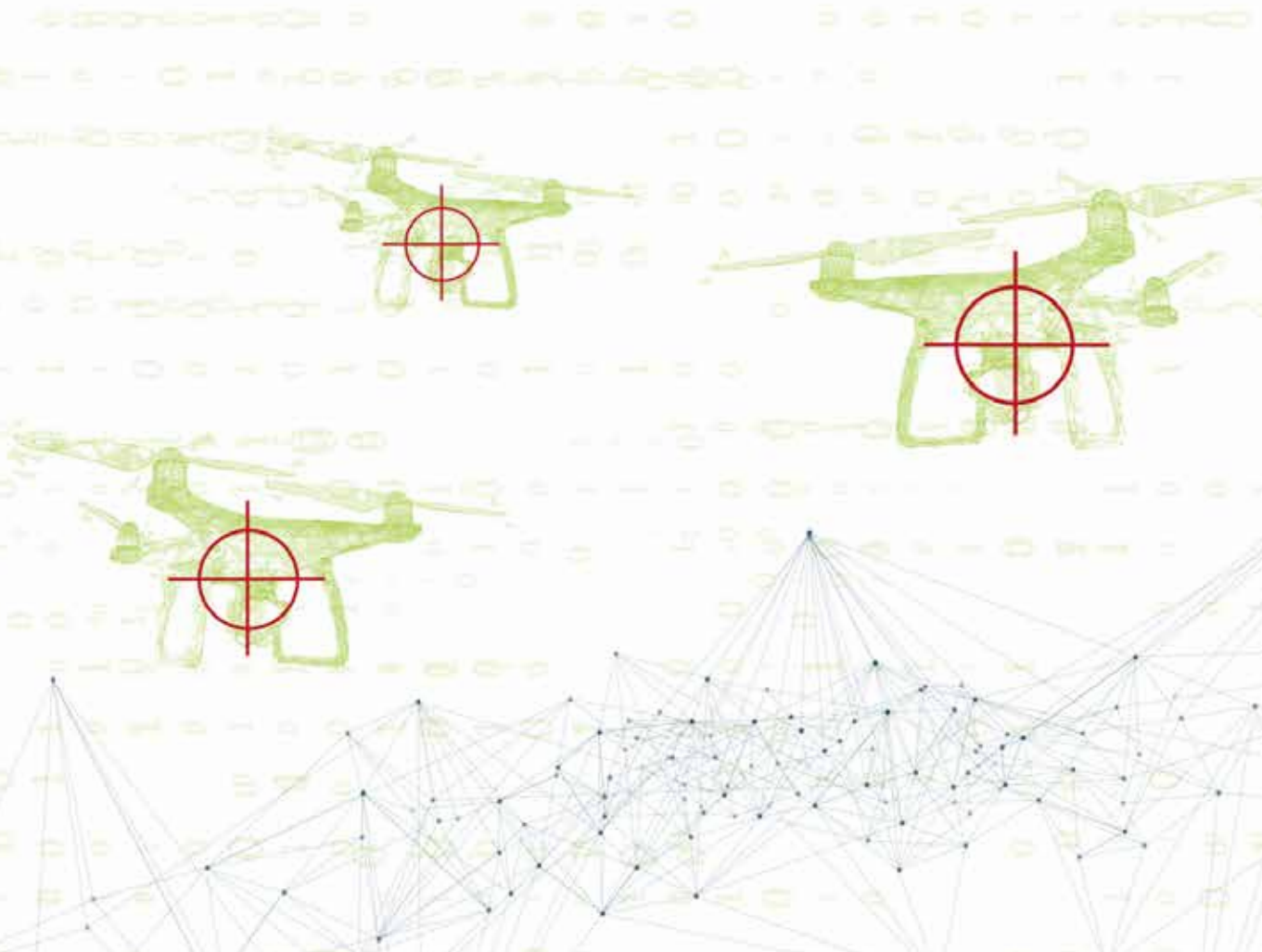
Foro Empresas Innovadoras

amper

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



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

ISBN: 978-84-09-75701-5

Versión resumida del informe final[01]

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

septiembre de 2025

Con la colaboración de::

01 Esta versión resumida ha sido extraída del informe completo. El informe completo y otros documentos complementarios se pueden descargar del sitio web del FEI. Esta versión no incluye referencias bibliográficas, que se pueden encontrar en el informe completo.

CONTEXTO y OBJETIVOS

Los diversos enfoques tecnológicos englobados en la **inteligencia artificial (IA)** han experimentado un crecimiento acelerado en la última década que ha impulsado su penetración en todas las capas de la sociedad. Hoy en día, afecta consciente o inconscientemente a miles de millones de personas y entidades en todos los países mediante el uso de **aplicaciones basadas en IA para desarrollar sus actividades diarias**, un proceso que se intensificará aún más en el futuro. El **impacto global de la IA como tecnología habilitadora se ve potenciado por su integración con otras tecnologías** como la microelectrónica, la robótica, la neurotecnología, los sensores, los sistemas de comunicaciones de banda ancha, los servicios digitales en la nube, la ciberseguridad y otras tecnologías emergentes como las tecnologías cuánticas o la biología sintética, con especial énfasis en la implicación para los ciudadanos a través del uso masivo de las redes sociales.

En vista de esta relevancia, el ***Foro de Empresas Innovadoras, FEI,*** (*http://foroempresasinnovadoras.com/*) elaboró durante 2024 un informe para evaluar la soberanía tecnológica de la Unión Europea (UE) en IA y la forma en la que España pudiera contribuir a ella en los próximos años, recomendando la puesta en marcha de algunas actuaciones con este propósito[02]. Tras el trabajo realizado en 2024 en el análisis de la autonomía estratégica de la UE, la FEI decidió centrar el esfuerzo en 2025 elaborando un **informe detallado sobre el impacto de la IA y su relevancia para la soberanía tecnológica europea en el sector de la defensa**. Este documento resume las ideas fundamentales del informe elaborado.

El análisis de los **determinantes geopolíticos** que afectan al papel global de la UE influye en el uso y despliegue de la IA en el sector de la defensa desde varias perspectivas. Se basa en la potencial revolución derivada de la IA en la **planificación, desarrollo táctico y operativo** que supone en la conducción de las operaciones militares, con cuestiones éticas y regulatorias muy relevantes.

Las **rivalidades geopolíticas** conducen no solo a una nueva carrera armamentista, sino también a una **competencia tecnológica global**. Las tecnologías disruptivas como la IA, la computación en la nube, las tecnologías cuánticas y los sistemas autónomos (por ejemplo, los drones autónomos) ya están dando forma al nuevo campo de batalla. En este escenario, el desarrollo tecnológico se acelerará aún más durante la presente década, y **la IA, como tecnología habilitadora y dual**, desempeñará un papel preeminente en todos los sistemas de armas avanzados y sistemas de toma de decisiones en el ámbito militar.

Desde la publicación del *Libro Blanco de la Defensa de la UE (Preparación 2030)* por parte de la Comisión Europea en marzo de 2025, el **debate en los Estados miembros de la UE y en las instituciones de la UE sobre las prioridades políticas, tecnológicas y presupuesta-**

02 http://foroempresasinnovadoras.com/wp-content/uploads/2024/10/2024-10-15-Informe-FEI-sobre-autonomia-estrategica-en-IA-VCON-PORTADA.pdf

rias relacionadas con estas cuestiones ha cobrado mayor protagonismo. Por este motivo, informar a la sociedad de la relevancia que la tecnología de IA tiene para la defensa y la seguridad comunes, valorando sus posibilidades, limitaciones y riesgos, así como la necesidad de implicarse decididamente en su desarrollo, se ha convertido en una cuestión esencial en la formulación de las políticas públicas europeas y para muchos Estados miembros en la evolución de los **compromisos de incremento de las inversiones en defensa derivadas de la Cumbre de la OTAN** celebrada en junio de 2025.

Además, el debate sobre la estructura y las prioridades del nuevo **Programa Marco de Investigación e Innovación** *(HE, Horizonte Europa 2028-2034)* comenzará en el segundo semestre de 2025 en el contexto del futuro **Fondo Europeo de Competitividad** incluido en el marco financiero plurianual de la UE 2028-2034 presentadas en julio de 2025. Todo ello deberá aprobarse antes de diciembre de 2027.

En este contexto, los documentos iniciales indican un **mayor esfuerzo en el desarrollo de tecnologías de doble uso, incluida la IA**, para lo que deben rediseñarse los instrumentos adecuados de financiación y participación con el fin de garantizar su eficiencia y adecuación en ese contexto. Concretamente, el **HE 2028-2034** estará estrechamente interconectado con otros programas de la UE como parte del marco finan**ciero plurianual** de la UE a partir de 2028.

Además, hay que tener en cuenta que, en el contexto español, el Ministerio de Defensa tendrá que elaborar en 2025-2026 la actualización de la *"Estrategia de Tecnología e Innovación para la Defensa (ETID)"* en la que, a buen seguro, **la IA jugará un papel habilitador muy relevante en todos los sistemas militares** que se incorporen a las Fuerzas Armadas españolas.

La evolución científica y tecnológica de la IA y la **introducción en el mercado de productos y servicios basados en la IA** se están produciendo a un ritmo muy rápido. Por estas razones, **el FEI fijó el horizonte temporal para el presente análisis en 2030**, pero abierto a considerar previsiones o estimaciones hasta 2035 relevantes desde la perspectiva de la defensa cuando exista una base documental para ello como ocurre con los proyectos a largo plazo de desarrollo de nuevos sistemas de defensa.

La **complejidad conceptual del uso de la inteligencia artificial en defensa** exige una consideración de su análisis desde varias **dimensiones complementarias**. En concreto, el informe adopta una **visión multidisciplinar** que integra las dimensiones tecnológica, socioeconómica, estratégica, táctica y operativa, así como ética y regulatoria. Brevemente, estas dimensiones abordan los siguientes elementos:

- **Dimensión tecnológica.** Aborda la evolución tecnológica de la IA en aquellas áreas con relevancia real o potencial para la defensa en el marco temporal de 2030.

