identificadas como de mayor urgencia en un proceso de priorización común.
- Ámbito: **nacional**. Por ahora, se trata de sistemas nacionales permanentes, combinadas con “maniobras” en cortos periodo de tiempo en las que participen ejércitos de varios países. Utilizable para los países que alcancen, voluntariamente, un compromiso de cofinanciación de las actuaciones y procedimientos de uso.

Recomendación R4. Ampliar el ámbito de aplicación del Reglamento Europeo de Semiconductores (Ley de Chips) para abordar el desarrollo de chips de IA para la defensa.

El objetivo es que, en el menor tiempo posible, la UE disponga de una **cadena de valor de semiconductores para defensa** que le permita disponer de los chips específicos que requiere para el desarrollo de sus sistemas armamentísticos con el mínimo de dependencias externas.

Esta extensión de *Chip Act* es necesaria para incluir y dotar con recursos adicionales comunitarios diversas actuaciones orientadas a disponer de circuitos integrados de IA específicos para los sistemas de defensa con el mayor grado posible de soberanía tecnológica europea. Sobre la base de que uno de los pilares del Chip Act (Pilar 1) es la creación de *Líneas Piloto*, España podría impulsar una línea piloto de chips IA para defensa, así como la experimentación con chips fotónicos y neuromórficos, implicando con ello a la industria y a los grupos de investigación existentes en varias universidades y centros de investigación.

Valoración cualitativa:

- Complejidad: **alta**. Implicaría un cambio en la Regulación de la UE (*Chips Act*) y el lanzamiento de algún gran proyecto de interés europeo (IPCEI).
- Coste: **alto**. Supondría incrementar el esfuerzo procedente del presupuesto comunitario en el contexto de las siguientes perspectivas financieras y complementarse con recursos nacionales.
- Urgencia: **media**. Las acciones más relevantes pueden empezar en 2028, pero los acuerdos deberían alcanzarse antes puesto que la puesta en marcha requiere tiempo.
- Ámbito: **comunitario**.

Recomendación R5. Aumentar los esfuerzos para atraer, retener y capacitar a especialistas en IA en áreas de interés para la defensa.

Dada la rápida evolución de la tecnología asociada a la IA y su convergencia con otras tecnologías emergentes, la UE deberá **incrementar el esfuerzo en la atracción, retención y formación de especialistas en IA** que puedan emplearse por la industria de defensa y por las Fuerzas Armadas para acelerar su adopción en Europa.

El objetivo perseguido con la recomendación propuesta es permitir a la UE **reducir el déficit estimado de especialistas en IA**, partiendo de diferencias existentes entre los Estados miembros. Su puesta en marcha se puede hacer mediante la creación de programas formativos conjuntos entre varios países y apoyados por la Comisión Europea y la industria de defensa que permitan actualizar los conocimientos del personal técnico existente, y atraer a especialistas de otras ramas.

Las prioridades formativas deberán estar alineadas con los gaps de la UE identificados en el Libro Blanco de la Defensa publicado en marzo de 2025. Desde el punto de vista instrumental, una opción posible es aprovechar las redes de universidades europeas, y la creación de un programa específico transversal con acciones del tipo CO-FUND Marie Curie, alimentado con recursos comunitarios y de los Estados miembros de la UE. Asimismo, se propone impulsar la creación de un área temática de defensa en los proyectos individuales (*starting, consolidator y advanced*) y sinérgicos del *European Research Council*.

Valoración cualitativa:

- Complejidad: **media**. Requiere desarrollar programas formativos a nivel europeo con competencias educativas nacionales.
- Coste: **medio-bajo**. Los recursos necesarios dependerán del número de especialistas necesarios y las áreas prioritarias que se seleccionen. Realizarlo en el contexto europeo puede implicar costes de movilidad.
- Urgencia: **alta**. Puede implementarse como un conjunto de acciones coordinadas entre actuaciones puestas en marcha en los Estados miembros.
- Ámbito: **comunitario y Estados miembros**

Recomendación R6. La UE debe apoyar la creación y el refuerzo de ecosistemas nacionales de IA en el ámbito de la defensa.

El apoyo a la **creación y fortalecimiento de ecosistemas nacionales de IA en defensa** se entiende como un prerrequisito para la creación de un **“ecosistema europeo”** flexible y suficientemente integrado que permita mejorar el posicionamiento europeo en un contexto global altamente competitivo.

Los ecosistemas nacionales deberían **focalizarse prioritariamente en aquellos ámbitos de la IA aplicada a la defensa en los que se cuente con un potente tejido industrial** y, desde el punto de vista de la UE, favorezcan el desarrollo de grandes proyectos de interés común europeo en los que la IA sea una tecnología clave. Asimismo, debería fomentarse la complementariedad de las áreas asumidas por los distintos actores para optimizar la inversión, sin impedir, cuando fuese conveniente, desarrollos en paralelo con enfoques complementarios para contribuir a la competitividad que permita el ajuste de los costes y una eventual comercialización posterior de los productos fuera de la UE.

Una opción es **partir del esfuerzo ya realizado por la Comisión Europea con las denominadas Factorías de IA**, para hacer evolucionar la actividad de algunas de ellas con un enfoque dual, disponer de zonas de acceso restringido, y asegurar su relación estable con las Fuerzas Armadas y la industria de defensa.

Valoración cualitativa:

- Complejidad: **alta**. Es necesario definir el tipo de ecosistemas de IA en defensa, su focalización temática, los núcleos iniciales, y la gobernanza, asegurando la especialización y la complementariedad.
- Coste: **medio-alto**. Será necesario inyectar recursos suficientes para conseguir un impacto relevante ligado a una “*hoja de ruta común*” en los recursos disponibles para alguna de las Factorías de IA.
- Urgencia: **media**. Se entiende como un proceso progresivo con la interacción con los ecosistemas existentes a nivel nacional.
- Ámbito: **UE con nodos en los Estados miembros** comprometidos en su financiación.

Recomendación R7. Poner en marcha una aceleradora europea de defensa basada en una cooperación entre la Comisión Europea y los Estados miembros.

Poner en marcha la creación de una aceleradora europea con una línea específica de apoyo a **startups disruptivas de IA** de carácter dual basada en la participación y cooperación público-privada y la participación de los Estados miembros que lo deseen a través de **aceleradoras nacionales de defensa**, en línea con lo previsto en el pilar de EIC del futuro HE 2028-2034.

Se pretende con ello evitar o limitar una fragmentación del proceso de aceleración de nuevas empresas tecnológicas de carácter dual. Una opción de implementación de la aceleradora es su **integración en el European Innovation Council (EIC)**, aunque dadas las especificidades propias del sector de la defensa, será necesario redefinir su actuación en TRLs bajos, y asegurar la coordinación con las **aceleradoras nacionales** y las puestas en marcha por el programa **DIANA de la OTAN** situadas en los países de la UE.

Valoración cualitativa:

- Complejidad: **media**. Los procesos de aceleración dependen de la asignación de recursos nacionales y de fondos privados. Su efectividad depende de la capacidad de abordar sucesivas rondas de financiación y reducir el riesgo de que startups europeas de defensa no escalen sus actividades fuera de la UE.
- Coste: **medio**. Las inversiones pueden limitarse a las primeras rondas de inversión para poder financiar anualmente unas 20-30 start-ups europeas. La financiación a start-ups puede comenzar en 2028 con el siguiente marco financiero plurianual, aunque es necesario realizar pilotos controlados en este periodo de transición.
- Urgencia: **media**. Deben existir previamente aceleradoras nacionales de defensa y el establecimiento de normas comunes.
- Ámbito: **UE** con impacto también en los Estados miembros.

Recomendación R8. Actualizar la *Estrategia de Tecnología e Innovación para la Defensa 2020* (ETID 2020) de España hasta 2030 dando prioridad a las tecnologías de IA alineadas con el programa *Readiness 2030* de la UE y los programas europeos para 2028-2034.

Es urgente acelerar el proceso de actualización de la ETID 2020 del Ministerio de Defensa con el fin de alinearla con las prioridades del programa “*Readiness 2030*” de la Comisión Europea, del Programa Europeo de Defensa, de las prioridades de la OTAN en relación con la IA, y de los programas de defensa y seguridad españoles relacionados. En ese proceso deben priorizarse explícitamente aquellas áreas relacionadas con la IA.

Este proceso de actualización deberá cumplimentarse lo antes posible para poder competir mejor con otros países y disponer de un marco de apoyo nacional que incremente la participación y liderazgo español en los programas comunitarios y de la OTAN. El proceso debería tener en cuenta las propuestas que la Comisión Europea haga en 2025 sobre el futuro Programa Marco de investigación e innovación de la UE HE 2028-2034 y los programas incluidos en el *Fondo Europeo de Competitividad*.

Valoración cualitativa:

- Complejidad: **baja**. Depende únicamente de la decisión del Ministerio de Defensa español.
- Coste: **bajo**. Se trata de un proceso de planificación junto a análisis de vigilancia y prospectiva tecnológica.
- Urgencia: **alta**. Es necesario culminar el proceso de actualización lo antes posible para poder priorizar actuaciones, dados los incrementos presupuestarios previstos, y asegurar el máximo nivel posible de soberanía tecnológica española.
- Ámbito: **España**.

Recomendación R9. Alinear la estrategia europea con escenarios realistas para lograr la soberanía tecnológica en IA para la defensa.

El análisis detallado de la soberanía tecnológica europea o española en IA de uso militar deberá alinearse con los **escenarios factibles hacia 2030** que se quieran promover conjuntamente desde una **postura realista** de la situación europea y de sus capacidades.

Los autores consideran que el **escenario realista** indicado previamente en este documento es apropiado para asegurar un papel destacado de España y debería considerarse como un objetivo político llegar a él en 2030. En todo caso, se considera necesario reevaluar periódicamente la situación de la soberanía tecnológica europea en IA, empleando indicadores sintéticos para ello, y definir un nuevo escenario realista alcanzable en el periodo 2030-2035 que tenga en cuenta la evolución de la tecnología de IA y los hitos alcanzados por la UE en el desarrollo y uso soberano de la IA en defensa hasta 2030, así como la reducción de dependencias tecnológicas conseguidas.

Este alineamiento deberá contemplar, asimismo, la **actualización de las prioridades que se establezcan para la defensa en las áreas tecnológicas relacionadas con la IA** como las de semiconductores, robótica, enjambres de sistemas autónomos (aéreos, terrestres y marítimos), análisis big data o neurotecnología.

Valoración cualitativa:

- Complejidad: **alta**. Para tener el impacto deseado debe ser acordado por los órganos comunitarios; sobre todo, si se desea disponer de un marco cuantitativo que ayude a la toma de decisiones.
- Coste: **bajo**. No implica la asignación de recursos cuantiosos en esta fase de planificación. Un problema diferente sería el coste de las decisiones que se tomen de acuerdo con ello.
- Urgencia: **media**. El objetivo es que este proceso se extienda hasta 2030 con actividades comenzando desde 2025.
- Ámbito: **UE y Estados miembros**

Recomendación R10. Establecer un *Observatorio de IA en Defensa* con una perspectiva multidimensional al servicio de todos los Estados miembros y coordinando los esfuerzos nacionales.

Dada la enorme velocidad a la que se produce el desarrollo de la IA en defensa se considera necesario la creación de un **Observatorio de la IA en Defensa** que tenga en cuenta la evolución de la tecnología desde las dimensiones indicadas en el presente informe: la científica-tecnológica, la socioeconómica, la táctica y operativa en los ejércitos, y la ética y regulatoria. No se trata, por tanto, de mantener una visión de vigilancia tecnológica, sino también de mercados, usuarios y contexto ético y regulatorio en el

que se emplea. Asimismo, permitiría evaluar el grado en el que la UE mejora su nivel de soberanía tecnológica en todos los eslabones de la cadena de valor de la IA aplicada a la defensa.

Debe tenerse en cuenta la posible **clasificación de parte de la documentación generada** y, por tanto, la posibilidad de restringir su uso por los diferentes actores del ecosistema de defensa europeo de acuerdo con los procedimientos que se establezcan en su puesta en marcha.

Este Observatorio podría ser coordinado por la **Comisión Europea** con el apoyo del Servicio Exterior de la UE, junto a la industria europea de defensa (p. ej. a través de la Agencia Europea de Defensa) y con la participación de expertos procedentes de la Comisión Europea y de los Estados miembros. El Observatorio también debería coordinar sus actividades con la OTAN (concretamente con la STO y DIANA) y, en temas concretos, con los existentes en otros países aliados estableciendo los **niveles de confidencialidad y clasificación de la información** que se consideren necesarios en cada caso.

Valoración cualitativa:

- Complejidad: **baja**. Puede basarse en las redes de expertos de diversas organizaciones y apoyarse en observatorios preexistentes en el mundo civil ampliando su campo de acción a las tecnologías duales y a la defensa.
- Coste: **bajo**. Aunque no implica una actividad costosa en proyectos de I+D, sí requiere disponer de recursos suficientes para coordinar la actividad y desarrollar estudios e informes concretos.
- Urgencia: **media**. Al menos, puede partirse de una coordinación y especialización de los observatorios existentes en temas de uso dual de la IA en los Estados miembros de la UE.
- Ámbito: **UE** con impacto en los **Estados miembros**.

Seguidamente, en la figura 8.2 se indica la **relación entre la complejidad y el tiempo previsto para la puesta en marcha de las recomendaciones propuestas** de acuerdo con la opinión subjetiva de los miembros del Grupo de Trabajo. Se ha tratado de representar en la figura el momento en el que la puesta en marcha de la recomendación debería producirse y el periodo en el que su implementación deberá llevarse a cabo para que puedan obtenerse sus efectos deseables.

Obsérvese que casi todas las recomendaciones propuestas comenzarían con el **actual marco financiero plurianual de la UE hasta 2027**, aunque deberán prolongarse en el periodo 2028-2034 con el próximo marco financiero plurianual. Este hecho puede condicionar el impacto de aquellas recomendaciones cuya implementación requiera disponer de abundantes recursos económicos comunitarios.

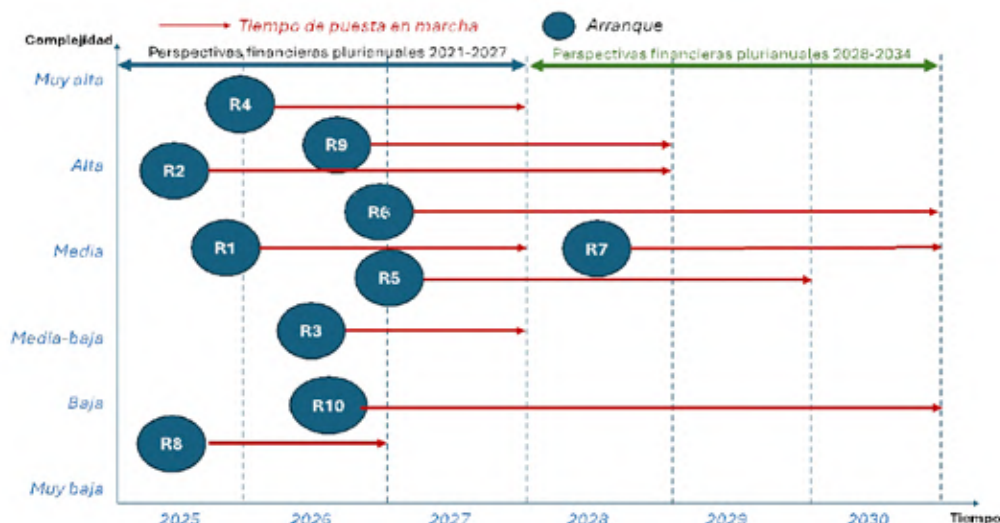


Figura 8.2. Urgencia y complejidad de las relaciones propuestas.
Fuente: elaboración propia

Previamente, se ha advertido de que **las recomendaciones propuestas no son totalmente independientes** y que el impacto perseguido puede obtenerse más eficientemente si se potencian las relaciones entre ellas y su ejecución concurrente. Las relaciones más relevantes se presentan esquemáticamente en la figura 8.3. Obsérvese que la mayor parte de ellas deben iniciarse en el periodo 2025-2027.

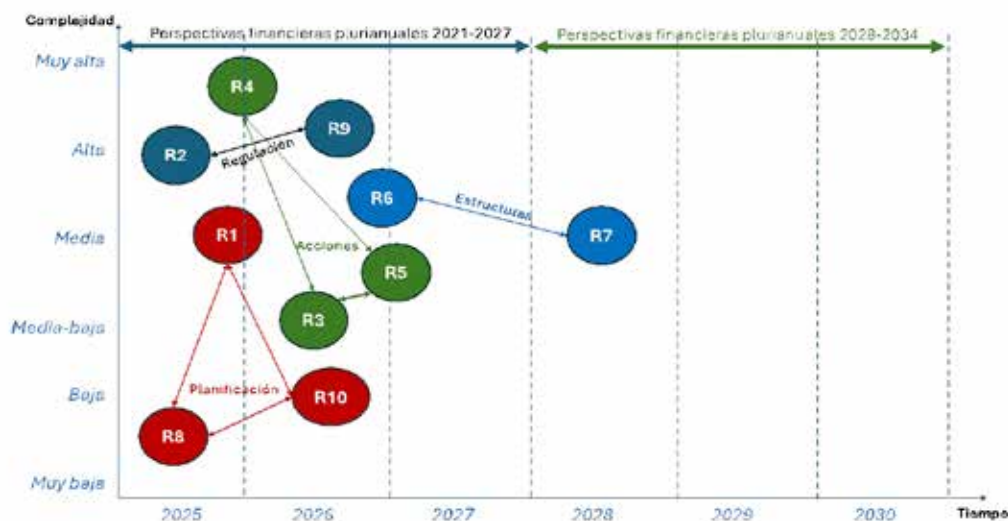


Figura 8.3 Relaciones principales entre las recomendaciones propuestas.
Fuente: elaboración propia

Algunas de estas relaciones hacen referencia a procesos de **planificación** (R1, R8 y R10), otras a acciones concretas de **apoyo al desarrollo de sistemas de IA** (R3, R4 y R5), otras a cuestiones **regulatorias** (R2 y R9) y, finalmente, otras están ligadas a la creación de **estructuras concretas** (R6 y R7).

8.4 Reflexión final

La revisión de las conclusiones extraídas del informe elaborado y las recomendaciones de actuación propuestas presentan un **panorama de la UE referido al liderazgo en el desarrollo y uso de la IA en defensa que se antoja difícil y complejo**. Por este motivo, estamos obligados a reaccionar con **urgencia y decisión**.

En la situación actual ese liderazgo en el desarrollo y uso de la IA en defensa, salvo en aspectos de aplicación muy concretos, no se encuentra en la UE. Si se extendiera el ámbito de la UE en relación con la IA en defensa al **européo** (al menos, con la inclusión de las capacidades del Reino Unido, Ucrania, Noruega y Suiza) **la situación mejora basada en el desarrollo y uso de sistemas de IA estimulados por su introducción en el conflicto militar de Ucrania** como ha sido expuesto en capítulos precedentes.

No obstante, será necesario **incrementar los esfuerzos futuros del uso de la IA en defensa con más recursos y de manera coordinada** manteniendo una visión integrada de todas las dimensiones analizadas.

Las recomendaciones propuestas en el presente informe van orientadas a **mejorar progresivamente y de forma realista la soberanía tecnológica de la UE en la interacción entre la IA y la defensa**. Se asume con ello la necesidad de reducir las dependencias actuales apoyándose, cuando sea necesario, en socios tecnológicos estables de la UE.

En el caso de **España** su posición en el uso de la IA en el ámbito de la defensa **no es muy diferente de la de otros países de la Unión**, aunque se haya visto lastrada por presupuestos de defensa reducidos durante años.

Sin embargo, desde una visión optimista creemos que el punto de partida de España en diversas áreas del desarrollo de sistemas de defensa con tecnologías de IA es mejor que en otros casos, fruto de varios elementos: el aprovechamiento del **esfuerzo realizado durante la última década en el proceso de digitalización**, el **despliegue de infraestructuras digitales**, y de su buena posición en el **sector del espacio**.

Aprovechar este posicionamiento es una **responsabilidad colectiva** que requiere un **análisis y debate sosegado y profundo** en un momento en el que la defensa y la seguridad han adquirido una gran relevancia y los Estados miembros han asumido compromisos mucho mayores. **Al desarrollo de este debate quiere contribuir el presente informe.**

REFERENCIAS

Esta sección también incluye las referencias empleadas en los anexos.

1. Abaimov, S., y Martellini, M. (2020). Artificial intelligence in autonomous weapon systems. 21st Century prometheus: Managing CBRN safety and security affected by cutting-edge technologies, 141-177.
2. Abbasi, A. Yadav, H. Yanikomeroglu, N. -D. Đào, G. Senarath and P. Zhu (2024). "HAPS for 6G Networks: Potential Use Cases, Open Challenges, and Possible Solutions," in IEEE Wireless Communications, vol. 31, no. 3, pp. 324-331, Doi: <https://doi.org/10.1109/MWC.012.2200365>
3. Abbasov, J. (2023) "Resource optimization with DRL-driven real-time service placement strategy in Edge-Cloud continuum".
4. Abraham, Y. (2024). 'Lavender': The AI machine directing Israel's bombing spree in Gaza. +972 Magazine, April 3, 2024. <https://www.972mag.com/lavender-ai-israeli-army-gaza/>
5. Acemoglu, D. (2024). The Simple Macroeconomics of AI. National Bureau of Economic Research Working Paper 32487.
6. Aftatah y Zebbara (2024). Comprehensive Survey on Secure Navigation for Intelligent Systems: Artificial Intelligence Approaches to GPS Jamming and Spoofing Detection. COCIA 2024, LNNS 1123, pp. 1–6, 2024. https://doi.org/10.1007/978-3-031-70411-6_17
7. Agerri, R. y Agirre, E. (2020). "Lessons learned from the evaluation of Spanish Language Models", 2022.
8. Aguado, Juan M., de Haro, Verónica, Gómez de Ágreda, Ángel y Pérez-Escolar, Marta (2024); El ecosistema de la desinformación: actores, estrategias y redes de valor "Desinformación y Defensa. Conflictos híbridos, entorno cognitivo y operaciones de influencia", Editorial Dickinson, ISBN: 978-84-1070-699-6
9. Ahmed, I., Galoppo, T. Hu, X.;Ding, Y. (2020). Graph Regularized Autoencoder and its Application in Unsupervised Anomaly Detection. 10.48550/arXiv.2010.15949. <https://doi.org/10.48550/arXiv.2010.15949>
10. Ajaykumar, S. (2023). Ethics of neurotechnology: The intersection of neuroscience and military applications. Expert Speak Digital Frontiers. Observer Research Foundation. Sep 05, 2023. <https://www.orfonline.org/expert-speak/ethics-of-neurotechnology#:~:text=Neurotechnology%20and%20neuropharmacology%20should%20not,outcome%20of%20using%20neurotechnology%20weapons.>
11. Ålander, M. (2024). Death by a Thousand Paper Cuts: Lessons from the Nordic-Baltic Region on Countering Russian Gray Zone Aggression. Carnegie Endowment for International Peace. November 14, 2024. <https://carnegieendowment.org/research/2024/11/russia-gray-zone-aggression-baltic-nordic?lang=en>

12. Allen, G. C. (2023). Blocking China's Access to AI Chips Matters to U.S. National Security. Retrieved from Center for Strategic & International Studies: <https://www.csis.org/analysis/blocking-chinas-access-ai-chips-matters-us-national-security>
13. Allen, G. C. (2024). The True Impact of Allied Export Controls on the U.S. and Chinese Semiconductor Manufacturing Equipment Industries. Wadhani AI Center, Center for Strategic and International Studies CSIS. November 2024. <https://www.csis.org/analysis/true-impact-allied-export-controls-us-and-chinese-semiconductor-manufacturing-equipment>
14. Anicho, O., Charlesworth, P., Baicher, G., Nagar, A., and Buckley, N. (2024). Comparative Study for Coordinating Multiple Unmanned HAPS for Communications Area Coverage.
15. ARTES (2024). ARTES Future Preparation 1A.127 Disruptive satcom Systems Design with Digital Generative Design. CSC (Connectivity and Secure Communications). ESA. 24th July 2024. <https://connectivity.esa.int/projects/artes-future-preparation-1a127-disruptive-satcom-systems-design-digital-generative-design>
16. Article 36 (2013). Killer Robots: UK Government Policy on Fully Autonomous Weapons, a commentary on the UK Ministry of Defense's 2011 Joint Doctrine Note on The UK Approach to Unmanned Systems). https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://article36.org/wp-content/uploads/2013/04/Policy_Paper1.pdf&ved=2ahUKEwjUnefrY6NAXtKvsDHR16C6MQFnoECBoQAQ&usg=AOvVaw2ZIMRxQkk_XxvUYCs14qCy
17. As.com 19/12/2024. Trident, la nueva arma láser en poder de Ucrania capaz de derribar aviones a más de 2 kilómetros. Disponible en línea: <https://as.com/actualidad/politica/trident-la-nueva-arma-laser-en-poder-de-ucrania-capaz-de-derribar-aviones-a-mas-de-2-kilometros-n/> (Accedido: 26-feb-2025)
18. ASD (2024). <https://defence-industry.eu/europes-defence-and-aviation-industries-welcome-supportive-eu-draghi-report/>
19. Audrey Fritz (2019). China's Evolving Conception of Civil-Military Collaboration, Center for Strategic and International Studies. Disponible en <https://www.csis.org/blogs/trustee-china-hand/chinas-evolving-conception-civil-military-collaboration>
20. Ayed, D.; P.-A. Dragan, E. Felix, Z. Mann, E. E. Salant, R. Seidl, A. Sidiropoulos, S. Taylor, and R. Vitorino (2022). "Protecting sensitive data in the cloud-to-edge continuum: The FogProtect approach," in 2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing (CCGrid), pp. 279–288.
21. Azarkhina, O. (2025). From Civilian Tech to Battlefield Edge. Ukraine's Dual-Use Innovations. Jornada de tecnologías duales. Fundación Círculo de Tecnologías para la Defensa y la Seguridad. Madrid, 8 de julio de 2025.
22. Aznar, F. (2024). La Guerra, Teoría para comprender los conflictos del Siglo XXI. Ed. El Viejo Topo. ISBN 978-84-19778-95-6.
23. Baietto, A., y Bihl, T. (2025). Generative Data for Neuromorphic Computing. Proceedings of the 58th Hawaii International Conference on System Sciences (págs. 7248-7258).

24. Baldwin, H. (2024). Critical Dual-Use Technologies: Commercial, Regulatory, Societal and National Security Challenges. Economics and Security Committee (ESC). 051 ESC 24 E rev.2 fin. NATO Parliamentary Assembly. 26 August 2024. <https://www.nato-pa.int/document/2024-du-al-use-technologies-report-baldwin-051-esc>
25. Baqués, J. (2024). La teoría de la guerra justa: el legado de Francisco de Vitoria. The Objective. 12 de marzo de 2024. <https://theobjective.com/internacional/2023-09-19/teoria-guerra-justa-francisco-vitoria/>
26. Barry, W., Metcalf, C., and Wilcox, B. (2025). Strategic Centaurs: Harnessing Hybrid Intelligence for the Speed of AI-Enabled War. Modern War Institute. January 17, 2025. <https://mwi.westpoint.edu/strategic-centaurs-harnessing-hybrid-intelligence-for-the-speed-of-ai-enabled-war/>
27. Baruzzi, V., Indiveri, G., y Sabatini, S. (2025). Recurrent models of orientation selectivity enable robust early-vision processing in mixed-signal neuromorphic hardware. *Nature Communications*, 1-15.
28. Bataille, M. (2024). Integrating Commercial Space for Military Applications in Europe: A Challenge and Opportunity. European Space Policy Institute. 5 September 2024. <https://www.espi.or.at/briefs/integrating-commercial-space-for-military-applications-in-europe-a-challenge-and-opportunity/>
29. Batra, G., Jacobson, Z., Madhav, S., Queirolo, A., & Santhanam, N. (2018). *Artificial-Intelligence Hardware: New opportunities for semiconductor companies*. Sidney: Mc Kinsey & Company.
30. Bebber, R. and Masshal, A. (2024). Cognitive Competition, Conflict, and War: An Ontological Approach. Hudson Institute. May 2024. <https://www.hudson.org/defense-strategy/cognitive-competition-conflict-war-ontological-approach-robert-jake-bebber>
31. Bendett, S. (2024). Russian UGV developments influenced by Ukraine War. *European Security and Defence*, 19.
32. Bendett, S. y Kirichenko, D. (2025). Battlefield Drones and the Accelerating Autonomous Arms Race in Ukraine. Modern War Institute at West Point, January 10, 2025. <https://mwi.westpoint.edu/battlefield-drones-and-the-accelerating-autonomous-arms-race-in-ukraine/>
33. Benjamin, M. (2013). *Drone Warfare. Killing by remote control*. Verso Books.
34. Berkol, A., y Demirtaş, İ. G. (2023). Exploring the Potential Interplay of GPT, Edge AI, and the Defense Industry. In *The International Conference on Artificial Intelligence and Applied Mathematics in Engineering* (pp. 239-249). Cham: Springer Nature Switzerland.
35. Berkowitz, M.J. (2024). America's Asymmetric Vulnerability to Navigation Warfare: Leadership and Strategic Direction Needed to Mitigate Significant Threats. National Security Space Association (NSSA). <https://nssaspace.org/wp-content/uploads/2024/07/NAVWAR-FINAL.pdf>
36. Bernal, A., Cartel, C., Singh, I., Cao, C. y Madreperla, O., (2020). Cognitive Warfare. *Johns Hopkins v NATO*. Fall 2020. <https://www.ejiltalk.org/cognitive-warfare-does-it-constitute-prohibited-force/#:~:text=Bernal%20et%20al,destabilising%20public%20institutions.>

37. Black, J. Eken, M., Parakilas, J., Dee, S., Ellis, C., Suman-Chauhan, K., Bain, R.J., Fine, H., Aquilino, M. Lebre, M.; et al. (2024). Strategic competition in the age of AI. Emerging risks and opportunities from military use of artificial intelligence. RAND Europe. Sep 6, 2024. https://www.rand.org/pubs/research_reports/RR3295-1.html
38. Bojor, L., Petrache, T., y Critescu, C. (2024). Emerging Technologies in Conflict: The Impact of Starlink in The Russia – Ukraine War. Land Forces Academy Review. Vol. XXIX, No. 2(114). DOI: <https://doi.org/10.2478/raft-2024-0020>
39. Bollfrass, A.K., Sabatino, E. Wiley, C. (2025). Space Capabilities to Support Military Operations in the European Theatre. IISS Research Papers. The International Institute for Strategic Studies. 30th January 2025. <https://www.iiss.org/research-paper/2025/space-capabilities-to-support-military-operations-in-the-european-theatre/>
40. Bondar, K. (2024). Understanding the Military AI Ecosystem of Ukraine. Center for Strategic and International Studies (CSIS). 12 November 2024. <https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine>
41. Bondar, K. (2025). Ukraine’s Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare. A report of the CSIS Wadhani AI Center. Center for Strategic & International Studies. March 6, 2025. <https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare>
42. Boole, G. (1854). An Investigation of the Laws of Thought on Which are Founded the Mathematical Theories of Logic and Probabilities.
43. Boozallen (2025). Artificial Intelligence for Space Missions. <https://www.boozallen.com/markets/space/artificial-intelligence-for-space-missions.html> (accedido el 4 de enero de 2025)
44. Borchert, H. (2024). The Very Long Game of Defense AI Adoption: Introduction.
45. Borrajo, D.; Juristo, N; Montes, C. y Pazos, J. (1993). Inteligencia artificial: métodos y técnicas. Ed. CEURA.
46. Boser, B. E., Guyon, I. M., & Vapnik, V. N. (1992). A Training Algorithm for Optimal Margin Classifiers. Proceedings of the Fifth Annual Workshop on Computational Learning Theory, 144–152.
47. Breiman, L. (2001). Random Forests. Machine Learning, 45(1), 5–32. DOI: <https://doi.org/10.1023/A:1010933404324>
48. Bourriez, N., Loizeau, A., Abdin, A. (2023). Spacecraft Autonomous Decision-Planning for Collision Avoidance: a Reinforcement Learning Approach. 74th International Astronautical Congress (IAC), International Astronautical Federation (IAF), Oct 2023, Baku, Azerbaijan. hal-04334473.
49. Bourzac, K. (2025). The U.S. will start manufacturing advanced chips. Spectrum IEEE, 40-41.
50. Bradford, A. (2024). Imperios digitales: La batalla global por la tecnología que marcará la geopolítica del futuro. Shackleton Books. 4 noviembre 2024. ISBN-10, 841361502X.
51. Breiman, L. (2001). Random Forests. Machine Learning, 45(1), 5–32. DOI:10.1023/A:1010933404324

52. Brock, A., Donahue, J., & Simonyan, K. (2019). Large Scale GAN Training for High Fidelity Natural Image Synthesis. International Conference on Learning Representations (ICLR).
53. Bruegel (2024). Mejino-López, J. y Wolf, G. A European defence industrial strategy in a hostile world. Policy Brief. Bruegel. 20 noviembre 2024. <https://www.bruegel.org/policy-brief/european-defence-industrial-strategy-hostile-world>
54. Buchanan, B. G. y Feigenbaum, E. A. (1978). DENDRAL and Meta-DENDRAL: Their Applications Dimension. Artificial Intelligence, 11, pp. 5-24.
55. Burikov, A. and Wolf, G. (2025). Defending Europe without the US: first estimates of what is needed. Bruegel. 21 February 2025. <https://www.bruegel.org/analysis/defending-europe-without-us-first-estimates-what-needed>
56. Burkacky, O., Patel, M., Pototzky, K., Tang, D., Vrijen, R., & Zhu, W. (2024). Generative AI: The next S-curve for the semiconductor industry? Mc Kinsey & Company.
57. C4ISRNET/AP (2019). "Sea Hunter autonomous vessel completes first transoceanic voyage". Disponible en línea: <https://www.defenseone.com/sponsors/2019/10/inside-look-autonomous-vessels-changing-warfighting/160768/> (Accedido: 3-3-2025).
58. C4ISRNET/AP (2024). "High-tech Sea drones sink another Russian warship, Ukraine says". <https://www.c4isrnet.com/unmanned/2024/03/05/high-tech-sea-drones-sink-another-russian-warship-ukraine-says/> (Accedido: 3-3-2025)
59. Campbell, T. (2017). Kardashev Scale Analogy: Long-Term Thinking about Artificial Intelligence. FutureGrasp, LCC. Disponible en línea: https://irp-cdn.multiscreensite.com/9297f8c7/files/uploaded/The%20Kardashev%20Scale-An%20AI%20Analogy_FINAL.pdf
60. Carlson, L., Arvelo, F., Cain, P., Meyer, S., Hatcher, D. (2023). Techno Warfare 2035. United States Army War College Class. 2023,
61. Cartwright, M. (2020). La guerra de los Cien Años: consecuencias y efectos (traducido por Padilla, N.). World History Encyclopedia. 6 marzo de 2020. <https://www.worldhistory.org/trans/es/2-1520/la-guerra-de-los-cien-anos-consecuencias-y-efectos/>
62. Caruso, A. M. (2024). "Energy Efficiency for Tactical Cloud, Edge and IoT Continuum: Helping the Military Dominate the Battlespace," 2024 IEEE International Workshop on Technologies for Defense and Security (TechDefense), Naples, Italy, pp. 144-148.
63. Caso, S. (2024). Emerging technologies in military space operations: current applications and future research for educational and training purposes, International Journal of Training Research, 25 Nov 2024. DOI: 10.1080/14480220.2024.2431482 <https://doi.org/10.1080/14480220.2024.2431482>
64. CB Insights (2024). 15 Tech Trends to watch closely in 2025. December 2024. <https://www.cbinsights.com/research/report/top-tech-trends-2025/>

65. CCDC (2020). Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R). Centro Conjunto de Desarrollo de Conceptos. CESEDEN. 2020. <https://publicaciones.defensa.gob.es/usos-militares-de-la-inteligencia-artificial-la-automatizacion-y-la-robotica-iaa-r-libros-pdf.html>
66. CCN (2024). CCN-CERT IA-04/24: Ciberamenazas y Tendencias. Centro Criptológico Nacional. Octubre de 2024. <https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7274-ccn-cert-ia-04-24-ciberamenazas-y-tendencias-edicion-2024/file.html>
67. Chang, E. (2024). The Role of AI in Managing Low Orbit Satellites. TelecomWorld101. December 24, 2024. <https://telecomworld101.com/the-role-of-ai-in-managing-low-orbit-satellites/>
68. Channamadhavuni, S., Thijssen, S., Jha, S., & Ewetz, R. (2021). Accelerating AI Applications using Analog In-Memory Computing: Challenges and Opportunities. GLSVLSI '21, Virtual Event, USA.
69. Chao-Yang Lu, Yuan Cao, Cheng-Zhi Peng, and Jian-Wei Pan (2022). Micius quantum experiments in space Rev. Mod. Phys. 94, 035001 (2022). July 6, 2022
70. Chapman, J.C. and Peters, N.A. (2022). Paving the Way for Satellite Quantum Communications November 9, 2022. Physics 15, 172. <https://physics.aps.org/articles/v15/172>
71. Chen, M., Tworek, J., Jun, H., Yuan, Q., Ponde, H. de O., Kaplan, J., Edwards, H., Burda, Y., Joseph, N., Brockman, G., Ray, A., & Sutskever, I. (2021). Evaluating Large Language Models Trained on Code. arXiv preprint arXiv:2107.03374.
72. Cherneva, K. (2024). How to Fight AI-Generated Fake News — With AI. Built-in. November 12, 2024. <https://builtin.com/artificial-intelligence/fight-ai-generated-fake-news>
73. Chesnokova, S. (2024). AI vs drones: Europe's top defence tech rounds of 2024. TFN (Tech funding News). November 11, 2024. <https://techfundingnews.com/ai-vs-drones-europes-top-defence-tech-rounds-of-2024/>
74. Cheung, S. (2024). "PRC Adapts Meta's Llama for Military and Security AI Applications," Jamestown Foundation. Disponible en línea: <https://jamestown.org/program/prcs-adaptation-of-open-source-llm-for-military-and-security-purposes/> (Accedido: 3-3-2025).
75. Chia, Y. K., Chen, G., Tuan, L. A., Poria, S., y Bing, L. (2023). Contrastive chain-of-thought prompting. arXiv preprint arXiv:2311.09277.
76. Chintalapati, B., Precht, A. Hanra, S., Laufer, R., Liwicki, M., Eickhoff, J. (2024). Opportunities and challenges of on-board AI-based image recognition for small satellite Earth observation missions. Advances in Space Research. Available online 26 March 2024. <https://doi.org/10.1016/j.asr.2024.03.053>
77. Chochtoulas, A. (2024). How Large Language Models are Transforming Modern Warfare. Is ChatGPT Applicable in the Military Domain? Joint Air Power Competence Centre. Journal Edition 37. May 2024
78. Chou, C., Manyika, J., y Neven, H. (2025). The Race to Lead the Quantum Future. How the Next Computing Revolution Will Transform the Global Economy and Upend National Security. Foreign Affairs. January/February 2025 (pp 154-167).

79. Chung, H. W., Hou, L., Longpre, S., Zoph, B., Tay, Y., Fedus, W., et al. (2024). Scaling instruction-finetuned language models. *Journal of Machine Learning Research*, 25(70), 1-53.
80. Chung, J., Gülcehre, C., Cho, K. y Bengio, Y. (2014). Empirical Evaluation of Gated Recurrent Neural Networks on Sequence Modeling, *CoRR*, abs/1412.3555.
81. Clapp, S. (2025). Defence and Artificial Intelligence. EPRS | European Parliamentary Research Service. PE 569.580. April 2025. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI\(2025\)769580_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf)
82. Claverie, B. (2025). Cognitive warfare: the new battlefield exploiting our brains. *Polytechnique Insights*, February 5th, 2025. <https://www.polytechnique-insights.com/en/columns/geopolitics/cognitive-warfare-the-new-battlefield-exploiting-our-brains/>
83. Claverie, B. and Cluzel, F. (2021). The Cognitive Warfare Concept. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf&ved=2ahUKewjGsPSI482KAXUv8L-sIHfmjlzMQFnoECBwQAQ&usg=AOvVaw2oLBYe6jnbURBkIF7OmUfL
84. Claverie, B., Du Cluzel, F. (2022). Chapter 2 – “Cognitive Warfare”: The Advent of The Concept of “Cognitics” in the Field of Warfare. *Proceedings of the first NATO scientific meeting on Cognitive Warfare (France) 21 June 2021. March 2022.* https://www.researchgate.net/publication/359991886_Cognitive_Warfare_The_Advent_of_the_Concept_of_Cognitics_in_the_Field_of_Warfare
85. Cluzel, F. (2021). Cognitive Warfare, a Battle for the Brain. STO-MP-AVT-211 KN3. STO NATO. [https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-HFM-334/\\$MP-HFM-334-KN3.pdf](https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-HFM-334/$MP-HFM-334-KN3.pdf)
86. Colussi I.A. (2025). International Trade Sanctions related to Dual-Use Goods and Technologies. *Athens Journal of Law - Volume 2, Issue 4 – Pages 237-252.* Octubre 2016. <https://doi.org/10.30958/ajl.2-4-3>
87. Comisión Europea (2020). Comunicación de la comisión al parlamento europeo, al consejo, al comité económico y social europeo y al comité de las regiones. Una estrategia europea de datos. <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0066&from=EN>
88. Comisión Europea (2023). Estrategia Espacial de la Unión Europea para la Seguridad y la Defensa. Comunicación Conjunta al Parlamento Europeo y al Consejo. JOIN (2023) 9. Dirección General de Industria de Defensa y Espacio. 10 marzo 2023. [https://ec.europa.eu/transparency/documents-register/detail?ref=JOIN\(2023\)9&lang=es](https://ec.europa.eu/transparency/documents-register/detail?ref=JOIN(2023)9&lang=es)
89. Comisión Europea (2024). Commission Staff working document on EDIP 8.7.2024 C(2024) 4822 final https://defence-industry-space.ec.europa.eu/document/download/f1e6ba44-4720-4f14-a991-a3a7f3afb475_en?filename=Staff%20Working%20Document%20on%20EDIP.PDF
90. Comisión Europea (2025a). The Road to the next Multiannual Financial Framework. COM/2025/46 final. 11 February 2025. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025DC0046>

91. Comisión Europea (2025b). White paper on the Future of European defence. Readiness 2030. 19 March 2025. https://commission.europa.eu/document/download/e6d5db69-e0ab-4bec-9dc0-3867b4373019_en?filename=White%20paper%20for%20European%20defence%20%E2%80%93%20Readiness%202030.pdf
92. Comisión Europea (2025c). AI Continent Action Plan. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM(2025) 165 final. Brussels, 9.4.2025. https://commission.europa.eu/document/download/f633985c-440a-4285-95c3-9fe16fd0fc65_en?prefLang=es
93. Comisión Europea (2025d). Annex to the AI Continent Action Plan. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM(2025) 165 final Annex. Brussels, 9.4.2025 [https://commission.europa.eu/topics/eu-competitiveness/ai-continent_es#:~:text=\(299.56%20KB%20%2D%20\),Descargar,-Enlaces%20relacionados](https://commission.europa.eu/topics/eu-competitiveness/ai-continent_es#:~:text=(299.56%20KB%20%2D%20),Descargar,-Enlaces%20relacionados)
94. Comisión Europea (2025e). Commission Staff Working Document Accompanying the document A dynamic EU budget for the priorities of the future: the Multiannual Financial Framework 2028-2034. SWD(2025) 570 final. Brussels, 16.7.2025. https://commission.europa.eu/document/download/9d8f303f-abfa-4385-b8d7-9b30034ff329_en?filename=SWD_2025_570_1_EN_autre_document_travail_service_part1_v6.pdf
95. Comisión Europea (2025f). A dynamic EU Budget for the priorities of the future - The Multiannual Financial Framework 2028-2034. Communication from The Commission to The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee of the Regions. COM(2025) 570 final Brussels, 16.7.2025. https://commission.europa.eu/document/download/26ff3426-b1db-44d5-ad9c-a646febb3222_en?filename=COM_2025_570_1_EN_ACT_part1_v6.pdf
96. Comisión Europea (2025g). Quantum Europe Strategy: Quantum Europe in a Changing World Communication from The Commission to The European Parliament and The Council. COM(2025) 363 final. Brussels, 2.7.2025. https://qt.eu/media/pdf/Quantum_Europe_Strategy_July_2025.pdf
97. Consejo de la Unión Europea (2022). Una Brújula Estratégica para reforzar la seguridad y la defensa de la UE en el próximo decenio. 21 marzo 2022. <https://www.consilium.europa.eu/es/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/>
98. Corral, D. (2025). Revolución cuántica, disrupción inimaginable. Instituto de Estudios Estratégicos. IEEE. 22/2025 27 de marzo de 2025. https://www.defensa.gob.es/documents/2073105/2320887/revolucion_cuantica_2025_dieeee22.pdf
99. Courtois, B. (2024). Combatting disinformation The AI war. Sopra Steria Next. <https://www.sopraSteria.com/insights/details/combating-disinformation-the-ai-war>
100. Cover, T. M., y Hart, P. E. (1967). Nearest neighbor pattern classification. IEEE Transactions on Information Theory, 13(1), 21–27. DOI:10.1109/TIT.1967.1053964

101. Cox, D. R. (1958). The regression analysis of binary sequences. *Journal of the Royal Statistical Society. Series B (Methodological)*, Volume 20, Issue 2, July 1958, Pages 215–23205. <https://doi.org/10.1111/j.2517-6161.1958.tb00292.x>
102. Csernaton, R. (2024). Charting the Geopolitics and European Governance of Artificial Intelligence. Carnegie Endowment for International Peace. March 6, 2024. <https://carnegieendowment.org/research/2024/03/charting-the-geopolitics-and-european-governance-of-artificial-intelligence?lang=en&center=europe>
103. Cullen, P.J. (2017). Understanding Hybrid Warfare. MCDC Countering Hybrid Warfare Project. A Multinational Capability Development Campaign Project. January 2017.
104. Danley, L. y Colder, B. (2023). The Building Resilience to Cognitive Warfare Technical Exchange Meeting. MITRE Corporation. Public Release 23-00371-18. September 2023. <https://www.mitre.org/news-insights/publication/building-resilience-cognitive-warfare-technical-exchange-meeting>
105. Danyk, Yuriy and Briggs, Chad M. (2023). “Modern Cognitive Operations and Hybrid Warfare.” *Journal of Strategic Security* 16, no. 1 (2023): 35-50. DOI: <https://doi.org/10.5038/1944-0472.16.1.2032> Available at: <https://digitalcommons.usf.edu/jss/vol16/iss1/3>
106. DARPA (2024). Catalyzing an Integrated Lunar Economy: Initial Results of the LunA-10 Capability Study. May 2024. <https://www.darpa.mil/news/2024/luna-10-economy-study>
107. David, W.; Pappalepore, P.; Stefanova, A. y Sarbu, B. A. (2019). *AI-Powered Lethal Autonomous Weapon Systems in Defence Transformation. Impact and Challenges*, Springer.
108. Davidson, N, (2016). A legal perspective: Autonomous weapon systems under international humanitarian law. ICRC, UNODA Occasional Papers, No. 30. Convention on Certain Conventional Weapons Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), 11 April 2016, <https://www.icrc.org/en/document/views-icrc-autonomous-weapon-system>
109. De Reus, N. M., Kerbusch, P., Schadd, M. and de Vos, A. (2021). Geospatial analysis for Machine Learning in Tactical Decision Support. STO-MP-MSG-184. NATO. <http://www.schadd.com/Papers/2021GeospatialanalysisforMachineLearninginTacticalDecisionSupport.pdf>
110. DefenseScoop (2024). Army Implements Generative AI Platform to Army Cloud. Disponible en línea: <https://sdi.ai/blog/the-most-useful-military-applications-of-ai/> (Accedido: 5-3-2025).
111. DefenseScoop (2024). Army set to issue new policy guidance on use of large language models. Disponible en línea: <https://defensescoop.com/2024/05/09/army-policy-guidance-use-large-language-models-llm/> (Accedido: 3-3-2025)
112. Deppe. C. and Schaal, G. (2024). Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept. *Front Big Data*. Doi: 10.3389/fdata.2024.1452129. PMID: 39552633; PMCID: PMC11565700. 01 November 2024. <https://pmc.ncbi.nlm.nih.gov/articles/PMC11565700/>
113. Devlin, J., Chang, M. W., Lee, K., y Toutanova, K. (2019). Bert: Pre-training of deep bidirectional transformers for language understanding. In *Proceedings of the 2019 conference of the North*

American chapter of the association for computational linguistics: human language technologies, volume 1 (long and short papers)

114. Dhanapala, I., Bharti, S., McGibney, A., y Rea, S. (2024). Towards a Reputation-based Trustworthy Edge-Cloud Continuum. Authorea Preprints.
115. Dhuliawala, S., Komeili, M., Xu, J., Raileanu, R., Li, X., Celikyilmaz, A., & Weston, J. (2023). Chain-of-verification reduces hallucination in large language models. arXiv preprint arXiv:2309.11495.
116. Di Mare, A. (2021). The Role of Space Domain Awareness Space Asset Resilience through Protection. Joint Air & Space Power Conference 2021. May 2021 <https://www.japcc.org/essays/the-role-of-space-domain-awareness/>
117. DIE (2024). Defence Industry Europe, “Indra demonstrates Crow C-UAS system at NATO anti-drone exercises”, 24 October 2024. See: <https://defence-industry.eu/indra-demonstrates-crow-c-uas-system-at-nato-anti-drone-exercises/>
118. DiEuliis, J. and Giordano, J. (2020). Redefining Neuroweapons: Emerging Capabilities in Neuroscience and Neurotechnology. PRISM No. 8, Vol. 3. National Defense University Press. Jan. 9, 2020. <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2053388/redefining-neuroweapons-emerging-capabilities-in-neuroscience-and-neurotechnology/>
119. Dobija, K. (2023). Countering Unmanned Aerial Systems (UAS) in Military Operations, Safety & Defense.
120. DoD (2024). Military and Security Developments Involving the People’s Republic of China. A Report to Congress 2024. Department of Defense. 18 December 2024. <https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF>
121. Doney, M. (2017). “Army Language Translation System Assists Soldiers’ Readiness,” JBSA News. Disponible en línea: <https://www.jbsa.mil/News/News/Article/1204354/army-language-translation-system-assists-soldiers-readiness/> (Accedido: 3-3-2025)
122. Dosovitskiy, A., Beyer, L., Kolesnikov, A., Weissenborn, D., Zhai, X., Unterthiner, T., y Houlsby, N. (2021). An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale. arXiv preprint arXiv:2010.11929
123. Draghi, M. (2024). The future of European competitiveness Part B | In-depth analysis and recommendations. September 2024. https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en#paragraph_47059
124. du Cluzel, F. (2021). Cognitive Warfare. NATO ACT Innovation Hub, 45. https://www.innovation-hub-act.org/sites/default/files/2021-01/20210122_CW%20Final.pdf.
125. E. Letta (2024). Much more than a market. June 2024. <https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf>

126. EDA (2023). Beyond 2040 - EDA analysis warns on future warfare trends and technology imperatives for European defence. European Defence Agency. 23 October 2023. <https://eda.europa.eu/news-and-events/news/2023/10/23/beyond-2040---eda-analysis-warns-on-future-warfare-trends-and-technology-imperatives-for-european-defence#:~:text=The%20main%20identified%20trends%20from,on%20space%20based%20enabling%20and>
127. EEAS (2024). 2nd EEAS Report on Foreign Information Manipulation and Interference Threats A Framework for Networked Defence. Report on FIMI threats. European Union External Action. January 2024. https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en#:~:text=Click%20to%20see%20full%20PDF%20document
128. EEAS (2025). 3rd EEAS Report on Foreign Information Manipulation and Interference Threats Exposing the architecture of FIMI operations. European Union External Action. March 2025. <https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf>
129. Ekelhof, M. y Paoli, G. (2020). Swarm Robotics: Technical and Operational Overview of the Next Generation of Autonomous Systems. UNIDIR. 8 April 2020. <https://unidir.org/publication/swarm-robotics-technical-and-operational-overview-of-the-next-generation-of-autonomous-systems/>
130. Elbaum, S. & Panter, J. (2024). AI Weapons and the Dangerous Illusion of Human Control. Foreign Affairs, 6 December 2024.
131. Entrust (2025). 2025 Identity Fraud Report. Entrust Cybersecurity Institute. 2025. <https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.entrust.com/sites/default/files/documentation/reports/2025-identity-fraud-report.pdf&ved=2ahUKEwjTrprkyLAXUXbvEDHdZtAksQFnoECBMQAQ&usq=AOvVaw1nfYXvtWZtrBqLGhyQmFvE>
132. Ergo Sum Team, Jackson, T., Richardson R., Ogletree, K., Moss, C. Liberato, R. (2024). Weaponizing Artificial Intelligence Generated Content. United States Army War College. 1st May 2024. <https://media.defense.gov/2024/Aug/30/2003535907/-1/-1/0/ERGO%20SUM%20MACHINA%20FINAL%20PRODUCT%20PDF%201.PDF>
133. ESA (2022). Smarter satellites: ESA Discovery accelerates AI in space. 12/05/2022. https://www.esa.int/Enabling_Support/Preparing_for_the_Future/Discovery_and_Preparation/Smarter_satellites_ESA_Discovery_accelerates_AI_in_space (accedido el 4 de enero de 2025).
134. ESA (2024). Artificial intelligence in space. https://www.esa.int/Enabling_Support/Preparing_for_the_Future/Discovery_and_Preparation/Artificial_intelligence_in_space (accedido el 4 de enero de 2025).
135. Escobar (2020). Mando y Control. Revista de Marina, Chile <https://revistamarina.cl/revistas/1986/1/escobar.pdf>
136. EU (2023). Joint Communication to The European Parliament and The Council. European Union Space Strategy for Security and Defence. JOIN (2023) 9 final. Brussels, 10.3.2023. [https://ec.europa.eu/transparency/documents-register/detail?ref=JOIN\(2023\)9&lang=en](https://ec.europa.eu/transparency/documents-register/detail?ref=JOIN(2023)9&lang=en)

137. European Commission (2019). Ethics Guidelines for Trustworthy AI. <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.
138. European Council (2021) European Peace Facility. Council Decision (CFSP) 2021/509 of 22 March 2021 <https://www.consilium.europa.eu/en/policies/european-peace-facility/>
139. European Council (2025). Special meeting of the European Council (6 March 2025). Conclusions. [https://urldefense.com/v3/__https://www.consilium.europa.eu/media/tzkadtec/20250306-european-council-conclusions-en.pdf__;!!D9dNQwwGXtA!Xmohgh2_RuOi8kttW692Zz3duPAFUh-3dJLcRr7ZN4SGn92MCuZnx9pYl4GWTLDKfEg-xrFXKZUoZjXn_EQ1ffl5w3OP3shWqZuMgWJZOBw\\$](https://urldefense.com/v3/__https://www.consilium.europa.eu/media/tzkadtec/20250306-european-council-conclusions-en.pdf__;!!D9dNQwwGXtA!Xmohgh2_RuOi8kttW692Zz3duPAFUh-3dJLcRr7ZN4SGn92MCuZnx9pYl4GWTLDKfEg-xrFXKZUoZjXn_EQ1ffl5w3OP3shWqZuMgWJZOBw$)
140. Eurospace (2023). Eurospace Position Paper: Recommendations for implementation of the EU Space Strategy for Security & Defence – October 2023. <https://eurospace.org/download/5540/?tmstv=1698328271>
141. EUSPA (2025). GNSS and Secure Satcom. User Technology Report. 28 January 2025. <https://www.euspa.europa.eu/tech-report>
142. Evanson, N. (2024). N.,” Goodbye to Graphics: How GPUs came to dominate AI and compute. TechnSpot. Disponible en línea: <https://www.techspot.com/article/2702-gpu-compute-ai/>
143. Evanson, N. (2025). What Are Chiplets and Why They Are So Important for the Future of Processors. Techspot. Disponible en línea: <https://www.techspot.com/article/2678-chiplets-explained/>
144. Eyre, H.A., Hynes, W., Ling, G., Occhipinti, J.A., Ayadi, R., Matthews, M., Abbott, R., and Love, P, (2023). From Neuroweapons to ‘Neuroshields’: Safeguarding Brain Capital for National Security. Rice University’s Baker Institute for Public Policy. August 10, 2023, <https://doi.org/10.25613/MS7G-YX19>
145. FEI (2024). Contribución de España a la soberanía tecnológica europea en inteligencia artificial. Análisis y recomendaciones de actuación. Foro de Empresas Innovadoras. Octubre 2024. <http://foroempresasinnovadoras.com/wp-content/uploads/2024/10/2024-10-15-Informe-FEI-sobre-autonomia-estrategica-en-IA-VCON-PORTADA.pdf>
146. Feijoo González, Claudio (2021). El gran sueño de China. Tecno-socialismo y capitalismo de Estado. Madrid: tecnos.
147. Fenstermacher, L., Uzhca, D., Larson, K., Vitiello, C., Shellman, S. (2023). New Perspectives on Cognitive Warfare. Dist A – Reference Number RH-23-124383 Case Reviewer: Keith Klug Case Number: AFRL-2023-2500).
148. Field, H. (2025). Scale AI announces multimillion-dollar defense deal, a major step in U.S. military automation. AI EFFECT. March 5, 2025. <https://www.cnbc.com/2025/03/05/scale-ai-announces-multimillion-dollar-defense-military-deal.html>
149. Fiott, D. (2024). Integrated Arsenal? Mapping Defence Industrial Relations Between Europe and Ukraine. ARES (Armament Industry European Research Group). December 2024. https://www.iris-france.org/wp-content/uploads/2024/12/ARES_2024_12_107_Ukraine_Defence_Industry_PolicyPaper.pdf

150. Fogarty, K. (2019). GaN versus Silicon for 5G. Retrieved from Semiconductor Engineering.
151. Fossaceca, J. (2023). Delivering on the promise of autonomous agents in the battlefield. Proc. SPIE, vol. 12538.
152. Freedberg, S. (2020). "Army Robots Hunt Tanks in Project Convergence", *Breaking Defense*. Disponible en línea: <https://breakingdefense.com/2020/09/army-robots-hunt-tanks-in-project-convergence/> (Accedido: 3-3-2025).
153. Freund, Y., & Schapire, R. E. (1997). A decision-theoretic generalization of on-line learning and an application to boosting. Journal of Computer and System Sciences. Volume 55, Issue 1, August 1997, Pages 119-139. <https://doi.org/10.1006/jcss.1997.1504>
154. Frías, C. (2024). Rusia, Ucrania y el campo de batalla «transparente». Documento de opinión 18/2024, Instituto Español de Estudios Estratégicos. 16 de febrero de 2024. https://www.iee.es/Galerias/fichero/docs_opinion/2024/DIEEO18_2024_CARFRI_Rusia.pdf
155. Friedman, J. H. (2001). Greedy Function Approximation: A Gradient Boosting Machine. Annals of Statistics.
156. FRONTEX (2023). High Altitude Pseudo Satellites: HAPS Final Report. FRONTEX: European Border and Coast Guard Agency. 2023. <https://www.frontex.europa.eu/innovation/eu-research/news-and-events/research-study-on-high-altitude-pseudo-satellites-project-closure-dMPhtc>
157. FUHEM 2025. Inteligencia artificial y armas autónomas: una combinación letal. 13 febrero, 2025. "Fundación FUHEM," Disponible en línea: <https://www.fuhem.es/> (Accedido: 15-feb-2025).
158. Funk, A., Vesteinsson, K., and Shahbaz, A. (2023). The Repressive Power of Artificial Intelligence. Freedom House, 2023. <https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence#generative>
159. Gady, S. (2023). "Ukraine's Use of AI-Powered Drones in the War Against Russia," The Diplomat. <https://thediplomat.com/2023/05/ukraines-use-of-ai-powered-drones-in-the-war-against-russia/>. [Accedido: 15-feb-2025].
160. Gallagher, J. y E. Oughton (2024). Transforming the Multidomain Battlefield with AI," Military Review. Disponible en línea: <https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2024-OLE/Multidomain-Battlefield-AI/> (Accedido: 3-3-2025).
161. García-Cantalapiedra, D. (2022). La estrategia de las Tres Guerras: la Guerra Política con características chinas dentro de la Gran Estrategia de la República Popular de China. Documento de Opinión IEEE Instituto Español de Estudios Estratégicos. 29/2022. Marzo de 2022. https://www.iee.es/Galerias/fichero/docs_opinion/2022/DIEEO29_2022_DAVGAR_China.pdf
162. García-García, E. (2025). DeepSeek y Trump 2.0: impacto en la industria, en la geopolítica global y en las políticas europeas. Elcano Policy Paper. Real Instituto Elcano. Julio 2025. <https://media.realinstitutoelcano.org/wp-content/uploads/2025/07/policy-paper-deepseek-y-trump-2-0-impacto-en-la-industria-en-la-geopolitica-global-y-en-las-politicas-eur.pdf>

163. Gautier, L. (2023). La era estratégica de la Guerra del Golfo. Le Grand Continent. 15 de agosto de 2023. <https://legrandcontinent.eu/es/2023/08/15/la-era-estrategica-de-la-guerra-del-golfo/>
164. GEC (2020). Pilares del Ecosistema de Desinformación y Propaganda de Rusia. Informe especial del GEC. Global Engagement Center. Departamento de Estado de los Estados Unidos. Agosto de 2020. <https://www.state.gov/russias-pillars-of-disinformation-and-propaganda-report/>
165. Giannopoulos, G., Smith, H., Theocharidou, M. (2021). The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305 https://publications.jrc.ec.europa.eu/repository/bitstream/JRC123305/conceptual_framework-reference-version-shortened-good_cover_-_publication_office_1.pdf
166. Giglou, H.B.; D'Souza, J. y Auer, S. (2023). LLMs4OL: Large Language Models for Ontology Learning. En T. R. Payne et al. Proceedings of the International Semantic Web Conference. ISWC 2023. Lecture Notes in Computer Science, vol. 14265.
167. Gil, A. (2023). Sistemas de armas autónomos letales. comentario a la posición española, con especial atención a algunos problemas jurídico-penales. Revista General de Derecho Administrativo. Mayo 2023. https://www.researchgate.net/publication/370985060_SISTEMAS_DE_ARMAS_AUTONOMOS_LETALES_COMENTARIO_A_LA_POSICION_ESPANOLA_CON_ESPECIAL_ATENCION_A_ALGUNOS_PROBLEMAS_JURIDICO-PENALES#:~:text=Copy,-link,-Abstract
168. Goberna (2025). Guerra Cognitiva y PSYOPS: los conceptos del fantasma en la máquina. Grupo Goberna. Febrero 2025. <https://grupogoberna.com/guerra-cognitiva-y-psyops-conceptos-fantasma/>
169. Gobierno de España (2025). Plan Industrial y Tecnológico para la Seguridad y la Defensa Ejercicio 2025. Abril 2025. <https://www.lamoncloa.gob.es/consejodeministros/resumenes/Documents/2025/230425-plan-industrial-y-tecnologico-para-la-seguridad-y-la-defensa.pdf>
170. Gómez de Agreda, A. (2020). Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R). Centro Conjunto de Desarrollo de Conceptos. Ministerio de Defensa. Julio de 2020. https://emad.defensa.gob.es/Galerias/CCDC/files/USOS_MILITARES_DE_LA_INTELIGENCIA_ARTIFICIALx_LA_AUTOMATIZACION_Y_LA_ROBOTICA_xIAAxRx._VV.AA.pdf
171. Gómez de Ágreda, A. (2024). IA en la defensa de la República de Corea y de Japón. Documento de análisis. IEEE. 78/2024 10/12/2024
172. Gómez-Pérez, A. (2023). Inteligencia artificial y lengua española. Discurso leído el día 21 de mayo de 2023, en su recepción pública, y contestación de S. Muñoz Machado. Real Academia Española. Madrid. <https://www.rae.es/sites/default/files/2023-05/Discurso%20de%20ingreso%20de%20Asuncion%20Gomez-Perez.pdf>
173. Gómez-Pérez, A. (2024). Ingeniería Ontológica, Discurso de entrada en la Real Academia de Ingeniería.
174. Gómez-Pérez, M. Fernández-López y O. Corcho (2004): Ontological Engineering: with examples from the areas of Knowledge Management, e-Commerce and the Semantic Web. Springer, London.

175. González, R. (2024). ¿Puede ser la IA confiable? Aufklärung, volumen 11, 2024 <https://10.18012/arf.v11iespecial.69910>
176. González-Agirre, A.; Pàmies, M.; Llop, J.; Baucells, I.; Da Dalt, S.; Tamayo, D.; Saiz, J. J.; Espuña, F.; Prats, J.; Aula-Blasco, J.; Mina, M.; Rubio, A.; Shvets, A.; Sallés, A.; Lacunza, I.; Pikabea, I.; Palomar, J.; Falcao, J.; Tormo, L.; Vázquez-Reina, L.; Marimon, M.; Ruíz-Fernández, V.; Villegas, M. (2025). Salamandra Technical Report, arXiv:2502.08489
177. Gosselin-Malo, E. (2025). "Estonia's Milrem reveals first look at new war robot", *Defense News*. Disponible en línea: <https://www.defensenews.com/industry/2025/02/17/estonias-milrem-reveals-first-look-at-new-war-robot/> (Accedido: 3-3-2025).
178. GovCon Wire (2025). Edge Computing, AI & 5G in DoD Tactical Ops. Disponible en línea: <https://www.govconwire.com/2025/01/dod-edge-computing-ai-5g-research-development/> (Accedido: 3-3-2025).
179. Grand Continent (2025). ¿Qué hay que hacer en la era Trump? El manifiesto europeo de Mario Draghi. Le Grand Continent. 19 de febrero de 2025. <https://legrandcontinent.eu/es/2025/02/19/que-hay-que-hacer-en-la-era-trump-el-manifiesto-europeo-de-mario-draghi/>
180. Grest, H. (2022). High-Altitude Platform Systems: Alternative, Supplement, or Competition to Satellites? JAPCC. Journal Edition 34. July 2022. https://www.japcc.org/wp-content/uploads/JAPCC_J34_Art-03_screen.pdf
181. Grigsby, C., Bridges N., McKinley, R.A., et al. (2023) Developing cognitive neuroscience technologies for defence against cognitive warfare. In: Masakowski YR, Blatny JM (eds) Mitigating and Responding to Cognitive Warfare. NATO Science and Technology Organization. <https://apps.dtic.mil/sti/trecms/pdf/AD1200226.pdf>
182. Guitton, M. J. (2021). Fighting the locusts: Implementing military countermeasures against drones and drone swarms. Scandinavian Journal of Military Studies, 4(1).
183. Guo, Z., Xue, X., Zhou, Q., & Zeng, X. (2024). Computing in Memory for Accelerating Light-Weighted On-Chip Learning in IoT Devices. 2024 IEEE 17th International Conference on Solid-State & Integrated Circuit Technology (ICSICT) |.
184. Gupta, S., & Jolly, X. (2024). Neuromorphic Photonic On-chip Computing. Preprints.org (www.preprints.org) |.
185. Gutiérrez Fandiño, A., Armegol Estapé, J., Pàmies, M., Llop Palao, J., Silveira Ocampo, J., Pio Carrino, C. y Villegas, M. (2022). "Maria: Spanish language models", Procesamiento del Lenguaje Natural, 68.
186. Gutierrez, P. (2024). GMV-led Project Develops AI-based Jamming and Spoofing Mitigation. December 26, 2024. <https://insidegnss.com/gmv-led-project-develops-ai-based-jamming-and-spoofing-mitigation/>

187. Gutiérrez-Caneda, B., y Vázquez-Herrero, J. (2024). Redrawing the Lines Against Disinformation: How AI Is Shaping the Present and Future of Fact-checking. *Tripodos*, (55), 55–74. <https://doi.org/10.51698/tripodos.2024.55.04>
188. H. Shortliffe (1976). *Computer-based Medical Consultations: MYCIN*. Elsevier Computer Science Library.
189. Hadley, G. (2024). Space Force Is Testing AI to Automate Ops—and Eyeing More. *Air&Space Forces Magazine*. Dec. 12, 2024, <https://www.airandspaceforces.com/space-force-testing-ai-automate-ops/>
190. Hagen (2024). Cognitive Warfare, Cybersecurity, and the AI Challenge. 16 de febrero de 2024. <https://www.linkedin.com/pulse/cognitive-warfare-cybersecurity-ai-challenge-raymond-andr%C3%A8-hagen-fvsef/>
191. Hambling, D. (2018). Swarm of drones attacks airbase, *New Scientist*, vol. 237.
192. Hanna, H. (2025). The Emerging Potential for Quantum Computing in Irregular Warfare. *Irregular Warfare Center*. January 28, 2025. Disponible en línea: <https://irregularwarfarecenter.org/publications/insights/the-emerging-potential-for-quantum-computing-in-irregular-warfare/>
193. Hao, S., Han, W., Yiang, T., Li, Y. Wu, H., Zhong, C., Zhouy, Z., (2024). Synthetic Data in AI: Challenges, Applications, and Ethical Implications. *arXiv.org*. 03 Jan 2024. <https://arxiv.org/html/2401.01629v1>
194. Harper, J. (2024). Combatant commands poised to scale targeting capabilities via Palantir’s Maven system. *DEFENSESCOOP*. May 30, 2024. <https://defensescoop.com/2024/05/30/combatant-commands-palantir-maven-scale-targeting-capabilities/>
195. Häyry, M. (2021). “Employing Lethal Autonomous Weapon Systems,” *Int. J. Appl. Philos.*
196. Heitor, M. (2024). Align, act, accelerate – Research, technology and innovation to boost European competitiveness, European Commission: Directorate-General for Research and Innovation, Publications Office of the European Union, 2024, <https://data.europa.eu/doi/10.2777/9106236>
197. Hendrycks, D., Burns, C., Basart, S., Zou, A., Mazeika, M., Song, D., & Steinhardt, J. (2020). Measuring massive multitask language understanding. *arXiv preprint arXiv:2009.03300*.
198. Hernández-García, Luis A. La zona gris: una aproximación conceptual desde las FAS. Documento de Opinión IEEE 34/2022. https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEO34_2022_LUISHER_Zona.pdf y/o enlace bie3 (consultado 2 de enero de 2025)
199. Hildmann, H.; E. Kovacs, F. Saffre, y A. Isakovic (2019). “Nature-Inspired Drone Swarming for Real-Time Aerial Data-Collection Under Dynamic Operational Constraints,” *Drones*, vol. 3, no. 3, p. 71.
200. Hinton, G. E., & Salakhutdinov, R. R. (2006). Reducing the Dimensionality of Data with Neural Networks. *Science*, 313(5786), 504–507. Jul 28;313(5786):504-7. doi: <https://doi.org/10.1126/science.1127647>

201. Ho, J. H., Kang, H., Pérez, J. et al. (2020). Spanish Pre-Trained BERT Model and Evaluation Data, PML4DC ICLR
202. Hochreiter, S. y Schmidhuber, J. (1997). "Long Short-Term Memory", *Neural Computation*, 9 (8), pp. 1735-1780.
203. Hochreiter, S. & Schmidhuber, J. (1997). Long Short-Term Memory. *Neural Computation*, 9(8), 1735–1780Hoffman, F. (2007): Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for policy Studies, Arlington (Virginia). https://www.potomac institute.org/images/stories/publications/potomac_hybridwar_0108.pdf
204. Hoffman, F., Neumayer, M., Jensen, B. (2024). The Future of Hybrid Warfare. Center for Strategic and International Studies (CSIS). July 8, 2024. <https://www.csis.org/analysis/future-hybrid-warfare>
205. Hoi tjinj, M. y van der Kist, J. (2025). Platforms on the Frontline: The Rise of the Platform Model in Defense Tech. *OpinioJuris*. 11 Feb 2025. <https://opiniojuris.org/2025/02/11/platforms-on-the-frontline-the-rise-of-the-platform-model-in-defense-tech/>
206. Hooker, L., and Wallace, C. (2025). Concern over Google ending ban on AI weapons. BBC. 5 February 2025. <https://www.bbc.com/news/articles/cy081nqx2zjo>
207. HuffingtonPost 04/12/2024.Los drones tirados de precio toman el control de la guerra. Disponible en línea: <https://www.huffingtonpost.es/global/los-drones-tirados-precio-toman-control-guerra.html>. (Accedido: 26-feb-2025)
208. HuffingtonPost 12/12/2024. Ucrania da un paso más en la guerra con el despliegue del súper robot caza droide con potente ametralladora. Disponible en línea: <https://www.huffingtonpost.es/global/ucrania-da-paso-mas-guerra-despliegue-super-robot-caza-droide-potente-ametralladora.html>. (Accedido: 26-feb-2025)
209. Hung, T. C., and Hung, T. W. (2022). How China's cognitive warfare works: a frontline perspective of Taiwan's anti-disinformation wars. *J. Glob. Sec. Stud.* 7:ogac016. doi: <https://doi.org/10.1093/jogss/ogac016>
210. Husain, A. (2024). The Military Applications of Artificial Intelligence in Space. *Forbes*. Aug 19, 2024. <https://www.forbes.com/sites/amirhusain/2024/08/19/the-military-applications-of-artificial-intelligence-in-space/> (accedido el 4 de enero de 2025)
211. IEEE (2024). La inteligencia artificial en la geopolítica y los conflictos. Cuadernos de Estrategia 226. IEEE. 2024
212. Iida, M. (2024). China's Chilling Cognitive Warfare Plans. War is entering a new, and very frightening, domain. *The Diplomat*. May 05, 2024. <https://thediplomat.com/2024/05/chinas-chilling-cognitive-warfare-plans/>
213. Impiombato, D., Attrill, N., Zhang, A., Ryan, F., Allen, B. (2024). Persuasive technologies in China: Implications for the future of national security. Policy Brief. ASPI (Australian Strategic Policy Institute). November 2024.