Desde esta dimensión, se ha prestado atención no solo a las técnicas propias de la IA sino también a su **convergencia con otras tecnologías emergentes** como son la microelectrónica, la robótica, las comunicaciones y los sensores cuánticos, la soluciones basadas en la **neurotecnología**, la ciberseguridad, la computación en el borde, la simulación (utilizando, por ejemplo, gemelos digitales), etc. También se menciona la necesidad de afinar algunas de las técnicas de IA desarrolladas en el ámbito civil para su uso en el contexto de la defensa.

- **Dimensión socioeconómica**. El análisis realizado se basa en la valoración del volumen del mercado de IA en defensa a partir de la situación en 2024 y con estimaciones de su evolución previsible hasta 2030 según diversos informes de entidades oficiales y consultoras; Asimismo, se analizan los cambios relacionados con su configuración y evolución en diversos países

La **estructura del sector empresarial de defensa relacionado con la IA** está evolucionando muy rápidamente, con frecuentes reconfiguraciones, fusiones y operaciones de adquisición entre sus principales actores. Asimismo, es relevante el incremento de startups con productos disruptivos en el ámbito de la defensa. Esta evolución se analiza en este documento a partir de informes de mercado emitidos por diversas entidades externas, que no necesariamente coinciden en sus estimaciones, utilizando la documentación públicamente disponible sobre los mismos.

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

- **Dimensión estratégica, táctica y operativa**. Esta dimensión aborda la forma en que el "campo de batalla" convencional se ve envuelto en un proceso acelerado de digitalización, y evoluciona desde un campo de batalla digital (proceso en curso) a un "campo de batalla inteligente" (proceso incipiente) con profundos cambios a nivel estratégico, táctico y operativo.

Desde esta dimensión, **se ha prestado especial atención a la forma en la que se está empezando a utilizar la IA en conflictos bélicos abiertos**. Dado que la dimensión militar del uso de la IA es muy amplia y no es posible abarcarla en su totalidad con datos no clasificados, este análisis se ha centrado en tres ámbitos de indudable actualidad. Son los siguientes: el **sector espacial de la defensa**, la evolución hacia la **guerra cognitiva** (en el contexto más amplio de la guerra híbrida) y el creciente uso de la IA en los **sistemas de toma de decisiones** vinculados a sistemas de armas autónomos o semiautónomos (SALA) o componentes de cadenas letales ("*killer chains"*) más amplias.

- **Dimensión ética y regulatoria**. Desde esta dimensión, se ha puesto el énfasis en los problemas éticos derivados de los procesos de toma de decisiones en los que los seres humanos pueden verse desplazados por el creciente uso de algoritmos de IA en contextos de aumento masivo de la información a manejar, y la reducción del tiempo disponible para tomar decisiones acertadas. Asimismo, se describen las interrelaciones con los enfoques regulatorios actuales de la IA y su posible aplicación al ámbito de la defensa.

Esta dimensión ha adquirido gran relevancia en los últimos años debido a las **consecuencias éticas r**elacionadas con el uso de la IA en la identificación automática de objetivos militares o en su uso en sistemas de armas semiautónomos. También se analiza la **falta de un consenso legislativo y regulatorio compartido** para abordar los usos de la IA de manera responsable en los asuntos militares.

Se trata de cuatro **dimensiones interrelacionadas**; dado que la evolución de una de ellas afecta a las demás, los impactos del uso de la IA en el sector de la defensa deben **analizarse de forma global**. En la Figura 1 se describe esquemáticamente la **relación entre las dimensiones indicadas** anteriormente y algunos de los elementos o factores clave identificados en cada una de ellas.

Figura 1. Dimensiones de la IA empleadas en la preparación del informe. Fuente: elaboración propia.

Objetivos específicos del informe

Con la expansión de las aplicaciones de IA, **los humanos ya no son los únicos agentes implicados en la toma de decisiones** en muchos ámbitos de la sociedad. Ni siquiera se

trata de algoritmos complejos que realizan cálculos de modelos complejos con mayor eficiencia y rapidez aprovechando sistemas de alto rendimiento, extrayendo datos de forma "inteligente" tanto de servidores como de Internet; también se trata de **sistemas que son capaces de "aprender de su entorno y evolucionar por sí mismos"**; a veces, en direcciones desconocidas y sorprendentes para los humanos involucrados.

La emergencia de la **inteligencia artificial generativa** en la sociedad, centrada primero en la interacción, análisis y elaboración de textos en lenguaje natural, y en los últimos años profundizando en el análisis y generación de contenidos de carácter multimodal (incluyendo también audio, imágenes, vídeo y programas informáticos), ha irrumpido con fuerza en los mercados globales.

Además, la evolución tecnológica de los sistemas de IA se ve potenciada por la integración paulatina de los **sistemas de realidad virtual y realidad aumentada** que están empezando a penetrar en los mercados de consumo masivo y profesionales. En los próximos años se espera que la evolución para integrar **sistemas holográficos** y **neurotecnología** continúe, aunque todavía se encuentra en estado experimental. Todas estas son también tecnologías inherentemente duales que se integrarán en los productos y servicios comercializados en los mercados civiles y militares.

La IA en defensa transformará la naturaleza del conflicto militar en el que los humanos coexistirán y, hasta cierto punto, compartirán decisiones con máquinas y algoritmos previamente entrenados capaces de aprender de su propio comportamiento. **Estamos pasando paulatinamente de un "campo de batalla digital" a un "campo de batalla inteligente".** Los próximos diez años serán testigos de esta transición en la que el acceso a sistemas de IA muy potentes estará al alcance de todos los ejércitos del mundo, aunque las capacidades de desarrollo de los sistemas más avanzados se limitarán a algunas potencias tecnológicas que cuenten con los recursos humanos, financieros y la voluntad política para aprovechar esa evolución.

En el contexto descrito anteriormente, los **objetivos específicos** de este i**nforme** son los siguientes:

- Analizar las **bases tecnológicas de la IA aplicada al ámbito de la defensa**, haciendo hincapié en su doble uso y su relación con otras tecnologías.
- Evaluar **cómo se utiliza la IA hoy en día en conflictos bélicos** (con información procedente de fuentes abiertas).
- Analizar el **uso de sistemas basados en IA relacionados con la defensa en la UE** con análisis de las interdependencias con los países proveedores, y su evolución en los próximos años.
- Determinar las **capacidades de España en IA para la defensa** y su previsible evolución en el contexto de la UE, adoptando una posición realista en el marco de la evolución de los presupuestos de defensa.

- Elaborar un conjunto de **recomendaciones de actuación** para las Administraciones Públicas y las empresas que sirvan de base para acordar medidas de posicionamiento y mejora en los respectivos ámbitos competenciales.

CONTEXTO DE USO DE LA IA EN EL SECTOR DE LA DEFENSA

El uso de la inteligencia artificial 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**. La relevancia de la IA no puede separarse del proceso de digitalización del que forma parte**, que comenzó años antes. Las **tres fases u oleadas** (véase figura 2) no pueden entenderse como procesos terminados que dan paso a la siguiente fase, sino **evoluciones del proceso de digitalización** que cada una sigue siguiendo sus propias especificidades a un rendimiento superior, pero al mismo tiempo con impactos cruzados en sus respectivos desarrollos.

La **primera fase** abarca un período que se extiende hasta principios del presente siglo. La digitalización fue impulsada por la expansión de la informática con sistemas de hardware y software más baratos y potentes que permitieron la democratización del acceso, impulsada por la progresiva digitalización de la información, la expansión de los centros de cómputo (inicialmente centralizados) y la automatización de tareas sencillas (rutinarias o bien definidas), ya sean administrativas o computacionales. **Esta fase no puede darse por terminada** ya que, de la mano de las mejoras en microelectrónica (por ejemplo, nuevos tipos de empaquetado de chips, menor consumo, mayor velocidad, altas frecuencias) y en arquitecturas y redes de superordenadores distribuidos, **las capacidades de procesamiento mejoran de forma continua.**

La primera fase posibilitó el comienzo de una **segunda fase** en la que las técnicas de captura y análisis de grandes volúmenes de datos (*big data analytics*), apoyadas en redes de alta velocidad, así como la sensorización del mundo físico con el despliegue de redes de sensores (*Internet of Things*, *IoT*), permitieron la recopilación de datos y el despliegue de sistemas de gestión y procesamiento de bases de datos en la nube. La expansión de los **sistemas de computación distribuidos y ubicuos** y la consecuente capacidad de automatizar procesos administrativos o de fabricación de mayor complejidad está dando forma a la sociedad actual.

La **tercera fase** comenzó gradualmente hace unos 20 años, pero se ha acelerado en la última década y seguirá evolucionando muy rápidamente. Esta fase se suma a las anteriores, facilitando **tres avances decisivos** impulsados por la adopción de la tecnología de IA. Estos son: la penetración de la **IA generativa** en la sociedad, permitiendo la generación de nueva información a partir de datos (sintéticos), texto, voz, imágenes o vídeos; la expansión de la **capacidad de procesamiento inteligente** 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 a los seres humanos en muchas de ellas con la expansión de los llamados **agentes inteligentes** (sistemas de IA especializados).

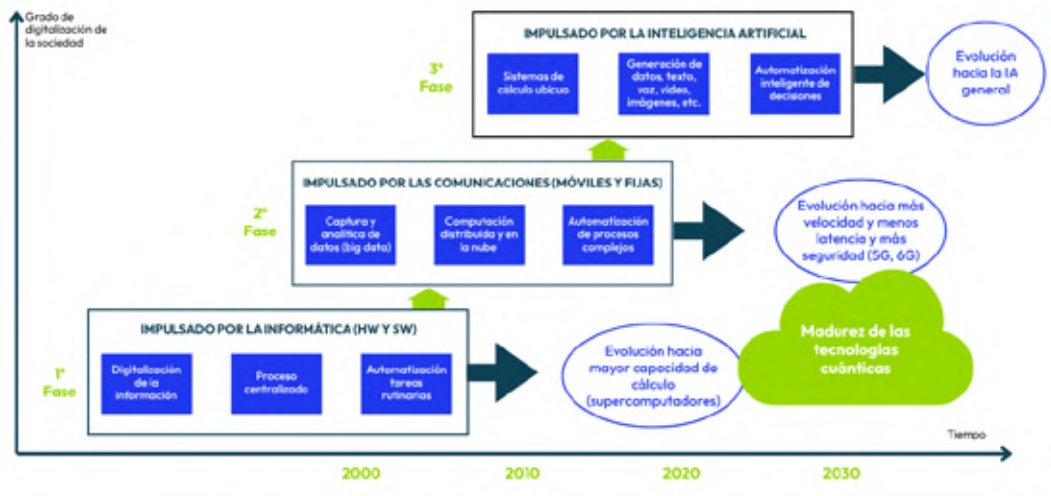


Figura 2. Fases principales del proceso de digitalización. Fuente: elaboración propia.

Es en esta tercera fase en la que se ha centrado la atención de este informe. Sin embargo, hay que tener en cuenta que esta tercera fase se apoya en las anteriores que no desaparecen, profundizando en el proceso de digitalización de la sociedad y, en particular, del sector de la defensa, cuyas tasas de adopción debidas a la evaluación de riesgos para sistemas con consecuencias letales son más lentas que las de los sectores civiles.

La sociedad avanza hacia una **cuarta fase del proceso de digitalización**, más lejana en el tiempo, pero cuyos elementos básicos ya se intuyen. La evolución de la capacidad de cómputo 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** (al ofrecer un rendimiento mucho mejor en velocidad y latencia), cuyo despliegue comenzará a finales de esta década, y con una rápida evolución de la **capacidad de razonamiento de los sistemas de IA** que nos acercará a una IA general.

En el **sector de la defensa**, el uso de la IA ha alcanzado un interés comparativamente mayor porque detrás de su adopción se encuentra la capacidad de mantener la **supremacía militar** entre las grandes potencias, inmersas en una carrera por lograr la ventaja competitiva deseada a través del despliegue de la IA. Este interés se sustenta en las ventajas que se pueden obtener al introducir la IA en múltiples sistemas militares como son los de mando y control multidominio, la guerra electrónica, la gestión inteligente de la nube de combate, las comunicaciones militares encriptadas, el proceso de diseño basado en datos de todas las plataformas militares, las constelaciones de satélites de órbita baja o en los sistemas de armas autónomas o semiautónomas letales, por nombrar algunos de los más relevantes.

Ya ha comenzado a producirse una transición hacia el llamado **"campo de batalla inteligente"**. En este nuevo marco, la superioridad en combate se consigue a través de la sinergia obtenida de la generación e integración masiva de datos en tiempo real (basados en un **campo de batalla progresivamente "transparente"** con millones de sensores en el que el movimiento de tropas y equipos es difícil de ocultar) y la aplicación de **algoritmos basados en IA para la toma de decisiones.** Este proceso se operacionaliza con la difusión de sistemas ligeros de mando y control, y el despliegue de múltiples vehículos con funcionamiento autónomo o semiautónomo que trabajan aisladamente o en enjambres.

Como sucede en todos los períodos históricos dominados por inestabilidades militares relevantes, el desarrollo tecnológico se está acelerando; en este contexto**, la transición al campo de batalla inteligente es imparable** y su expansión transformará la naturaleza del conflicto militar. Con el tiempo, este proceso se expandirá a todos los ejércitos y se superpondrá tanto en los campos de batalla convencionales como en los digitales, **cambiando profundamente la planificación, las tácticas y las operaciones militares**.

Relevancia geopolítica de la IA

Un factor adicional al puramente tecnológico que otorga a la IA una especial relevancia en relación con la defensa es su **dimensión geopolítica**. En la actualidad, la batalla entre las grandes potencias por el dominio de las tecnologías emergentes, de las que la IA se ha convertido en una tecnología habilitadora fundamental, se basa en un doble conjunto de intereses geopolíticos:

1. La necesidad de **acelerar el uso de la tecnología de IA** para el desarrollo de sistemas más avanzados que logren una **mayor competitividad** y, con ello, la **supremacía en los mercados internacionales** de productos y servicios tecnológicos, incluyendo el control inteligente de las rutas comerciales y de las infraestructuras de comunicaciones .

2. **Impedir que las potencias opositoras tengan acceso a tecnologías avanzadas de IA** que puedan utilizarse para debilitar la posición propia, ya sea en mercados civiles o militares, mediante el establecimiento de restricciones a la exportación y sanciones sobre componentes, sistemas o herramientas (por ejemplo, para el diseño o la fabricación) necesarios para el acceso o el desarrollo de sistemas basados en IA; todos ellas, medidas impulsadas por decisiones unilaterales o multilaterales.

Ambos elementos se combinan en el **enfrentamiento tecnológico entre Estados Unidos y China**, exacerbado en el campo de la tecnología de semiconductores y la IA, que, a su vez, depende en gran medida del uso de circuitos integrados específicos para obtener un mayor rendimiento. La dimensión geopolítica de la IA ha adquirido relevancia global con **impactos relevantes en terceros países** que se convirtieron en actores clave de la

cadena de valor de la IA, como la UE, el Reino Unido, Taiwán, Japón, Corea del Sur, India, Israel, Canadá, Australia, Rusia y otros; y, por supuesto, también impacta, como usuarios de sistemas basados en IA, en todos los países del mundo. Por estas razones, **la adopción de la IA en defensa se ha considerado una prioridad para las potencias militares**, con aumentos significativos en los presupuestos asignados al desarrollo y la adquisición de soluciones de IA.

La **UE**, anclada al bloque occidental y, desde el punto de vista de la defensa, muy dependiente hasta ahora de la **OTAN**, se encuentra constreñida en un proceso de globalización en el que **ha dejado de ser líder en muchos ámbitos tecnológicos**. Por ello, la UE era plenamente consciente desde 2020 de la **necesidad de aumentar su nivel de soberanía tecnológica** como parte de su estrategia política a largo plazo para lograr una mayor autonomía estratégica en muchos ámbitos, como la defensa y la seguridad.

Desde la perspectiva de la UE, **la soberanía tecnológica se ha convertido en un elemento facilitador clave 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 áreas estratégicas clave y de cooperar con los socios cuando sea necesario"*.

La figura 3 representa esquemáticamente este **papel facilitador de la soberanía tecnológica** basada en la capacidad de asegurar el suministro de productos críticos (como sucede con las tierras raras para múltiples productos electrónicos), la capacidad de fabricar componentes y sistemas (como son los dispositivos semiconductores) y el acceso al conocimiento tecnológico de doble uso. Desde el punto de vista tecnológico, la tecnología digital está jugando un papel cada vez más importante en todos ellos.

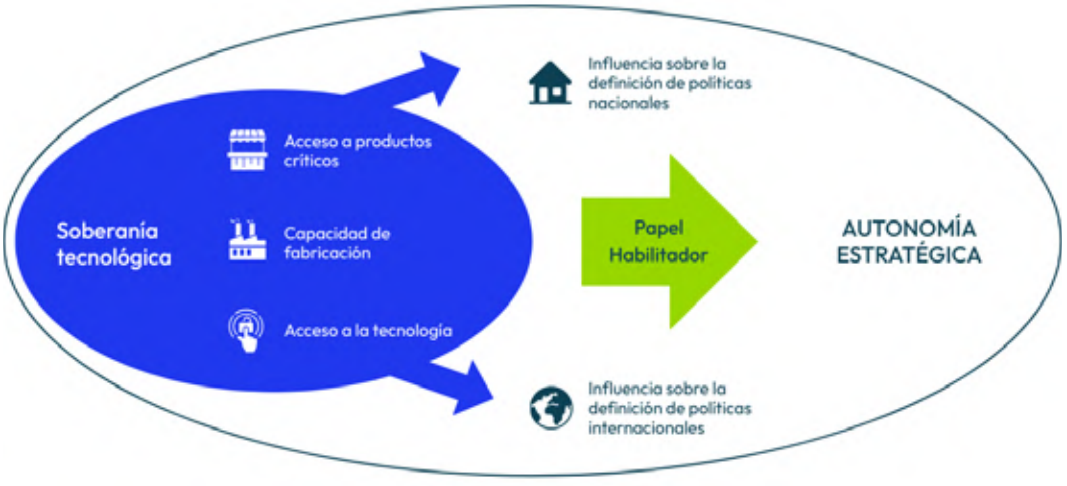


Figura 3. Relación entre autonomía estratégica y soberanía tecnológica. Fuente: León (2024)

La UE, en función de la posición de dominio desde el punto de vista tecnológico que tenga en un momento dado en algunas tecnologías clave, ha desarrollado **políticas públicas** específicas dentro de la UE y en el ámbito internacional complementadas con otras en sus Estados miembros, con el objetivo de **mejorar su soberanía tecnológica** y reducir la brecha existente con los países líderes.