214. Instant Connect (2023). Real-Time Language Translation – Military PTT. Disponible en línea: <https://www.instantconnectnow.com/military/real-time-language-translation/> (Accedido: 3-3-2025)
215. IRDS (2023). International Roadmap Devices and Systems (IRDS). IEEE.
216. ISDEFE (2024). Capacidades Militares en el Ámbito Europeo de la Defensa. Volumen 1 Serie Cuadernos Tecnológicos. Cuadernos de Isdefe. Junio 2024. ISBN: 978-84-09-62256-6
217. Ishida, S., Nishitsutsumi, Y., Kashioka, H., Taguchi, T., Shineha, R. (2023). A comparative review on neuroethical issues in neuroscientific and neuroethical journals. *Front. Neurosci.*, 14 Volume 17 September 2023 <https://doi.org/10.3389/fnins.2023.1160611>
218. Isik, M. (2023). A Survey of Spiking Neural Network Accelerator on FPGA. *Journal of Latex Class, IEEE*, 1-15.
219. Istace, T. & Costas, M. (2024). Research Brief Between Science-Fact and Science-Fiction: Innovation and Ethics in Neurotechnology. The Geneva Academy of International Humanitarian Law. May 2024. <https://www.geneva-academy.ch/joomlatools-files/docman-files/Between%20Science-Fact%20and%20Science-Fiction%20Innovation%20and%20Ethics%20in%20Neurotechnology.pdf>
220. Jeroen Kusters, D. B. (2025). Deloitte Center for Technology, Media & Telecommunications. Retrieved from 2025 global semiconductor outlook: <https://www2.deloitte.com/us/en/insights/industry/technology/technology-media-telecom-outlooks/semiconductor-industry-outlook.html>
221. Jiang, A.Q., Sablayrolles, A., Mensch, A., Bamford, C., Chaplot, D.S., Casas, D.D., Bressand, F., Lengyel, G., Lample, G., Saulnier, L., Lavaud, L.R., Lachaux, M., Stock, P., Scao, T.L., Lavril, T., Wang, T., Lacroix, T., y Sayed, W.E. (2023). Mistral 7B. ArXiv, abs/2310.06825.
222. Jones, S.G. (2025a). The Tech Revolution and Irregular Warfare: Leveraging Commercial Innovation for Great Power Competition. Center for Strategic & International Studies. January 30, 2025. <https://www.csis.org/analysis/tech-revolution-and-irregular-warfare-leveraging-commercial-innovation-great-power>
223. Jones, S.G. (2025b). Russia's Shadow War Against the West. Center for Strategic & International Studies. March 18, 2025. <https://www.csis.org/analysis/russias-shadow-war-against-west>
224. Jones, S. y McCabe (2025). Russia's Battlefield Woes in Ukraine. CSIS Brief. Center for Strategic and International Studies. June 2025. Disponible en línea: <https://www.csis.org/analysis/russias-battlefield-woes-ukraine>
225. Joshi, A., Spilbergs, A., & Mīkelsone, E. (2024). AI-Enabled Drone Autonomous Navigation and Decision Making for Defence Security. In *Environment, Technologies, resources. Proceedings of the International Scientific and Practical Conference* (Vol. 4, pp. 138-143).
226. Jospin, L. V., Laga, H., Boussaid, F., Buntine, W. y Bennamoun, M. (2022). "Hands-On Bayesian Neural Networks—A Tutorial for Deep Learning Users," in *IEEE Computational Intelligence Magazine*, vol. 17, no. 2, pp. 29-48, May 2022, doi: 10.1109/MCI.2022.3155327. <https://ieeexplore.ieee.org/document/9756596>

227. JRC (2021). The landscape of Hybrid Threats: A conceptual model. EUR 30585 EN 2021. Joint Research Centre. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC123305/conceptual_framework-reference-version-shortened-good_cover_-_publication_office_1.pdf
228. Jumper, J., Evans, R., Pritzel, A., Green, T., Figurnov, M., Ronneberger, O. et al. (2021). Highly Accurate Protein Structure Prediction with AlphaFold. *Nature*, 596(7873), 583-589.
229. Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G. (2023). Hybrid threats: a comprehensive resilience ecosystem, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/37899, JRC129019. https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf
230. Kallenborn, Z. (2022). InfoSwarms: Drone Swarms and Information Warfare. The US Army War College Quarterly: Parameters.
231. Kalpokas, I. (2024). Post-Truth and Information Warfare in their Technological Context. *Applied Cybersecurity & Internet Governance. ACIG*, vol. 4, no. 2, 2024. <https://doi.org/10.60097/ACIG/190407>
232. Kania, E. B. (2022). Minds at War China's Pursuit of Military Advantage through Cognitive Science and Biotechnology. *PRISM* 8, NO. 3. https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Kania_82-101.pdf
233. Karadeniz, G.; A. Ozcan, M. Bayram, y G. Ince (2023). Simulation of counter-UAV tactics against drone swarms: a serious game approach. In: 10th International Conference on Recent Advances in Air and Space Technologies (RAST), pp. 1–6.
234. Kelleher, A. (2022). Moore's Law - Now and in the future. Obtenido de INTEL: <https://download.intel.com/newsroom/2022/manufacturing/Intel-Moores-Law-Investor-Meeting-Paper-final.pdf>
235. Khaki, A. M., y Choi, A. (2025). Optimizing Deep Learning Acceleration on FPGA for Real-Time and Resource-Efficient Image Classification. *Applied Sciences MDPI*, 1-13.
236. Khalyeyev, D., Bureš, T., Hnětynka, P. (2023). Towards Characterization of Edge-Cloud Continuum. In: Batista, T., Bureš, T., Raibulet, C., Muccini, H. (eds) *Software Architecture. ECSA 2022 Tracks and Workshops. ECSA 2022. Lecture Notes in Computer Science*, vol 13928. Springer
237. Khan AN, Ihalage AA, Ma Y, Liu B, Liu Y, Hao Y (2021). Deep learning framework for subject-independent emotion detection using wireless signals. *PLoS ONE* 16(2): e0242946. February 3, 2021. <https://doi.org/10.1371/journal.pone.0242946>
238. Khan, S. M., y Mann, A. (2020). AI Chips: What they are and why they matter. *CSET (Center for Security and Emergency Technology)*.
239. Kiaei, P.; Schaumont, P, "SoC Root Canal!" *IACR Transactions on Cryptographic Hardware and Embedded Systems* ISSN 2569-2925, Vol. 2022, No. 4, pp. 751–773.
240. Kirichenko, D. (2025). Ukraine hopes robot army can counter Russia's battlefield advantages, *Atlantic Council*. Disponible en línea: <https://www.atlanticcouncil.org/blogs/ukrainealert/ukraine-hopes-robot-army-can-counter-russias-battlefield-advantages/> (Accedido: 3-3-2025)

241. Klaus, M. (2024). Transcending weapon systems: the ethical challenges of AI in military decision support systems. *Humanitarian Law & Policy*. September 24, 2024. <https://blogs.icrc.org/law-and-policy/2024/09/24/transcending-weapon-systems-the-ethical-challenges-of-ai-in-military-decision-support-systems/>
242. Koch, W. (2021). On Digital Ethics for Artificial Intelligence in Hybrid Military Operations. STOMP-IST-190 (NATO). © Fraunhofer FKIE. 2021.
243. Kori, G. S.; M. Kakkasageri, V. Hiremath, P. M. Chanal, R. Pujar, y V. A. Telsang (2024). Cognitive Swarm Drones Attack Model: A Grey Wolf Optimization Approach. In *IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, pp. 1–6.
244. Kormych, B., Malyarenko, T, Wittke, C. (2023). Rescaling the legal dimensions of grey zones: Evidence from Ukraine. *Global Policy*. Volume 14, Issue 3. June 2023 <https://doi.org/10.1111/1758-5899.13233>
245. Kosal M., y Putney J. (2023). Neurotechnology and international security: Predicting commercial and military adoption of brain-computer interfaces (BCIs) in the United States and China. *Politics Life Sci.* 2023 Apr;42(1):81-103. doi: 10.1017/pls.2022.2. PMID: 37140225 <https://pubmed.ncbi.nlm.nih.gov/37140225/>
246. Kott, A. (2018). Intelligent autonomous agents are key to cyber defense of the future army networks. *The Cyber Defense Review*, 3(3), 57-70.
247. Kozyreva, A., Lewandowsky, S., & Hertwig, R. (2020). Citizens Versus the Internet: Confronting Digital Challenges with Cognitive Tools. *Psychological Science in the Public Interest*, 21(3), 103-156. <https://doi.org/10.1177/1529100620946707>
248. Kratos (2024). Towards Complete Space Domain Awareness. How RF Data Fills the Gaps in Orbital, Link and Terrestrial SDA. <https://www.kratosdefense.com/download/rf-space-situational-awareness-whitepaper>
249. Krelina, M. (2021). Quantum technology for military applications. *EPJ Quantum Technology*, vol. 8 (2021). <https://www.sipri.org/publications/2025/sipri-background-papers/introduction-military-quantum-technology-policymakers>
250. Krelina, M. (2025). An introduction to military quantum technology for policymakers. SIPRI Background Paper. March 2025. DOI: <https://doi.org/10.55163/DRDQ1599>
251. Kurt, G.A., Khoshkholgh, M., Alfattani, S., Ibrahim, A., Darwish, T., Alam, S., Yanikomeroglu, H., Yongacoglu, A. (2021). A vision and Framework for the High-Altitude Platform Station (HAPS) Networks of the Future. arXiv:2007.15088v4 [cs.IT] 18 Mar 2021.
252. Kwik, J, Zwanenburg, M., Cheya, T. and Joep, A. (2025). Controlling Military Artificial Intelligence: Harnessing Rules of Engagement and Military Directives. T.M.C. Asser Institute for International & European Law, ASSER Policy Brief No. 2025-01 February 03, 2025. <https://ssrn.com/abstract=5132731> or <http://dx.doi.org/10.2139/ssrn.5132731>

253. Lacey, G., Taylor, G., & Areibi, S. (2016). Deep Learning on FPGAs: Past, Present and Future. researchgate.net.
254. Lachow, I. (2017). The upside and downside of swarming drones. *Bulletin of the Atomic Scientists*, 73, 101 - 96.
255. Lahmann (2024). European Security and the Threat of 'Cognitive Warfare'. Beware of the Algorithmic Ministry of Truth. *Verfassungsblog*. Europe's Geopolitical Coming of Age: Adapting Law and Governance to Harsh International Realities. 3 noviembre de 2024. <https://verfassungsblog.de/european-security-and-the-threat-of-cognitive-warfare/>
256. Lange, L. (2024). Decoding China's AI-powered "Algorithmic Cognitive Warfare". Special Competitive Studies Project. November 2024. <https://www.scsp.ai/resource/decoding-chinas-ai-powered-algorithmic-cognitive-warfare/>
257. Marco Lanzagorta (2012). *Quantum Radar*". Morgan & Clypool Publishers. Synthesis Lectures on Quantum Computing.
258. Latheef S. (2023). Brain to Brain Interfaces (BBIs) in future military operations; blurring the boundaries of individual responsibility. *Monash Bioeth Rev*. 2023 Jun;41(1):49-66. doi: <https://doi.org/10.1007/s40592-022-00171-7> . PMID: 36550229.
259. Lavadia, M. L. (2025). Public Spectrum February 12, 2025. <https://publicspectrum.co/military-fortifies-frontline-against-llm-ai/>
260. Lavoix. H., Taboy, T., Valantin, J.M. (2025). La IA en las raíces de la guerra: gramática de una nueva geopolítica. *Grand Continent*. 8 de enero de 2025. <https://legrandcontinent.eu/es/2025/01/08/la-ia-en-las-raices-de-la-guerra/>
261. Le Scao, T., Fan, A., Akiki, C., Pavlick, E., Ilić, S., Hesslow, D. et al. (2023). Bloom: A 176b-parameter open-access multilingual language model.
262. Lebrete, M., Ogden, T., Black, J. (2024). Cross-cutting technologies in Chinese space activities: Raising the risk of hybrid threats. *Hybrid CoE Paper 22*. December 2024. <https://www.hybridcoe.fi/publications/hybrid-coe-paper-22-cross-cutting-technologies-in-chinese-space-activities-raising-the-risk-of-hybrid-threats/>
263. LeCun, Y., Bottou, L., Bengio, Y., & Haffner, P. (1998). Gradient-Based Learning Applied to Document Recognition. *Proceedings of the IEEE*, 86(11), 2278–2324. <https://doi.org/10.1109/5.726791>.
264. León (2024). Tendencias en las tecnologías para el aumento de capacidades humanas. Academia de las Artes y las Ciencias Militares (ACAMI). 2024. Ed. Astorga: ELC-Ediciones La Crítica. <https://www.acami.es/publicacion/el-aumento-de-las-capacidades-humanas-libro/>
265. León (2025a). El papel de las tecnologías duales en la defensa y seguridad europea. Academia de las Ciencias y las Artes Militares ACAMI. Sección de Prospectiva de la Tecnología Militar. 3/2025. <https://www.acami.es/wp-content/uploads/2025/03/Tecnologias-duales-en-la-defensa-europea-web.pdf>

266. León, G. (2023). Relevancia geopolítica de las tecnologías duales. Consecuencias y oportunidades para reforzar la soberanía tecnológica de la Unión Europea, UPM Press. ISBN: 978-84-18661-44-0
267. León, G. (2024). Tendencias en las tecnologías para el aumento de capacidades humanas. Academia de las Artes y las Ciencias Militares (ACAMI). 2024. Ed. Astorga: ELC-Ediciones La Crítica. <https://www.acami.es/publicacion/el-aumento-de-las-capacidades-humanas-libro/>
268. León, G. (2025). Contexto y repercusión del «Informe Draghi» desde la perspectiva europea de la Defensa y la Seguridad. Academia de las Ciencias y las Artes Militares. Marzo 2025. Monografías y Ensayos Nº 13. <https://www.acami.es/publicacion/informe-draghi-y-la-defensa-y-seguridad-europeas/>
269. León, G. (2025). Contexto y repercusión del «Informe Draghi» desde la perspectiva europea de la Defensa y la Seguridad. Serie de monografías y ensayos. Número 13. Academia de las Ciencias y las Artes Militares. Marzo de 2025.
270. Letta, E. (2024). Much more than a market – Speed, Security, Solidarity Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens. April 2024. <https://european-research-area.ec.europa.eu/documents/letta-report-much-more-market-april-2024>
271. Lewis, Patrick, Ethan Perez, Aleksandra Piktus, Fabio Petroni, Vladimir Karpukhin, Naman Goyal, Heinrich Küttler, Mike Lewis, Wen-tau Yih, Tim Rocktäschel, et al. (2020). Retrieval-augmented generation for knowledge-intensive nlp tasks. *Advances in Neural Information Processing Systems*, 33:9459–9474.
272. Li, B., Gu, J., & Jiang, W. (2019). Artificial Intelligence (AI) chip technology review. *International Conference on Machine Learning, Big Data and Business Intelligence (MLBDBI)* (pp. 114-117). Taiyuan (China): IEEE.
273. Li, C., Lammie, C., Le Gallo, M., & Rajendran, B. (2024). Efficient Deployment of Transformer Models in Analog In-Memory Computing Hardware. *arXiv:2411.17367*.
274. Li, D. (2023). Analysis the principle of AI Chip principle and the State-of-the-art applications. *Highlights in Science, Engineering and Technology*, Volume 76.
275. Li, Z., Zhang, Y., & Wang, J. (2020). A survey of FPGA design for AI era. *Journal of Semiconductors*.
276. Liu, R.; Guo, Y.; J. Nie, Q. Hu, Z. Xiong, H. Yu, and M. Guizani (2022). Intelligent Edge-Enabled Efficient Multi-Source Data Fusion for Autonomous Surface Vehicles in Maritime Internet of Things. In *IEEE Transactions on Green Communications and Networking*, vol. 6, pp. 1574–1587.
277. Liu, W., Wu, M., Wan, G. y Xu, M. (2024). Digital Twin of Space Environment: Development, Challenges, Applications, and Future Outlook. *Remote Sens.* 2024, 16(16), 3023; 18 August 2024. <https://doi.org/10.3390/rs16163023>
278. Liu, Y., Ott, M., Goyal, N., Du, J., Joshi, M., Chen, D., y Stoyanov, V. (2019). RoBERTa: A Robustly Optimized BERT Pretraining Approach. *arXiv preprint arXiv:1907.11692*.

279. Loizou, C. and Ippolito, V. (2024). Europe's future capabilities in space and in the higher atmosphere. Defence Industry Europe. January 29, 2024. <https://defence-industry.eu/europes-future-capabilities-in-space-and-in-the-higher-atmosphere/>
280. López-García, A. (2024). El efecto de las tecnologías cuánticas en la estrategia de seguridad militar. LISA News. 9 de octubre de 2024.
281. Luna-Alcoba, M. (2024). Caja morfológica del concepto de «guerra híbrida». Revista Del Instituto Español De Estudios Estratégicos (22), 131–166 / 491. <https://revista.ieee.es/article/view/6132> . Consultado 2 de enero de 2025.
282. Lupiáñez, M. (2024). Cómo hacer frente a un ataque cognitivo: Prototipo de detección de la propaganda y manipulación en operaciones psicológicas dirigidas a civiles durante un conflicto. Revista del Instituto Español de Estudios Estratégicos n.º 22 - Año: 2023 - Págs.: 61 a 93. mayo 2024. https://publicaciones.defensa.gob.es/media/downloadable/files/links/r/e/revista_ieee_22.pdf
283. M. Draghi (2024). The future of European Competitiveness. 9 September 2024. https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en?prefLang=es&etrans=es#paragraph_47059
284. Machado Cuellar, Leidy & Rodríguez, Leonardo y Orduz, Sergio & Saavedra Mora, David & Murcia Torrejano, Valentín & Riascos, Andrea & Hernández, Heimar & Méndez Pastrana, Diego. (2020). Aplicación de nuevas tecnologías en el fortalecimiento de la cadena Agroindustrial. December 2020. ISBN: 978-958-15-0593-7
285. Mantua, J. (2023). China's Focus on the Brain Gives it an Edge in Cognitive Warfare. July 6, 2023. <https://irregularwarfare.org/articles/chinas-focus-on-the-brain-gives-it-an-edge-in-cognitive-warfare/>
286. Manuel, R. (2024). Overland AI Secures Funding for Tactical Autonomous Driver Software, The Defense Post. Disponible en línea: <https://thedefensepost.com/2024/05/21/overland-tactical-autonomous-driver-software/> (Accedido: 3-3-2025).
287. Marahrens, S., and Schröfl, J. (2024). The Russia-Ukraine Conflict from a Hybrid Warfare Cognitive Perspective. The Defence Horizon Journal. April 25, 2024. <https://tdhj.org/blog/post/russia-ukraine-hybrid-cognitive-warfare/>
288. Marin, D. (2024). Luna-10, la iniciativa de DARPA para sostener una base lunar. 31 mayo, 2024. <https://danielmarin.naukas.com/2024/05/31/luna-10-la-iniciativa-de-darpa-para-sostener-una-base-lunar/>
289. Marma, K.J. (2025). Cognitive Warfare: The Invisible Frontline of Global Conflicts. Modern Diplomacy, February 12, 2025. <https://moderndiplomacy.eu/2025/02/12/cognitive-warfare-the-invisible-frontline-of-global-conflicts/>
290. Márquez, J. E. (2023). Technological developments and implications of autonomous military drones: prospects in global geopolitics. Revista Tecnológica-ESPOL, 35(1), 137-151.

291. Maschmeyer, L., Abrahams, A., Pomerantsev, P., Yermolenko, V. (2023) Donetsk don't tell – 'hybrid war' in Ukraine and the limits of social media influence operations. *Journal of Information Technology & Politics* 2025, VOL. 22, No. 1, 49–64 Routledge. © 2023 <https://doi.org/10.1080/19331681.2023.2211969>
292. Masip-Bruin, X.; E. Marín-Tordera, S. Sánchez-López, J. Garcia, A. Jukan, A. J. Ferrer, A. Queral, A. Salis, A. Bartoli, M. Cankar, C. Cordeiro, J. Jensen, and J. Kennedy (2021). "Managing the Cloud Continuum: Lessons Learnt from a Real Fog-to-Cloud Deployment," *Sensors* (Basel, Switzerland), vol. 21.
293. McCarthy, J.; Minsky, M. L.; Rochester, N. and Shannon, C. E. (1955): A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence. <http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html>
294. McCormick, T. (2014) Lethal Autonomy: A Short History: How killer robots became more than just scary science fiction. *Foreign Policy*. January 24, 2014, <https://foreignpolicy.com/2014/01/24/lethal-autonomy-a-short-history/>
295. McCreight, R. (2023). Neuro-Cognitive Warfare: Inflicting Strategic Impact via Non-Kinetic Threat. *Small Wars Journal*. September 2023. <https://smallwarsjournal.com/2022/09/16/neuro-cognitive-warfare-inflicting-strategic-impact-non-kinetic-threat/>
296. McCreight, R. (2024). The war inside your mind: unprotected brain battlefields and neuro-vulnerability. *Academia Biology*. 2024-02-06 <https://doi.org/10.20935/AcadBiol6156>
297. McCulloch, W. S. y Pitts, W. (1943). A Logical Calculus of the ideas immanent in Nervous Activity. *Bulletin of Mathematical Biophysics*, 5, 115-133.
298. Mendi, A. F. (2023). Edge ai technology in the defense industry via reinforcement learning in simulation environments. *Gümüşhane Üniversitesi Fen Bilimleri Dergisi*, 13(3), 718-732.
299. Meng, Y., Xudong, Z., Jianwen, Z., Xinxin, X., Changling, W., & Fang, W. (2023). A Ultra-Low Power System Design Method of AI Edge Computation. 2023 19th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD).
300. Mezzacappa, E. et al. (2024). "Simulation experimentation of swarms: methodologies and analyses," *Proc. SPIE 13051, Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications V*, vol. 13051, pp. 1305108-1–1305108-10.
301. Microsoft (2023). Sophistication, scope, and scale: Digital threats from East Asia increase in breadth and effectiveness. *Microsoft Threat Intelligence*. September 2023. <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1aFyW>
302. Mikolov, T., Chen, K., Corrado, G. y Dean, J. (2013). Efficient Estimation of Word Representations in Vector Space, *arXiv preprint*, arXiv:1301.3781.
303. Mikulski, D.; G. Hudas, y F. Lewis (2014). Special issue: intelligent behaviors in military unmanned systems, *J. Def. Model. Simul.*, vol. 11, pp. 3-4.

304. Miller, S. (2023). Cognitive warfare: an ethical analysis. *Ethics Inf Technol* 25, 46 (2023). <https://doi.org/10.1007/s10676-023-09717-7>
305. MINDEF (2023). Resolución 11197/2023 de 29 de junio, de la Secretaría de Estado de Defensa, por la que se aprueba la Estrategia de desarrollo, implantación y uso de la Inteligencia Artificial en el Ministerio de Defensa. Boletín Oficial del Ministerio de Defensa. <https://publicaciones.defensa.gob.es/media/downloadable/files/links/2/0/20230706.pdf>
306. Minsky, M., & Papert, S. (1969). *Perceptrons: An Introduction to Computational Geometry*. MIT Press. ISBN 0 262 13043 2. An expanded edition was further published in 1988 (ISBN 9780262631112)
307. Molier, J.A. (2018). Algunos problemas éticos de las tecnologías militares emergentes. Documento de opinión 16/2018. Instituto Español de Estudios Estratégicos (IEEE).
308. Moliner, J.A (2024b). Ética y control humano significativo en sistemas de armas autónomos letales regidos por la Inteligencia Artificial. Comunicaciones Académicas. ACAMI. 26 de marzo de 2024.
309. Moliner, J.A, (2024). Ética y control humano significativo en sistemas de armas autónomos letales regidos por la Inteligencia Artificial. Academia de las Ciencias y las Artes Militares. Sección de Prospectiva de la Tecnología Militar ACAMI.
310. Moliner, J.A. (2020). La ética militar y su importancia para el militar profesional. Tesis Doctoral. UNED. 15 de julio de 2020.
311. Moliner, J.A. (2021). La ética militar como marco de reflexión sobre la guerra y la profesión militar. Ministerio de Defensa. ISBN 978-84-9091-607-0. 2021.
312. Moliner, J.A. (2023a). Valores éticos frente al uso de sistemas de armas letales autónomos. *Revista Española de Defensa*, 403, marzo 2023, pp. 32-33.
313. Moliner, J.A. (2023b). Dimensión ética y moral de posibles conflictos militares en el espacio exterior. *Araucaria*. *Revista Iberoamericana de Filosofía, Política, Humanidades y Relaciones Internacionales*, año 25, nº 53. Segundo cuatrimestre de 2023. ISSN 1575-6823 e-ISSN 2340-2199
314. Moliner, J.A. (2024). Raíces y antecedentes de la teoría de la guerra justa. Apuntes sobre las restricciones en el uso de la fuerza en diferentes civilizaciones. *Global Strategy Report* 4/2024.
315. Moore, G. E. (1965). Craming more components onto integrated circuits. *Electronics*.
316. MSC (2025). Munich Security Report 2025. Multipolarization. <https://securityconference.org/en/publications/munich-security-report-2025/>
317. Munasinghe, I., Perera, A., & Deo, R. C. (2024). A Comprehensive Review of UAV-UGV Collaboration: Advancements and Challenges. *Journal of Sensor and Actuator Networks*, 13(6), 81. <https://doi.org/10.3390/jsan13060081>
318. NATO (2024). NATO's Overarching Space Policy, 30 May 2024. https://www.nato.int/cps/en/natohq/official_texts_190862.htm

319. Nayuni, I.E.S. (2024). Generative AI models for Fake News detection. Cyber Security and Networks Forensic. Insights2Techinfo. https://insights2techinfo.com/generative-ai-models-for-fake-news-detection/?utm_source=perplexity
320. Neuberger, A. (2025). Spy vs. AI. How Artificial Intelligence Will Remake Espionage. Foreign Affairs. January 15, 2025. <https://www.foreignaffairs.com/united-states/spy-vs-ai>
321. Nikoula, D., McMahon, D. (2024). Cognitive Warfare: Securing Hearts and Minds. Information Integrity Lab. University of Ottawa, July 2024. <https://infolab.uottawa.ca/common/Uploaded%20files/PDI%20files/InfoLab%20-%20Cognitive%20Warfare,%20Securing%20Hearts%20and%20Minds.pdf>
322. Niinistö, S. (2024). Safer together: A path towards a fully prepared Union. 30 October 2024. https://commission.europa.eu/topics/defence/safer-together-path-towards-fully-prepared-union_en
323. NIST (2025). Managing Misuse Risk for Dual-Use 3 Foundation Models. Second Public Draft. NIST AI 800-1.2pd 1 U.S. AI Safety Institute. January 2025 <https://doi.org/10.6028/NIST.AI.800-1.2pd>
324. Nørgaard, K. & Linden-Vørnle, M. (2021). Cyborgs, Neuroweapons, and Network Command. Scandinavian Journal of Military Studies. 4. 94-107. 10.31374/sjms.86.
325. Nvidia Developer Blog (2025). "Deploy Large Language Models at the Edge with NVIDIA IGX Orin". Disponible en línea: <https://developer.nvidia.com/blog/deploy-large-language-models-at-the-edge-with-nvidia-igx-orin-developer-kit/> (Accedido: 5-3-2025)
326. OECD (2023), The Space Economy in Figures: Responding to Global Challenges, OECD Publishing, Paris, <https://doi.org/10.1787/fa5494aa-en>
327. OECD (2024). OECD Economic Outlook. December 2024. <https://www.oecd.org/en/topics/economic-outlook.html>
328. OECD (2025). VC investments in AI by industry. <https://oecd.ai/en/data?selectedArea=investments-in-ai-and-data&selectedVisualization=vc-investments-in-ai-by-industry>
329. Ondrej Burbacky, J. D. (2022). The semiconductor decade: A trillion-dollar industry. Retrieved from Mc Kinsey & Company: <https://www.mckinsey.com/~media/mckinsey/industries/semiconductors/our%20insights/the%20semiconductor%20decade%20a%20trillion%20dollar%20industry/the-semiconductor-decade-a-trillion-dollar-industry-v3.pdf?shouldIndex=false>
330. Onsu, M. A. P. Lohan, B. Kantarci (2024). Leveraging Edge Intelligence and LLMs to Advance 6G-Enabled Internet of Automated Defense Vehicles. arXiv:2501.06205v1 [cs.NI] 28 Dec. (Accedido: 6-feb-2025).
331. ONU (2022). Contrarrestar la desinformación para promover y proteger los derechos humanos y las libertades fundamentales. Informe del secretario general de las Naciones Unidas. Asamblea General. 12 agosto 2022. <https://undocs.org/es/A/77/287>
332. OpenAI (2023). GPT-4 System Card. <https://cdn.openai.com/papers/gpt-4-system-card.pdf>
333. OpenAI. (2024). Sora: Generating realistic and imaginative video from text. OpenAI Blog.

334. Ördén, H. (2024). The neuropolitical imaginaries of cognitive warfare. *PRIO* Volume 55, Issue 6. October 2024 <https://doi.org/10.1177/09670106241253527>
335. Palantir (2023). AI, Automation, and the Ethics of Modern Warfare (Defense AI Ethics, #1). Palantir Blog. April 7, 2023. <https://blog.palantir.com/ai-automation-and-the-ethics-of-modern-warfare-df1f0b212397>
336. Panella, C. The US Air Force is teaching AI to navigate aircraft in case GPS gets taken out in a future fight. *Business Insider*. May 13, 2024. <https://www.businessinsider.com/air-force-teaching-ai-to-navigate-aircraft-gps-is-gone-2024-5>
337. Panella, C. The US Air Force is teaching AI to navigate aircraft in case GPS gets taken out in a future fight. *Business Insider*. May 13, 2024. <https://www.businessinsider.com/air-force-teaching-ai-to-navigate-aircraft-gps-is-gone-2024-5>
338. Pang, B., Lee, L. y Vaithyanathan, S. (2002). Thumbs Up? Sentiment Classification using Machine Learning Techniques. En *Proceedings of the 2002 Conference on Empirical Methods in Natural Language Processing (EMNLP 2002)*, Association for Computational Linguistics, 2002, pp. 79-86.
339. Pang, G. (2022). The AI Chip Race. *IEEE Intelligent Systems*, 111-112.
340. Paoli, G.C. y Afina, Y. (2025). AI in the Military Domain: A briefing note for states. UNIDIR. March 10, 2025. <https://unidir.org/publicata la digitalitary-domain-briefing-note-states/>
341. Park, T., Liu, M. Y., Wang, T. C., & Zhu, J. Y. (2019). Semantic Image Synthesis with Spatially-Adaptive Normalization. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2019.
342. Pasquini, N. (2024). Naval Research Lab Completes Development of Satellite-Servicing Robotics. US Department of Defense. Nov. 15, 2024. <https://www.defense.gov/News/News-Stories/Article/Article/3966145/naval-research-lab-completes-development-of-satellite-servicing-robotics/>
343. Pauly, J. (2024). Technology: Disconnecting the Gordian Node. In: Tobias Bunde/Sophie Eisentraut/Leonard Schütte (eds.), *Munich Security Report 2024: Lose-Lose?* Munich: Munich Security Conference, February 2024, 95-101, <https://doi.org/10.47342/BMQK9457>
344. Pauwels, E. (2024). Preparing for Next-Generation Information Warfare with Generative AI. CIGI Paper No. 310. Center for International Governance Innovation. December 11, 2024. <https://www.cigionline.org/publications/preparing-for-next-generation-information-warfare-with-generative-ai/>
345. Penedo, G., Dey, A. K., Santilli, A., Fernando, A., Goyal, S., Magalhães, G., y Joulin, A. (2023). The Falcon LLMs: Boosting Open-Source Language Models with Data and Compute. *arXiv preprint arXiv:2306.01116*.
346. Peral-García, D. Cruz-Benito, J., García-Peñalva, F.J. (2024). Systematic literature review: Quantum machine learning and its applications. *Computer Science Review*. Vol 51. February 2024. <https://doi.org/10.1016/j.cosrev.2024.100619>

347. Pérez-Martínez, F. (2024). Digitalización e inteligencia artificial en los futuros escenarios de conflicto: hacia una defensa inteligente. Toma de Posesión como Académico de Número de la Real Academia de Doctores de España. RADE. 12 de junio de 2024. https://www.rade.es/imageslib/ACTIVIDADES/TEXTOS/PEREZ%20MARTINEZ,%20Felix_Discursoingreso.pdf
348. Pijlers, P. (2024). Legislation as an Instrument of Cognitive Warfare. En "Aspects of Cognitive Warfare". The DFefense Horizon Journal. April 2024. ISBN: 978-3-200-10166-1.
349. Pióro, L. J. Sychowiec, K. Kanciak, and Z. Zieliński (2024). "Application of Attribute-Based Encryption in Military Internet of Things Environment," *Sensors* (Basel, Switzerland), vol. 24.
350. Pool, R. (2025). Drones with Edge AI: The Future of Warfare? *EE Times Europe*. March 5, 2025. <https://www.eetimes.eu/drones-with-edge-ai-the-future-of-warfare/>
351. Praks, H. (2024). Hybrid CoE Working Paper 32: Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage. May 30, 2024. <https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240530-Hybrid-CoE-Working-Paper-32-Russias-hybrid-threat-tactics-WEB.pdf>
352. Precedence Research (2025). AI in Aerospace and Defense Market Size, Report by 2034.
353. Probasco, E. (2024). Building the Tech Coalition. How Project Maven and the U.S. 18th Airborne Corps Operationalized Software and Artificial Intelligence for the Department of Defense. Policy Brief. Center for Security and Emerging Technology. August 2024. <https://cset.georgetown.edu/publication/building-the-tech-coalition/>
354. Pujol, I. (2024). La guerra cognitiva convierte la mente en un campo de batalla. *Revista Española de Defensa*. Octubre 2024.
355. Pujol, I. y Dinh, Q. (2024). The battle for the mind: understanding and addressing cognitive warfare and its enabling technology. Center for the governance of change (CGC). IE University. April 2024. © 2024, CGC Madrid, Spain.
356. Pujol, I., Xuan, Q. (2024). The Battle for the Mind. Understanding and addressing cognitive warfare and its enabling technologies. IE University's Center for the Governance of Change (CGC). 19 abril 2024. <https://www.ie.edu/university/news-events/news/deceptive-use-ai-technology-is-turning-mind-main-battlefield-21st-century-according-ie-university/>
357. Pultarova, T., (2025). Starlink satellites: Facts, tracking and impact on astronomy. *SPACE*. January 9, 2025. <https://www.space.com/spacex-starlink-satellites.html>
358. Putric, T. (2022a). Neuroweapons: The Future of Warfare. (LAPSAP/DEMS4709) 2022. <https://yourreview.journals.yorku.ca/index.php/yourreview/article/view/40734/36981>
359. Putric, T. (2022b). The Sixth Domain: Neurowarfare, Neuroweapons, and the Future of Counterterrorism. *Revue YOUR Review* (York Online Undergraduate Research). <https://yourreview.journals.yorku.ca/index.php/yourreview/article/view/40734>
360. Quinlan, J.R. (1986). Induction of decision trees. *Machine Learning* 1, 81–106. March 1986. <https://doi.org/10.1007/BF00116251>

361. Quinlan, J.R. (1993). C4.5: Programs for Machine Learning. Morgan Kaufmann Publishers Inc. ISBN:978-1-55860-240-3. January 1993.
362. Radford, A., Kim, J. W., Hallacy, C., Ramesh, A., Goh, G., Agarwal, S., y Sutskever, I. (2021). Learning transferable visual models from natural language supervision. In International conference on machine learning (pp. 8748-8763). PmLR.
363. Radford, A., Kim, J. W., Xu, T., Brockman, G., McLeavey, C., y Sutskever, I. (2022). Robust Speech Recognition via Large-Scale Weak Supervision. arXiv preprint arXiv:2212.04356.
364. Radovanovic, M., Petrovski, A., Behlic, A., Chaari, M. Z., Hashimov, E. G., Fellner, R., & Agbeyangi, A. (2024). Unleashing autonomous forces: Integrating AI-driven drones in modern military strategy, 3(77), 55-69.
365. RAND (2013). Redefining Information Warfare Boundaries for an Army in a Wireless Word. United States Army. RAND Corporation monograph series.
366. Radford, A., Wu, J., Child, R., Luan, D., Amodel, D. y Sutskever, I. (2019). Language Models Are Unsupervised Multitask Learners, OpenAI Blog, 1 (8).
367. Rashed, M. y Bang, H. (2024). Role of AI in nano-satellite constellations for autonomy.
368. Rauta, V. (2020) Towards a typology of non-state actors in 'hybrid warfare': proxy, auxiliary, surrogate and affiliated forces. Cambridge Review of International Affairs, 33 (6). pp. 868-887. ISSN 1474-449X doi: <https://doi.org/10.1080/09557571.2019.1656600>
369. Rauta, W. (2025). Countering state-sponsored proxies: Designing a robust policy. Hybrid CoE Paper No. 23. ISBN 978-952-7591-18-5 (web). February 2025. <https://www.hybridcoe.fi/publications/hybrid-coe-paper-23-countering-state-sponsored-proxies-designing-a-robust-policy/>
370. Rawat, D. B. (2022, December). Artificial intelligence meets tactical autonomy: Challenges and perspectives. In 2022 IEEE 4th International Conference on Cognitive Machine Intelligence (CogMI) (pp. 49-51). IEEE.
371. Reino Unido (2021). National AI Strategy, HM Government. Disponible en línea: <https://www.gov.uk/government/publications/national-ai-strategy>
372. Reino Unido (2022). Defence AI Strategy, Ministerio de Defensa. Disponible en línea: <https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy>
373. Reino Unido (2023). Ministry of Defence, Defence Command Paper: Defence's responses to a more contested and volatile world. Disponible en línea: <https://www.gov.uk/government/publications/defence-command-paper-2023-defences-response-to-a-more-contested-and-volatile-world>
374. Reis, J., Cohen, Y., Melão, N., Costa, J., & Jorge, D. (2021). High-tech defense industries: developing autonomous intelligent systems. Applied Sciences, 11(11), 4920.
375. Ricart, R.J. (2024). Waking Up Slowly: Defense AI in Spain. In: Borchert, H., Schütz, T., Verbovsky, J. (eds) The Very Long Game. Contributions to Security and Defence Studies. Springer, Cham. https://doi.org/10.1007/978-3-031-58649-1_12

376. Rico Sennrich, Barry Haddow, y Alexandra Birch (2016). Neural Machine Translation of Rare Words with Subword Units. In Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers), pages 1715–1725, Berlin, Germany. ACL
377. Rivera, J.P., Mukobi, B., Reuel, A., Lamparth, M., Chandler, S., Schneider, J. (2024). Escalation Risks from Language Models in Military and Diplomatic Decision-Making. FAccT '24: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency. 05 June 2024. Pages 836 – 898 <https://doi.org/10.1145/3630106.3658942>
378. Rodriguez-Fernandez, V., Carrasco, A. Cheng, J., Scharf, E., Siew, P.M., Linares R. (2024). Language Models are Spacecraft Operators. <https://arxiv.org/pdf/2404.00413v1>
379. Rojas, E., Lopez-Pajares, D., Alvarez-Horcajo, J., Llopis Sánchez, S. (2023). The Cloud Continuum for Military Deployable Networks: Challenges and Opportunities. In: Katsikas, S., et al. Computer Security. ESORICS 2022 International Workshops. ESORICS 2022. Lecture Notes in Computer Science, vol 13785. Springer, Cham.
380. Rojas-Orozco, C. (2021). Alcance y perspectivas del concepto de ius post bellum en derecho internacional. Revista Latinoamericana de Derecho. Febrero 2021. DOI: <https://doi.org/10.29263/lar06.2021.05>
381. Rombach, R., Blattmann, A., Lorenz, D., Esser, P., & Ommer, B. (2022). High-Resolution Image Synthesis with Latent Diffusion Models. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2022.
382. Rosemary, J. y Abraham, A.M. (2024). Quantum Machine Learning Techniques for Network Defense: Comparative Study of Quantum vs. Classical Approaches. Vol. 2 No. 12 (2024): IRJAEM Vol.02 Issue 12- December 2024. DOI: <https://doi.org/10.47392/IRJAEM.2024.0564>
383. Rosenblatt (1958). The Perceptron: A Probabilistic Model for Information Storage and Organization in the Brain. Psychological Review, 65 (6), 386-408. <https://doi.org/10.1037/h0042519>
384. Rosenblueth, N. Wiener and J. Bigelow (1943). Behavior, Purpose and Teleology. Philosophy of Science, 10, 18-24. Disponible en línea: <https://www.cambridge.org/core/journals/philosophy-of-science/article/abs/behavior-purpose-and-teleology/73ACBBEC616CE78767088694F357D57B>
385. Rosendo, A. Costan, P. Valdúriez, G. Antoniu (2022). Distributed intelligence on the edge-to-cloud continuum: A systematic literature review, Journal of Parallel and Distributed Computing 166 71–94.
386. Roziere, B., Gehring, J., Gloeckle, F., Sootla, S., Gat, I., Tan, X. E., et al. (2023). Code Llama: Open foundation models for code. arXiv preprint arXiv:2308.12950.
387. Ruiz S., Valera L., Ramos P., Sitaram R. (2024). Neurorights in the Constitution: from neurotechnology to ethics and politics. Philos Trans R Soc Lond B Biol Sci. 2024 Dec 2; <https://doi.org/10.1098/rstb.2023.0098>
388. Rumelhart, G. Hinton and R. Williams (1986). Learning representations by back-propagating errors. Nature, 323, 533-536. <https://www.nature.com/articles/323533a0#citeas>

389. Saballa, J. (2021). "Israel Deploys Semi-Autonomous Machine Gun Robot to Gaza Border", *The Defense Post*. Disponible en línea: <https://thedefensepost.com/2021/07/01/israel-machine-gun-robot-gaza-border/> (Accedido: 3-3-2025).
390. Sahoo, P., Singh, A. K., Saha, S., Jain, V., Mondal, S., & Chadha, A. (2024). A systematic survey of prompt engineering in large language models: Techniques and applications. arXiv preprint arXiv:2402.07927.
391. Salmón, E. (2004). Introducción Al Derecho Internacional Humanitario. Instituto de Democracia y Derechos Humanos (Pontificia Universidad Católica de Perú) y Comité Internacional de la Cruz Roja, idih3.pmd 5 30/06/2004. <https://www.corteidh.or.cr/tablas/r25212.pdf>
392. SandboxAQ (2024). SandboxAQ announces AQNav—World's first commercial real-time navigation system powered by AI and quantum to address GPS jamming', 25 June 2024.
393. Santopinto, F. (2024). The EU, Artificial Military Intelligence and Autonomous Lethal Weapons. Defence and Security Industry Programme. IRIS (Institut de relations internationales et stratégiques). April 2024.
394. Saranya, T; J. Deyamala, S. Sellamuthu, and I. Priyadharshini, "A Secure Framework for MIIoT: TinyML-powered Emergency Alerts and Intrusion Detection for Secure Real-time Monitoring," in 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 13-21, 2024
395. Scazzieri, L. (2025). Towards an EU 'defence union'? Policy brief. Centre for European Reform, 30 de enero de 2025. <https://www.cer.eu/publications/archive/policy-brief/2025/towards-eu-defence-union>
396. Schoeni, D., and Vestner T. (eds), Ethical Dilemmas in the Global Defense Industry, Ethics, National Security, and the Rule of Law (New York, 2023; online edn, Oxford Academic, 23 Mar. 2023), <https://doi.org/10.1093/oso/9780190675813.001.0001>
397. Schwartz, E. (2024). The (im)possibility of responsible military AI governance. Humanitarian Law & Policy. December 12, 2024. <https://blogs.icrc.org/law-and-policy/2024/12/12/the-im-possibility-of-responsible-military-ai-governance/>
398. Serhan, Y. (2024). How Israel Uses AI in Gaza—And What It Might Mean for the Future of Warfare. TIME, December 18, 2024. <https://time.com/7202584/gaza-ukraine-ai-warfare/>
399. Serrano, A. V., Subies, G. G., Zamorano, H. M., García, N. A., Samy, D., Sánchez, D. B. y Jimenez, A. B.: "RigoBERTa: A State-of-the-Art Language Model for Spanish", 2022.
400. Shah, D. (2024). Artificial Intelligence in Addressing Space Pollution. Journals Journal of Research in Mechanical Engineering Volume 10 ~ Issue 2 (2024) pp: 09-13 ISSN(Online):2321-8185 www.questjournals.org
401. Shastri, B., Talt, A., Ferreira de Lima, T., Pernice, W., Bhaskaran, H., Wright, C., & Prucnal, P. (2021). Photonics for artificial intelligence and neuromorphic computing. Nature Photonics, 102-114.

402. Shaw, J. and Kirkpatrick, S. (2024). Future Space Domain Awareness Needs for National Security Space. Center for Strategic and International Studies (CSIS). October 31, 2024 <https://www.csis.org/analysis/future-space-domain-awareness-needs-national-security-space>
403. Shwe, T. and M. Aritsugi (2024). "Towards an Edge-Fog-Cloud Serverless Continuum for IoT Data Processing Pipeline," in 2024 IEEE International Conference on Big Data and Smart Computing (BigComp), pp. 349–350, 2024.
404. Shyalika, R. Wickramarachchi, y A. Sheth, "A Comprehensive Survey on Rare Event Prediction," arXiv preprint, Oct. 2024. [Online]. Available: <http://arxiv.org/abs/2309.11356>.
405. Shyam, P., Sastry, G., Askell, A., Agrwall, S., Herbert-Voss, A., Krueger, G., Henighan, T., Child, R., Ramesh, A., Ziegler, D. M., Wu, J., Winter, C., Hesse, C., Chen, M., Sigler, E., Litwin, M., Gray, S., Chess, B., Clark, J., Berner, C., Mccandlish, S., Radford, A., Sutskever, I. y Amodel, D. (2020). "Language Models Are Few-Shot Learners".
406. SIA (Semiconductor Industry Association) & BCG (Boston Consulting Group). (2025). Strengthening the U.S. Semiconductor Supply Chain.
407. Siman, B. (2024). AI and Microtargeting Disinformation as a Security Threat to the Protection of International Forces. The Defence Horizon Journal. May 23, 2024. <https://tdhj.org/blog/post/ai-disinformation-security/>
408. Simmons, D., Raisch, K., Gueller, K., Chun, N., McCray, M. (2024). Back to the Futures. A Look into the Future Through the Lens of the Past. United States Army War College. 9 May 2024.
409. Simon, F. M., Altay, S., & Mercier, H. (2023). Misinformation reloaded? Fears about the impact of generative AI on misinformation are overblown. Harvard Kennedy School Misinformation Review, 4(5). DOI: <https://doi.org/10.37016/mr-2020-127>
410. Sipola, T., Alatalo, J., Kokkonen, T., & Rantonen, M. (2022). Artificial Intelligence in the IoT Era: A Review of Edge AI Hardware and Software. Proceedings of the 31st Conference of Open Innovations Association FRUCT & IEEE, 320-331.
411. Smith B. (1982) Reflection and Semantics in a Procedural Language. PhD. Thesis, MIT, Cambridge, MA. Prologue reprinted in Brachman and Levesque (1985).
412. Smith, M. S. (2024). Challenges are coming for Nvidia's crown. SPECTRUM IEEE, 40-44.
413. Space Systems Command (2025). Space Domain Awareness and Combat Power. United States Space Force. <https://www.ssc.spaceforce.mil/Program-Offices/Space-Domain-Awareness-Combat-Power> (accedido el 3 de enero de 2025)
414. Srirama, S. N. (2024). Distributed edge analytics in edge-fog-cloud continuum. Internet Technology Letters, e562.
415. Srivastava, A., Rastogi, A., Rao, A., Shoeb, A. A. M., Abid, A., Fisch, A., et al. (2022). Beyond the imitation game: Quantifying and extrapolating the capabilities of language models. arXiv preprint arXiv:2206.04615.

416. Strategic Defence Review (2025). Making Britain Safer: secure at home, strong abroad. Ministry of Defence: United Kingdom.
417. Steene, S. and Jenks, C. (2023). The Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy. Lieber Institute. Nov 13, 2023. <https://lieber.westpoint.edu/political-declaration-responsible-military-use-artificial-intelligence-autonomy/>
418. Steene, S. b Jenks, C. (2023). The Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy. Articles of War. Nov 13, 2023. <https://lieber.westpoint.edu/political-declaration-responsible-military-use-artificial-intelligence-autonomy/>
419. Takagi, K. (2024). Cognitive Centric Warfare: Modelling Indirect Approach in Future Warfare. Journal of Information Warfare. June 30, 2024. <https://www.hudson.org/corruption/cognitive-centric-warfare-modelling-indirect-approach-future-warfare-koichiro-takagi>
420. Takagi, K. (2025). Is the PLA Overestimating the Potential of Artificial Intelligence? JFQ 116, 1st Quarter 2025. Disponible en: <https://digitalcommons.ndu.edu/cgi/viewcontent.cgi?article=1189&context=joint-force-quarterly>
421. Team, G., Anil, R., Borgeaud, S., Alayrac, J. B., Yu, J., Soricut, R., ... & Blanco, L. (2023). Gemini: a family of highly capable multimodal models. arXiv preprint arXiv:2312.11805.
422. Tedae (2025). El sector de la consultoría urge a reactivar Europa con la aplicación inmediata de los informes Draghi y Letta. 6 febrero 2025. <https://tedae.org/defensa/el-sector-de-la-consultoria-urge-a-reactivar-europa-con-la-aplicacion-inmediata-de-los-informes-draghi-y-letta/>
423. Thangavel, K., Sabatini, R. Gardi, A., Ranasinghe, K., Hilton, S., Servidia, P., Spiller, D. (2024). Artificial Intelligence for Trusted Autonomous Satellite Operations. Progress in Aerospace Sciences. Volume 144.
424. Théron, P.; A. Kott, M. Drasar, K. Rządca, B. LeBlanc, M. Pihelgas, L. Mancini, y F. De Gaspari, "Reference Architecture of an Autonomous Agent for Cyber Defense of Complex Military Systems," Springer, 2020.
425. Thiele, R. (2020). Artificial Intelligence – A key enabler of hybrid warfare. Hybrid CoE Working Paper 6. The European Centre of Excellence for Countering Hybrid Threats. March 2020. https://www.hybridcoe.fi/wp-content/uploads/2020/07/WP-6_2020_rgb-1.pdf
426. Tian, X et al. (2024). Experimental demonstration of drone-based quantum key distribution, Physical Review Letters, 15 Nov. 2024. DOI: <https://doi.org/10.1103/PhysRevLett.133.200801>
427. Tjong Kim Sang, F. E. y De Meulder, F.: "Introduction to the CoNLL-2003 Shared Task: Language-Independent Named Entity Recognition", en Proceedings of the Seventh Conference on Natural Language Learning at HLT-NAACL 2003, 2003.
428. Tomaswick, A. (2025). Drones on your mind? Brain-controlled UAVs take a step forward. Electronics 360. 11 April 2025. 2025.<https://electronics360.globalspec.com/article/22181/drones-on-your-mind-brain-controlled-uavs-take-a-step-forward>

429. Torchio, G. y Tasin, F. (2025). The Paris Summit: Au Revoir, global AI Safety? European Policy Center (EPC). 14/02/2025. <https://www.epc.eu/en/publications/The-Paris-Summit-Au-Revoir-global-AI-Safety~61ea68>
430. Touvron, H., Lavril, T., Izacard, G., Martinet, X., Lachaux, M.-A., Lacroix, T., ... & Scialom, T. (2023). LLaMA: Open and Efficient Foundation Language Models. arXiv preprint arXiv:2302.13971.
431. Trager, R. and Luca, L. (2022). Killer Robots Are Here—and We Need to Regulate Them. Foreign Policy. May 11, 2022. <https://foreignpolicy.com/2022/05/11/killer-robots-lethal-autonomous-weapons-systems-ukraine-libya-regulation/>
432. Tran, J., Puri, P., Logue, J., Jacques, A., Zhang, L., Langeland, K., Nacouzi, G., Briggs, G.J. Artificial Intelligence and Machine Learning for Space Domain Awareness. The Development of Two Artificial Intelligence Case Studies. RAND Corporation. Sep 30, 2024. https://www.rand.org/pubs/research_reports/RRA2318-2.html
433. Tran, J., Puri, P., Logue, J., Jacques, A., Zhang, L., Langeland, K., Nacouzi, G., Briggs, G.J. Artificial Intelligence and Machine Learning for Space Domain Awareness. The Development of Two Artificial Intelligence Case Studies. RAND Corporation. Sep 30, 2024. https://www.rand.org/pubs/research_reports/RRA2318-2.html
434. Troianovski, A. (2022). Vladimir Putin habla de ‘desnazificar’ Ucrania. ¿Por qué? New York Times. 17 de abril de 2022. <https://www.nytimes.com/es/2022/04/17/espanol/nazi-ucrania-putin.html>
435. Tucker, P. (2025). “Pentagon to Test How Generative AI Would Perform in Fight with China,” Defense One. Disponible en línea: <https://www.defenseone.com/technology/2025/01/pentagon-test-how-generative-ai-would-perform-fight-china/> (Accedido: 3-3-2025).
436. Tucker, P. y Hlad, J. (2025). Pentagon to build AI for war planning in Europe and Asia. Defense One, March 5, 2025. <https://www.defenseone.com/technology/2025/03/pentagon-build-ai-war-planning-europe-and-asia/403506/>
437. Turing, A. (1950). Computing Machinery and Intelligence. Mind, 59, 433-460. <https://www.jstor.org/stable/2251299?origin=JSTOR-pdf>
438. UE (2023). EU Space Strategy for Security and Defence for a stronger and more resilient European Union. https://defence-industry-space.ec.europa.eu/eu-space-strategy-security-and-defence-stronger-and-more-resilient-eu-2023-03-10_en
439. UE (2024). 2024/1689 REGLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n. o 300/2008, (UE) n. o 167/2013, (UE) n. o 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689>
440. Ukrainian Govt. (2024). Ukrainian Government, “Agreement on Security Cooperation between Spain and Ukraine”, 27 May 2024. See: <https://www.president.gov.ua/en/news/ugoda-pro-spiv-robitnictvo-u-sferi-bezpeki-mizh-ukrayinoyu-ta-91145>

441. UN (2024). Artificial intelligence in the military domain and its implications for international peace and security. Resolution adopted by the General Assembly on 24 December 2024. A/RES/79/239. <https://undir.org/publication/ai-military-domain-briefing-note-states/>
442. UNESCO (2021). Ethical issues of neurotechnology. Comité Internacional de Bioética. December 2021 ISBN: 978-92-3-100551-0 <https://doi.org/10.54678/QNKB6229>
443. UNESCO (2023). Unveiling the neurotechnology landscape: scientific advancements innovations and major trends. 2023. ISBN: 978-92-3-100606-7 <https://doi.org/10.54678/OCBM4164>
444. Unsworth, J. (2017). Neuroethics Meets Just War Theory: Ethical Issues and the Development of the Third Offset Strategy. Simons Center Special Report, Ethics of Future Warfare, 2017. <https://thesimonscenter.org/wp-content/uploads/2018/05/Ethics-Symp-pg149-157.pdf>
445. Unver, H.A. (2024). Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights. IN-DEPTH ANALYSIS Requested by the DROI subcommittee. European Parliament. PE 754.450. May 2024. [https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA\(2024\)754450_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450_EN.pdf)
446. Usmanov, I. y M. Chernychka, “Maritime Autonomous Weapon Systems from the Standpoint of International Humanitarian Law,” Lex Portus, 2022.
447. Vakiliipour P, Fekrvand S. (2024). Brain-to-brain interface technology: A brief history, current state, and future goals. *Int J Dev Neurosci*. 2024 Aug;84(5):351-367. doi: 10.1002/jdn.10334. Epub 2024 May 6. PMID: 38711277.
448. Van Maarseveen, H. (2023). XILINX Vitis: AI A journey through the evolution of AI Hardware. Kindle e-book.
449. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. *Advances in Neural Information Processing Systems*, 30, 5998–6008. <https://arxiv.org/abs/1706.03762>
450. Vaughn, S. (2025). AI Dependence and Political Blind Spots Undermine Beijing’s War Strategy. Analysis, Asia Program. March 18, 2025. <https://www.fpri.org/article/2025/03/ai-dependence-and-political-blind-spots-undermine-beijings-war-strategy/>
451. Vergara, J.; J. F. Botero, and L. Fletscher, “A Comprehensive Survey on Resource Allocation Strategies in Fog/Cloud Environments,” *Sensors* (Basel, Switzerland), vol. 23, 2023.
452. Vestner, T. (2024). Rules of Engagement as a Regulatory Framework for Military Artificial Intelligence. Lieber Institute West Point. Aug 27, 2024 <https://lieber.westpoint.edu/rules-engagement-regulatory-framework-military-artificial-intelligence/>
453. ViDAR (2025). Passive Wide Area Search for Any Mission. AI Sensors. Visual detection and Ranging (ViDAR). <https://shield.ai/vidar/> (accedido el 4 de enero de 2025)
454. Voo, J. and Singh, V. (2025). Competition in cyberspace: a distorted representation. ISIS. <https://www.iiss.org/online-analysis/charting-cyberspace/2025/04/competition-in-cyberspace-a-normalised-misrepresentation/>

455. Wainscott-Sargent, A. (2024). Leveraging AI in Space: Experts Assess the Impact on the Defense and Space Domain. *Via Satellite*. August 2024. <https://interactive.satellitetoday.com/via/september-2024/leveraging-ai-in-space-experts-assess-the-impact-on-the-defense-and-space-domain>
456. Wald, D. y Fields, K. (2024). Generative AI is Now in Space. Here's Why That's a Big Deal. *Air&Space Forces Magazine*. Sept. 4, 2024. <https://www.airandspaceforces.com/generative-ai-space-big-deal/>
457. Wallace, D.A., Reeves, S., Hart, C. (2023). Technologically Enabled Surrender Under the Law of Armed Conflict. *Chicago Journal of International Law*. Summer 2023. <https://cjl.uchicago.edu/online-archive/technologically-enabled-surrender-under-law-armed-conflict>
458. Wang, R. (2025). Washington May Regret Overextended AI Chip Controls. *Foreign Policy*. April 30, 2025. <https://foreignpolicy.com/2025/04/30/h20-nvidia-chips-ai-china-restrictions/>
459. Wang, X., Wei, J., Schuurmans, D., Le, Q., Chi, E., Narang, S., ... & Zhou, D. (2022). Self-consistency improves chain of thought reasoning in language models. *arXiv preprint arXiv:2203.11171*.
460. Wanyana, R. (2025). Cognitive Warfare: Does it Constitute Prohibited Force? *EJIL: Talk! Blog of the European Journal of International Law*. January 30, 2025. <https://www.ejiltalk.org/cognitive-warfare-does-it-constitute-prohibited-force/>
461. Washington, MA, Dinh, DT, Ibarra, CA, Kua, SC (2023). A Brief Primer on the Concept of the Neuroweapon for U.S. Military Medical Personnel. *J Spec Oper Med*. 2023 Dec 29; 23(4):70-74. <https://doi.org/10.55460/SX1S-ZO4J> PMID: 37976420.
462. Waterman, S. (2024). As Space Gets More Crowded, Space Force Needs New AI Tools to Keep Up: Experts. *Air&Space Forces Magazine*. Dec. 6, 2024. <https://www.airandspaceforces.com/experts-space-domain-awareness-ussf-ai-tools/>
463. Watling, J., y Reynolds, N. (2025). Tactical Developments During the Third Year of the Russo–Ukrainian War. *The Royal United Services Institute for Defence and Security Studies (RUSI)*.
464. Wei, J., Wang, X., Schuurmans, D., Bosma, M., Xia, F., Chi, E., ... & Zhou, D. (2022). Chain-of-thought prompting elicits reasoning in large language models. *Advances in neural information processing systems*, 35, 24824-24837.
465. Weinberg, G. V. "Prediction of UAV Swarm Defeat with High-Power Radio Frequency Fields," *IEEE Transactions on Electromagnetic Compatibility*, vol. 64, pp. 2157–2162, 2022.
466. White, S. R. (2017). Closer than you think: The implications of the Third Offset strategy for the US Army.
467. Wilbor, D. (2025). The Challenge of AI-Enhanced Cognitive Warfare: A Call to Arms for a Cognitive Defense. *Small Wars Journal*. 22 January 2025. <https://smallwarsjournal.com/2025/01/22/the-challenge-of-ai-enhanced-cognitive-warfare-a-call-to-arms-for-a-cognitive-defense/>
468. Wilkinson, M.; Dumontier, M. and Aalbersberg, I. (2016): «The FAIR Guiding Principles for Scientific Data Management and Stewardship». *Sci Data*, 3, 160018. <https://doi.org/10.1038/sdata.2016.18>

469. Wilson, J. (2025). AI, war and (in)humanity: the role of human emotions in military decision-making. *Humanitarian Law & Policy*. February 20, 2025. <https://blogs.icrc.org/law-and-policy/2025/02/20/ai-war-and-in-humanity-the-role-of-human-emotions-in-military-decision-making/>
470. Wolff, G., A. Steinbach and J. Zettelmeyer (2025). 'The governance and funding of European rearmament'. Policy Brief 15/2025, Bruegel. <https://www.bruegel.org/policy-brief/governance-and-funding-european-rearmament>
471. Xia, X., Chen, F., He, Q. et al., (2024). "EdgeShield: Enabling Collaborative DDoS Mitigation at the Edge," in *IEEE Transactions on Mobile Computing*, vol. 23, no. 12, pp. 14502-14513, Dec. 2024, doi: 10.1109/TMC.2024.3443260
472. Xu, W.; Song, S.; Z. Gao, L. Lai, Y. Sun, and W. Luo, "Latency-Aware MIIoT Service Strategy in UAV-Assisted Dynamic MMEC Environment," *IEEE Internet of Things Journal*, vol. 11, pp. 22220–22231, 2024.
473. Yao, S., Yu, D., Zhao, J., Shafran, I., Griffiths, T., Cao, Y., & Narasimhan, K. (2023). Tree of thoughts: Deliberate problem solving with large language models. *Advances in neural information processing systems*, 36, 11809-11822.
474. Yao, S., Zhao, J., Yu, D., Du, N., Shafran, I., Narasimhan, K., & Cao, Y. (2023). React: Synergizing reasoning and acting in language models. In *International Conference on Learning Representations (ICLR)*.
475. Yao, Y.; S. Huang, L. Dong, F. Wei, H. Chen and N. Zhang (2022): «Kformer: Knowledge Injection in Transformer Feed-Forward Layers». En *Natural Language Processing and Chinese Computing*. Cham: Springer International Publishing, 131-143; D. Dai, L. Dong, Y. Hao, Z. Sui, B. Chang and F. Wei (2022): «Knowledge neurons in pre-trained transformers». En *Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*. Dublin, Ireland: Association for Computational Linguistics, 8493-8502.
476. Young, A., Dean, M., Plank, J., & Rose, G. (2019). A Review of Spiking Neuromorphic Hardware. *IEEE Access*, 135606-135620.
477. Yuste, R. (2023). La neurotecnología, al acceder al centro de nuestra actividad mental, bypasea todos los filtros que tenemos en el cuerpo. CNIO. 19 diciembre 2023. <https://www.cnio.es/es/noticias/rafael-yuste-neurotecnologia-al-acceder-al-centro-nuestra-actividad-mental-bypasea-todos>
478. Zaidan, E., Ibrahim, I.A. (2024). AI Governance in a Complex and Rapidly Changing Regulatory Landscape: A Global Perspective. *Humanit Soc Sci Commun* 11, 1121 (2024). <https://doi.org/10.1057/s41599-024-03560-x>
479. Zhang, L., Langeland, K., Tran, J., Logue, J., Puri, P.; Nacouzi, G., Jacques, A., and Briggs, G.J. (2024). Artificial Intelligence and Machine Learning for Space Domain Awareness. Characterizing the Impact on Mission Effectiveness. RAND Corporation. Nov 21, 2024. ISBN: 978-1-9774-1447-2 https://www.rand.org/pubs/research_reports/RRA2318-1.html

480. Zhenling, S., Qi, L., KANEKO, H., Li, H., & Meng, L. (2024). Optimization and Deployment of DNNs for RISC-V-based Edge AI. *Proceedings of the 2024 IEEE International Conference on Real-time Computing and Robotics*, 200-205.
481. Zhihong, J., Xiaolei, C., Xiao, H., Hui, L. Ceccarelli, M. (2022). Progress and Development Trend of Space Intelligent Robot Technology. *SPACE: SCIENCE & TECHNOLOGY*. 25 Jan 2022 Vol 2022. Article ID: 9832053 <https://doi.org/10.34133/2022/9832053>
482. Zhong, S., Su, L., Mingkun Xu, M., Loke, D., Yu, B., & Yishu Zhang, Y. (2025). Recent Advances in Artificial Sensory Neurons: Biological Fundamentals, Devices, Applications and Challenges. *Micro-Nano Letters*, 1-49.
483. Zhu, Y., Kiros, R., Zemel, R., Salakhutdinov, R., Urtasun, R., Torralba, A., & Fidler, S. (2015). Aligning books and movies: Towards story-like visual explanations by watching movies and reading books. In *Proceedings of the IEEE international conference on computer vision* (pp. 19-27).
484. Zieliński, Z., K. Wrona, J. Furtak, and J. Chudzikiewicz (2021). Reliability and Fault Tolerance Solutions for MIoT, *IEEE Communications Magazine*, vol. 59, pp. 36–42.
485. Ziemer, C.T., Rothmund, T. (2024). Psychological Underpinnings of Misinformation Countermeasures: A Systematic Scoping Review. *Journal of Media Psychology*, vol. 36, no. 6, pp. 397–409, Nov. 2024, <https://doi.org/10.1027/1864-1105/a000407>

ANEXOS.

Anexo 1. Listado de acrónimos

1. AAPP: Administraciones Públicas
2. ADAS: Sistemas Avanzados de Asistencia al Conductor
3. AEE: Agencia Espacial Española
4. AICA: Autonomous Intelligent Cyberdefence Agent (NATO)
5. AIGC: Artificial Intelligence Generated Content
6. AIS: Automatic Identification System
7. API: Application Interface
8. ASN: Neuronas Sensoriales Artificiales
9. AIRIS: Artificial Intelligence Retraining In Space
10. AIMC: Computación analógica en memoria
11. APM: Advanced Persistent Manipulators
12. ARTES: Advanced Research in Telecommunications Systems
13. ASAT: Antisatellite (... weapon)
14. ASIC: Circuito Integrado de Aplicación Especifica (Application Specific Integrated Circuits)
15. ASPI: Australian Strategic Policy Institute
16. ATLAS: A Toroidal LHC ApparatuS
17. BBI: Brain to Brain Interface
18. BCI: Brain Computer Interface
19. BIC: Business Incubator Centre
20. BNN: Bayesian Neural Network
21. BOC: Binary Offset Carrier
22. BREGO: Block-box for an optimized GNSS spectrum monitoring network using AI
23. B2B: Business to Business
24. B2C: Business to Customer
25. CAGR: Compound Annual Growth Rate
26. CART: Classification and Regression Trees
27. CAS: China Academy of Sciences

28. CCN: Centro Criptológico Nacional
29. CDTI: Centro para el Desarrollo Tecnológico y la Innovación
30. CEA: Comisariat d'Energie Atomique
31. CEADRON: Centro de sistemas y tecnologías antidrón
32. CEI: Consejo Europeo de Investigación
33. CERN: European Organization for Nuclear Research
34. CESGA: Centro de Supercomputación de Galicia
35. CESTIC: Centro de Sistemas y Tecnologías de la Información y las Comunicaciones
36. CETEDEX: Centro Tecnológico de Desarrollo y Experimentación (INTA)
37. CIA (Esp.): Centro de Inteligencia Artificial
38. CIA: Central Intelligence Agency
39. CIFAS: Centro de Inteligencia de las Fuerzas Armadas
40. CIMA: Centro de Instrucción de Medicina Aeroespacial
41. CNN: Convolutional Neural Network
42. COINCIDENTE: Cooperación en Investigación Científica y Desarrollo en Tecnologías Estratégicas
43. CPU: Procesadores tradicionales de propósito general
44. CSS: Civil Security Space (ESA)
45. CUCO: Computación cuántica en industrias estratégicas
46. CUDA: Arquitectura de dispositivos unificados de cómputo (Compute Unified Device Architecture)
47. DARPA: Defense Advanced Research Programs Agency
48. DDoS: Distributed Denegation of Service
49. DEEP: Data Exploitation and Enhanced Processing
50. DEFIS: Dirección General de Industria de Defensa y Espacio (Comisión Europea)
51. DGAM: Dirección General de Armamento y Material
52. DISCRETION: Disruptive SDN Secure Communications for European Defence
53. DIU: Defence Innovation Unit
54. DL: Deep learning
55. DMA: Digital Markets ct
56. DSTL: Defence Science & Technology Laboratory

- 57. DRAM: Memoria dinámica de acceso aleatorio
- 58. DSA: Digital Services Act
- 59. EEAS: European External Action Service
- 60. EGNOS: European Geostationary Navigation Overlay Service
- 61. EIC: European Innovation Council
- 62. EPI: European Processor Initiative
- 63. EPL: Ejército Popular de Liberación
- 64. ESA: European Space Agency
- 65. ESMC: European Semiconductor Manufacturing Company
- 66. ET: Ejército de Tierra
- 67. EUDIS: EU Defence Innovation Scheme
- 68. EuroQCI: European Quantum Communication Infrastructure
- 69. EUSPA: EU Agency for the Space Programme
- 70. Euro-QCI: European Quantum Communications Infrastructure
- 71. EUV: Extreme Ultra Violet
- 72. EW: Electronic Warfare
- 73. FANETC: Flying Ad-hoc NETwork & distributed mobile Tactical Cloud
- 74. FANDANGO: FAke News discovery and propagation from big Data ANalysis and artificial intelliGence Operations
- 75. FAS: Fuerzas Armadas
- 76. FCAS: Future Combat Air System
- 77. FDA: Food and Drugs Administration
- 78. FEI: Foro de Empresas Innovadoras
- 79. FIMI: Foreign Information Manipulation and Interference,
- 80. FinFET: Transistores de efecto de campo Fin
- 81. FPGA: Arreglos Programables en campo (Field Programmable Gate Arrays)
- 82. FRONTEX: European Border and Coast Guard Agency
- 83. GAN: Redes Generativas Adversarias
- 84. GCS: Galileo Ground Control Segment
- 85. GEO: Geostationary Earth Orbit

86. GEODSS: Ground-Based Electro-Optical Deep Space Surveillance
87. GLONASS: Global'naya Navigatsionnaya Sputnikovaya Sistema
88. GNC: Guidance, Navigation and Control
89. GNSS: Global Navigation Satellite Systems
90. GPS: Global Positioning System
91. GPU: Unidades de Procesamiento Gráfico (Graphic Processing Units)
92. GRU: Gate Recurrent Unit
93. GSIP: Global Space Innovation Project
94. GT: Grupo de Trabajo
95. HAPS: High Altitude Platform Systems
96. HOPAS: Hybrid Online Policy Adaptation Strategy
97. Hybrid CoE: Hybrid Centre of Excellence
98. HYFUTEC: Hybrid Warfare: Future and Technologies
99. H2020: Horizon 2020
100. IA: Inteligencia Artificial
101. IAC: International Astronautical Congress
102. IAF: International Astronautical Federation
103. IMU: Inertial Measurement Unit
104. iMUGS2: Integrated Modular Unmanned Ground System 2
105. INS: Inertial Navigation System
106. ILRS: International Lunar Research Station (China)
107. INTA: Instituto Nacional de Técnica Aeroespacial
108. IoT: Internet de las cosas
109. IP: Propiedad Intelectual
110. IPB: Intelligence Preparation of the Battlefield
111. IRDS: Hoja de Ruta Internacional para Dispositivos y Sistemas
112. IRIS2: Infrastructure for Resilience, Interconnectivity and Security by Satellite
113. ISA: Instruction Set Architecture
114. ISAC: Information Sharing and Analysis Centre
115. ISIS: The Islamic State of Iraq and Syria