Sin embargo, **no es posible que la UE obtenga plena soberanía tecnológica en el ámbito de la IA**, especialmente si se quiere profundizar la acción de la UE en un marco de relaciones multilaterales en el que la IA se integrará en múltiples productos manufacturados en los que se basa la capacidad de exportación de la Unión. Sin garantizar el acceso a componentes específicos de IA que Europa no fabrica o con restricciones de los proveedores para su integración y exportación a terceros países, **la UE tiene una soberanía tecnológica limitada en IA.**

Esta débil posición de partida de la UE también se refleja en los **mercados militares**, donde la dependencia tecnológica europea, como pone de manifiesto el caso de los semiconductores para IA y la prestación de servicios de IA basados en plataformas digitales para la toma de decisiones (por ejemplo, en sistemas de mando y control), plantea un reto urgente que debe abordarse con recursos adicionales y voluntad política sostenida. Hay que tener en cuenta que, en este campo, los proveedores también imponen algunas **limitaciones al uso futuro de los sistemas militares adquiridos**, como se ha demostrado fehacientemente en la guerra de Ucrania.

El ámbito civil y el de defensa se entrelazan en múltiples aplicaciones tecnológicas en las que las **características duales** emergen como factores clave de su evolución. De hecho, esta situación se concreta en el caso de la IA con el uso de grandes modelos de lenguaje (LLM), chips de IA, generación de contenidos multimedia o herramientas para la generación de datos sintéticos que, aunque inicialmente se desarrollaron para mercados civiles, se utilizan cada vez más en el sector de la defensa embebidos en productos militares avanzados. Esta adopción podría implicar la necesidad de algunas **adaptaciones o procesos de ajuste para cumplir con los requisitos militares y controlar los riesgos potenciales relacionados con su uso**.

Una consecuencia directa de este hecho es la influencia que ha tenido en los gobiernos la definición de **estrategias de acceso impuestas a otros países** para el uso y control de tecnologías como la IA en los mercados civiles. Los casos de China y Estados Unidos muestran la tendencia a fortalecer el control de la transferencia de tecnología entre las esferas civil y militar, incluso cuando se apliquen enfoques diferentes en cada uno de esos países.

En los *Estados Unidos*, el objetivo de la **integración civil-militar** es aumentar la cooperación entre el gobierno de los Estados Unidos y las empresas de tecnología en las operaciones de investigación y desarrollo (I+D), fabricación y mantenimiento. El enfoque elegido se ha

basado en grandes licitaciones en contratos de defensa para el suministro de sistemas o plataformas de armas innovadoras, o en proyectos de investigación disruptivos de menor envergadura financiados por agencias como ***DARPA*** (*Advanced Defence Research Projects Agency*), en los que también se busca la participación de universidades y centros de investigación como parte de un ecosistema de defensa complejo. Además, la existencia de una **red de laboratorios nacionales** financiados directamente por el presupuesto federal de los Estados Unidos permite el desarrollo de proyectos avanzados de defensa en tecnologías emergentes con un alto grado de confidencialidad.

Por otro lado, *China*, en el contexto de un plan orientado y dirigido por el gobierno, pasó en los últimos años del concepto de **"*integración civil-militar*"** a la ***"fusión civil-militar"*** con la creación de la *Comisión Central para el Desarrollo de la Fusión Civil-Militar (MCF*) en enero de 2017. Actualmente, China está impulsando activamente la integración de la IA en su estrategia militar como un **habilitador crítico de la futura guerra "inteligente"**. No es fácil evaluar hasta qué punto el sistema de control de la información utilizado por el gobierno chino influirá en la capacidad de entrenar sus sistemas de IA. En todo caso, las diversas restricciones a la exportación de importaciones de alta tecnología de doble uso a China (como los semiconductores o algunas herramientas software) pueden ralentizar, pero no detener, el desarrollo de la IA militar, al impulsar el desarrollo de sistemas propios.

A medida que se intensifica la **competición entre Estados Unidos y China**, existe un **riesgo creciente de que las armas habilitadas por la incorporación de la IA proliferen sin un enfoque regulatorio común o un consenso sobre su uso** mediante la participación de muchos otros países en su desarrollo y uso.

En 2025 han surgido varios **acontecimientos geopolíticos** de relieve que pueden afectar al **uso de la IA en defensa en el contexto europeo**:

- El impacto de una **guerra arancelaria provocada por *Estados Unidos*** y respondida por otros países, incluida la UE, sobre multitud de productos, tanto materias primas como productos tecnológicos, con cambios continuos en los porcentajes propuestos o aplicados, generando incertidumbres y perturbando el comercio mundial.

- La posición de Estados Unidos con su **oposición a la regulación digital europea** y, expresamente, a la regulación de la IA que impone condiciones a las empresas estadounidenses en su operación en la UE. Posición, en parte compartidas por empresas europeas que conlleva la ralentización de su puesta en marcha.

- Un **cambio unilateral en la actitud de Estados Unidos de apoyar a Ucrania en su defensa de Rusia sin contar con la UE**; situación que, desde una perspectiva tecnológica, ha llevado a amenazas de impedir el uso de tecnologías esenciales para alimentar la

inteligencia del ejército ucraniano o el despliegue de armas necesarias para defenderse de ataques aéreos.

- El objetivo de **búsqueda de una solución al conflicto de Gaza sin contar con la UE**, proporcionando a Israel armas sofisticadas o acelerar el desarrollo de otras con el posible distanciamiento de Estados Unidos con respecto a la posición ya existente de la UE. Las consecuencias del conflicto también han provocado en algunos Estados miembros de la Unión Europea la reducción de la cooperación militar con Israel.

- Acuerdo conseguido en la *Cumbre de la OTAN* de junio de 2025 para **aumentar los gastos de defensa hasta el 5% del PIB de los países miembros de la OTAN hasta 2035** (con un 3,5% destinado a capacidades militares y un 1,5% a infraestructuras y ciberseguridad y otros gastos relacionados indirectamente con la defensa) con una evaluación intermedia de la situación en 2029.

Ante estos acontecimientos, la **respuesta de la UE** se ha fundamentado en un amplio debate entre los Estados miembros para conciliar los deseos políticos y económicos con el nivel de riesgo existente, y ha derivado en la **adopción de diversas medidas** relacionadas con la defensa a un ritmo muy superior al que ha sido habitual en el pasado:

1. **Brújula estratégica para la competitividad**. En enero de 2025, la Comisión Europea presentó un documento marco para la mejora de la competitividad con una nueva hoja de ruta para recuperar 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**. En febrero de 2025, la Comisión Europea presentó la comunicación titulada *"El camino hacia el próximo marco financiero plurianual MFP"* con el objetivo de iniciar el debate para transformar el futuro presupuesto de la UE.
4. **Medidas para el rearme de la UE**. El 4 de marzo de 2025, el presidente de la Comisión Europea anunció el "*Plan Europeo de Rearme*" centrado en utilizar todas las palancas financieras disponibles para impulsar a los Estados miembros a aumentar rápida y significativamente el gasto en capacidades de defensa.
5. El 19 de marzo de 2025, la Comisión presentó el ***Libro Blanco sobre el futuro de la defensa europea / Preparación para 2030***, que dio lugar a un proceso de debate en profundidad sobre las prioridades y la financiación europeas en materia de defensa. El documento incluye las prioridades identificadas en los sistemas europeos de tecnología de defensa en los que deben concentrarse las inversiones adicionales. Se identificaron prioridades en la defensa aérea y antimisiles, los sistemas de artillería, incluidas las capacidades de ataque de precisión en profundidad, los drones de misiles y municiones y los sistemas

antidrones, los elementos de apoyo estratégico, incluso en relación con el espacio y la protección de infraestructuras críticas, la movilidad militar, el ciberespacio, la IA y la guerra electrónica.

6. La aprobación por parte del Consejo de la UE en mayo de 2025 del **Reglamento sobre medidas de seguridad para Europa (SAFE)** para recaudar hasta 150.000 millones de euros en los mercados de capitales. El objetivo previsto de SAFE no es solo facilitar el acceso a los recursos financieros, sino también reforzar e integrar el mercado europeo de la defensa. El Reglamento SAFE incluye la condición de que *"los contratos públicos conjuntos deben contener el requisito de que el coste de los componentes originarios de fuera de la Unión, según los Estados AELC del EEE, y Ucrania, no supere el 35 % del coste estimado de los componentes del producto final".*
7. El 17 de junio de 2025, la Comisión Europea adoptó el ***Ómnibus de Preparación para la Defensa***, un paquete integral destinado a establecer una mentalidad de preparación para la defensa en toda la Unión Europea con modificaciones en diversas regulaciones. Esta iniciativa pretende facilitar inversiones en defensa de hasta 800.000 millones de euros durante los próximos cuatro años, y permitir a los Estados miembros y a la industria responder con rapidez y eficacia a las crecientes amenazas.
8. El 10 de julio de 2025 se pudo acceder a los borradores de los **reglamentos del *Fondo de Competitividad* y de *Horizonte Europa*** para el periodo 2028-2034 en los que se consolida el interés en dotar de mayor peso al desarrollo de tecnologías duales.
9. Finalmente, el 16 de julio la Comisión Europea publicó su propuesta para el ***Marco financiero plurianual MFP 2028-2024*** que enmarcará el proceso de negociación presupuestaria en los próximos dos años entre el Consejo y el Parlamento Europeo.

Todas estas medidas producidas en pocos meses impulsan y son reflejo de la **voluntad política de la UE para crear el escenario de defensa necesario** para abordar los retos comunes de seguridad presentes y futuros, donde **la tecnología, y en concreto la IA, jugará un papel destacado**.

LA EVOLUCIÓN DE LA IA COMO UNA TECNOLOGÍA DE USO DUAL

Del dato al conocimiento

La **Comisión Europea ha definido los sistemas de IA** como *"sistemas de software (y a veces hardware) diseñados por humanos que, enfrentados a 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 no estructurados, razonando con conocimiento, procesando la información derivada de estos datos y decidiendo las mejores acciones a tomar para lograr el objetivo"*. En función de la complejidad de la tarea que resuelve la inteligencia artificial, la literatura distingue **tres tipos de inteligencias artificiales**: la **IA especializada**, la **IA general** y la **"singularidad"**.