- 116.ISR: Intelligence, Surveillance, Recognition
- 117.ISTAR: inteligencia, vigilancia, adquisición de objetivos y reconocimiento
- 118.ISS: International Space Station
- 119.ITIF: Information Technology and Innovation Foundation
- 120.IVA: Agentes virtuales inteligentes
- 121.I+D: Investigación y Desarrollo
- 122.IVERES: Identificación, Verificación y Respuesta.
- 123.JADC2: Joint All Domain Command and Control
- 124.JAXA: Japan Aerospace Exploration Agency
- 125.JRC: Joint research Centre (EU)
- 126.KNN: K nearest neighbours
- 127.KSP: Kerbal Space Program
- 128.KSPDG: Kerbal Space Program Differential Games suite
- 129.LEO: Low Earth Orbit
- 130.LHC: Large Hadron Collider
- 131.LIDAR: Laser Imaging Detection and Ranging
- 132.LLM: Large Language Model
- 133.LNO: Oxido de Litio y Niquel
- 134.LSTM: Long Short-Term Memory
- 135.MaaS: Malware as a Service
- 136.MBS: Military Brain Sciences
- 137.MCEE: Mando Conjunto del Ciberespacio
- 138.MDI-QKD: QKD independiente del dispositivo de medición
- 139.MDMP: Military Decision-Making Process
- 140.MEO: Medium Earth Orbit
- 141.ML: Machine learning
- 142.MLP: Multilayer Perceptron
- 143.M&S: Modelado y Simulación
- 144.NATO: North Atlantic Treaty Organization
- 145.NASA: National Aeronautics and Space Agency

- 146.NAVWAR: Navigation War
- 147.NM: Nanómetros
- 148.NOAA: National Oceanic and Atmospheric Administration
- 149.NRO: National Recognition Office (US)
- 150.NSSA: National Security Space Association
- 151.NIH: National Institute of Health
- 152.NIMBUS: Neurological Intelligent Monitoring and Brain Utilisation System
- 153.NIST: National Institute of Standards and Technology
- 154.NLP: Natural Language Processing
- 155.NPN Redes Fotónicas Neuronales
- 156.N3: Next-Generation Nonsurgical Neurotechnology
- 157.OBC: On-board Computer
- 158.OEM: Original Equipment Manufacturer
- 159.ONU: Organización de las Naciones Unidas
- 160.OST: Outer Space Treaty
- 161.OTAN: Organización del Tratado del Atlántico Norte
- 162.PCCh: Partido Comunista de China
- 163.PCM: Memoria de cambio de fase
- 164.PERTE: Proyectos Estratégicos para la Recuperación y Transformación Económica
- 165.PIB: Producto Interior Bruto.
- 166.PNT: Positioning, Navigation and Timing
- 167.PNOTS: Programa Nacional de Observación de la Tierra por Satélite
- 168.PSYOPS: Psychological Operations
- 169.QAOA: Quantum Approximate Optimization Algorithm
- 170.QBI: Quantum Benchmarking Initiative
- 171.QCaaS: Computación Cuántica como Servicio
- 172.QEC: Quantum Error Correction
- 173.QESS: Quantum Experiments at Space Scale
- 174.QKD: Quantum Key Distribution
- 175.QML: Quantum Machine Learning

- 176.QNN: Quantum Neural Network
- 177.QPU: Quantum Processing Unit
- 178.QuASAR: Quantum-Assisted Sensing and Readout (DARPA)
- 179.QSVM: Quantum Support Vector Machine
- 180.QW: Quantum Warfare.
- 181.RA: Realidad Aumentada
- 182.REAIM: Responsible AI in the Military Domain
- 183.REPMUS: Robotic Experimentation and Prototyping with Maritime Unmanned Systems.
- 184.RF: Radio Frequency
- 185.RINEX: Receiver INdependent Exchange
- 186.RISC-V: Reduced Instruction Set Computer - V
- 187.RL: Reinforcement Learning
- 188.RNN: Recurrent Neural Networks
- 189.rQOPS: Reliable Quantum Operations Per Second
- 190.RoQS: Robust Quantum Sensors
- 191.RRAM: Memoria de acceso aleatorio resistiva
- 192.RTVE: Radio Televisión Española
- 193.RuMoD: Russian Ministry of Defense,
- 194.RV: Realidad virtual
- 195.R2C2: Rapid and Resilient Command and Control
- 196.SAR: Sistema de Alerta Rápida (UE)
- 197.SatCen: European Union Satellites Centre
- 198.SCORE: Signal Corps Orbiting Relay Experiment
- 199.SDA: Space Domain Awareness
- 200.SDA: Space Development Agency
- 201.SIA: Semiconductor Industry Association
- 202.SIMD: Instrucción única, datos múltiples (Single Instruction Multiple Data)
- 203.SiP: Sistema en empaquetado (System in Package)
- 204.SML: Modelos de lenguaje pequeños (Small Language Models)
- 205.SoC: Sistema en chip (System on Chip)

- 206.SPSS: Statistical Package for the Social Sciences
- 207.SSA: Space Situational Awareness
- 208.ST: Soberanía Tecnológica
- 209.STM: Space Traffic Management
- 210.TDOA: mediciones de diferencia de tiempo de llegada
- 211.TEDAE: Asociación española de empresas tecnológicas de defensa, seguridad, aeronáutica y espacio
- 212.TEXBAT: Texas Spoofing Test Battery
- 213.THeMIS: Tracked Hybrid Modular Infantry System
- 214.TICs: Tecnologías de la información y las comunicaciones
- 215.TRL: Technology Readiness Level
- 216.TSMC: Taiwan Semiconductor Manufacturing Company
- 217.TTPO: Technology Transfer Programme Office (ESA)
- 218.UE: Unión Europea
- 219.UGV: Vehículos terrestres no tripulados
- 220.URSS: Unión de Repúblicas Socialistas Soviéticas
- 221.US: United States
- 222.USSF: US Space Force
- 223.US2QC: Underexplored Systems for Utility-Scale Quantum Computing)
- 224.UK: United Kingdom
- 225.US2QC: Underexplored Systems for Utility-scale Quantum Computing
- 226.VAE: Autocodificadores variacionales
- 227.VLOT: Vertical Landing and Take-Off
- 228.VPN: Virtual Private Network
- 229.VQA: Algoritmos Cuánticos Variacionales
- 230.VQC: Variational Quantum Circuits
- 231.VRE: Virtual Reality Environment
- 232.WEF: World Economic Forum
- 233.WoS: Web of Science
- 234.XAI Inteligencia Artificial Explicable IA en el espacio.

Anexo 2.

Evolución tecnológica del aprendizaje basado en redes de neuronas artificiales

A2.1. Aprendizaje automático clásico

Las aplicaciones de la IA hoy en día pueden resultar sorprendentes; pero **comparten una serie de principios y técnicas que surgen en la segunda mitad del siglo XX en lo que ahora se denomina “aprendizaje automático clásico”**. Las revisamos brevemente para señalar que en realidad se trata de un continuo de invenciones y hallazgos que parten de la Estadística.

Las técnicas de aprendizaje clásico pertenecen a la categoría del aprendizaje supervisado. Se basan en el concepto básico de clasificación: dada una entrada descrita por sus características en un espacio de características que pueden ser numéricas o categóricas, se trata de conseguir un modelo que actúe como separador de los diferentes tipos que podemos encontrar a la salida del sistema.

- **Regresión logística (1958)**

La regresión logística es un modelo estadístico que se usa para predecir la probabilidad de una variable binaria en función de una o más variables numéricas independientes (Cox, 1958). Esto se logra aplicando una **función logística** (sigmoide) sobre una combinación lineal de las entradas. **Se considera parte del aprendizaje automático cuando los coeficientes del modelo se obtienen mediante entrenamiento.**

Uno de los usos más conocidos fue el de identificar los mensajes de correo electrónico de tipo *spam* (clasificación), también se aplicó a la predicción de enfermedades y análisis de riesgos en finanzas (predicción). Se incorporó a varios paquetes de software estadístico como *SPSS (Statistical Package for the Social Sciences)* y viene implementada en prácticamente cualquier biblioteca de programación. **Su limitación principal es que supone una relación lineal entre las variables independientes**, y también que si entre las muestras de entrenamiento hay valores atípicos la función se acaba adaptando para identificar bien estos valores a costa de peores resultados para los demás.

Aunque está ya superado por otros enfoques, establece las bases metodológicas para las tareas de clasificación y predicción, que comparte con todos los enfoques de aprendizaje supervisado. **Cuanto mayor y más variado sea el *dataset*, y cuantas más épocas (vueltas de ajuste) se hagan, mejor será el modelo** -esto es, los parámetros se acercarán más a un modelo hipotético que acertara el 100% de las veces. Aunque hasta el último cuarto del siglo pasado no había grandes *datasets*, ya se empezaba a vislumbrar la **necesidad de muchos recursos de cómputo para obtener modelos de calidad.**

Los coeficientes de la combinación lineal de entradas se representan con matrices para facilitar la programación de estos algoritmos. Varios métodos más avanzados y unas cuantas décadas de desarrollo más tarde, esto dará lugar a la necesidad de usar GPUs para procesar modelos grandes.

- **Vecinos más cercanos KNN (K nearest neighbours)**

Es un algoritmo de aprendizaje supervisado que, **en vez de entrenar un modelo, almacena el conjunto de datos de entrenamiento y toma decisiones basadas en la cercanía de nuevos ejemplos a los ejemplos vistos previamente.** Para clasificar o predecir, busca los k vecinos más cercanos al nuevo punto en el espacio de características, de acuerdo con alguna **métrica de distancia** (euclidiana, Manhattan, etc.) y usa sus etiquetas para inferir la salida por votación o promedio (Cover et al., 1967).

A pesar de ser un método de aprendizaje supervisado, **no necesita entrenamiento porque no genera un modelo.** Esto limita la explicabilidad del modelo y su evaluación por expertos humanos. Otro problema es que, para realizar las inferencias, debe calcular la distancia de cada dato de entrada con todos los del dataset de entrenamiento lo que puede provocar grandes latencias. También sufre el problema de la “*maldición de la dimensionalidad*”, cuando el número de dimensiones (características) crece, la distancia deja de reflejar similitud; esto es, las distancias vienen a ser casi iguales entre todos los puntos. A pesar de ello, se ha usado con éxito para clasificación de imágenes, reconocimiento de dígitos manuscritos, y sistemas de recomendación.

- **Máquinas de Soporte Vectorial (SVM) — 1992**

Las **Máquinas de Soporte Vectorial** (SVM en inglés) son **algoritmos de aprendizaje supervisado utilizados tanto para clasificación como para regresión** (Boser et al., 1992). Su objetivo principal es encontrar el hiperplano óptimo que separa las distintas clases en un espacio de características, maximizando el margen entre ellas.

Si pensamos en dos características y dos tipos (clases) se trata de encontrar la recta que mejor separa los puntos de un tipo de los de otro, buscando los puntos fronterizos y trazando la recta que pasa lo más lejos posible de esos puntos fronterizos.

Cuando los puntos no están claramente separados (clases no linealmente separables), se usan unas **funciones “kernel”** que los proyectan a un espacio de más dimensiones donde sí están separados (ejemplos de *kernels* son: lineal, polinómico, radial, sigmoide, etc.). Dado un *dataset* de entrenamiento que contiene los puntos en el espacio de características y la etiqueta de la clase a la que pertenecen, se entrena una función de decisión que es una función lineal con pesos para cada dimensión, y se consigue el valor de estos pesos, de forma similar a como se ha explicado para la regresión logística.

Las SVM se han usado para filtrado de correo spam, clasificación de documentos, reconocimiento de objetos y rostros en fotografías, análisis de datos genéticos y clasificación de proteínas, y detección de anomalías en ciberseguridad y detección de fraude en transacciones financieras. Son problemas de clasificación que usan datos con muchas dimensiones, y en su momento fueron el método más avanzado.

Sus **limitaciones** tienen que ver con lo costoso de su entrenamiento con conjuntos de datos (*dataset*) muy grandes (necesarios para obtener resultados suficientemente precisos); la difícil selección de la función *kernel*; y la interpretabilidad de los modelos resultantes comparados con los árboles de decisión.

- **Árboles de Decisión — 1986–1993**

Los árboles de decisión son modelos de predicción/clasificación en forma de estructura de árbol, donde **cada nodo representa una decisión de clasificación, las ramas salientes representan los resultados y las hojas finales contienen la clase o valor de salida**. En la figura A2.1 se puede observar un árbol de decisión creado sobre el dataset de viajeros del *Titanic*⁴¹⁹ (ejemplo típico utilizado en formación). Los nodos son las preguntas sobre algún atributo, las ramas que salen de las respuestas (sí/no) y cuando llegamos a un nodo hoja tenemos la respuesta y su probabilidad en el dataset. Esto mismo se podría usar para responder a la pregunta “qué hubiera pasado si...” (predicción), pasando un hipotético nuevo pasajero descrito por sus características⁴²⁰.

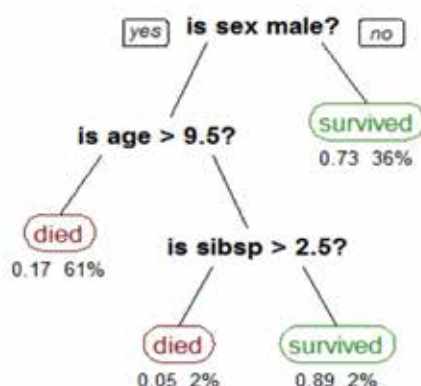


Figura A2.1. Árbol generado con CART (*Classification and Regression Trees*) sobre el Titanic dataset. Fuente: <https://www.kaggle.com/c/titanic/data>

No obstante, **sufren problemas de sobreajuste, inestabilidad -pequeños cambios de datos pueden generar árboles muy distintos, y poca precisión en tareas complejas**. Pero su

419 Titanic - Machine Learning from Disaster. <https://www.kaggle.com/c/titanic/data>

420 Dependiendo del criterio de partición que se use para definir las preguntas, hay variantes como ID3 (Quinlan, 1986), que usa una medida de entropía; C4.5 (Quinlan, 1993) que mejora al anterior con poda y soporte para datos continuos, o CART Classification and Regression Trees (1986) que usa una medida denominada índice Gini y soporta regresión.

sencillez a la hora de implementarlos e interpretar sus resultados los hicieron muy **útiles en combinación con sistemas expertos para tareas de clasificación** como el diagnóstico médico, clasificación de riesgos de crédito, predicción de abandono escolar, procesamiento de texto y datos de tablas.

- **Bosques aleatorios 2001**

Un refinamiento a los árboles de decisión son los **Bosques Aleatorios** (*Random Forests*) (Breiman, 2001). Son **algoritmos de aprendizaje por ensamblado** que combinan múltiples árboles de decisión entrenados sobre diferentes subconjuntos del conjunto de datos, elegidos aleatoriamente y seleccionando un subconjunto aleatorio de características para buscar la partición. La predicción final se realiza mediante votación o promedio, lo que mejora la precisión y estabilidad. Con esto **se buscaba mejorar los resultados de los árboles de decisión en cuanto a estabilidad y sobreajuste**.

Se han usado en clasificación-bioinformática, detección de fraude, modelado de riesgos financieros, diagnóstico clínico. Son **menos interpretables que los árboles de decisión y no dan buenos resultados cuando hay muchas dimensiones y algunas son irrelevantes**, motivo por el cual normalmente se usan tras haber realizado una selección de las características de interés (ingeniería de características). Todas las bibliotecas de programación tienen implementaciones de **Bosques Aleatorios**. Se solían entrenar sobre hardware estándar (CPUs convencionales).

- **Boosting (AdaBoost, Gradient Boosting) — 1995–2001**

“*Boosting*” es también una técnica de ensamblado de modelos que **usa árboles de decisión, pero en lugar de ponerlos en paralelo los combina de forma secuencial, de forma que cada nuevo modelo intenta corregir los errores cometidos por los anteriores**. El modelo final es una combinación ponderada de todos. Las variantes más difundidas son *AdaBoost* (*Adaptive Boosting*) (Freund & Schapire, 1997) y *Gradient Boosting* (Friedman, 2001). Se han usado con éxito para ranking en motores de búsqueda, predicción del abandono de usuarios y detección de fraude financiero. Su entrenamiento es secuencial y tiene muchos hiper-parámetros lo que puede complicar el entrenamiento. Se han entrenado tanto sobre CPUs como sobre GPUs.

A2.2. El aprendizaje profundo: del Perceptrón al Transformer

Las redes de neuronas artificiales tienen sus orígenes en 1943, cuando los pioneros Rosenblueth, Wiener y Bigelow (Rosenblueth et al., 1943) estudiaron las similitudes entre los dispositivos electrónicos y los sistemas biológicos. Ese mismo año, McCulloch y Pitts (1943) propusieron imitar la cognición humana mediante un modelo de neurona artificial basado en el comportamiento binario (activo-inactivo) de la neurona biológica y su similitud con el comportamiento encendido-apagado de los interruptores. Este modelo de célula artificial

dio lugar a la rama de la **inteligencia artificial conexionista**, y se considera el precursor de las neuronas artificiales y del aprendizaje profundo.

En 1958, Rosenblatt creó el **Perceptrón**, una red neuronal de una capa capaz de aprender y que fue pionera en el reconocimiento de imágenes y en clasificar fotos. Un avance relevante, con gran impacto en nuestros días, fue el **algoritmo de retropropagación del gradiente** del error (Rumelhart et al., 1986) para el entrenamiento de redes de neuronas profundas. Se denominan así ya que concatenan varias capas de neuronas, denominadas **capas ocultas**.

Este algoritmo, en el segundo decenio del siglo XXI, resultó clave para el desarrollo del denominado **“aprendizaje profundo”** y de la **inteligencia artificial generativa**. A continuación, se detallan las **técnicas más relevantes en el dominio del aprendizaje profundo**.

El Perceptrón

El **perceptrón** (Rosenblatt, 1958) fue el **primer modelo de una neurona artificial capaz de aprendizaje supervisado simple**. El concepto de neurona artificial se inspira en el de la biología. Recibe señales de entrada por los axones, y mediante una operación sencilla de álgebra lineal, calcula el valor resultado como la suma del producto de cada entrada por su peso, para finalmente pasar este resultado a una función de activación que da el valor de salida (puede ser un valor binario verdadero-falso)⁴²¹.

Su **proceso de aprendizaje** es sencillo, si tenemos un conjunto de muestras de entrada con las salidas esperadas de cada una (se llaman etiquetas), se pasan las entradas y el resultado obtenido se compara con la salida esperada (etiqueta). Si son diferentes, se van variando los pesos de las señales de entrada. Según se pasan más datos de prueba, se van modificando los pesos para ajustarse mejor a los ideales.

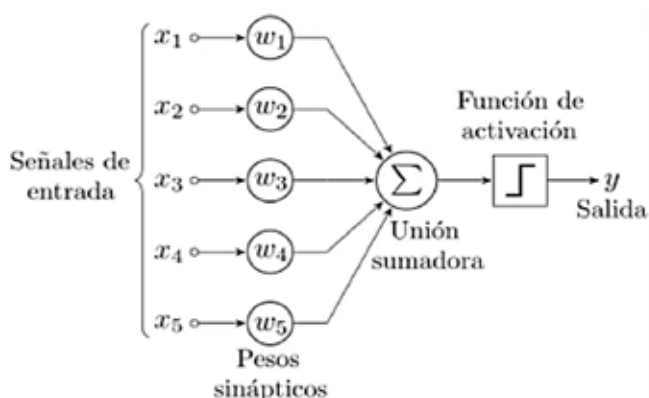


Figura A2.2 Perceptrón. Fuente: Rosenblatt (1958)

421 Nótese que las entradas y los pesos se pueden representar como matrices de 1 dimensión, y el valor que se pasa a la función de activación es el resultado de multiplicar estas dos matrices.

Se diseñó para **simular el aprendizaje de patrones visuales básicos**, y se usó para la clasificación binaria de patrones y para reconocimiento de caracteres simples (poniendo una neurona en paralelo para cada carácter). Tuvo una implementación experimental en hardware llamada **Mark I perceptrón**. En 1969 se demostró que solo valía para resolver problemas lineales, cuyas soluciones pudieran separarse mediante rectas (problema del XOR) y se abandonó esta línea de investigación (según indican, este fue el primer invierno de la IA) (Minsky & Papert, 1969).

Para ilustrar su funcionamiento, en la figura A2.3 se representa un **ejemplo de entrenamiento e inferencia de una neurona capaz de reconocer el dígito 3 en una imagen**.

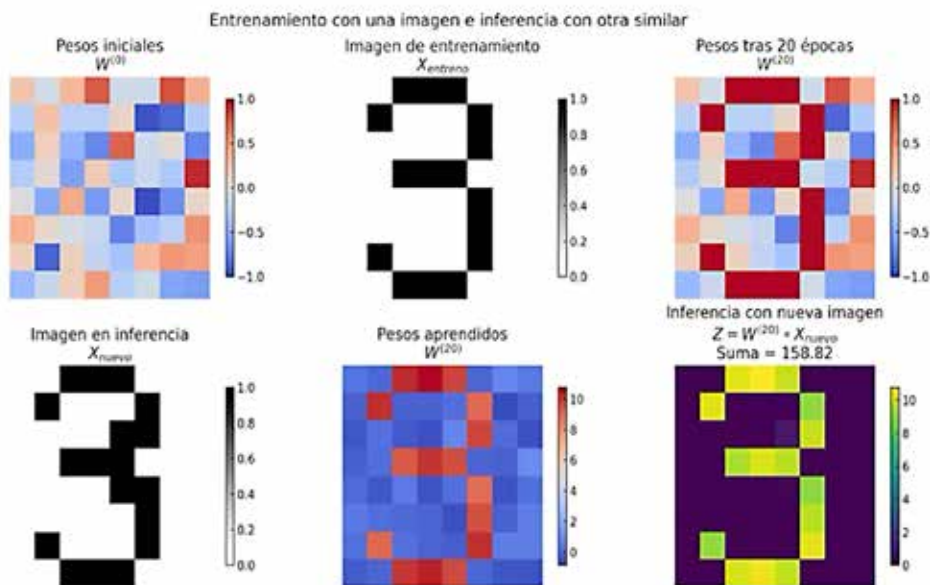


Figura A2.3. Entrenamiento e inferencia.

En la parte de arriba se representa la **matriz bidimensional de pesos** con la que se inicializa la neurona, y la imagen del dataset de entrenamiento que muestra lo que tiene que aprender a reconocer (es una matriz bidimensional de píxeles). En la parte de arriba a la derecha se observa la **matriz de pesos después de 20 vueltas de ajuste** (épocas), realizado mediante la función matricial que se ve arriba. Es fácil darse cuenta de que la neurona ha captado los patrones necesarios para reconocer un 3 -cosa que en la matriz inicial de pesos no ocurría.

Las líneas de abajo corresponden a la **inferencia**: en la intermedia se presenta una muestra para reconocer que no es exactamente la que se ha aprendido, pero que sigue siendo

claramente un 3. Al aplicarle la matriz de pesos aprendidos, obtenemos como resultado el valor 158.82 que consideramos en la fase de validación aceptable para reconocer el 3.

El uso de un *dataset* para entrenamiento, las matrices que van modificándose en cada paso del entrenamiento mediante operaciones matriciales, y su modificación para reducir el error entre lo que en cada paso es capaz de reconocer y lo que se le muestra, son **elementos básicos de cualquier sistema de aprendizaje basado en redes neuronales, desde este inicial Perceptrón hasta los Transformers**.

Las redes neuronales multicapa (década de 1960)

Las **redes neuronales multicapa** (*Multilayer Perceptron, MLP*) (Rumelhart et al., 1986) están compuestas por varias capas de neuronas: una de entrada, una o más capas ocultas y una capa de salida. Esta arquitectura permite modelar relaciones complejas y resolver problemas no linealmente separables.

Se puede considerar cada capa como un perceptrón, de esta forma una capa toma las señales de entrada de su capa anterior (o la entrada para la primera), y las recibe en sus neuronas a través de sus pesos y realizan la función de activación cada una de ellas; y las salidas de una capa se conectan a las entradas de la capa siguiente. Las capas que no son ni de entrada ni de salida del sistema se llaman “*capas ocultas*” porque su proceso no es visible externamente, y esta es una de las principales razones por las que se reduce la explicabilidad de los modelos de este tipo⁴²² (véase figura A2.4).

Esta técnica necesita *datasets* de entrenamiento y capacidad de cómputo cada vez mayores, al tener que encontrar los valores enfocados de muchos más parámetros (los de las conexiones entre neuronas)⁴²³.

422 Cuantas más capas ocultas existan, mayor profundidad de procesamiento -de aquí el nombre de aprendizaje profundo. Recordemos que, si cada neurona se puede representar como una matriz, una capa se maneja con una matriz con una dimensión más, y las aplicaciones de capa se pueden manejar como multiplicaciones de estas matrices. Esta es la relación entre las matrices y los exigentes requisitos de cómputo del aprendizaje profundo.

423 Otra dificultad es que el sobreajuste sea capaz de reconocer perfectamente las muestras que aparecen en el dataset, pero no acertar en muestras que pueden aparecer en la inferencia que no se hubieran visto en el entrenamiento. Las primeras implementaciones se programaron en el lenguaje FORTRAN, y ahora la mayoría de las bibliotecas especializadas contienen alguna.

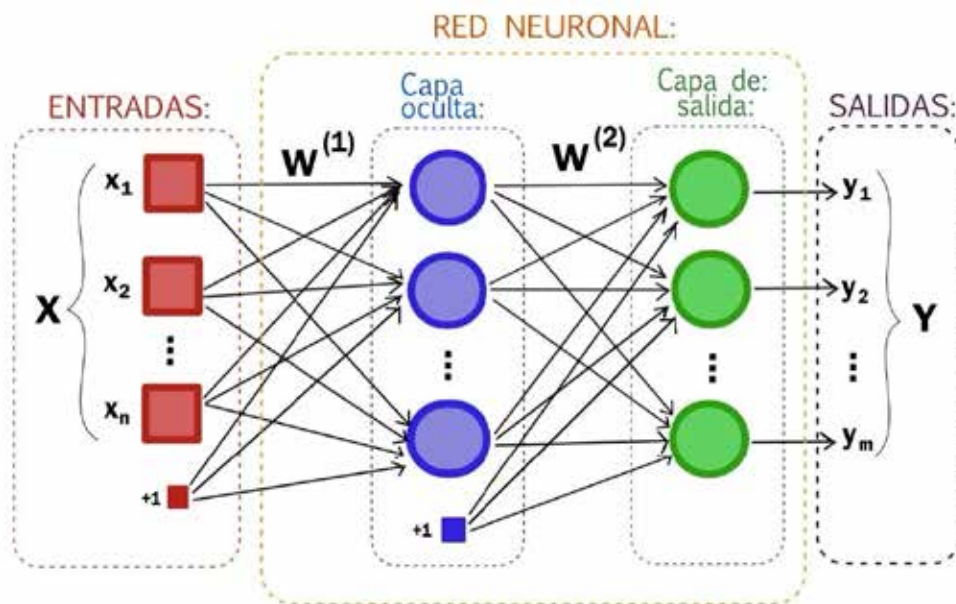


Figura A2.4 Estructura típica de una red neuronal multicapa. Fuente: <https://www.linkedin.com/pulse/7-consejos-para-trabajar-con-redes-neuronales-en-rod%C3%ADguez-mgs/>

Siendo el método más avanzado de su época, se utilizó para muchas aplicaciones relacionadas con el reconocimiento de patrones, proceso de señal, predicción de series temporales, etc.⁴²⁴.

Redes Neuronales Convolucionales (CNN) — 1989 / 1998

Las CNN (LeCun et al., 1998) **son redes neuronales especialmente diseñadas para procesar datos con estructura matricial**. Incorporan capas convolucionales compuestas por filtros (pequeñas ventanas) que aprenden a reconocer patrones de forma automática, con lo que pueden detectar bordes, formas y patrones geométricos.

Estos filtros no se programan manualmente, sino que se aprenden en el proceso de entrenamiento de toda la red, formando jerarquías. Es el propio proceso de entrenamiento el que selecciona los filtros más útiles para reconocer los elementos que aparecen con frecuencia en el dataset de entrada⁴²⁵. En la figura A2.5. se representa el **proceso de activación en una red convolucional aplicando tres filtros a una imagen base**.

⁴²⁴ Aunque el concepto se desarrolló justo después del Perceptrón, y permite resolver problemas no linealmente separables, no se empezó a usar de forma general hasta la década de 1980 con la publicación del algoritmo de entrenamiento por retropropagación.

⁴²⁵ Por ejemplo, en un sistema de identificación de elementos en imágenes, suele haber una primera capa que detecta bordes, líneas, esquinas o colores; la segunda capa combina estos resultados para reconocer curvas, formas o texturas.

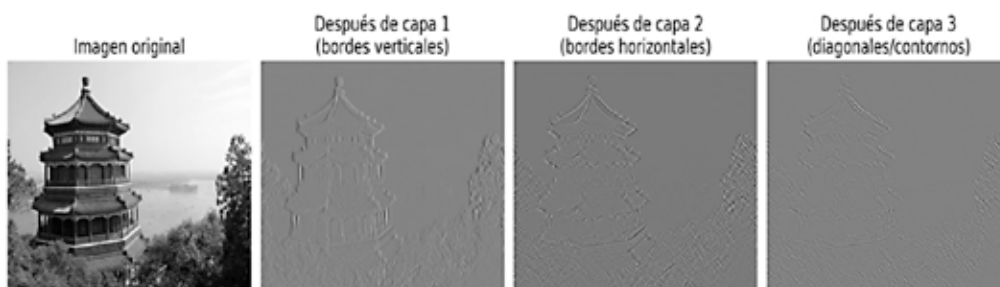


Figura A2.5 Proceso de activación en una red convolucional: aplicación secuencial de tres filtros sobre una imagen base. Fuente: La imagen base es parte del conjunto de imágenes de ejemplo de scikit-learn. Fuente: <https://scikit-learn.org/>

En la figura A2.6 se puede ver un esquema del funcionamiento del modelo convolucional. Se puede decir que este tipo de redes neuronales representan un avance radical en lo que respecta al tratamiento de imágenes y su aplicación al diagnóstico por imágenes médicas, visión artificial en robótica y reconocimiento facial, por ejemplo. **Estas aplicaciones tienen también utilidad en el ámbito de la Defensa y la Seguridad.**

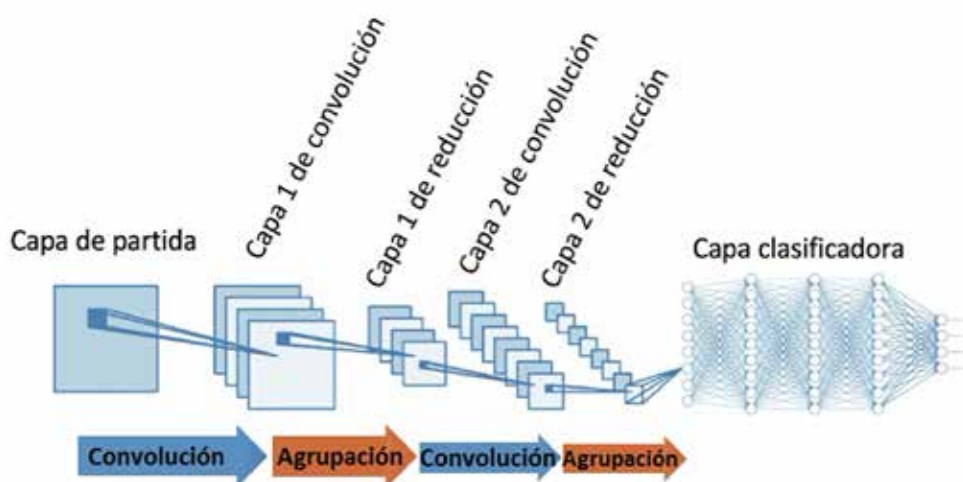


Figura A2.6 Modelo convolucional. Fuente: Machado et al., 2020.

También comienzan a cobrar relevancia problemas que aún hoy en día siguen limitando la aplicación de las técnicas de aprendizaje profundo: **requieren grandes volúmenes de datos para alcanzar niveles aceptables de calidad, necesitan muchos recursos de cómputo para el entrenamiento** (que se basa en el cálculo de tensores -matrices con muchas dimensiones), y la **falta de explicabilidad-interpretabilidad de estos modelos**.

Las siguientes capas reconocen partes de objetos como ruedas, alas, ventanas, y las últimas capas detectan objetos como aviones, camiones, bicicletas, etc.

Aunque las primeras implementaciones se desarrollaron en lenguaje C funcionando sobre CPUs (arquitectura *LeNet* diseñada por el autor del enfoque Yan LeCun), hoy hacen uso de GPUs y aceleradoras IA.

Redes Neuronales Recurrentes (RNN) y LSTM — 1995

En las capas ocultas encontramos conexiones “hacia atrás”, desde la salida de neuronas en capas más cercanas a la salida, hacia la entrada de capas anteriores, lo que les confiere la posibilidad de considerar tanto los valores actuales de entrada como valores anteriores⁴²⁶.

Es un **mecanismo de “memorización”** útil para trabajar con series temporales y secuencias de datos como los textos. La parte de la red que se encarga de aprender la relación de un valor con los anteriores se llama “puerta” y por eso las versiones modernas también se llaman **GRU** (*Gate Recurrent Unit*).

Una vez enunciado el mecanismo, este se refina con puertas (de entrada, de olvido y de salida) que controlan el flujo de información y retención de memoria, que dan lugar a las **LSTM** (Long Short-Term Memory) memorias de corto y largo plazo (Hochreiter & Schmidhuber, 1997). La figura A2.7 presenta un esquema básico de su funcionamiento.

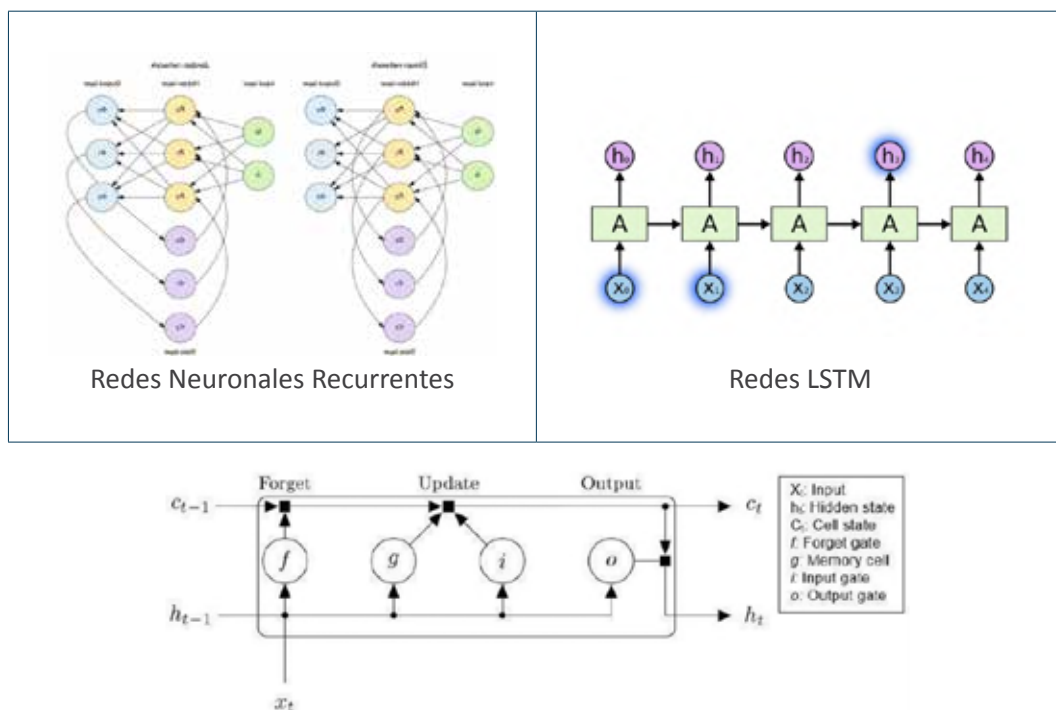


Figura A2.7 Redes neuronales recurrentes. Fuente: Hochreiter & Schmidhuber, 1997

426 Las redes neuronales recurrentes fueron introducidas por Elman y Jordan en 1986-1990.

Estos sistemas ya se entrenaron directamente con GPUs, y **con ellos comienza la exploración del uso de la IA para lenguaje**, con aplicaciones como traducción automática (*seq2seq*), modelado del lenguaje, reconocimiento y generación de voz. Quizás su uso más extendido tiene que ver con las series temporales, que están en la base de muchos problemas de predicción como los relacionados con el mantenimiento de equipos industriales.

Con todo, a lo complejo de su entrenamiento como en el resto de los modelos previos hay que añadir la **dificultad de entrenamiento con secuencias largas** y que no se puede paralelizar como en las CNN. Una década más tarde los **Transformers** han superado a estos modelos en el proceso de lenguaje.