Hoy en día, hay muchas ***inteligencias artificiales especializadas***, también conocidas como *IA estrecha o débil*, que son altamente efectivas para realizar tareas específicas. Estos sistemas pueden evolucionar y mejorar interactuando con otras IA especializadas. A través de procesos de interacción, agregación y negociación, avanzan gradualmente hacia la resolución de tareas cada vez más complejas. La ***Inteligencia Artificial General*** *(Artificial General Intelligence, AGI)*, también conocida como *IA fuerte*, sería capaz, si se consiguiera, de replicar una amplia gama de capacidades cognitivas humanas, como la resolución de tareas complicadas y heterogéneas, la planificación, el aprendizaje, el razonamiento o la capacidad de abstracción y generalización.

En los últimos años ha surgido el concepto de ***Inteligencia Artificial Generativa*** *(Generative Artificial Intelligence, GAI).* Se refiere a una tecnología que puede generar textos, imágenes, videos, programas informáticos, entre otros. Permite el desarrollo de sistemas de IA (o sistemas multiagente) que pueden colaborar para realizar tareas simples o complejas. En el nivel más avanzado se encuentra la **singularidad tecnológica**, que es la capacidad de un sistema de inteligencia artificial para generar otra inteligencia artificial mejor que la que ya existe.

En esta revolución, **la inteligencia artificial está y será acompañada por otras tecnologías habilitadoras**, como los dispositivos semiconductores, la Web y la Web 2.0, el internet de las cosas, el almacenamiento masivo de datos y la computación en la nube; las cadenas de bloques; la robótica, y el metaverso, que nos conducirá a una realidad híbrida, entre lo físico y lo virtual. Al mismo tiempo, la **integración de la IA con otras tecnologías emergentes** como la computación cuántica, la computación neuromórfica, la neurotecnología o los chips implantados en humanos para aumentar sus capacidades físicas, cognitivas y de comunicación con otros dispositivos también están contribuyendo a acelerar esta revolución tecnológica.

En este contexto, la **toma de decisiones en tiempo real requiere una interpretación compartida tanto de los datos como de los metadatos que se intercambian**. Los problemas de heterogeneidad aparecen en los protocolos de comunicación, la sintaxis de los datos y la semántica de los modelos, y causan problemas de interoperabilidad a la hora de intercambiar y compartir datos y tomar decisiones. Además, hay que tener en cuenta otros aspectos importantes, como la gobernanza de los datos, la duplicación de datos, las incoherencias de los datos, la falta de sesgo, los niveles de certeza, la granularidad de los datos y el lenguaje utilizado para representar los datos. Entran en juego las **dimensiones no técnicas**, incluidos los aspectos regulatorios relacionados con el cumplimiento, la propiedad intelectual y los derechos de acceso, y los marcos contractuales entre proveedores y clientes.

Un **marco de razonamiento** ampliamente utilizado para la conceptualización, la progresión de los datos brutos a una comprensión más profunda es la denominada **pirámide del conocimiento** (véase la figura 4).

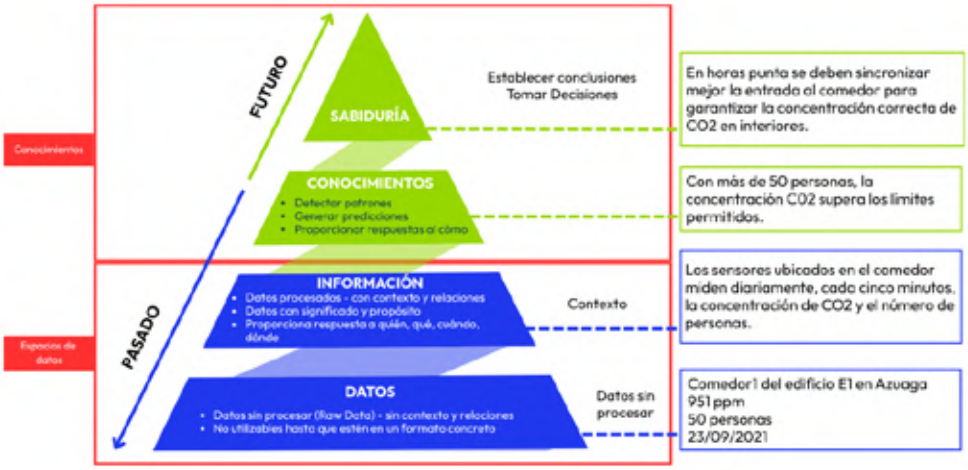


Figura 4. La pirámide del conocimiento: de los datos a la toma de decisiones. Fuente: Elaboración propia.

La **pirámide del conocimiento** ayuda a comprender cómo se adquiere, organiza, representa y procesa la información jerárquicamente, desde los niveles más básicos hasta los más complejos. Tiene **cuatro niveles**: **datos**, **información**, **conocimiento** y **sabiduría**. Cada nivel de la pirámide se construye sobre los anteriores, progresando desde los datos brutos hasta la toma de decisiones en el nivel superior. El ejemplo de la Figura 4 en $C0_2$ (derecha) muestra cómo los datos brutos se transforman progresivamente en conocimiento útil para la toma de decisiones.

Para aprender, razonar o tomar decisiones correctas de acuerdo con el marco regulatorio que sea adecuado en cada caso, es necesario analizar los procesos iterativos que componen la **cadena de valor del dato** que permite utilizar los datos para la toma de decisiones (véase Figura 5). Este enfoque está impulsando un proceso de **ingeniería basado en datos** en el que el uso de los **gemelos digitales** de los productos promete desarrollos con ciclos de vida más cortos y flexibles.

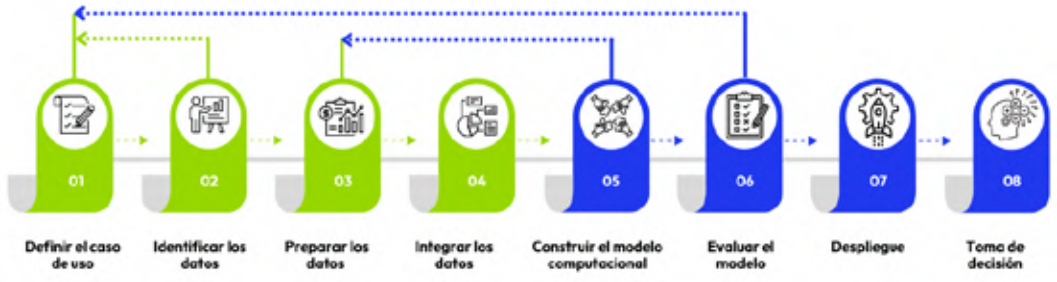


Figura 5. Cadena de valor basada en datos. Fuente: Elaboración propia.

El papel de los modelos

Es importante recordar que la evolución de la IA está estrechamente ligada a los avances en hardware y al crecimiento de los volúmenes de datos, y al desarrollo de modelos computacionales y algoritmos. **Los modelos computacionales son abstracciones del mundo físico o virtual,** y contienen el conocimiento esencial para que los sistemas de IA aprendan, razonen, tomen decisiones, adapten su comportamiento y proporcionen explicaciones trazables para esas decisiones.

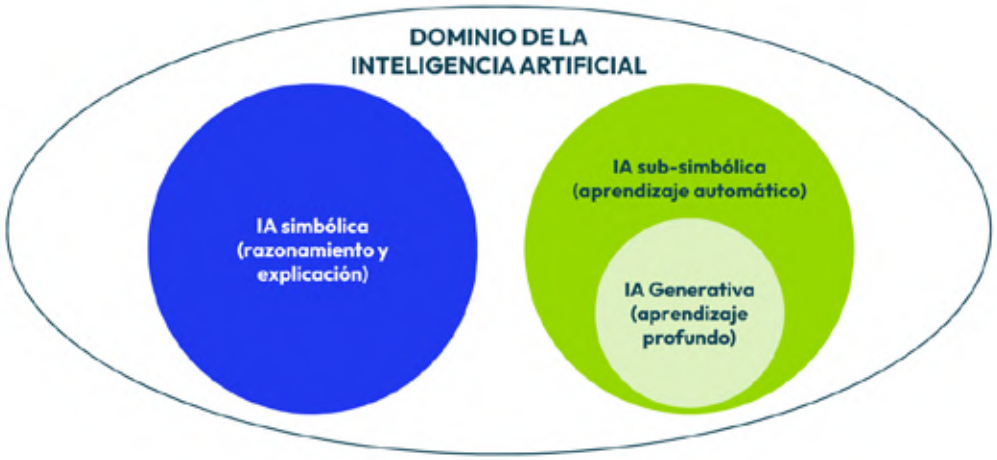


Figura 6. Principales áreas de la inteligencia artificial. Fuente: Gómez-Pérez (2024) https://raing.es/pdf/publicaciones/discursos_de_ingreso/Discurso_Ingenieria_Ontologica.pdf .

Los **modelos simbólicos** pertenecen al área de la IA centrada en la representación del conocimiento y el razonamiento. Se basan en el *álgebra de Boole* (1854) y en los principios de la lógica, que permiten a estos sistemas realizar razonamientos y proporcionar explicaciones de sus inferencias y deducciones. Durante el siglo XX, estas técnicas jugaron un papel clave en el desarrollo de los *sistemas expertos*. Frente a la escasez de datos y recursos informáticos, los ingenieros adquirieron conocimientos de expertos en la materia y documentos especializados.

Las **técnicas más utilizadas** son: lógica, reglas o heurísticas, taxonomías, ontologías y grafos de conocimiento. Estos enfoques se basan en símbolos para definir los conceptos clave y las relaciones entre ellos dentro de un dominio. Téngase en cuenta que los algoritmos infieren nuevos datos y conocimientos a partir de la información existente, específicamente a través de la inferencia deductiva para reducir las opciones de búsqueda. De esta manera, reducen efectivamente la explosión combinatoria en el espacio de búsqueda.

Las **técnicas de IA que aprenden y predicen nuevos conocimientos a partir de grandes conjuntos de datos** se encuentran en el área de la **IA subsimbólica**. Este campo tiene dos

ramas principales: una basada en la estadística, que genera patrones utilizando modelos probabilísticos comúnmente denominados **aprendizaje automático clásico** ("*machine learning*"), y otra inspirada en la estructura y función del cerebro conocida como **aprendizaje profundo** ("*deep learning*").

Las técnicas de **aprendizaje automático** generalmente se clasifican en función del tipo de problema que se aborda y la disponibilidad de **datos etiquetados**. El **aprendizaje supervisado** implica el entrenamiento con datos etiquetados, mientras que el **aprendizaje no supervisado** funciona sin datos etiquetados. Además, en situaciones en las que los modelos deben actualizarse con frecuencia durante el funcionamiento en función de su estado actual y sus posibles acciones, se utilizan técnicas de **aprendizaje por refuerzo**.

El **aprendizaje profundo** es una rama del aprendizaje automático que utiliza redes neuronales artificiales con muchas capas (llamadas *redes neuronales profundas*) para aprender automáticamente patrones con miles de millones de parámetros a partir de grandes conjuntos de datos. El aprendizaje profundo desempeña un papel crucial en los modelos modernos de IA.

La **IA generativa se basa en el aprendizaje profundo**. A diferencia del aprendizaje automático tradicional, que a menudo requiere la extracción manual de características, las nuevas arquitecturas y algoritmos han sido "alimentados" con volúmenes masivos de datos, lo que les permite **descubrir automáticamente patrones, características y relaciones complejas**. Esta capacidad ha mejorado significativamente su rendimiento en tareas como la comprensión y generación del lenguaje humano, imágenes, videos, música, programas informáticos, entre otros.

Un gran avance en esta evolución fue la introducción de la **arquitectura "Transformer"**, que introdujo dos conceptos clave: **tokens** y **atención.** Los **tokens** representan la unidad mínima de significado, mientras que el **mecanismo de atención** relaciona todas las palabras en una secuencia. Juntas, estas innovaciones revolucionaron el procesamiento del lenguaje natural al permitir la creación de potentes modelos lingüísticos mediante la captura de patrones y relaciones contextuales dentro de los textos. El tamaño de los modelos de lenguaje se mide por el número de **parámetros** (variables de ajuste en las redes neuronales a las que se puede dar un peso). Los modelos de lenguaje, en versiones más avanzadas, han dado lugar a los **Grandes Modelos de Lenguaje (LLM),** los **Modelos de Difusión**, los **Modelos Fundacionales**, los **Modelos de Lenguaje Pequeño**, los **Modelos Cuantizados** y los **Modelos Destilados.** La mayoría de los modelos fundamentales son abiertos y se pueden descargar desde *Hugging Face*.

La **ingeniería de sugerencias** ("*prompt engineering"*) es la técnica utilizada para guiar un modelo de lenguaje hacia la generación de la respuesta deseada. Para producir respuestas confiables y precisas, las indicaciones deben elaborarse y diseñarse cuidadosamente. Sin embargo, los modelos pueden producen ***alucinaciones*** que disminuyen

la credibilidad de las respuestas. Las alucinaciones son respuestas inventadas, errores fácticos, respuestas incoherentes, entre otras. Para solucionar este problema, **las técnicas de generación aumentada de recuperación mejoran el rendimiento del modelo con contexto adicional** más allá de sus datos de entrenamiento originales. Al recuperar información relevante de fuentes externas, el modelo puede mejorar la precisión y la credibilidad de sus resultados.

Además de las alucinaciones, otro desafío crítico en el modelo de lenguaje es el ***sesgo***. **El sesgo se refiere a la presencia de patrones injustos, desequilibrados o prejuiciosos en la respuesta de un modelo que es causada por la presencia de estereotipos o desigualdades en los datos de entrenamiento** relacionados con el género, la raza, la cultura o la política, entre otros. Abordar el problema del sesgo requiere la curación de datos y una evaluación continua para detectarlos en una etapa temprana, lo que ayuda a prevenir resultados y decisiones perjudiciales que podrían tener un impacto negativo en individuos o grupos. Es bien sabido que algunos sesgos de género y raza son necesarios, hasta cierto punto, 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.**

En los últimos años, ha aparecido el **enfoque neurosimbólico**, que **combina la IA simbólica con la IA generativa** inyectando conocimiento de ontologías y grafos de conocimiento en LLM preentrenados. Los **grafos de conocimiento de datos fácticos estructurados** se pueden aprovechar para entrenar y validar la veracidad de los textos generados, reducir las alucinaciones y proporcionar transparencia al rastrear la fuente de las respuestas. El **ajuste fino de los LLM con grafos de conocimiento** ayuda a reducir el sesgo y mejora la precisión en dominios específicos.

En todo caso, esto implica que **el proceso de construir modelos no solo es caro, sino también arriesgado.** En el caso de**l** uso de la IA generativa en defensa, algunas preguntas son cruciales para **poder adoptarlas de manera generalizada**: ¿Sería posible que un ejército comprara un modelo de decisión entrenado en otro país, amigo o neutral, sin poder estar seguro de las condiciones y el conjunto de datos con los que ha sido entrenado? ¿Es posible asegurarse de que el modelo no tenga puertas traseras?

La necesidad de responder a estas preguntas ha motivado la puesta en marcha de **varios proyectos para adaptar los LLM, las técnicas de sugerencias (*prompts*) y las herramientas de IA generativa** para hacer frente a las necesidades en el ámbito de defensa.

Hardware/Chips de IA para defensa

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 por un proceso específico**, expresado en nanómetros. Este parámetro define aspectos clave

como la frecuencia de funcionamiento, la densidad por 2 milímetros, el rendimiento de la oblea y el consumo de energía. Esta no es una medida física exacta, pero **se utiliza para distinguir entre diferentes generaciones de chips.**

La **reducción del tamaño de los dispositivos** permite que muchos más dispositivos (circuitos más complejos, sistemas verdaderos) se integren en la misma área, por lo que a medida que disminuye el tamaño del nodo, el coste de diseño del chip aumenta, no linealmente. Sin embargo, los costes de fabricación de los prototipos son más elevados porque la amortización de los equipos y el coste de las mascarillas (procesos más complejos y de menor dimensión) son mayores. La Figura 7 (derecha) muestra el **aumento del coste del diseño de chips** (ingeniería de diseño más fabricación, encapsulación y pruebas de prototipos).

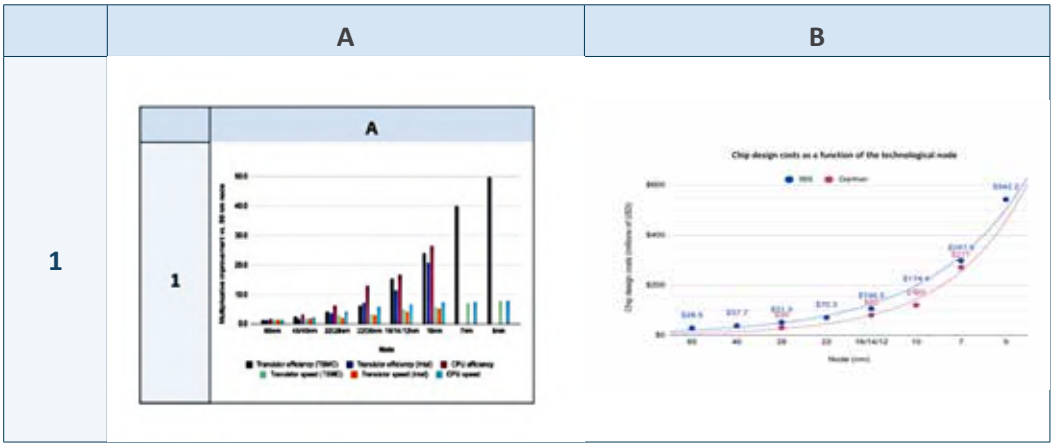


Figura 7 (izquierda.) Eficiencia y velocidad en comparación con el nodo de 90 nm; (derecha) Coste de diseñar un chip basado en el nodo tecnológico. Fuente: Khan y Mann (2020) https://cset.georgetown.edu/wp-content/uploads/AI-Chips%E2%80%94What-They-Are-and-Why-They-Matter-1.pdf

El *IEEE Rebooting Computing Initiative's International Roadmap for Devices and Systems (IRDS*) define las tendencias clave en la tecnología de semiconductores (véase la figura 8). Lo hace a través de tres **enfoques complementarios**: "*More Moore"* impulsa el escalado convencional, "*More than Moore"* integra nuevas funcionalidades y "*Beyond CMOS"* investiga futuros reemplazos para las tecnologías informáticas tradicionales. Obsérvese la importancia adquirida de los sistemas en chip (*System-on-Chip, SoC*) en diferentes nodos tecnológicos, y los sistemas en un único empaquetamiento (*System-in-Package, SiP*) para diferentes tipos de chips.