Autoencoders — 2006

Un autoencoder (Hinton & Salakhutdinov, 2006) **es un tipo de red neuronal diseñada para aprender una representación comprimida (codificada) de los datos de entrada y luego reconstruirlos a partir de esta representación**. El objetivo del *autoencoder* es minimizar la diferencia entre los datos de entrada y los datos reconstruidos, permitiendo así que la red aprenda representaciones eficientes de los datos. Son útiles para comprimir datos, detectar anomalías, para reducir el número de dimensiones con el que representar datos y como parte del preentrenamiento de redes profundas (son parte de los Transformers).

Desde un punto de vista intuitivo se puede plantear la pregunta de cómo es posible codificar por ejemplo puntos del espacio 3D en un plano 2D (reducción de 3 a 2 de las dimensiones); el enfoque consiste en no codificar todos los puntos del espacio 3D lo que obviamente es imposible con 2D, sino que son solo unos cuantos puntos 3D los que se van a proyectar en 2D y basta con conseguir que la función de proyección no ponga dos puntos 3D de los que interesan en el mismo punto 2D. Dicho de otra forma, **esta técnica ofrece mejores resultados cuanto más dispersos sean los espacios de características de la entrada**.

Su arquitectura consta de dos componentes principales, como se muestra en la figura A2.8 (obsérvese que no hay conexiones recurrentes):

Codificador (*encoder*): reduce las dimensiones de los datos de entrada, creando una representación compacta conocida como espacio latente o código (o cuello de botella).

Decodificador (*decoder*): reconstruye los datos originales a partir de la representación comprimida generada por el codificador, y los muestra a la salida.

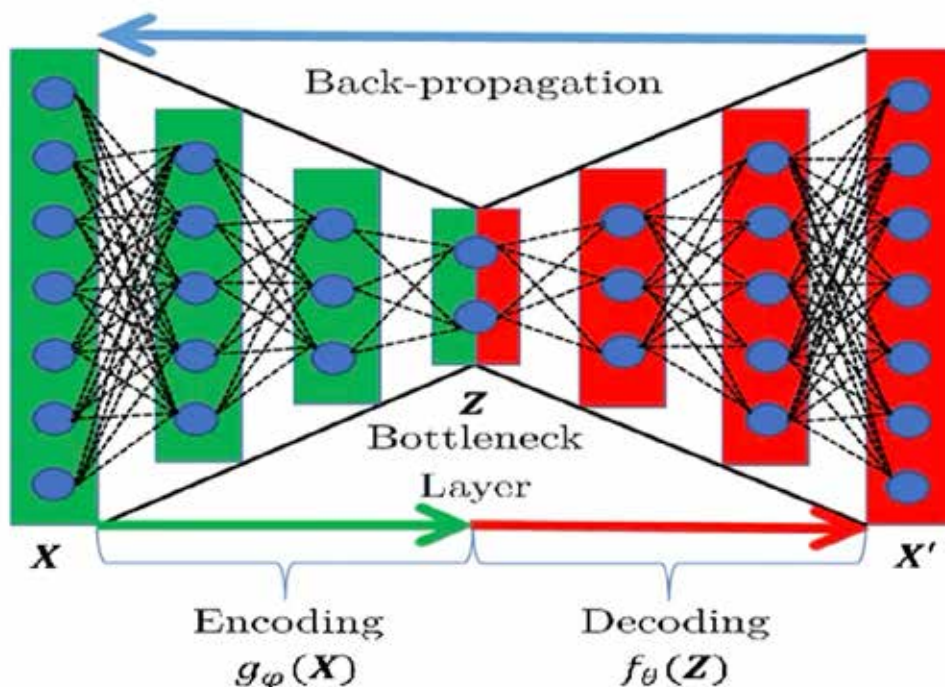


Figura A2.8. Autoencoder. Fuente: Ahmed et al, 2020.

Transformers — 2017

Los **Transformers** (Waswani et al. 2017) poseen una arquitectura basada en el concepto de “atención”⁴²⁷. Con ello, prescinde del uso de recurrencia y convoluciones, y es capaz de **procesar secuencias completas** (como frases o párrafos) **en paralelo**, y de capturar dependencias a largo plazo mediante mecanismos de **atención cruzada**.

La arquitectura “**Transformer**” ha permitido enormes avances en el procesamiento del lenguaje natural, desde la traducción automática hasta la redacción, el resumen, la respuesta a preguntas, el análisis semántico o la generación conversacional. También se usa para la *Inteligencia Artificial Generativa*, y visión por ordenador, y hay trabajos recientes que los aplican a series temporales.

Los modelos entrenados con esta arquitectura aprenden representaciones profundas del lenguaje y son capaces de generalizar a tareas muy diversas. Además, su capacidad para procesar secuencias en paralelo y capturar dependencias de largo alcance los ha hecho especialmente eficaces y escalables.

⁴²⁷ Resulta paradójico que, en unos tiempos en los que los seres humanos parecen estar perdiendo esta capacidad, la atención sea un mecanismo esencial del aprendizaje automático.

A partir de esta base han surgido los **modelos fundacionales**: grandes modelos preentrenados sobre enormes volúmenes de texto (corpus), capaces de adaptarse a múltiples tareas. Entre ellos se encuentran los **modelos grandes de lenguaje (LLM)**, que no solo utilizan la arquitectura Transformer, sino que la escalan a miles de millones de parámetros⁴²⁸. Son arquitecturas complejas en donde hay muchas capas de redes neuronales muy conectadas.

De hecho, **el mecanismo de atención requiere varias capas que relacionan las palabras de una frase con todas las demás**. Para entrenarlas no sólo es necesario contar con *datasets* enormes -en la literatura especializada se empieza a cuestionar la calidad de los nuevos modelos una vez que ya se han usado grandes subconjuntos de la Web-; también es necesaria una gran potencia de cómputo y memoria para trabajar con estos grandes modelos. Otro gran problema es el de su **explicabilidad**, ya que están compuestos por un gran número de capas de redes neuronales definidas por los pesos de sus enlaces. La integración del mecanismo de atención con el razonamiento simbólico es otro de los puntos activos de investigación.

La **arquitectura “Transformer”** se basa en un modelo simétrico compuesto por dos grandes bloques: el **codificador** y el **decodificador**. El primero recibe una secuencia de entrada y la transforma en una representación contextualizada de cada elemento, a partir de la cual el decodificador, basándose en lo que ha generado hasta el momento, produce paso a paso una secuencia de salida. Los dos bloques están formados por varias capas, y cada capa tiene tres componentes principales: un **mecanismo de atención**, una **red feedforward** y operaciones de **normalización con conexiones residuales**.

Los pasos del procesamiento son los siguientes:

- El procesamiento comienza con la conversión de las palabras o tokens en una secuencia de identificadores numéricos.
- Cada token se transforma luego en un **vector de embedding**, una representación densa y continua que captura su significado/semántica en el contexto del entrenamiento, y que puede estar **integrado en el Transformer**, o inyectado por un modelo externo.
- A estos vectores se les suma una **codificación de posición**, que añade información sobre el orden de aparición de cada token.

⁴²⁸ ChatGPT es un ejemplo de modelo conversacional construido sobre un LLM basado en Transformer, que puede mantener diálogos coherentes, seguir instrucciones y adaptarse al estilo del usuario. Estos sistemas usan de los Transformers su estructura de codificación, atención y generación secuencial, y añaden capas de entrenamiento específico o del control del comportamiento en contextos interactivos (las consultas o prompts).

- El resultado es un conjunto de **vectores de entrada** que contienen información de la estructura de la secuencia y de la semántica de sus elementos.
- Esta información pasa al **codificador** que se encarga de construir una representación contextualizada de la frase completa.
- En cada capa del codificador, el mecanismo de atención transforma cada uno de estos vectores en tres representaciones distintas mediante multiplicaciones por matrices de pesos entrenables:
 - ▀ una consulta (*query*), que representa qué tipo de información necesita esa palabra para comprender su papel en la frase;
 - ▀ una clave (*key*), que describe lo que esa palabra puede ofrecer a las demás;
 - ▀ y un valor (*value*), que contiene la información que efectivamente puede compartir.

Estos tres vectores se obtienen a partir del mismo vector de entrada, pero mediante operaciones matriciales distintas.

- A continuación, cada token realiza su consulta con todas las claves de la secuencia para calcular la relevancia de cada una y combinarlas de forma ponderada, lo que da como resultado una nueva representación para cada token, enriquecida con información de su contexto.
- Estos pasos se hacen en paralelo con todos los tokens de la frase, y los resultados se pasan por otra red ("*feedforward*") que hace transformaciones más complejas y favorece la abstracción.
- Tanto el resultado del mecanismo de atención como el de esta red se combinan con la entrada original mediante conexiones residuales, y se normalizan.
- El bloque codificador se ejecuta varias veces, para refinar progresivamente la representación interna de la secuencia.

En la figura A2.9 se pueden ver esquemáticamente los pasos de procesamiento de una arquitectura "Transformer".

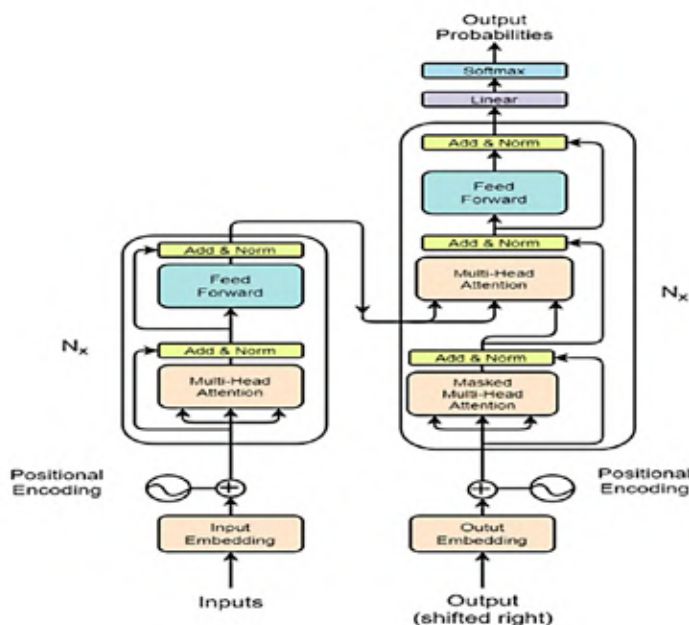


Figura A2.9 Pasos de procesamiento de una arquitectura "Transformer". Fuente: Vaswani et al, 2017.

El entrenamiento de un Transformer se realiza a partir de un corpus de texto, donde cada ejemplo contiene una entrada y una salida esperada. El modelo genera una predicción y se compara con la salida correcta utilizando una función de pérdida (o de error). El error resultante se propaga hacia atrás por todas las capas mediante retropropagación, ajustando todos los pesos. Durante el entrenamiento, el decodificador usa la técnica de recibir la salida correcta sin el último token, para que aprenda a predecirlo basándose en los anteriores (*teacher forcing*).

Una vez entrenado, en la fase de inferencia o predicción, el modelo funciona de forma autorregresiva: dado un texto de entrada, el *codificador* produce su representación contextual, y el *decodificador* comienza a generar la salida palabra por palabra. En cada paso, el *decodificador* utiliza la información que ha generado el *codificador*, y las palabras que ha generado previamente, con lo que produce la lista de siguientes palabras más probables, hasta llegar a un *token de finalización*.

Este mecanismo permite la **generación autónoma de texto coherente**, y es la base del funcionamiento de los **modelos generativos actuales**.

Anexo 3.

Progresiva convergencia de la IA con las tecnologías cuánticas y su previsible impacto en el sector de la defensa.

A3.1. Introducción

Las **tecnologías cuánticas**, entendidas como la **aplicación industrial de los principios de la mecánica cuántica**, han adquirido una notable presencia en nuestra vida cotidiana. Muchos de los avances tecnológicos de los que se beneficia la sociedad, desde los láseres y los microprocesadores digitales hasta las resonancias magnéticas, las tomografías por emisión de positrones, los televisores LED, las células solares y los superconductores, se basan en **fenómenos cuánticos**. Como exponente de su importancia, el año 2025 ha sido declarado *“Año de la Ciencia y la Tecnología Cuántica”* por las Naciones Unidas.

En la actualidad, se identifican **cuatro áreas clave** en este ámbito: la **computación cuántica**, la **simulación cuántica**⁴²⁹, la **criptografía cuántica** (ligada a las comunicaciones), y los **sensores y metrología cuánticas**. Si bien no es sencillo prever el alcance total de estos avances ni cuando las tecnologías estarán maduras y plenamente disponibles en la sociedad integradas en una nueva generación de productos, procesos y servicios, sí se puede afirmar que **abren un camino revolucionario** en la forma en la que se procesará la información, se protegerán los datos y se explorará la naturaleza.

El desarrollo de las **tecnologías cuánticas** se está realizando al mismo tiempo que se acelera el desarrollo y penetración en la sociedad de las tecnologías de **inteligencia artificial**. Ambas comparten la consideración de **tecnologías habilitadoras y de carácter dual** (potencial uso en aplicaciones civiles y militares) lo que les confiere una **relevancia estratégica** que se concretará cuando su convergencia alcance un grado de madurez suficiente para impulsar su uso conjunto en múltiples áreas de aplicación. Se trata de un nuevo dominio al que se ha empezado a denominar *QuantumAI*.

El presente **Anexo 3** pretende ofrecer una **panorámica actual y previsible evolución en los próximos diez años de la convergencia entre la IA y las tecnologías cuánticas**. Aunque esta convergencia tendrá relevancia en todos los sectores socioeconómicos, el presente Anexo pretende focalizar este análisis en el **ámbito de la defensa** con el objetivo de evaluar las consecuencias que pueden tener en el futuro en la denominada *“guerra cuántica inteligente”*. Se trata de un concepto sobre la que se ha empezado a elucubrar, definir algunas áreas e investigar y experimentar con nuevos productos y soluciones, a pesar de que, previsiblemente, su entrada en el mercado, salvo en aspectos puntuales, no se materializará hasta la próxima década.

429 Se analizará en este Anexo 3 la simulación junto con la computación cuántica siguiendo a la UE (Comisión Europea, 2025g).

Debe señalarse que **no se ha pretendido con el presente Anexo ofrecer un análisis científico y tecnológico detallado de las bases de la convergencia tecnológica citada, sino ofrecer una visión de carácter estratégico de la misma** y de su previsible evolución. El objetivo es que sirva de base para evaluar el impacto que pueda alcanzar, los elementos que la caracterizarían y las barreras e impulsores políticos y socioeconómicos para hacerla realidad en un marco de confrontación geopolítica y tecnológica creciente.

Esta visión se concretará en la **posición relativa de la Unión Europea (UE)** en comparación con el esfuerzo realizado por otras potencias tecnológicas con las que compite, fundamentalmente, Estados Unidos y China, así como los esfuerzos emprendidos desde la OTAN. Es relevante en este contexto la publicación por parte de la Comisión Europea en julio de 2025 de la Comunicación titulada *“Quantum Europe Strategy: Quantum Europe in a Changing World”* (Comisión Europea, 2025g) como marco de actuación y discusión colectiva para poder ser un jugador global relevante en la batalla tecnológica global.

A3.2. Estado actual de las tecnologías cuánticas

A3.2.1. Computación Cuántica

La denominada **computación de altas prestaciones** (*High-Performance Computing, HPC*), se refiere a un concepto relativo a sistemas con las más altas capacidades de computación posibles en cada momento histórico. Las tecnologías de HPC se han desarrollado para abordar las crecientes necesidades computacionales de las diferentes ramas científicas y tecnológicas mediante la disponibilidad de **ordenadores con arquitecturas especializadas capaces de realizar un procesamiento paralelo masivo**⁴³⁰.

Si bien la capacidad de cálculo de los ordenadores ha ido mejorando exponencialmente con los años de acuerdo con la **ley empírica de Moore**, esta ley tiene una limitación física clara: llegará un momento en que el tamaño de los transistores no pueda reducirse más al entrar en la **escala atómica**, momento que ya está muy cerca. A pesar de ello, se puede **extender la capacidad computacional** actual mediante la especialización del diseño de chips cuya arquitectura esté adaptada para la resolución óptima de ciertos problemas: como ejemplo, **unidades de procesamiento (CPU) de propósito general** con diseño en 3D, o **unidades de procesamiento gráfico (GPU) de propósito más específico** (p.ej. las empleadas como aceleradores para IA).

Un **supercomputador con una arquitectura distribuida de muchos nodos** equivale a varios ordenadores trabajando de forma concurrente y en paralelo. Con él se pueden obtener prestaciones elevadas asignando múltiples nodos de proceso a tareas concretas. Además,

430 El primer puesto en el ranking Top 500 de junio de 2025 sitúa en primer lugar al supercomputador “El Capitán” del Lawrence Livermore Lab (LLL) en Estados Unidos con una potencia de 1.742 Eflops/s basado en un HPE Cray EX255a <https://top500.org/>

también es posible **trabajar en red entre varios supercomputadores** compartiendo datos y tiempo de cálculo en tiempo real aprovechando el despliegue de redes de comunicación de gran velocidad.

Todos los países avanzados disponen de uno o más supercomputadores (públicos o privados) conectados en red ofreciendo servicios a su comunidad científica y tecnológica. En España se dispone de la **Red Española de Supercomputación (RES)**⁴³¹ formada por 14 instituciones que comparten el acceso a sus máquinas de supercomputación. El equipo más potente disponible en España es el **MareNostrum 5** (véase figura A3.1) que alcanza una potencia de computación pico de 314 PFlops. Este modelo se reproduce a nivel europeo con la iniciativa *EuroHPC-JointUndertaking* (*EuroHPC-JU*) que permite el **acceso de los investigadores a supercomputadores situados en varios países europeos**⁴³².



Figura A3.1. Supercomputador MareNostrum 5 del BSC.

Fuente: <https://www.bsc.es/ca/marenostrum/marenostrum-5>

Sin embargo, a pesar de la continua mejora en la capacidad de cálculo que ofrecen los supercomputadores más potentes, **siguen existiendo límites computacionales**. Uno de los aspectos fundamentales que impulsan el desarrollo de **ordenadores cuánticos** es su potencial teórico para resolver problemas de enorme complejidad en **periodos de tiempo imposibles de alcanzar por los supercomputadores convencionales** en base a una capacidad de paralelización muy superior. Al aprovechar principios de la física cuántica, las computadoras cuánticas podrían procesar problemas masivamente complicados a órdenes de magnitud más rápido que las máquinas modernas más potentes. Para una computadora

431 <https://www.res.es/>

432 <https://eurohpc-ju.europa.eu/>

Un punto fundamental en el que la UE ha centrado sus prioridades es en la soberanía tecnológica; sobre todo, aquello que concierne a la industria de los semiconductores. Reflejado en la “Chips Act”:

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_es

cuántica, los retos computacionales que podrían tardar miles de años en completarse en un computador convencional podrían reducirse a minutos.

En términos generales, el término “**superioridad cuántica**” se refiere a disponer de un **ordenador cuántico hipotético capaz de superar a todos los métodos clásicos de empleo de un superordenador para resolver algún problema**, incluso empleando métodos aproximados. Un ordenador cuántico capaz de lograr la ventaja o superioridad cuántica debería ofrecer un beneficio significativo y práctico más allá de todos los métodos de computación clásicos conocidos: **calcular soluciones de una manera que sea más barata, rápida o precisa que cualquier alternativa clásica disponible**.

La clave para ellos es disponer de **algoritmos cuánticos**. Estos algoritmos funcionan almacenando y manipulando información de una manera inaccesible para los ordenadores convencionales, lo que permite conseguir enormes aceleraciones en la resolución de ciertos problemas de física teórica hasta ahora intratables⁴³³.

Como ejemplo de estos problemas con muchas variables que interactúan de manera complicada se puede indicar el **modelado del comportamiento de los átomos individuales en una molécula**; problema muy complejo, debido a que todos los electrones interactúan entre sí. La identificación de **nueva física en un super-colisionador de partículas** (como los existentes en el CERN en Ginebra) también es un problema complejo que no se puede resolver con las computadoras clásicas a cualquier escala⁴³⁴.

En un ámbito de investigación más aplicada *Google* ha explorado⁴³⁵, en colaboración con la empresa química *BASF*, que los ordenadores cuánticos serán capaces de **simular con precisión el óxido de litio y níquel (LNO)**, un material utilizado en las **baterías**. El LNO es un material difícil de producir industrialmente y algunos aspectos de su química no se comprenden bien, pero ofrece una huella ambiental menor que el óxido de litio y cobalto de uso común, e incluso ya se han explorado alternativas al uso de cobalto en baterías. Simular el comportamiento mecánico cuántico del LNO podría mejorar el proceso de producción industrial y, en última instancia, poder **fabricar mejores baterías**.

Esta **necesidad de disponer de una mayor capacidad de computación también se manifiesta en el dominio de la IA** en los que los modelos de IA más complejos llevan al límite la capacidad del hardware convencional existente y exigen un enorme consumo de energía en

433 <https://www.ibm.com/think/topics/quantum-computing>

434 Los experimentos ATLAS y CMS del Gran Colisionador de Hadrones (LHC, por sus siglas en inglés) en el Laboratorio Europeo de Física de Partículas (CERN) de Ginebra (Suiza) han observado, por primera vez y de forma independiente en septiembre de 2024, el entrelazamiento cuántico entre dos quarks top, la partícula elemental más pesada que se conoce. Este fenómeno permite que dos partículas estén vinculadas sin importar la distancia a la que se encuentren. Fuente: The ATLAS Collaboration. Observation of quantum entanglement with top quarks at the ATLAS detector. *Nature* 633, 542–547 (2024). <https://doi.org/10.1038/s41586-024-07824-z>

435 <https://blog.google/technology/research/google-quantum-computer-real-world-applications/>

grandes centros de proceso de datos. Existe evidencia de que algunos algoritmos cuánticos podrían ser capaces de tratar conjuntos de datos de forma disruptiva, **acelerando algunos problemas actuales del aprendizaje automático.**

El elemento computacional básico en la tecnología cuántica es el bit cuántico, qbit o cúbit. Un **cúbit** puede comportarse como un *bit* y almacenar un *cero* o un *uno*, pero también puede ser una **combinación ponderada de cero y uno al mismo tiempo.** Cuando se combinan, los cúbits en superposición pueden escalar exponencialmente. Dos qubits pueden calcular con cuatro piezas de información, tres pueden calcular con ocho y cuatro pueden calcular con dieciséis. Sin embargo, **cada cúbit solo puede generar un único bit de información al final del cálculo.**

Actualmente, se están implementando **ordenadores cuánticos basados en diferentes tecnologías.** Las más avanzadas son los basados en **superconductores, trampas de iones, átomos fríos, fotónica** y los basados en **tecnologías del silicio.** Para cada uno de estos enfoques de diseño, los ordenadores cuánticos cuentan con características muy diferentes. Hoy en día no se puede declarar una tecnología concreta de implementación de cúbits como la “ganadora” entre las que se encuentran en desarrollo, prosiguiéndose una fase de maduración tecnológica y experimentación en la que se han involucrado los gobiernos de todas las grandes potencias tecnológicas, y muchas grandes empresas.

Algunas de las **medidas de calidad básicas** en las que difieren los diferentes enfoques y plataformas de experimentación construidas son: tiempos de coherencia, ratios de error de las puertas lógicas cuánticas, número de cúbits (bits cuánticos) o conectividad entre cúbits. Un área muy activa de investigación en la computación cuántica **es la de la mejora de estos parámetros** para poder resolver problemas reales. En la figura A3.2 se indica una tabla con los diferentes enfoques actuales en el desarrollo de computadores cuánticos y los países detrás de ellos (Comisión Europea, 2025g).

Technology platform	Superconducting	Ion traps	Cold atoms	Photonics	Spin qubits
 EU machines	 17	 6	 8	 5	 3
 UK machines	4	6	0	5	2
 USA machines	26	7	4	2	0
 Canada machines	13	0	0	1	0
 China machines	2	0	0	0	0
 ROW ²⁹ machines	1	0	0	1	3

Figura A3.2. Plataformas tecnológicas para la computación cuántica.
Fuente: Comisión Europea (2025g)

Obsérvese en la figura que la posición de la UE en el desarrollo de I+D en computación cuántica no es mala, aunque sí representa una fragmentación de esfuerzos; por una parte, provocada por la inmadurez de la tecnología, y por otra parte, por visiones nacionales.

Lo que si tienen en común todos los ordenadores cuánticos en desarrollo es que **no son máquinas universales**. Aunque su diseño implica la universalidad teórica (es decir, poder realizar un conjunto de operaciones que nos permita realizar cualquier operación unitaria), **el “ruido” que tienen sus cúbits que conlleva tiempos de coherencia⁴³⁶ limitados impiden utilizar esta universalidad**. Cuánto más tiempo se mantenga la coherencia, más tiempo útil existe para ejecutar los algoritmos cuánticos.

Esta limitación tiene solución teórica mediante la denominada **corrección cuántica de errores (EQC)**, pero todavía no se dispone de ordenadores cuánticos de suficiente calidad para que esto sea posible y escalable, aunque sí empiezan a desarrollarse algunos prototipos. La no universalidad de los ordenadores cuánticos actuales limita las aplicaciones de estos dispositivos; algoritmos cuánticos reconocidos como el de factorización, el de estimación de fase o el de búsqueda requieren de esta propiedad.

Para poder **comparar entre ordenadores cuánticos y entre ellos y los supercomputadores convencionales** se suele emplear la métrica denominada **rQOPS** (*Reliable Quantum Operations Per Second*) que cuenta las *operaciones que siguen siendo fiables durante la duración de un algoritmo cuántico práctico para que haya una garantía de que se ejecutará correctamente*⁴³⁷. Para resolver problemas científicos reales, el ordenador cuántico deberá conseguir prestaciones de, al menos, **un millón de rQOPS**, con una tasa de error, como máximo, de **10⁻¹²** (una por cada billón de operaciones)⁴³⁸.

La competición por disponer de ordenadores cuánticos relevantes que cumplan estas condiciones de tolerancia a fallos se acelera. Tres ejemplos de grandes empresas lo atestiguan: *Google*, *Microsoft* e *IBM*. Se trata de **pasos importantes hacia la construcción de una computadora cuántica a gran escala y con corrección de errores antes de lo que se esperaba hace un par de años**. Se está más cerca de que ese objetivo sea una realidad.

436 La decoherencia se produce cuando desaparecen las condiciones necesarias para que un sistema que se encuentra en un estado cuántico entrelazado se mantenga. Deja de comportarse según la mecánica cuántica cuando se dan unas condiciones determinadas, pasando a comportarse a partir de ese instante como dictan las leyes de la física clásica.

437 Como los cúbits son propensos a errores, utilizar cúbits individuales directamente en un cálculo no da resultados correctos. Para evitarlo, se necesita crear qubits lógicos como unidades tan controlables como lo son los bits de la computación clásica, agrupando varios cúbits físicos. Al crear un grupo, es posible representar información correcta en su conjunto, aunque algunos cometan errores. Google en diciembre de 2024 ha anunciado el diseño de un cúbit lógico a partir de 105 cúbits físicos con una tasa de errores muy baja. https://www.digitalskillsinstitute.com/articles/detail/google-anuncia-un-hito-hacia-la-computacion-cuantica-sin-errores_20241219/

438 Un rQOPS se define por el número Q de cúbits lógicos en el sistema cuántico multiplicado por la velocidad del reloj lógico del hardware f : $rQOPS = Q \cdot f$
<https://azure.microsoft.com/en-us/blog/quantum/2023/06/21/microsoft-achieves-first-milestone-towards-a-quantum-supercomputer/>

En diciembre de 2024 *Google Quantum AI* anunció el procesador “**Willow**”, chip de computación cuántica superconductor de 105 cúbits con mejoras significativas en la corrección de errores cuánticos, logrando una **reducción de errores exponencial a medida que escala el número de cúbits**⁴³⁹.

En febrero de 2025, *Microsoft* anunció el descubrimiento de un **nuevo estado de la materia** que, según dice, respaldará un avance en la computación cuántica con la presentación del **chip cuántico Majorana 1**⁴⁴⁰ (véase figura A3.3). Se trata de la primera **unidad de procesamiento cuántico (QPU)** desarrollada y accesible.

El chip podría usarse para acelerar el descubrimiento de fármacos, el desarrollo de baterías y la carrera hacia el dominio de la IA con una **corrección de errores mucho más eficiente y menos compleja** que con los enfoques actuales. No está claro cuando se dispondrá de un ordenador cuántico libre de errores y plenamente operativo; los optimistas, entre ellos algunas startups, pronostican que sucederá a finales de esta década, pero, probablemente, no se introducirán en el mercado hasta **mediados de la próxima década**⁴⁴¹.

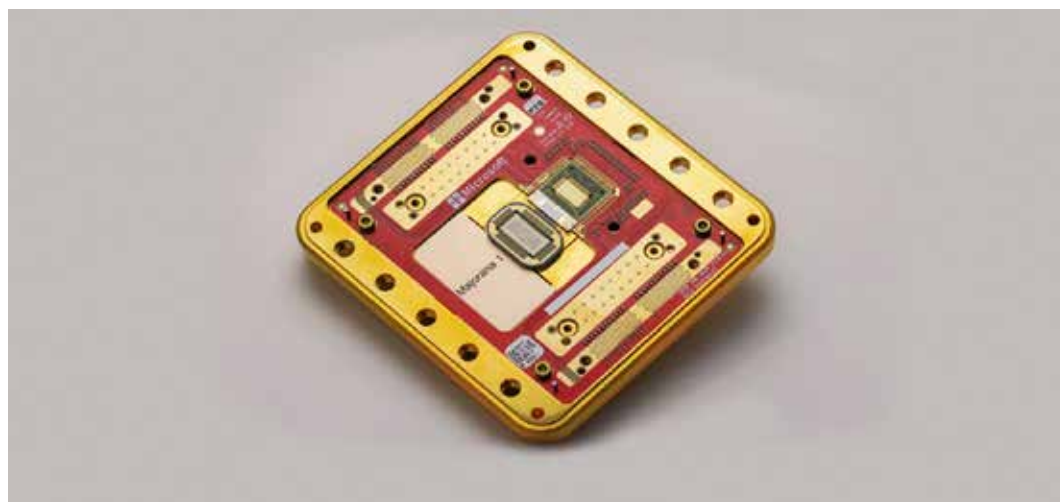


Figura A3.3. Chip Majorana 1 de Microsoft.

Fuente: <https://news.microsoft.com/source/latam/noticias-de-microsoft/microsoft-presenta-majorana-1-el-primer-procesador-cuantico-del-mundo-impulsado-por-qubits-topologicos/>

IBM ha desvelado en junio de 2025 su **hoja de ruta de computación cuántica** con planes detallados para construir una **computadora cuántica libre de errores** (12 cúbits físicos por

439 <https://blog.google/intl/es-es/productos/tecnologia/presentamos-willow-nuestro-chip-cuantico-de-ultima-generacion/>

440 Este chip (a modo de microprocesador) aprovecha las propiedades de un material llamado “cúbit topológico”, que produce partículas que no son ni líquidas, ni sólidas, ni gaseosas. Majorana 1 está diseñado para escalar hasta un millón de cúbits en un solo chip. <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-quantum-computing>

441 Según McKinsey el 72% de los ejecutivos tecnológicos, inversores y académicos en computación cuántica cree que veremos una computadora cuántica totalmente tolerante a fallos para 2035. El 28% restante piensa que no se alcanzará hasta 2040 o más tarde.

cúbit lógico) y con una capacidad computacional significativamente mayor que las máquinas existentes para 2028. Espera que la computadora esté disponible para los usuarios a través de la nube para 2029. La máquina propuesta, llamada **Starling**, consistirá en una red de módulos, cada uno de los cuales contiene un conjunto de chips⁴⁴². Eso no quiere decir que se podrá adquirir como cualquier otro ordenador.

Otro elemento clave para comprender el interés gubernamental asociado es que la tecnología cuántica es **dual** puesto que los problemas a resolver pueden ser de interés tanto para mercados civiles como militares; no es extraño por ello que las agencias de financiación militares les hayan prestado atención. Los recientes avances en tecnologías cuánticas prometen grandes beneficios para la defensa y la seguridad, incluidas las **comunicaciones ultraseguras**, la **mejora de la detección en el campo de batalla** y la **optimización de la logística**, entre otras muchas que se han empezado a explorar.

El programa **US2QC**⁴⁴³ (*Underexplored Systems for Utility-Scale Quantum Computing*) de la agencia DARPA de *Estados Unidos* y su **Iniciativa de Benchmarking Cuántico**⁴⁴⁴ supone la búsqueda de un **enfoque riguroso para evaluar sistemas cuánticos** que podrían resolver problemas que están más allá de las capacidades de las computadoras clásicas (ideas para construir un ordenador cuántico relevante industrialmente en 2033). *DARPA* y *Microsoft* han firmado un acuerdo para comenzar la fase final del programa en la que Microsoft tiene la intención de construir un **prototipo tolerante a fallos basado en cúbits topológicos** en pocos años, un paso hacia la computación cuántica a gran escala con **ordenadores de más de un millón de cúbits**.

Mientras que todo eso ocurra, la pregunta pertinente es conocer **qué podemos hacer con los ordenadores cuánticos limitados de los que se dispone actualmente**. En primer lugar, la **experimentación**: con ellos se puede permitir entender mejor la física de su funcionamiento, y buscar aplicaciones que no requieran una “computación perfecta”; es decir, que puedan ser útiles, aunque todavía haya errores. Actualmente, ya se dispone de dispositivos capaces de **superponer y entrelazar varios estados cuánticos de forma controlada y programable** como un excelente **campo de pruebas para explorar la física cuántica** que hasta hace pocos años era inimaginable. El desarrollo de ordenadores cuánticos sin errores está avanzando muy deprisa.

Hay que recalcar que **los ordenadores cuánticos no son puramente cuánticos**: solo su hardware tiene propiedades cuánticas, pero **su software de control es clásico** y se realiza desde un ordenador convencional. De este contexto surge la idea de **hibridar la computación cuántica con la convencional** y explotar la parte clásica para ayudar o asistir a la

442 <https://www.technologyreview.com/2025/06/10/1118297/ibm-large-scale-error-corrected-quantum-computer-by-2028/>

443 <https://www.darpa.mil/research/programs/underexplored-systems-for-utility-scale-quantum-computing>

444 <https://www.darpa.mil/research/programs/quantum-benchmarking-initiative>

cuántica. De esta hibridación surgen, por ejemplo, los algoritmos cuánticos variacionales (VQA) que se utilizan para explorar aplicaciones en simulación cuántica, **aprendizaje cuántico automático** (“*quantum machine learning*”) y problemas de optimización entre otros.

Desde un punto de vista práctico, el **objetivo de experimentación con los ordenadores cuánticos** disponibles actualmente puede abordarse con **diversos enfoques**:

- **Colaborar con un grupo de investigación** que desarrolle estos dispositivos. Este caso, generalmente mediante proyectos financiados por las administraciones públicas, es excepcional y no es una solución escalable para la industria, aunque es crucial para el desarrollo de enfoques y soluciones científicas en TRLs bajos.
- **Acceder a varios ordenadores cuánticos disponibles en la nube** mediante un sistema de suscripción que puede requerir de grandes inversiones. Grandes empresas como *Amazon*, *IBM* o *Microsoft* ofrecen estas alternativas que permiten explorar el uso para un determinado tipo de aplicaciones críticas para la entidad, y facilitar la formación de especialistas⁴⁴⁵.
- **Adquirir un ordenador cuántico** de un proveedor que lo posea. Este enfoque es muy costoso y requiere disponer de un equipo humano altamente especializado. La justificación de la inversión debe estar ligada a la exploración de casos de uso que se consideren cruciales para la entidad. Debe tenerse en cuenta que se trata de una tecnología inmadura por lo que, muy probablemente, el equipo adquirido será obsoleto en un corto periodo de tiempo, pero la experiencia y conocimiento del equipo humano implicado será muy valiosa.

Existen muchas **iniciativas en todo el mundo y también en la UE** para el desarrollo y despliegue de ordenadores cuánticos. Todas las grandes potencias tecnológicas están involucradas porque son conscientes de que la competición tecnológica iniciada en torno a la computación cuántica puede tener vencedores que podrán dominar el mercado en la próxima década e influir en muchos sectores socioeconómicos, entre ellos el de defensa.

Referido a la situación española, en enero de 2022 arrancó la iniciativa **Quantum Spain**⁴⁴⁶ con cinco objetivos:

- Adquirir e instalar un **ordenador cuántico** en el *Barcelona Supercomputing Center* basado en tecnología de cúbits superconductores.

445 Los modelos de computación cuántica basados en la nube (a menudo llamados Computación Cuántica como Servicio – QCaaS) están disponibles comercialmente hoy en día. Algunas plataformas, como Microsoft Azure Quantum o Amazon Braket, ofrecen acceso a computadoras cuánticas de varios fabricantes dentro de un ecosistema.

446 <https://quantumspain-project.es/investigacion/>

- Adquirir e instalar **simuladores cuánticos HPC** para ser utilizados en proyectos sobre tecnologías cuánticas. Estos simuladores se encontrarán en el BSC-CNS, CESGA y SCAYLE.
- **Proveer acceso** al ordenador cuántico y a los simuladores HPC a través de los canales de la Red Española de Supercomputación.
- Apoyar a las universidades y centros de investigación en el estudio y **desarrollo de algoritmos** cuánticos y sus aplicaciones en la IA.
- Crear programas de **formación**, workshops, escuelas, seminarios y otras iniciativas a través del programa *TalentQ*.

En 2025 ya están en marcha **tres iniciativas españolas para disponer de ordenadores cuánticos**: en Cataluña, en el País Vasco y en Galicia. Además, diversas entidades públicas y privadas han llegado a acuerdos para acceder a plataformas de computación cuántica en la nube proporcionadas por grandes empresas multinacionales.

En febrero de 2025 se presentó en el *BSC* el ordenador cuántico digital con tecnología 100% europea que forma parte de **Quantum Spain**. A la integración en el supercomputador *MareNostrum 5* se unirá el ordenador cuántico adjudicado al *BSC* por *EuroHPC JU* de la Comisión Europea.

El ordenador cuántico de **EuroHPC MareNostrum Ona** será un **ordenador cuántico analógico** en forma de ‘*annealer*’ (recocido) cuántico⁴⁴⁷ que se empezará a instalar en 2025⁴⁴⁸. El sistema de primera generación ofrecerá al menos **10 cúbits físicos**, con capacidades que aumentarán tanto en tiempos de coherencia como en número de qubits para la tercera generación. Ambos sistemas ofrecen tecnologías complementarias y conforman la infraestructura cuántica del BSC, reforzando su papel como actor clave en el panorama europeo de la computación avanzada.

Por otro lado, **IBM instalará en Euskadi el IBM Quantum System Two**, el ordenador cuántico en red de IBM más potente del mundo. Su instalación y puesta en funcionamiento se producirá durante el último trimestre de 2025 en el *IBM-Euskadi Quantum Computational Center*, ubicado en el nuevo edificio *Ikerbasque* de Donostia⁴⁴⁹.

447 El recocido cuántico (quantum annealing) es un método de optimización que utiliza los principios de la física cuántica para encontrar el mínimo global de una función objetivo,

448 <https://www.bsc.es/es/noticias/noticias-del-bsc/firma-del-contrato-de-adquisici%C3%B3n-del-ordenador-cu%C3%A1ntico-de-eurohpc-ubicado-en-el-bsc>

449 <https://www.basquequantum.eus/es/ibm#:~:text=IBM%20instalar%C3%A1%20en%20Euskadi%20el,nuevo%20edificio%20Ikerbasque%20de%20Donostia>

Finalmente, el **Centro de Supercomputación de Galicia (CESGA)** alberga un ordenador cuántico denominado **QMIO** con tecnología de *Fujitsu*. Desde mayo de 2024 su uso está abierto a la comunidad científica (un 20% del tiempo se distribuye a través de la Red Española de Supercomputación (RES))⁴⁵⁰.

Mientras no se disponga de un ordenador cuántico universal, se trabaja en **modelos computacionales alternativos**: la **simulación** y la **emulación** cuánticas y la **computación inspirada** en la cuántica.

- La **simulación cuántica**, también conocida como computación cuántica analógica, soluciona problemas de alta complejidad al modelar su comportamiento con un sistema cuántico específico.
- La **emulación cuántica** se centra en aproximar el comportamiento de ordenadores y simuladores cuánticos, mediante algoritmos especializados que pueden ejecutarse en superordenadores clásicos.
- La **computación inspirada en la cuántica** plantea nuevas soluciones clásicas descubiertas a partir de herramientas de emulación y de entender cómo funcionan los algoritmos de los ordenadores cuánticos.

Al mismo tiempo, han comenzado a financiarse proyectos como **CUCO (Computación cuántica en industrias estratégicas)**⁴⁵¹ pensando en sus futuras aplicaciones industriales. Liderado por GMV, el proyecto CUCO persigue avanzar el estado del arte de algoritmos cuánticos y aplicar ese conocimiento a una serie de pruebas de concepto en distintos **sectores estratégicos** de la economía española como son los de la Energía, Financiero, Espacio, Defensa y Logística. Dos de los casos de estudio del proyecto **CUCO** tienen relación con la **aplicación de Quantum Machine Learning (QML) a la defensa**:

- QML y su aplicación en problemas de observación de la Tierra.
- QML y su aplicación a problemas de inteligencia de señales.

Más recientemente, tras la participación en el proyecto europeo “*EuroQCS*” y su correlato a nivel nacional “*Quantum Spain*”⁴⁵² se ha lanzado por el gobierno español en abril de

450 <https://www.xunta.gal/es/notas-de-prensa/-/nova/001723/apertura-del-qmio-comunidad-cientifica-atraera-talento-inversiones-galicia-promovera>

451 <https://www.cuco.tech/>

452 <https://quantumspain-project.es/>

2025 la **Estrategia Cuántica de España 2025-2030**⁴⁵³. Supone un respaldo gubernamental al posicionamiento español en tecnologías cuánticas.

Puede decirse como resumen, que la situación de la computación cuántica está pasando de una fase experimental muy ligada a la física cuántica a otra de **ingeniería de la computación cuántica** que en un plazo de unos diez años permitiría disponer de ordenadores cuánticos fiables con suficientes *rQOPS* como para resolver problemas significativos imposibles de resolver actualmente.

Su adopción va a suponer un cambio disruptivo en las tecnologías de la información y las comunicaciones como supuso el microprocesador hace medio siglo. Su uso estará, como se verá posteriormente a la IA y las redes de comunicación. Supondrá también la base para recrudecer la **batalla por la supremacía tecnológica entre grandes potencias**.

A3.2.2. Comunicaciones Cuánticas

La **comunicación cuántica** tiene como objetivo **transmitir información de forma segura a grandes distancias**. Para ello, recurre al *entrelazamiento* y a la “*teleportación cuántica*” para extender las distancias entre la comunicación entre el transmisor y el receptor. La comunicación cuántica a largas distancias requiere **repetidores cuánticos** debido a la pérdida de fotones y al problema de decoherencia ya mencionado.

Un **repetidor cuántico** es un nodo intermedio que funciona de manera similar al amplificador de las redes ópticas clásicas, pero debe obedecer el **teorema de no clonación**. De hecho, el repetidor cuántico permite entrelazar cúbits de nodos finales. Cuando dos nodos finales están entrelazados, se puede aprovechar el efecto de la teletransportación cuántica. Esto significa que la información cuántica se puede teletransportar sin necesidad de enviar un fotón físicamente; sólo se requiere una comunicación clásica.

Para garantizar la seguridad, además, se utilizarán conceptos como el entrelazamiento⁴⁵⁴ y el principio de no clonación para implementar la **distribución cuántica de claves (QKD)** entre distintos puntos, de manera que sea **resistente a ataques cuánticos y clásicos**. La distribución de claves cuánticas (**QKD**) es la **aplicación más madura de la comunicación cuántica**.

El objetivo es **distribuir una clave secreta entre dos o más partes para datos cifrados distribuidos a través de canales clásicos**. Debido al teorema de no clonación, cualquier espía debe realizar una medición que sea detectable por las partes en comunicación. En la figura

453 Estrategia de Tecnologías Cuánticas de España 2025-2030. Ministerio para la Transformación Digital y de la Función Pública. https://digital.gob.es/dam/es/portalmtdfp/comunicacion/sala-de-prensa/comunicacion_ministro/2025/04/2025-04-24/EstrategiaTecnologiasCuanticas_compressed.pdf

454 Fenómeno cuántico por el que dos partículas comparten la misma función de onda por lo que cualquier operación que se haga sobre una de ellas afectará inmediatamente a la otra.

A3.4 se puede ver esquemáticamente la implementación del **concepto de distribución cuántica de claves** (Giles, 2019). Obsérvese la existencia de un canal clásico y otro cuántico.

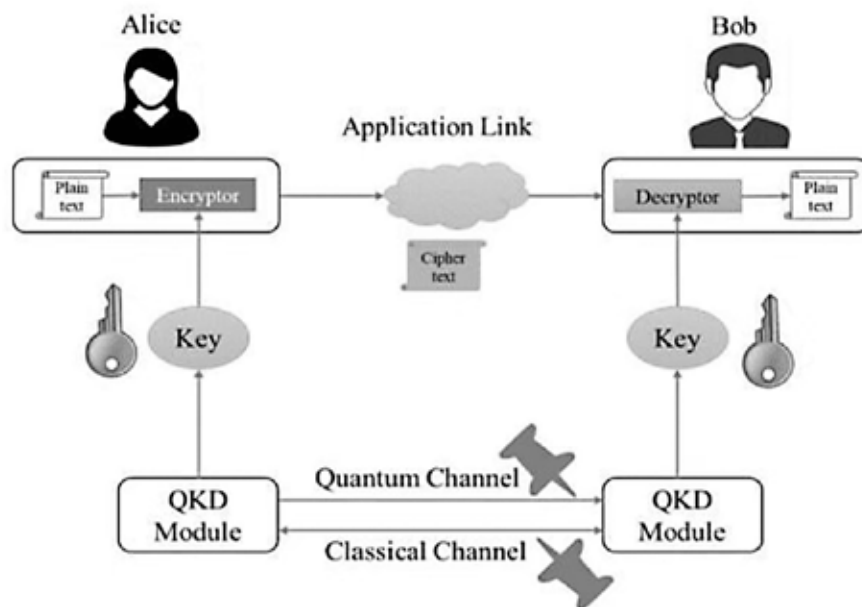


Figura A3.4: Distribución cuántica de claves. Fuente: Quantum Key Distribution Source: Martin Giles, "What is Quantum Communication?", MIT Technology Review, 14 Feb 2019. URL: <https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/>

El siguiente paso, actualmente probado en experimentos, es el **QKD independiente del dispositivo de medición (MDI-QKD)**. Es un protocolo cuántico que no sólo reemplaza los repetidores confiables (aún no son cuánticos, ni admiten entrelazamiento) por repetidores seguros, sino que también sirve como "conmutador". Eso significa que se puede empezar a construir la topología y la infraestructura habituales de una red en estrella. En la red MDI-QKD, **los ataques al nodo central físicamente no pueden revelar la clave ni revelar información confidencial**. Posteriormente, los nodos centrales serán reemplazados por el interruptor y el repetidor cuánticos, y se logrará disponer de una red de información cuántica completamente funcional.

Utilizando **fibras ópticas obscuras convencionales** se han empezado a desplegar redes cuánticas experimentales en varios países europeos para aplicaciones duales basados en la distribución cuántica de claves. Ejemplos de avances en **comunicaciones cuánticas de uso dual** incluyen un experimento de 2024 que demostró con éxito el uso de distribución cuántica de claves (QKD) utilizando un sistema basado en **vehículos aéreos no tripulados (UAV)** (Tian et al., 2024).

En el caso español es interesante mencionar dos **iniciativas públicas relacionadas**⁴⁵⁵:

⁴⁵⁵ <https://media.realinstitutoelcano.org/wp-content/uploads/2025/04/policy-paper-tecnologias-cuanticas-como-apostar-y-acertar-desde-espana-y-la-ue.pdf>

- **Plan Complementario de Comunicación Cuántica:** mediante acuerdo del Ministerio de Ciencia con seis Comunidades Autónomas y el CSIC: 73,5 millones de euros (2022-2024) este Plan involucra una red de actores principales, incluyendo el CSIC y las Comunidades Autónomas del País Vasco, Cataluña, Galicia, Madrid y Castilla y León. El programa busca fortalecer la ciberseguridad y el desarrollo de tecnologías cuánticas en España mediante las alianzas con las Comunidades Autónomas. Entre los objetivos se destacan el avance de la infraestructura de comunicaciones cuánticas y la creación de una red nacional que respalde la iniciativa paneuropea EuroQCI, para comunicaciones seguras a nivel continental.
- **PERTE Aeroespacial:** 125 millones de euros (2024-2026). Gestionado por el CDTI, incluye dos proyectos clave dentro de su componente de Compra Pública de Innovación enfocados en la Distribución Cuántica de Claves en el ámbito aeroespacial: QKD GEO y QKD LEO, utilizando satélites en órbitas geoestacionaria (GEO) y de baja órbita terrestre (LEO), respectivamente.

También en España, y en el contexto de su uso experimental en defensa, merece la pena destacar la existencia del **Centro de prueba de Comunicaciones cuánticas del programa DIANA de la OTAN** situado en la UPM (Campus de Montegancedo) con una red experimental desplegada en la Comunidad de Madrid⁴⁵⁶.

En abril de 2025 se ha concluido el **despliegue de los sistemas de Quantum Key Distribution (QKD) de MadQCI**. Gracias a una colaboración estratégica con algunos de los principales proveedores europeos y globales de tecnología cuántica, la infraestructura de Madrid está equipada con soluciones que ya están siendo probadas en condiciones reales⁴⁵⁷. **MadQCI** está alineada con los programas europeos, especialmente **EuroQCI** (*European Quantum Communications Infrastructure*), que tiene como objetivo la construcción de una red cuántica paneuropea apoyada por la Comisión Europea en colaboración con los Estados miembros y la Agencia Europea del Espacio⁴⁵⁸.

EuroQCI estará compuesta por un segmento terrestre basado en redes de comunicaciones de fibra que conectan lugares estratégicos a nivel nacional y transfronterizo, y un segmento espacial basado en satélites cuánticos. Será una parte integral de IRIS², el sistema de comunicación segura de la UE basado en el espacio en desarrollo.

456 <https://www.diana.nato.int/resources/site1/general/test%20centres/diana-affiliated-network-test-centres-20250603.pdf>

457 Entre los proveedores participantes se encuentran HEQA, ID Quantique, Luxquanta, KEEQuant, Quantum Industries, QTI y Toshiba. Además, en los próximos meses se incorporarán nuevos sistemas desarrollados por Q*Bird y ThinkQuantum. <https://madqci.es/2025/04/14/en-el-dia-mundial-de-la-cuantica-la-red-cuantica-de-madrid-avanza-con-paso-firme/>

458 EuroQCI comienza con la implementación de redes cuánticas nacionales que se integrarán posteriormente en la EuroQCI <https://euroqci-spain.eu/>

MadQCI forma parte del proyecto europeo *DISCRETION*⁴⁵⁹, que explora **cómo aplicar la infraestructura de comunicaciones cuánticas (QCI) en entornos de defensa y misión crítica**. Uno de los hitos más relevantes en mayo de 2025 fue la demostración en vivo de una **conexión cuántica segura entre España, Portugal e Italia**, evidenciando cómo QKD puede ofrecer comunicaciones ultra protegidas, interoperables y adaptadas a escenarios multinacionales reales: reforzar la ciberseguridad post-cuántica, garantizar la resiliencia de infraestructuras sensibles y favorecer el despliegue de tecnologías de doble uso (civil y militar), desarrolladas bajo estándares europeos de soberanía e innovación.

El escenario de red cuántica más comúnmente considerado y realizado implica el uso de **satélites cuánticos**. La ventaja de los satélites es la **posibilidad de utilizar la comunicación óptico-fotónica para la transmisión de información cuántica**, donde las pérdidas en el enlace satélite-tierra son menores que las pérdidas entre dos nodos terrestres muy separados. Sin embargo, **la comunicación de fotones ópticos en el canal de espacio libre a distancias cortas se puede realizar utilizando, por ejemplo, drones**.

La mejor manera sería **utilizar el espectro de microondas empleado por la comunicación inalámbrica clásica**. Sin embargo, la comunicación que utiliza el espectro de microondas a nivel de fotones individuales es aún más compleja. La **tecnología de fotón único de microondas** implica una mayor dificultad para generar y detectar fotones individuales por el ambiente ruidoso en las bandas de microondas.

A3.2.3. Sensores y Metrología Cuánticas

Los **sensores cuánticos** son capaces de **medir propiedades físicas con una precisión notablemente superior a la de los sensores tradicionales**. Por ejemplo, pueden detectar diferencias mínimas de temperatura o cambios en el campo electromagnético o de presión con una exactitud muy superior a la disponible hoy día por otros sensores.

El desarrollo de tecnologías de **detección cuántica** permitiría mejorar exponencialmente las capacidades de **conciencia situacional**. Concretamente, los sensores cuánticos ayudarán a superar las complejidades y vulnerabilidades de los sistemas actuales y proporcionarán una mayor precisión, una mayor sensibilidad y rangos mejorados.

También en este caso, **la tecnología de sensores cuánticos empieza a converger con la microelectrónica**. En la figura A3.5 se muestra un **sensor cuántico integrado** desarrollado en tecnologías C-MOS.

⁴⁵⁹ <https://discretion-eu.com/>

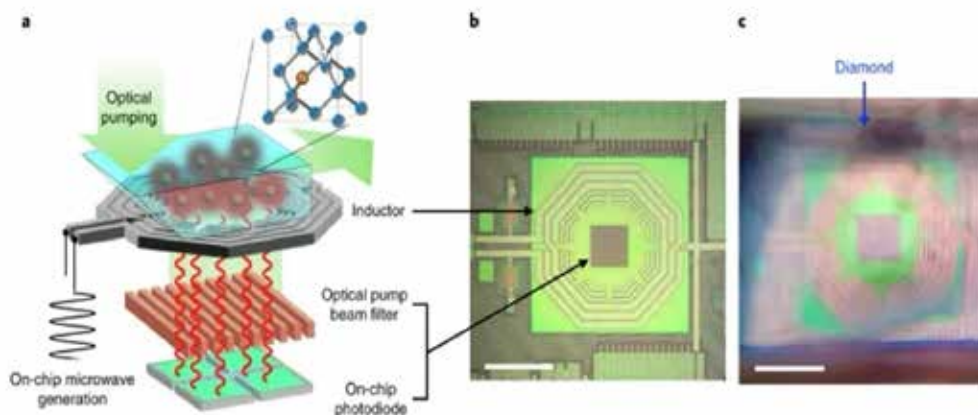


Figura A3.5. Sensor cuántico integrado en CMOS basado en centros de vacantes de nitrógeno.

Fuente: <https://quantumpedia.uk/will-quantum-technology-transform-the-nature-of-warfare-e1d835e5d182>

Una de las aplicaciones más relevantes de la sensórica cuántica es la posibilidad de **detectar objetos muy pequeños** que no es posible detectar con sensores convencionales. El caso de interés dual al que se ha dedicado más atención en los últimos años es el denominado “**radar cuántico**”.

Radar Cuántico

El tradicional sistema de radar utiliza ondas electromagnéticas clásicas para detectar los objetivos. **El radar cuántico generaliza el concepto de radar**, siendo la novedad que utiliza un número relativamente pequeño de fotones. En este contexto se permite usar los **fenómenos cuánticos para incrementar la sensibilidad del sistema de detección**. Por otra parte, es fundamental el poder detectar objetivos en zonas con turbulencias y nubes.

El radar cuántico es una tecnología que utiliza fotones (partículas) entrelazados, en vez de ondas electromagnéticas, como método de detección de objetos. Recuérdese que el principio de “entrelazamiento cuántico” dice que dos partículas se pueden unir entre sí y que cualquier variación que tenga una partícula se manifiesta en la otra, sin importar la distancia. Cada par de entrelazado cuántico conduce a un proceso llamado **iluminación cuántica**⁴⁶⁰, donde la información sobre el entorno de una partícula se puede inferir al estudiar la otra partícula.

En un **sistema de radar cuántico**, ya enunciado en 2012 por Lanzagorta⁴⁶¹, el primer fotón se mantiene en el dispositivo mientras que su fotón “gemelo” se envía como frecuencia de microondas a los posibles objetivos. Cuando el segundo fotón encuentra un obstáculo, el

⁴⁶⁰ Enhanced Sensitivity of Photodetection via Quantum Illumination <https://www.science.org/doi/10.1126/science.1160627>

⁴⁶¹ Marco Lanzagorta (2012). Quantum Radar”. Morgan & Clypool Publishers. Synthesis Lectures on Quantum Computing.

fotón estático cambia inmediatamente su estado. Esto implica que **cuando algo le sucede al fotón que está viajando, se puede observar sus variaciones en el fotón retenido.**

Como en los radares convencionales, al localizar un blanco algunos fotones vuelven al radar, y **los ordenadores del sistema al comparar los fotones “gemelos” pueden calcular las propiedades físicas del objeto reflejado**, tales como su tamaño, forma, velocidad, ángulo de ataque y otras características del objeto.

Además, gracias a estas nuevas particularidades de los “*fotones entrelazados*” **los radares cuánticos son resistentes a las interferencias.** La inviolabilidad del “entrelazado” sucede porque al intentar manipular o modificar el fotón que está viajando se “pierden las características cuánticas de los fotones” y esto se manifiesta en el fotón retenido. Esta particularidad sería detectada por el radar cuántico empleando algoritmos específicos⁴⁶², lo que implica una gran ventaja en la *Guerra Electrónica*.

Existen abundantes posibilidades de utilizar **técnicas de detección cuántica en el ámbito de la defensa.** El potencial es diverso e ilimitado, aunque en la actualidad hay retos que es necesario superar.

- Los **sensores cuánticos** tienen el potencial de detección, identificación y seguimiento de objetivos como submarinos furtivos, proporcionando alerta temprana de lanzamientos de misiles balísticos, proporcionando una navegación ultra precisa, etc.
- Los **giroscopios y acelerómetros cuánticos** realizan mediciones de alta **precisión**, lo que proporciona una guía precisa en entornos sin GPS.
- En la tecnología PNT (Posicionamiento, Navegación y Temporización), el uso de sistemas basados en átomos fríos proporciona la capacidad de **navegar con precisión en un entorno sin GPS.**

La **metrología cuántica**, por su parte, utiliza la mecánica cuántica para mejorar la trazabilidad de las mediciones dentro del *Sistema Internacional de Unidades* y que sean comparables, reproducibles y robustas.

A3.3. Utilización de las tecnologías cuánticas en el ámbito de la defensa

Concepto de “guerra cuántica”

El empleo de las tecnologías cuánticas para aplicaciones militares permite **introducir nuevas capacidades, mejorar la eficacia y aumentar la precisión.** Su realización efectiva conduciría

⁴⁶² Hay varios protocolos considerados para el radar cuántico, como: Radar cuántico interferométrico, Iluminación cuántica (QI), Radar cuántico híbrido y Radar cuántico Maccone-Ren.

en el futuro a plantear un **escenario de “guerra cuántica”**, en la que se deben establecer nuevas estrategias, doctrinas, políticas y éticas militares diferentes de las habituales.

Por este motivo, se están incrementando los programas de financiación de **proyectos militares de I+D con tecnologías cuánticas por todas las potencias tecnológicas**. Son Estados Unidos y China quienes están dedicando mayor esfuerzo (Corral, 2025).

La rivalidad entre China y Estados Unidos en tecnologías cuánticas está creciendo⁴⁶³. Ambos países son conscientes de que la superioridad militar puede depender en la próxima década de cómo se lidere esta tecnología y su convergencia con la de semiconductores y la de IA.

Un informe de septiembre de 2024 del grupo de expertos estadounidense *Information Technology and Innovation Foundation (ITIF)* sobre la capacidad de innovación cuántica de China destacó que, a diferencia de Estados Unidos, que se centra en la creación de conocimiento, **China pone más énfasis en la implementación de tecnología**, con el objetivo de transformar rápidamente las innovaciones en productos tangibles.

En el caso de China, el Gobierno cuenta con el *Laboratorio Nacional de Ciencias de la Información Cuántica*, dotado con 10.000 millones de dólares, como centro de desarrollo de la tecnología cuántica y coordinador entre la Academia China de Ciencias, institutos gubernamentales de investigación, universidades y empresas. China cuenta con la mayor red de comunicaciones cuánticas del mundo, de 12.000 kilómetros de longitud, que une las principales ciudades con redes seguras. Además, China cuenta desde diciembre de 2024 con un **computador cuántico Tianyan-504**, dotado con un chip *Xiaohong* de 504 cúbits⁴⁶⁴.

La UE lleva a cabo un esfuerzo cuántico centrado en el ámbito militar como parte del *Fondo Europeo de Defensa (FED)* que se ha incluido como un **área prioritaria** en la convocatoria de 2024. Debe tenerse en cuenta, en todo caso, que existen múltiples proyectos clasificados de desarrollo y uso de tecnologías cuánticas en diversos países.

La **guerra cuántica** (*Quantum Warfare, QW*) se refiere a un tipo de guerra que utiliza tecnologías cuánticas para aplicaciones militares que afectan las capacidades de inteligencia, seguridad y defensa de todos los dominios bélicos, y marca el comienzo de nuevas estrategias militares, doctrinas, escenarios y cuestiones de paz y ética (Sivrastava, 2025). En ella, la computación, las comunicaciones y la sensórica cuántica se combinan con otras tecnologías militares convencionales e integran en productos militares.

Existen aplicaciones militares particulares de la tecnología cuántica para diversos **dominios militares** (terrestre, aéreo, espacial, electrónica, cibernética, submarino) así como en

463 <https://www.thinkchina.sg/technology/big-read-china-us-rivalry-enters-field-quantum-technology>

464 <https://thequantuminsider.com/2024/12/06/china-introduces-504-qubit-superconducting-chip/>

aplicaciones de **ISTAR** (inteligencia, vigilancia, adquisición de objetivos y reconocimiento). En la figura A3.6 (Krelina, 2021) se representa esquemáticamente un escenario futuro de guerra cuántica.



Figura A3.6. Fuente: https://www.researchgate.net/figure/Sketch-of-quantum-warfare-utilizing-various-quantum-technology-systems_fig1_350341569 (Krelina, 2021)

Los **usos militares más relevantes de las tecnologías cuánticas** podrían centrarse en el entrenamiento y ejecución de modelos sofisticados de IA que puedan predecir las acciones del adversario, procesar datos instantáneos en la zona de guerra, y un sistema de intercambio de información muy seguro.

La **capacidad de simular y modelar entornos complejos en el campo de batalla** es otra área crítica en la que la computación cuántica está preparada para tener un gran impacto. Los métodos de simulación tradicionales con frecuencia tienen limitaciones para poder capturar la imprevisibilidad inherente del conflicto que emplea tácticas descentralizadas y fluidas. El empleo de **juegos de guerra mejorados cuánticamente** podría revolucionar este proceso al permitir a los estrategas militares **ejecutar numerosos escenarios potenciales en paralelo**, explorando no solo estrategias conocidas, sino también resultados nuevos e imprevistos. Estas simulaciones ofrecerían información sin precedentes sobre los comportamientos de los adversarios, los riesgos operativos y las oportunidades tácticas, lo que conduciría a una planificación estratégica más eficaz (Hanna, 2025).

Algunas empresas consultoras han empezado a analizar la **evolución del mercado de guerra cuántica** en 2023 y estimar previsiones de crecimiento hasta 2031. En la figura A3.7 se ve una de estas estimaciones tanto en el subsector de computación (incluyendo simulaciones) como en el de comunicaciones cuánticas realizada por la empresa Insight Ace Analytic que estima una CAGR hasta 2031 del 16,8%. En la figura se indican algunas de las empresas relevantes.

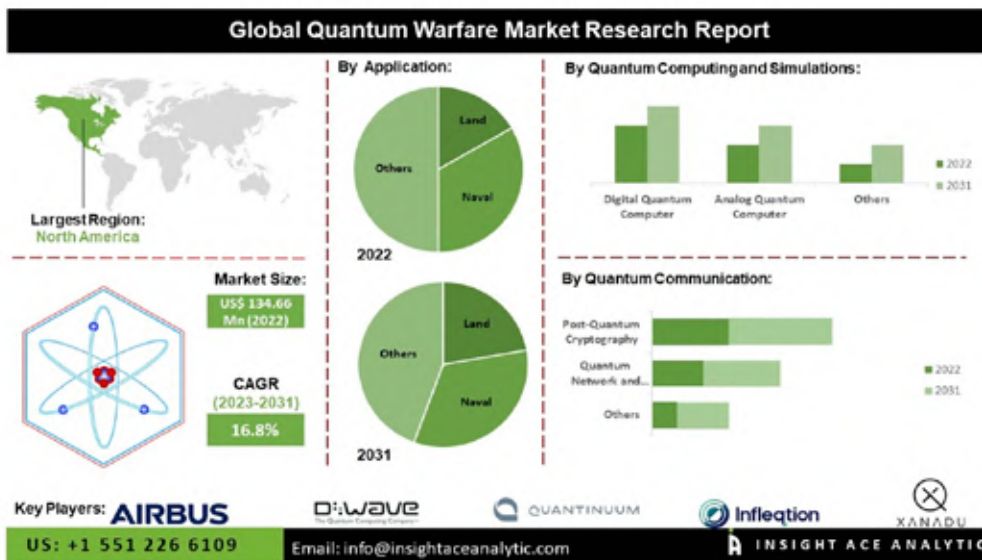


Figura A3.7. Mercado de guerra cuántica.

Fuente: <https://www.insightaceanalytic.com/report/quantum-warfare-market/2053>

Las tecnologías cuánticas ofrecen oportunidades estratégicamente significativas para el espacio que puede considerarse un ejemplo de “sector dual”. Las tecnologías de comunicación cuántica segura ya están integradas en iniciativas espaciales clave de la UE, como EuroQCI/IRIS² y la misión pionera del gravímetro espacial cuántico. Las actividades espaciales de la UE también abarcan el avance de los sistemas de navegación inercial cuántica, incluidos los prototipos basados en sensores ópticos cuánticos en el marco del programa Galileo, para el posicionamiento autónomo en entornos en los que los sistemas mundiales de navegación (GNSS) han sido intencionadamente desactivados o falsificados. Se espera que estos prototipos se prueben a bordo de los satélites Galileo en los próximos años para evaluar su potencial de despliegue operativo. Paralelamente, también se están evaluando relojes cuánticos para futuras actualizaciones de Galileo.

También se espera que la computación cuántica mejore la **ingeniería espacial** a través de capacidades computacionales avanzadas, incluso para mejorar la comprensión humana

del universo. Un gran número de aplicaciones espaciales cuánticas también tienen un gran potencial para fines militares y de inteligencia.

La **guerra electrónica cuántica** puede revolucionar las operaciones militares en el espacio durante la siguiente década como se representa en la figura A3.8. Como puede observarse se pretenden combinar redes satelitales con enlaces cuánticos (en órbitas GEO, LEO y MEO) con plataformas de alta altitud (HAP) y UAV interconectados entre sí y con estaciones terrestres empleando distribución cuántica de claves (QKD).

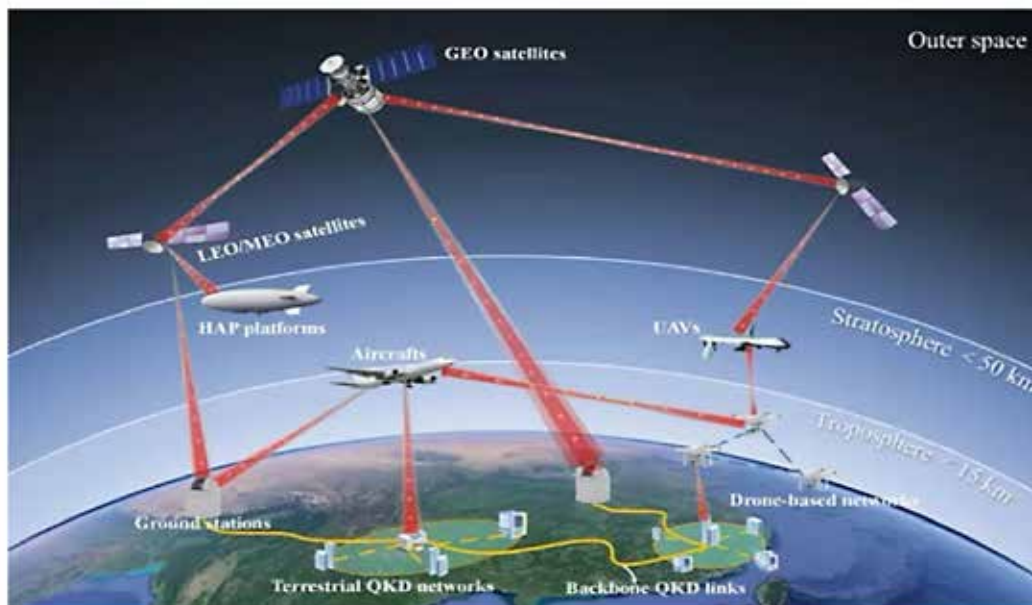


Figura A3.8. Guerra electrónica cuántica. Fuente: <https://quantumpedia.uk/will-quantum-technology-transform-the-nature-of-warfare-e1d835e5d182>

En junio de 2024, *SandboxAQ* (empresa escindida de *Alphabet*), anunció el sistema **AQNav**, que **combina la detección cuántica con la IA** para proporcionar navegación en tiempo real sin depender de la señal GNSS (*SandboxAQ*, 2024).

Reloj Atómico con Fines de Defensa

Otro problema en el que la **sensórica cuántica** puede posibilitar un salto tecnológico revolucionario es en la **medición precisa del tiempo**. Los relojes cuánticos, también conocidos como **atómicos** por basarse en los átomos para su funcionamiento, son mucho más precisos que cualquier reloj convencional. En lugar de tomar la rotación de la Tierra como referencia para medir el tiempo, algo que puede sufrir ligeras variaciones debido a múltiples factores (gravitatorios, geológicos, climáticos...), un **reloj cuántico** se basa en los átomos.

Simplificando su funcionamiento, **en estos relojes se proyecta luz o radiación electromagnética sobre un átomo y sus niveles de energía cambian en un proceso estable que puede medirse, estableciéndose como una *escala de tiempo***. El estándar utilizado para ello es el *cesio* porque es el elemento químico más fiable, puesto que la práctica totalidad de sus átomos responden del mismo modo a la radiación electromagnética⁴⁶⁵.

Se trata de una necesidad que surge en diversos escenarios; uno de ellos es en la **navegación satelital** (p.ej. con GPS) en la que el posicionamiento preciso requiere una referencia temporal de altísima precisión. Además de las mejoras en materia de navegación y posicionamiento –lo que influye también en el **guiado de misiles**–, abre la puerta al despliegue de **redes militares encriptadas** que dependen de una referencia temporal altamente sincronizada. Con ello se obtienen ventajas en escenarios de guerra electrónica donde los milisegundos pueden ser determinantes.

A comienzos de 2025 el gobierno británico anunció el desarrollo de un **reloj cuántico con fines de Defensa** por el *Defence Science and Technology Laboratory* (DSTL) con el objetivo de *“mejorar la precisión en materia de Inteligencia, vigilancia y reconocimiento al reducir la dependencia de la tecnología GPS mucho más susceptible de ser bloqueada”*⁴⁶⁶. El objetivo es que en cinco años pueda comenzar a utilizarse en operaciones militares. El nuevo **reloj cuántico** mejorará la precisión en materia de inteligencia, vigilancia y reconocimiento al reducir la dependencia de la tecnología GPS, mucho más susceptible de ser bloqueada por el enemigo. La precisión del prototipo de este reloj, por ahora muy voluminoso, es tal que **perderá menos de un segundo en miles de millones de años**⁴⁶⁷.

Pasos hacia el “*Tricorder de Star Trek*”

En la famosa serie de ciencia ficción *Star Trek* el médico que quería hacer un control médico a un miembro de la tripulación de la nave *Enterprise*, le bastaba con apuntar un dispositivo especial el famoso “*tricorder*” o “*trigrabador*”, en la dirección del paciente.

En la Universidad de Stanford en 2015 se ha desarrollado un nuevo sistema de diagnóstico inspirado en el anterior de ciencia ficción. Este nuevo instrumento puede ser usado para descubrir tejidos orgánicos de consistencia diferente de los otros como es el caso de las células cancerígenas También puede ser utilizado para **detectar explosivos ocultos en la maleta de un terrorista**. En ambos casos, **un sensor cuántico tiene una precisión mayor que la de los rayos X y sin necesidad de contacto con el material a analizar**.