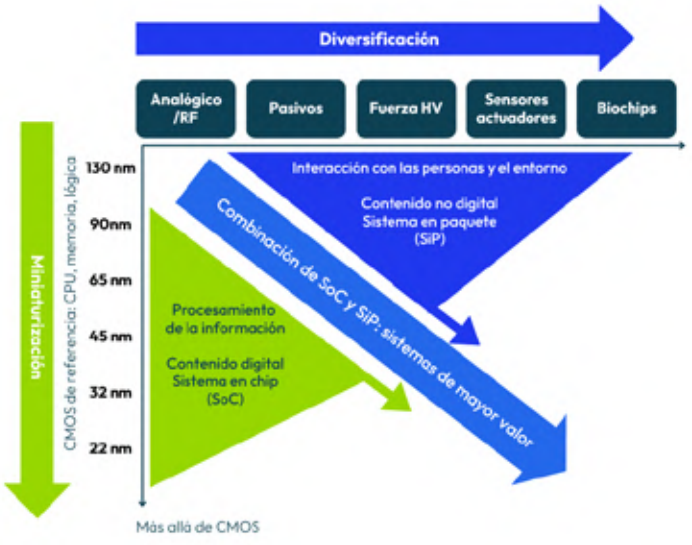


Figura 8. Hoja de ruta para sistemas integrados Fuente: IRDS (2023) https://irds.ieee.org/images/files/pdf/2023/2023IRDS_BC.pdf

Chips para aplicaciones de defensa

Los **requisitos que deben cumplir los chips para su uso en defensa** son más exigentes que los de uso civil. Entre sus características se encuentran:

- **Rango de temperatura y tolerancia ambiental:** la temperatura de funcionamiento puede variar entre -55ºC y +125ºC (a veces hasta +200ºC), mientras que las de uso civil suelen funcionar entre 0 y 70ºC. Deben ser resistentes a golpes y vibraciones en condiciones extremas. Deben protegerse contra la humedad y la corrosión de la niebla salina.

- **Fiabilidad y longevidad**: Tasa de fallos muy baja en sistemas de misión crítica. La vida útil debe ser de 15 a 30 años.

- **Seguridad y anti-manipulación**: deben contar con sistemas de arranque seguros, mecanismos de autodestrucción y encriptación de hardware. Deben contar con protección electromagnética (EMI/EMC). Su cadena de suministro debe ser segura con un seguimiento estricto, a menudo, integrado en “fábricas seguras”.

- **Endurecimiento por radiación (*rad-hard*):** diseñado para resistir rayos gamma, rayos cósmicos y bombardeo de neutrones. Tolerancia a dosis ionizantes totales entre 100 Krad y 1Mrad.

- **Proceso de fabricación y materiales**: Los nodos tecnológicos son más grandes que los de los chips comerciales en cuanto a robustez (90 nm, 120 nm, 180 nm). Los nodos muy pequeños (5 nm) son muy sensibles a la radiación, por lo que no cumplen con los requi-

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

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

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. Ejemplos de doble uso son los chips utilizados en las antenas 5G o los radares de los coches; procesadores de alto rendimiento que se utilizan en centros de datos para el entrenamiento de IA y en simulaciones militares o criptografía avanzada; un chip de IA utilizado en un teléfono inteligente puede ser el mismo que se utiliza en los sistemas de reconocimiento de imágenes de los drones militares.

El GaN se ha utilizado desde hace algunos años en chips de defensa por sus propiedades de alta movilidad de electrones y velocidad de saturación, que permiten el desarrollo de dispositivos de alta frecuencia. Funcionan a altos voltajes sin comprometer el rendimiento en aplicaciones de alta potencia. También disipan el calor de manera efectiva y pueden ofrecer salidas de alta potencia en espacios físicos pequeños. Las **principales aplicaciones** actuales son: 1) Sistemas de guiado 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, comunicación en la banda W de 75-110 GHz); 5) Armas de energía dirigida (las ondas milimétricas de alta potencia se pueden utilizar como armas para desactivar dispositivos electrónicos enemigos).

Tipos de chips para su uso en IA

Los chips de IA se definen como **procesadores de datos de alta eficiencia y velocidad** que son los adecuados para **entrenar o inferir respuestas de modelos de IA**. Pueden manejar operaciones con matrices multidimensionales (llamadas tensores) a gran escala mediante el uso de computación paralela desde modelos de IA (redes neuronales, aprendizaje profundo y transformadores). Dependiendo de su construcción, los chips de IA se pueden clasificar en *Unidades de Procesamiento Gráfico* (GPU); *Matrices de puertas programables en campo* (FPGA); y *Circuitos Integrados de Aplicación Específica* (ASIC), que incluyen aceleradores de IA, circuitos neuromórficos y Memoria de Inteligencia Artificial en Computación (AIMC). La Figura 9 muestra estas relaciones entre los diferentes tipos de chips de IA.

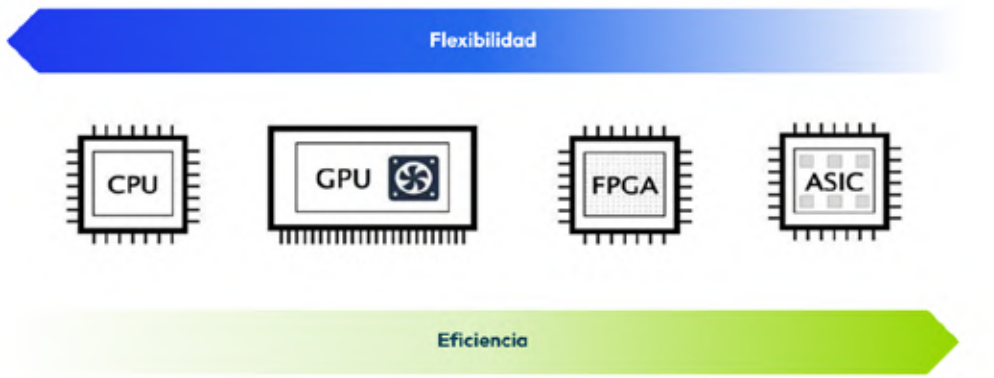


Figura 9. Clasificación general de los chips de IA según su construcción. De izquierda a derecha, aumentan su eficiencia energética; De derecha a izquierda aumenta tu flexibilidad.
Fuente: Li (2023). https://doi.org/10.54097/kvs7yr94

La GPU es un chip procesador de imágenes que muestra la información que se va a mostrar, proporciona señales de escaneo a la pantalla y la controla. La intención original del diseño de la GPU era abordar la necesidad de **computación paralela a gran escala en el procesamiento de imágenes**. Se utiliza en la fase de entrenamiento de los modelos de IA. Además, su estructura de hardware no se puede configurar de manera flexible, ya que es fija; y ejecutar un algoritmo es menos eficiente en una GPU que en una FPGA, por ejemplo.

Las GPU son el tipo de chip de IA predominante en los centros de datos de IA en la nube, aunque cada vez se utilizan más combinaciones de CPU con **aceleradores de IA** (chips con arquitecturas ASIC especializadas). Las GPU más extendidas hoy en día son las de la empresa *Nvidia*. La mayoría de los centros de datos en la nube albergan el H100 y el H200. En 2025 se comenzará a instalar el B200, mejorando sustancialmente las prestaciones del H100. La plataforma software denominada CUDA ayuda a los desarrolladores a utilizar los numerosos núcleos de una GPU Nvidia.

Un ASIC es un chip optimizado y personalizado para una aplicación específica. Los ASIC para tareas específicas de IA logran un mejor rendimiento y eficiencia energética en comparación con las GPU y las CPU. Tanto los ASIC como los FPGA implican ciclos de diseño largos y costosos, pero los ASIC han optimizado el hardware, a costa de perder flexibilidad para implementar cambios. **Están especializados en la implementación y ejecución de modelos de aprendizaje automático entrenados**, lo que permite predicciones y toma de decisiones en tiempo real en múltiples aplicaciones. Es decir, procesan de manera eficiente los datos de entrada a través de modelos de IA para generar predicciones rápidas y confiables: son adecuados para inferencias. Los chips dedicados (ASIC) son más eficientes que las GPU, lo que deja a las GPU para el entrenamiento con grandes cantidades de datos. Se estima que **para 2030 la solución más extendida será una arquitectura de chip especializada (ASIC) y FPGA con un rendimiento óptimo para tareas específicas de IA.**

Además de los requisitos militares para los equipos de procesamiento en el borde ("*edge computing*"), existe la **necesidad de poder realizar inferencias localmente** (en algunos casos, muy pocos, también entrenamiento), con latencias mínimas y poco acceso a la red (intermitente o desconectado). Para que sea posible la inferencia en el borde, los modelos deben haberse optimizado para dispositivos con recursos limitados. El mayor reto al que se enfrentan los chips de IA en dispositivos en el borde es el **consumo de energía**. Estos chips suelen estar alimentados por pilas muy pequeñas (*pilas de botón*) y además deben tener una duración significativa, ya que no es fácil sustituirlas porque se suelen encontrar en entornos de difícil acceso.

Proyectos de financiación pública para chips de IA en el sector de la defensa

Diversos países tecnológicamente avanzados, a través de sus agencias de investigación militar han iniciado proyectos para desarrollar chips adaptados a los requisitos del sector de la defensa. En el caso de Estados Unidos, **DARPA** (*Defense Advanced Research Projects Agency*) gestiona varios programas de **desarrollo de chips de IA para defensa**:

- **CHIPS_Programme** (*Common Heterogeneous Integration and IP Reuse Strategies*) busca crear un ecosistema de bloques de propiedad intelectual modulares y reutilizables (propiedad intelectual, IP), que puedan integrarse en sistemas utilizando tecnologías de integración existentes y emergentes, facilitando diseños de circuitos integrados más flexibles y reduciendo los costos y tiempos de desarrollo.

- **IDEA Programme** (*Intelligent Electronic Assets*) pretende 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. Su objetivo es acelerar el desarrollo de sistemas electrónicos de próxima generación y reducir la dependencia de grandes equipos de diseño especializados.

- **DARPA.MIL SAHARA Programme** (*Structured Array Hardware for Automatically Realized Applications*) tiene como objetivo ampliar el acceso a las capacidades de fabricación de Estdos Unidos para abordar los desafíos en el desarrollo seguro de chips personalizados para sistemas de defensa. El programa busca automatizar la conversión de diseños de FPGA a ASIC estructurados, mejorando el rendimiento y reduciendo el consumo de energía en aplicaciones militares.