465 En términos de reloj cuántico de cesio, un segundo equivaldría a 9.192.631.770 ciclos.

466 <https://www.publico.es/opinion/columnas/supremacia-cuantica-oculta-ia.html>

467 Ha sido desarrollado entre DSTL, Inflection, Aquark Technologies, HCD Research y el Imperial College London, https://storage.printfriendly.com/downloads/pdf_1739123473_42ec3bA4.pdf

Todo surge a partir de un **concurso lanzado por DARPA para detectar explosivos incluso invisibles a los detectores de metales**. El funcionamiento básico es el siguiente:

- Emisión de microondas hacia el área a examinar. Estas ondas hacen vibrar las moléculas de varios materiales según la frecuencia característica de cada material. Las vibraciones generan ondas ultrasonidos que se difunden en el aire. Estas señales características son recogidas por sensores apropiados lo cual nos permite tener un cuadro detallado de la composición del material analizado.
- Este sistema puede ser usado también en Oncología ya que los tejidos enfermos absorben la energía de las microondas de diagnóstico no invasivo en forma diferente de los sanos y vibran de forma diversa.
- Se trata de un sistema no invasivo, no es peligroso como los rayos X y muy preciso debido a la combinación de las características de las microondas y los ultrasonidos (¡¡calor + sonido !!).

Implicaciones de la computación cuántica en la guerra irregular (Hanna, 2025)

A medida que la computación cuántica comience a emerger de la investigación teórica hacia la aplicación práctica, puede alterar significativamente el panorama de la guerra irregular y el conflicto de la zona gris, que prosperan en la complejidad, la ambigüedad y la explotación de las asimetrías tecnológicas e informativas. Por ejemplo, **una nación hostil equipada con capacidades de descifrado mejoradas cuánticamente podría interceptar y descifrar comunicaciones militares**, lo que haría que las operaciones seguras fueran vulnerables y develara información de inteligencia crítica.

Del mismo modo, el procesamiento de datos cuánticos podría permitir analizar grandes cantidades de datos interceptados en tiempo real y **descubrir patrones operativos o vulnerabilidades**. A medida que continúa evolucionando, la capacidad de procesar y analizar rápidamente grandes cantidades de datos podría cambiar el equilibrio de poder, introduciendo enfoques completamente nuevos para el conflicto que antes eran inimaginables.

Iniciativas de tecnologías cuánticas de las grandes potencias en defensa

Actores globales como **Estados Unidos y China** están invirtiendo fuertemente en el espacio y el ejército aplicaciones de la cuántica, incluida la navegación independiente del Sistema Mundial de Navegación por Satélite (GNSS), las comunicaciones seguras por satélite y terrestres, el LIDAR cuántico y los radares cuánticos mejorados.

En el caso de **China** el esfuerzo gubernamental es muy relevante desde hace diez años, inicialmente en comunicaciones cuánticas, con el ambicioso programa chino de **Experimentos**

Cuánticos a Escala Espacial (QUESS), que se centra en el satélite **Micius** lanzado en 2016. **Micius** ha permitido varios logros históricos en la comunicación cuántica, incluida una *videollamada cifrada cuántica de 2017 entre China y Austria*, que cubrió 7.600 kilómetros, y *experimentos de comunicación segura con Rusia*. China también ha dado un gran paso adelante en la construcción de una red global de comunicación cuántica al establecer con éxito un **enlace ultra seguro de distribución de claves cuánticas (QKD) entre Beijing y Sudáfrica**.

Los **avances de China en computación cuántica** son también notables desde el comienzo de la presente década. Empleando diversos enfoques tecnológicos están demostrando que pueden conseguir la *superioridad cuántica* en su competición con Estados Unidos.

En 2020, científicos de la *Universidad de Ciencia y Tecnología de China (USTC)* dieron a conocer **Jiuzhang**, una **computadora cuántica fotónica** con el que resolvió un problema muy complejo (*Gaussian boson sampling*) utilizado en el experimento *Sycamore* de *Google* en 200 segundos que le habría llevado a una supercomputadora clásica más de 2.500 millones de años. En la figura A3.9 puede verse su esquema de funcionamiento.

Las versiones posteriores, como **Jiuzhang 2.0** mejoraron aún más el rendimiento, y **Jiuzhang 3.0** (en 2023) podría rastrear 255 fotones a la vez, un gran salto comparado con las prestaciones del original⁴⁶⁸. El éxito ha sido demostrar que puede **controlar y detectar cientos de fotones en una sola ejecución sin perder la coherencia cuántica**, y que pueden construirse interferómetros fotónicos a gran escala con gran estabilidad y precisión.

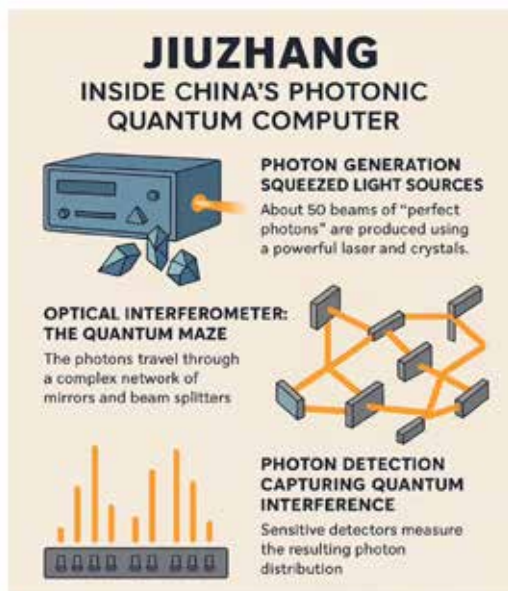


Figura A3.9. Concepto de funcionamiento del computador chino Jiuzhang. Fuente: <https://trustinscience.com/2025/06/10/jiuzhang-inside-chinas-photonic-quantum-computer/>

468 <https://trustinscience.com/2025/06/10/jiuzhang-inside-chinas-photonic-quantum-computer/>

La batalla continúa. El prototipo de **Jiuzhang 4.0**, diseñado para integrar más de **2.000 fotones**, está a punto de romper los récords existentes de la supremacía cuántica y redefinir la competición de la computación cuántica entre grandes potencias⁴⁶⁹.

No es el único enfoque. En 2021, investigadores de la misma universidad presentaron otra máquina denominada **Zuchongzhi 2.1**. En este caso se trata de un **procesador cuántico superconductor de 66 cúbits** que demostró una ventaja cuántica significativa sobre las supercomputadoras clásicas. En 2023, el mismo equipo anunció **Zuchongzhi 3.0**, un procesador de 105 qubits, que superó las de Google por un factor de hasta un millón en tareas de muestreo específicas.

En marzo de 2025 **Zuchongzhi 3.0** superó las últimas puntuaciones de *Sycamore* en seis órdenes de magnitud, estableciendo el récord más alto para un sistema superconductor desvelado públicamente. En la figura A3.10 puede verse el procesador cuántico (QPU) empleado que compite con el *Willow* de Google.

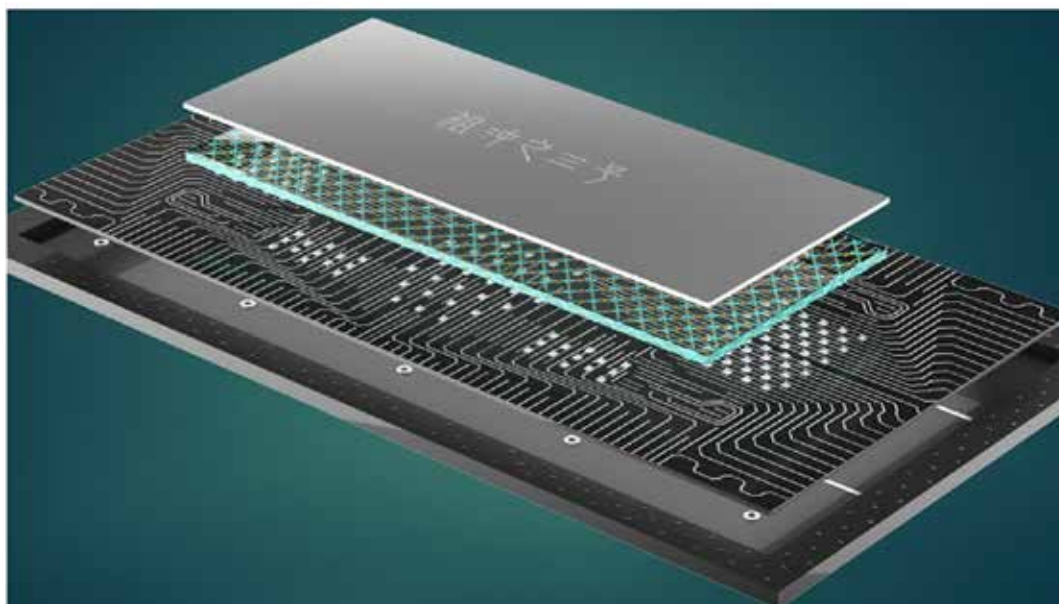


Figura A3.10. Procesador cuántico (QPU) de Zuchongzhi 3.0. Fuente: <https://www.livescience.com/technology/computing/china-achieves-quantum-supremacy-claim-with-new-chip-1-quadrillion-times-faster-than-the-most-powerful-supercomputers>

Lentamente, China también se mueve en el terreno comercial favoreciendo la creación de startups en tecnologías cuánticas. Como ejemplo de estos avances, una startup china, *Origin Quantum*, ha presentado en mayo de 2025 **Tianji 4.0**, un sistema de medición y control cuántico superconductor de última generación capaz de soportar ordenadores cuánticos con más de 500 cúbits⁴⁷⁰.

469 <https://english.news.cn/20250304/071338fca3b54de1bf46306470ce2520/c.html>

470 <https://quantumzeitgeist.com/china-launches-origin-tianji-4-0/>

Para apoyar este esfuerzo, **China** ha anunciado en marzo de 2025 el lanzamiento de un fondo **de inversión respaldado por el gobierno de 138.000 millones de dólares** para apoyar las tecnologías emergentes con el objetivo de fortalecer su competitividad global⁴⁷¹. El fondo, estructurado como una asociación público-privada, invertirá en proyectos de alto riesgo y a largo plazo en sectores como la **computación cuántica**, la **inteligencia artificial**, los **semiconductores** y las **energías renovables**. Dado el enfoque de fusión militar-civil del gobierno chino es muy probable que estas inversiones fortalezcan el escalado de startups con tecnologías duales que fomenten la convergencia entre las tecnologías priorizadas.

En el caso de los **Estados Unidos** es destacable el **programa de sensores cuánticos robustos RoQs promovido por DARPA**. Los sensores cuánticos son muy prometedores para el avance de las capacidades de defensa. Sin embargo, **estos sensores son frágiles tienen muchas limitaciones cuando se implementan en entornos reales** como plataformas móviles. Las vibraciones, las interferencias electromagnéticas y otras perturbaciones ambientales degradan su rendimiento, limitando su utilidad operativa. Las soluciones basadas en el aislamiento de los sensores o el uso de blindajes voluminosos son caras y no permiten su despliegue generalizado.

Para reducir estos problemas, DARPA ha iniciado en febrero de 2025 el programa de **Sensores Cuánticos Robustos (RoQS)**⁴⁷² que buscará desarrollar **sensores cuánticos resistentes a las alteraciones ambientales**, asegurando que puedan operar de manera confiable fuera de un laboratorio sin sacrificar su sensibilidad para poder integrar estos sensores en las plataformas del Departamento de Defensa. Los objetivos concretos del programa son:

- Desarrollar arquitecturas de sensores que pueden suprimir las perturbaciones ambientales.
- Desarrollo de matrices compactas que diferencien entre ruido y señales significativas.
- Exploración de sistemas atómicos avanzados para una mayor estabilidad en condiciones dinámicas.

Las estrategias seguidas por Estados Unidos y China en el desarrollo de las tecnologías cuánticas desde una perspectiva de uso dual no son similares. En la Tabla A3.1 se presentan algunos hitos destacados de ambos países atendiendo a diferentes factores técnicos y geoestratégicos.

471 <https://thequantuminsider.com/2025/03/07/china-launches-138-billion-government-backed-venture-fund-includes-quantum-startups/>

472 <https://www.darpa.mil/news/2025/quantum-sensors-defense-platforms>

Domain	Metric	United States	China
Research & Theory	Foundational Algorithms	Shor, Grover, QAOA, VQE	Strong in quantum simulation and communication theory
Hardware Platforms	Qubit Diversity	Superconducting (Google, IBM), Ion Traps (IonQ)	Superconducting (USTC, Origin Quantum), Photonics (Jiuzhang)
Quantum Supremacy	Milestones	Google's Sycamore (2019), Willow (2024)	Jiuzhang (2020), Zuchongzhi 3.0 (2025)
Investment	Funding Model	Mixed: federal + private (e.g. Google, IBM)	Massive state-led funding (\$15B+ total)
Industry Ecosystem	Commercial Activity	Rich startup scene (IonQ, Rigetti); partnerships with AWS, Microsoft	Origin Quantum, Baidu Qian Shi, Huawei QC cloud
Government Strategy	Policy & Planning	National Quantum Initiative (2018), DOE & DARPA support	Five-Year Plans (since 2016), Quantum S&T Megaproject
Quantum Communication	Global QKD & Satellite	Limited (early R&D phase)	Leader: Micius satellite, Beijing-Vienna & Beijing-South Africa QKD
Quantum Computing	Error Correction & Fault-Tolerance	Willow (Google, 2024): first logical qubit	Zuchongzhi: raw performance, less focus on error correction
Workforce & Talent	Quantum Researchers	Top universities (MIT, Caltech, Harvard); industry-academic synergy	Large academic base (USTC, CAS); government-directed
Global Influence	Tech Diplomacy	Open innovation, global academic collaborations	Bilateral partnerships (Russia, BRICS), closed ecosystem

Tabla A3.1. Comparativa entre las estrategias cuánticas de Estados Unidos y China. Fuente: <https://asiatimes.com/2025/07/us-china-in-a-defining-race-for-quantum-supremacy/#>

La reciente presentación del presupuesto de defensa para 2026 de Estados Unidos con 179.000 millones de euros para las actividades de investigación y desarrollo⁴⁷³ refleja un **cambio estratégico para acelerar la integración de la tecnología cuántica, la IA y los sistemas espaciales como eje de la mejora de las capacidades de defensa.**

Los programas relacionados con la cuántica, aunque fragmentados y a menudo clasificados, están ganando terreno a través de iniciativas de servicios cruzados en detección, cifrado y navegación, con convergencia visible en aplicaciones satelitales y espaciales. Por su lado, el desarrollo de la IA ligado a sistemas autónomos, que abarcan drones, robots y sistemas de apoyo a la toma de decisiones, recibirían más de 2.200 millones de dólares en financiación, lo que refleja el despliegue operativo generalizado en todos los dominios.

Todos los ejemplos presentados tienen un uso dual. Eso ha hecho incrementar el interés entre alianzas de defensa en acelerar el intercambio de información para asegurar el liderazgo. Una iniciativa de carácter multilateral en tecnologías cuánticas para la defensa

⁴⁷³ <https://thequantuminsider.com/2025/07/03/quantum-ai-and-space-anchor-pentagons-deep-tech-convergence-strategy/>

es la lanzada en 2024 por la OTAN denominada **Comunidad Cuántica Transatlántica** con la ambición de convertirse en “*una alianza preparada para la tecnología cuántica*”⁴⁷⁴. La Comunidad reunirá a expertos cuánticos de los gobiernos nacionales, la industria, el mundo académico, los organismos de financiación y las instituciones de investigación, y ayudará a fomentar la innovación aliada que permitirá a la OTAN proteger su ventaja tecnológica.

Ante esta avalancha de desarrollos y con una competición feroz entre China y Estados Unidos, es importante analizar el **posicionamiento de la UE**. La Comisión Europea ha anunciado que desarrollará su **Hoja de Ruta de Tecnología cuántica para 2026**, alineando las prioridades en materia civil, de seguridad y comunidades de defensa. Esto ayudará a coordinar las inversiones en la próxima generación de productos cuánticos sensores, incluidos los de gravimetría, navegación y detección avanzada de amenazas.

El objetivo, ambicioso, de la UE expresado en la hoja de ruta de computación y simulación cuántica incluida en su estrategia cuántica (Comisión Europea, 2025g) que se hará pública en 2026 es que **para 2035, se convierta en el primer continente en alcanzar una escala de miles de cúbits corregidos por plataforma**, un umbral considerado necesario para resolver problemas del mundo real. Es un umbral y un objetivo que requiere esfuerzos combinados entre la Comisión Europea y los Estados miembros.

La UE, a partir de los desarrollos en el actual programa **Quantum Flagship** está planificando lanzar un primer **Pathfinder Flight de gravimetría espacial cuántica** después de 2030 para disponer de una red a gran escala de gravímetros terrestres, aéreos y espaciales. También se explorará la integración de la gravimetría cuántica en las misiones de seguimiento de la red segura IRIS² prevista para el final de esta década. Estos esfuerzos apoyarían tanto la investigación científica como las aplicaciones estratégicas de doble uso.

La Comisión Europea también ha puesto en marcha medidas para **aprovechar las tecnologías con potencial de doble uso, incluida la cuántica, para la defensa** a través del *Fondo Europeo de Defensa* y el *Plan de Innovación en Defensa de la UE (EUDIS, EU Defence Innovation Scheme)*. La premisa subyacente de la Comisión es que todas estas actividades “*garanticen que los desarrollos cuánticos sigan siendo accesibles, seguros y estén libres de regulaciones de exportación de terceros países, al tiempo que se alinean con los objetivos europeos de defensa y seguridad*”.

Asimismo, pretende firmar en 2025 un **acuerdo de cooperación con la ESA** para el desarrollo de una hoja de ruta específica para el espacio (*Quantum Technology Roadmap in space*). También el desarrollo de otra hoja de ruta tecnológica en 2026 para **detección cuántica en espacio y defensa**.

⁴⁷⁴ https://www.nato.int/cps/en/natohq/news_227241.htm

En paralelo, varios Estados miembros de la UE ya incluyen **inversiones en sus programas gubernamentales de defensa para desarrollar tecnologías cuánticas**. Algunos ejemplos son:

- Francia: sensores cuánticos para la defensa (PROQCIMA)⁴⁷⁵.
- Alemania: comunicaciones y sensores cuánticos.
- Italia: sensores de átomos fríos y navegación libre de señal GNSS.
- Austria: relojes cuánticos y sensores inerciales.
- Finlandia: sistemas portátiles de detección cuántica para uso en defensa.

Disponer de computadores, redes de comunicaciones y sensores con tecnologías cuánticas permitirá abordar problemas en defensa; este proceso tendrá avances significativos si se **consolida su relación con la IA**. Este es el objeto de la siguiente sección.

A3.4. Convergencia entre las tecnologías cuánticas y la IA en Defensa

Una vez descrita la evolución de las tecnologías cuánticas, esta sección aborda cómo, en los próximos años, y de forma paulatina, **las tecnologías cuánticas se integrarán progresivamente con la IA** tal y como se indica esquemáticamente en la figura A3.11. Esta convergencia, aplicada a la defensa, servirá como base de la futura implementación de la denominada **“guerra cuántica inteligente”**, integrada en todos los dominios militares (Chapman y Peters, 2022).

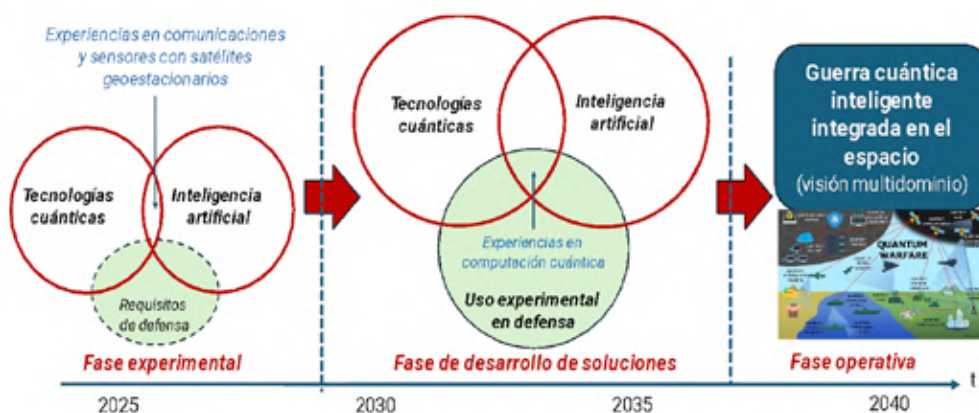


Figura A3.11. Interacción entre tecnologías cuánticas e IA para posibilitar la guerra cuántica inteligente. Fuente: elaboración propia

En la figura, se ha planteado esta evolución en un periodo temporal dilatado desde 2025 a 2040 y en **tres fases diferenciadas**.

⁴⁷⁵ <https://quantique.france2030.gouv.fr/acces-aux-marches/programme-proqcima>

- En la fase **experimental** (2025-2030) se está empezando a analizar como la IA (sobre todo, el aprendizaje automático) puede complementar a la tecnología cuántica o aprovecharse de ella. Eso ocurre, sobre todo, en los ámbitos de comunicaciones y sensores cuánticos, áreas más maduras que la computación cuántica. Es una fase en la que los centros de investigación, start-ups, y las agencias públicas de I+D son los tipos de entidades que toman el protagonismo. El rol de las Fuerzas Armadas se puede limitar a experimentar con algunas soluciones y a definir cuáles serían los requisitos necesarios para su uso en el futuro.
- En la fase de **desarrollo de soluciones** (2030-2035) se asume que la computación cuántica haya madurado lo suficiente como para complementar las comunicaciones y la sensórica cuánticas y proporcionar la base para un desarrollo tecnológico real, en gran medida, de carácter dual. Será el turno del sector industrial de defensa para desarrollar sistemas reales que puedan ser experimentados en escenarios reales.
- En la fase **operativa** (2035-2040) esta convergencia desembocará en su uso en operaciones militares reales, fundamentalmente por parte de las grandes potencias que serán celosas en compartir la información. Será el momento del despliegue de los sistemas de guerra cuántica inteligente.

Seguidamente, se analizan las **razones que justifican la convergencia entre las tecnologías cuánticas y la inteligencia artificial**. Krelina (2025) describe algunos ejemplos de la convergencia entre la IA y las tecnologías cuánticas en el ámbito de la defensa

La computación cuántica puede ayudar a la IA a procesar rápidamente grandes conjuntos de datos, acelerando así los procesos de IA y los modelos de entrenamiento. La computación cuántica puede permitir que las aplicaciones de IA alcancen los siguientes hitos, que eventualmente pueden respaldar el **progreso hacia una IA general (AGI)**⁴⁷⁶.

- Potencia computacional mejorada, lo que permite el procesamiento rápido de datos y los cálculos necesarios para una IA general.
- Resolución más eficiente de problemas, lo que impulsa el razonamiento y la toma de decisiones avanzados de la IA.
- Capacidades de aprendizaje mejoradas, que son críticas para la adaptabilidad de AGI en diversas tareas y entornos.
- Procesamiento paralelo, que mejora el análisis y la síntesis de la información.
- Manejo más fácil de estructuras de datos complejas, lo que proporciona a la IA herramientas para procesar y comprender información compleja.

476 <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-quantum-computing>

Un ámbito que está cobrando relevancia es el desarrollo de software especializado como los compresores de modelos de IA para hacer que los sistemas de IA sean más rápidos, más baratos, energéticamente eficientes, y que no dependan de la “nube”. La idea es detectar y eliminar conexiones neuronales que no se emplean. Ello permitiría introducirlos en pequeños dispositivos (como teléfonos móviles) al reducir los requisitos de memoria (entre el 50% y el 80%). Una herramienta de este estilo es CompactfAI API desarrollada por la empresa española Multiverse Computing que utiliza técnicas inspiradas en la computación cuántica. Se está empezando a experimentar con su uso en drones para aplicaciones de defensa.

En el sentido inverso, **la IA puede mejorar el desarrollo, la optimización y las aplicaciones prácticas de la computación cuántica**. Estas son algunas áreas de la computación cuántica que podrían beneficiarse de la IA:

- *Corrección de errores*. El aprendizaje automático predice y corrige errores de computación cuántica, mejorando la fiabilidad de los ordenadores cuánticos.
- *Reducción de ruido*. La IA puede analizar los patrones de ruido para desarrollar estrategias de reducción.
- *Diseño y optimización de algoritmos cuánticos*. Ambos procesos pueden ocurrir a través del aprendizaje por refuerzo similar al de la IA.
- *Control de hardware cuántico*. La IA puede automatizar la calibración de dispositivos cuánticos y ajustar dinámicamente sus parámetros de control.
- *Gestión de recursos*. La IA puede ayudar a asignar qubits de manera eficiente y optimizar la programación de tareas cuánticas.
- *Simulación y emulación*. La IA puede mejorar las simulaciones de sistemas cuánticos para pruebas de algoritmos y hardware, así como ayudar a la investigación emulando procesos cuánticos en hardware clásico.
- *Benchmarking y análisis de rendimiento*. La IA puede desarrollar sofisticadas herramientas de evaluación comparativa para evaluar y comparar dispositivos y algoritmos cuánticos.
- *Sistemas híbridos cuántico-clásicos*. La IA puede optimizar la distribución de tareas entre procesadores clásicos y cuánticos, maximizando la eficiencia general.

Aprendizaje automático cuántico (QML). La IA puede mejorar el entrenamiento de los modelos QML al mejorar el rendimiento y la aplicabilidad.

El último de los puntos indicados, el **aprendizaje automático cuántico (QML)** es un campo emergente que combina la computación cuántica con técnicas tradicionales de aprendizaje automático para **mejorar la eficiencia y la precisión de los algoritmos de aprendizaje automático** como el muestreo cuántico, el álgebra lineal, donde el aprendizaje automático se trata del procesamiento de vectores complejos en un sistema lineal de alta dimensión, o **redes neuronales cuánticas**.

QML se basa en aprovechar las propiedades únicas de la mecánica cuántica, como la superposición y el entrelazamiento. Con ello, **QML puede procesar y analizar conjuntos de datos complejos de manera más rápida y efectiva que los métodos clásicos de aprendizaje automático**. En la figura A3.12 se comparan ambos enfoques.

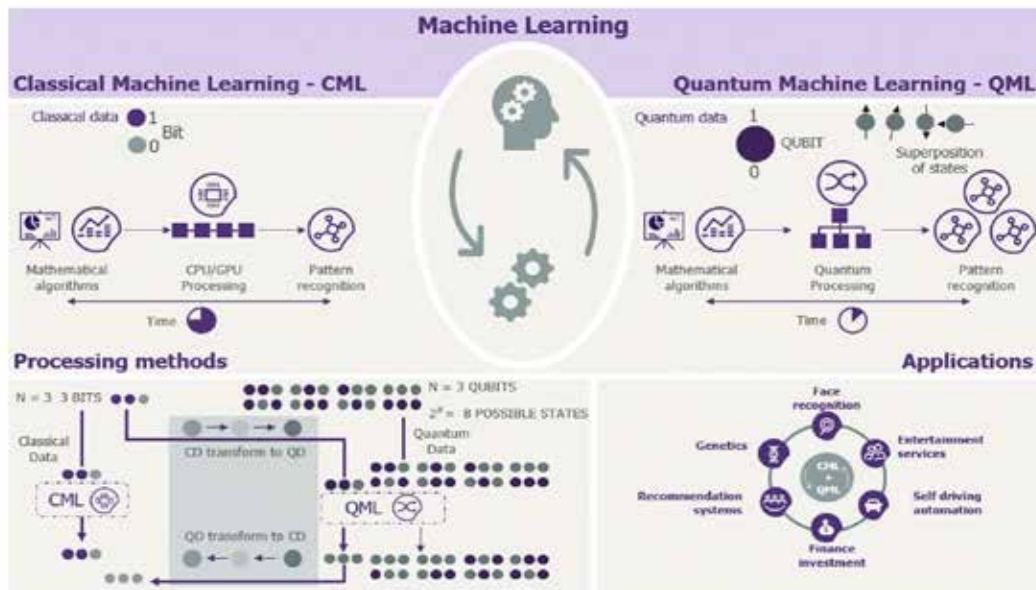


Figura A3.12. Comparación CML y QML. Fuente: <https://thequantuminsider.com/2020/05/28/quantum-machine-learning-is-the-next-big-thing/>

- En el **aprendizaje automático cuántico**⁴⁷⁷, las computadoras cuánticas se utilizan para procesar datos, entrenar modelos y optimizar soluciones, a menudo mejorando el rendimiento de los algoritmos clásicos de aprendizaje automático. Algunas áreas presentadas en la literatura en la que el número de artículos ya es elevado son (Peral-García et al., 2024):
- **Codificación de datos cuánticos:** El primer paso en QML consiste en codificar datos clásicos (por ejemplo, imágenes, texto o números) en estados cuánticos. Este proceso se conoce como **mapeo de características cuánticas**, donde los datos clásicos se transforman en un formato que las computadoras cuánticas pueden manipular.
- **Entrenamiento de modelos cuánticos:** Los algoritmos cuánticos se utilizan para entrenar modelos de aprendizaje automático. Las versiones cuánticas de algoritmos clásicos, como las **máquinas de vectores de soporte cuántico** (QSVM) y las **redes neuronales cuánticas** (QNN), tienen como objetivo encontrar patrones en los datos mucho más rápido que sus contrapartes clásicas.

477 <https://medium.com/@hassaanidrees7/quantum-machine-learning-the-next-frontier-in-ai-76a258ca1239>

- **Optimización cuántica:** Las computadoras cuánticas sobresalen en la resolución de problemas de optimización, que son fundamentales para muchas tareas de ML, como minimizar las funciones de pérdida. Algoritmos como el **Algoritmo de Optimización Aproximada Cuántica (QAOA)** y el **Solucionador Cuántico Propio Variacional (VQE)** se utilizan para encontrar de manera eficiente los parámetros óptimos para los modelos de ML.
- **Modelos híbridos cuántico-clásicos:** Dado que las computadoras cuánticas actuales aún se encuentran en las primeras etapas de desarrollo, muchos modelos QML son **híbridos**, lo que significa que combinan el procesamiento clásico y cuántico. En esta configuración, los ordenadores cuánticos se utilizan para tareas específicas, como la optimización o los cálculos de matrices, mientras que los ordenadores clásicos se encargan del resto.

Desde el punto de vista de aplicaciones concretas, algunas de las **áreas en las que QML podría emplearse**, no necesariamente ligadas a la defensa, son:

- Optimización financiera y logística).
- Reconocimiento de patrones para reconocimiento de voz e imágenes.
- Aceleración del entrenamiento de redes neuronales.
- Simulación científica en tiempo real.
- Modelado climático.
- Diseño y comprensión de nanopartículas.
- Creación de nuevos materiales a través de mapas moleculares y atómicos.
- Modelado molecular para descubrir nuevos fármacos e investigación médica.
- Comprender la composición más profunda del cuerpo humano.
- Fomentar la exploración espacial.
- Creación de una seguridad conectada completa a través de la fusión con IoT y cadenas de bloques.

Para **fortalecer los mecanismos de defensa de la red mediante QML** se pueden explorar varios enfoques, incluido el desarrollo de modelos híbridos, la mejora de la eficiencia y la escalabilidad de los algoritmos QML y la mejora de la resistencia de los sistemas de defensa de la red contra amenazas sofisticadas.

Los resultados de varios casos de estudio muestran que los algoritmos QML, como QSVM y QNN, superan a los enfoques clásicos en cuanto a precisión, escalabilidad y resiliencia frente a amenazas sofisticadas (Rosemary y Abraham, 2024)⁴⁷⁸.

El uso de **modelos híbridos cuántico-clásicos** significa que las técnicas de QML deben combinarse con los métodos tradicionales de ML para lograr resultados óptimos. QML se emplearía para acelerar partes específicas del aprendizaje automático, como el preproce-

⁴⁷⁸ Los tres casos de uso clave para las técnicas QML en la defensa de la red fueron: detección de intrusiones, análisis de malware y detección de anomalías.

samiento de datos, la optimización o las operaciones matriciales. No obstante, persisten dos problemas:

- Limitaciones actuales del hardware cuántico que limitan la escalabilidad y la precisión de los algoritmos QML.
- Falta de estandarización en los protocolos y marcos QML que dificultan la comparación y combinación de diferentes técnicas de QML, lo que, a su vez, dificulta el desarrollo de mecanismos de defensa de red robustos y eficientes.

A pesar de todos los problemas abiertos y la relativa inmadurez de las tecnologías ya empiezan a comercializarse **aplicaciones de defensa con sistemas que combinan la IA con tecnologías cuánticas**. Veremos muchas más en los próximos años.

Como ejemplo, una de estas aplicaciones es la desarrollada por la empresa alemana *Quantum Systems* (se trata de uno de los primeros unicornios europeos en defensa)⁴⁷⁹ que ha desvelado en junio de 2025 su plataforma de mando y control **MOSAIC UXS (Multi-Domain Command and Control Platform for Unmanned Systems)**⁴⁸⁰. Entre otras muchas funcionalidades posee un módulo de inteligencia de misión basado en IA (*AI-Powered Mission Intelligence*). Su objetivo es permitir la planificación y ejecución de la misión, incluido el posicionamiento optimizado de los componentes de la misión y su ajuste en tiempo real.

Otro caso relevante es el de la empresa *Zena Tech*⁴⁸¹ que ha desarrollado con éxito su primer **prototipo de computación cuántica diseñado para procesar grandes conjuntos de datos para soluciones de drones de IA**⁴⁸². El prototipo, probado a través del proyecto de pronóstico meteorológico *Clear Sky*, demuestra la **capacidad de analizar cantidades masivas de datos de sensores de drones en tiempo real**. Su impacto futuro en sistemas de mando y control que tengan que integrar información en tiempo real procedente de enjambres con un número muy elevado de drones para la toma de decisiones es evidente.

Finalmente, la empresa *SandboxAQ* comercializa desde junio de 2024 **AQNav**⁴⁸³. Se trata de una tecnología innovadora diseñada para la **navegación por aire, tierra y mar cuando las señales GNSS están interferidas o no están disponibles**. Hasta la fecha, **AQNav** se ha

479 Quantum Systems ya se ha asegurado varios contratos importantes de defensa, incluso con las fuerzas armadas alemanas, españolas y británicas. Su dron insignia, el Vector AI, ha sido probado en Ucrania, que se ha convertido en un importante campo de pruebas en el campo de batalla para las tecnologías de doble uso. <https://thenextweb.com/news/german-dual-use-drone-maker-becomes-unicorn-defence-tech-boom>

480 <https://quantum-systems.com/blog/2025/06/03/quantum-systems-launches-mosaic-uxs/>

481 ZenaTech es una empresa de software SaaS empresarial de drones de IA con una cartera de soluciones que ayudan a los clientes empresariales y gubernamentales a mejorar las operaciones de misión crítica. <https://www.zenattech.com/es/>

482 https://www.stocktitan.net/news/ZENA/zena-tech-creates-first-quantum-computing-prototype-enabling-zblekez1torn.html?utm_source=perplexity

483 <https://www.sandboxaq.com/press/sandboxaq-announces-aqnav---worlds-first-commercial-real-time-navigation-system-powered-by-ai-and-quantum-to-address-gps-jamming>

experimentado en cuatro tipos de aviones diferentes, desde aviones monomotor hasta grandes aviones de transporte militar.

AQNav es un **sistema de navegación geomagnética que aprovecha algoritmos de IA patentados, potentes sensores cuánticos y el campo magnético de la corteza terrestre**. AQNav proporciona una solución de navegación en tiempo real, independiente del terreno y que no se puede interferir en todo tipo de condiciones meteorológicas en situaciones en las que las señales de GPS no están disponibles, se perturban o se falsifican.

Como ocurre con tecnologías emergentes, algunos autores también han planteado **problemas éticos derivados del uso de las tecnologías cuánticas en defensa**. Entre ellos se incluye el riesgo derivado de mayores capacidades de vigilancia que infrinjan los derechos de privacidad y la posibilidad de crear nuevas armas químicas o biológicas a través de **simulaciones moleculares empleando computadores cuánticos**.

Si a este contexto de las tecnologías cuánticas se le añaden los problemas éticos ya abordados en este informe generados por el uso de la IA en defensa, **la convergencia tecnológica entre ambas hace que la necesidad de disponer de un marco de gobernanza global adquiera mayor urgencia**.

En resumen, los **futuros usuarios de tecnologías cuánticas militares con IA** tendrán que decidir si es mejor esperar a que las tecnologías maduren más o invertir tiempo y recursos en experimentos y recursos humanos que les permitan tener una posición de ventaja frente a sus competidores. Será necesario, decidir en base a un seguimiento estrecho de los avances técnicos y del comportamiento de los competidores.

Mientras tanto, los **gobiernos de todos los países desarrollados**, incluyendo la **UE**, impulsan el desarrollo de la convergencia de las tecnologías cuánticas con la IA asignando para ello crecientes recursos económicos.

Empresas miembros del Foro de Empresas Innovadoras (FEI):



Situación y tendencias en el uso de la inteligencia artificial en el sector de la defensa

septiembre de 2025