La Comisión Europea y las Agencias Europeas, a través del **Fondo Europeo de Defensa (FED)**, así como la **Agencia Europea de Defensa (EDA)**, han lanzado convocatorias para proyectos de investigación y desarrollo en microelectrónica y semiconductores, buscando reforzar la autonomía tecnológica europea en sectores clave como la defensa y el espacio. Además, en Europa, la **Agencia Espacial Europea (ESA)** financia proyectos destinados a desarrollar componentes semiconductores capaces de operar en entornos espaciales extremos, incluyendo la resistencia a la radiación y a las temperaturas extremas.

LA DIMENSIÓN SOCIO-ECONÓMICA DE IA EN DEFENSA

Mercado de IA militar

La relevancia del uso de la IA en el sector de la defensa proviene de que no solo transforma la estrategia militar y de seguridad, sino que también **impulsa el desarrollo económico e industrial**. La integración de la IA en los sistemas de defensa genera un ecosistema de innovación donde convergen las industrias tecnológica, aeroespacial y de ciberseguridad, fortaleciendo la soberanía tecnológica y reduciendo la dependencia de proveedores externos. Además, la inversión en IA para la defensa estimula la creación de puestos de trabajo altamente cualificados en sectores clave como la ingeniería de software, la robótica y el análisis de datos. Asimismo, mejora la competitividad de las empresas en el mercado global, promoviendo la exportación de soluciones avanzadas en seguridad y tecnología civil-militar de doble uso.

El **impacto socioeconómico de la IA** depende de tres componentes clave: **software**, **hardware** y **servicios**. El desarrollo de software (50% del mercado) estimula la creación de empleo especializado en áreas como el análisis de datos y la programación avanzada, mientras que la fabricación de hardware impulsa las industrias tecnológicas e incrementa la demanda de componentes de alta tecnología, beneficiando a las economías locales e internacionales. Por otro lado, los servicios asociados generan nuevas oportunidades económicas en consultoría estratégica, capacitación y mantenimiento técnico, fortaleciendo así el mercado laboral y promoviendo una mayor inversión en innovación tecnológica.

El mercado de la IA militar está experimentando un crecimiento notable. Según *The Business Research Company*, ha crecido a una sólida CAGR del 16,72% desde 2019, alcanzando los 9.671 millones de dólares en 2024 y proyecta que alcanzará un valor de 19.740 millones en 2029, con una CAGR del 15,1%. *Precedence Research* (2024) estima que el mercado mundial de IA en el ejército fue de 9.560 millones de dólares de Estados Unidos en 2024, y que crecerá hasta 10.790 millones en 2025, estimando que alcanzará los 32.170 millones para 2034, con una tasa de crecimiento CAGR del 12.9% entre 2024 y 2034. Este crecimiento está impulsado por la mayor adopción de vehículos aéreos no tripulados (UAV), los programas de modernización militar y un aumento de los presupuestos de defensa a nivel mundial.

Mercados por región

Las **cuotas de mercado de IA militar por región** en 2023 revelan que América del Norte representó el 36%, **Europa el 30%,** Asia-Pacífico el 24%, América Latina el 6% y Oriente Medio y África el 4%. Europa, con un 30% en 2023, tiene un peso destacado, aunque el desarrollo y funcionamiento de sus sistemas puede depender de componentes, software y Propiedad Intelectual (PI) de otros países, principalmente de Estados Unidos en el ámbito

de la OTAN. La cuota de Europa también está creciendo de forma constante, lo que sugiere que los presupuestos de defensa incorporan **más capacidades impulsadas por la IA**.

En 2024, el **mercado combinado de las tres principales naciones europeas**, Reino Unido, Francia y Alemania, para la IA en defensa generó ingresos de 2.348,8 millones de dólares, según *Grand View Research*. Por segmento, **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 IA militar en Europa alcance unos ingresos previstos de 4.090 millones de dólares para 2030**. Es importante tener en cuenta que si los países de la UE siguen comprando grandes cantidades de sistemas y tecnologías –ya sea hardware, software o servicios– a proveedores no pertenecientes a la UE, la industria europea de defensa seguirá siendo más pequeña de lo deseable.

Un indicador relevante es la **publicación de patentes relacionadas con la IA en la industria aeroespacial y de defensa**. Desde 2020 (datos de *Global Data Patent Analytics*), Estados Unidos representó el 44%, seguido de China (37%) y Corea del Sur (7%). **El conjunto de la UE, el Reino Unido y Turquía solo representa el 5,4% de las patentes presentadas en este ámbito**.

No existe un indicador público unificado que refleje con precisión el volumen del **mercado de la IA en el sector militar en España, y con las de la ESA.** En 2024, el presupuesto de inversión en defensa de España fue de 13.100 millones de euros. No cabe duda de que la IA ya juega un papel importante en la industria de defensa española y en el mercado nacional. **Aplicando un factor conservador del 0,3%, se estima que la IA podría haber representado unos ingresos potenciales de más de 40 millones de euros en España**.

Según datos de la OTAN de 2021, **España estuvo presente en grandes programas en los que la IA juega un papel relevante**, como Aegis (AMD), Barracuda (UAV), BlueScan (ASW), Future Combat Air System (FCAS, plataforma aérea), Harpoon Block II (misiles), Patriot (AMD), RQ-11 RAVEN (UAV), SWORD (simulación), ScanEagle (plataforma aérea) o nEUROn (plataforma aérea).

El informe de 2025 de la *Oficina Nacional de Prospectiva y Estrategia* de la *Presidencia del Gobierno de España* destaca el proyecto **MPC16 del Ejército del Aire** para el mantenimiento predictivo de los aviones *Eurofighter*, el **Sistema Logístico Predictivo del Ejército (SILPE**), el **gemelo digital integrado en las fragatas F-110** o el **Módulo de Mantenimiento Predictivo Embarcado (MAPRE)** para buques de la Armada. Asimismo, el Ministerio de Defensa español 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 2024.

Además, el Ministerio de Defensa ha iniciado un **proceso estratégico para integrar los sistemas de IA en la toma de decisiones del Ejército, tanto a nivel técnico como operativo.** En 2024 se definieron las necesidades técnicas para investigar cómo automatizar este proceso utilizando la IA. Actualmente, la iniciativa se encuentra en una fase inicial.

Caracterización de la IA para el sector industrial de la defensa

La mayor parte de la industria de defensa de Europa se encuentra en sus estados miembros occidentales, especialmente en el Reino Unido, Francia, Alemania e Italia. Normalmente, **estos países apoyan las iniciativas industriales de defensa de la UE si creen que sus propias industrias se beneficiarán**. No hay ninguna empresa de defensa de la UE entre las 10 primeras del mundo por ingresos en 2022. Entre los 20 primeros se pueden contar tres empresas europeas, *Leonardo*, *Airbus* y *Thales.*

La **Base Industrial y Tecnológica de Defensa (BITD)** española contaba en 2021 con más de 520 empresas, aunque solo unas 350 ofrecían productos o servicios en el ámbito de la defensa. El número de empleos directos en defensa se situó en torno a los 22.000 empleos directos, y la facturación asociada fue de 6.300 millones de euros, lo que supuso el 15% de sus ventas totales (civiles y militares). Esta actividad tiene un efecto impulsor principalmente en los grandes programas de desarrollo de plataformas armamentísticas, especialmente para las empresas de nivel 1 y 2, pero también para otros subcontratistas y pymes de la cadena de suministro. Estas últimas categorías representan alrededor del 85% del total de empresas de la industria de defensa española. En términos de cuota de mercado, **el 1,5% de las empresas representan el 75% de todo el mercado** lo que indica una concentración muy elevada.

El **informe anual** de la *Dirección General de Armamento y Material del Ministerio de Defensa* español (2024) señala que en 2022 las ventas totales de la industria nacional de defensa fueron de 7.435 millones de euros, con ventas indirectas al Ministerio de Defensa español 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 se duplican. Aunque no existe una cifra oficial unificada, **se estima que la IA en defensa generó más de 40 millones de euros en 2024, lo que supone un 0,3% del presupuesto nacional de defensa**. La inversión está creciendo, impulsada por la transformación digital y la demanda de capacidades avanzadas.

Varias empresas españolas del sector de la defensa están incorporando soluciones de IA en sus proyectos y sistemas. En 2024 destacan *Indra, GMV, Airbus Defence and Space Spain, SENER, Expal, Tecnobit (Grupo Oesia), Amper, Swarming Technologies & Solutions (Grupo Zelenza), Escribano Mechanical & Engineering* M*ultiver*se Computing y Aertec. Importantes empresas multinacionales, a través de sus filiales y oficinas en España, contribuyen a la transferencia de tecnología, la innovación y la competitividad en el sector de la defensa, fortaleciendo tanto las capacidades locales como la colaboración internacional en proyectos estratégicos. Se mencionan los más relevantes:

- ***BAE Systems*** ha establecido una filial en España.
- ***Thales*** tiene una fuerte presencia en varias empresas.
- ***Leonardo*** participa activamente en programas aeroespaciales y de defensa.
- ***Lockheed Martin*** cuenta con oficinas y unidades de apoyo en España para gestionar proyectos y contratos con las Fuerzas Armadas y organismos gubernamentales.
- ***Boeing*** cuenta con un centro de desarrollo (Boeing Research & Technology Europe, BRTE).
- ***Raytheon Technologies*** está representada en España a través de filiales o unidades locales que permiten la integración y soporte de sistemas de defensa, como misiles y radares.
- ***Northrop*** opera con oficinas regionales que facilitan la coordinación de proyectos, el apoyo a contratos y la participación en iniciativas de colaboración con entidades locales.

El apoyo público a la I+D es una de las herramientas estratégicas para el desarrollo de una base tecnológica e industrial en la defensa. Cada país tiene un enfoque muy diferente a la hora de comparar el porcentaje de financiación pública destinada a I+D dedicado a la defensa, como se muestra en la Figura 10.

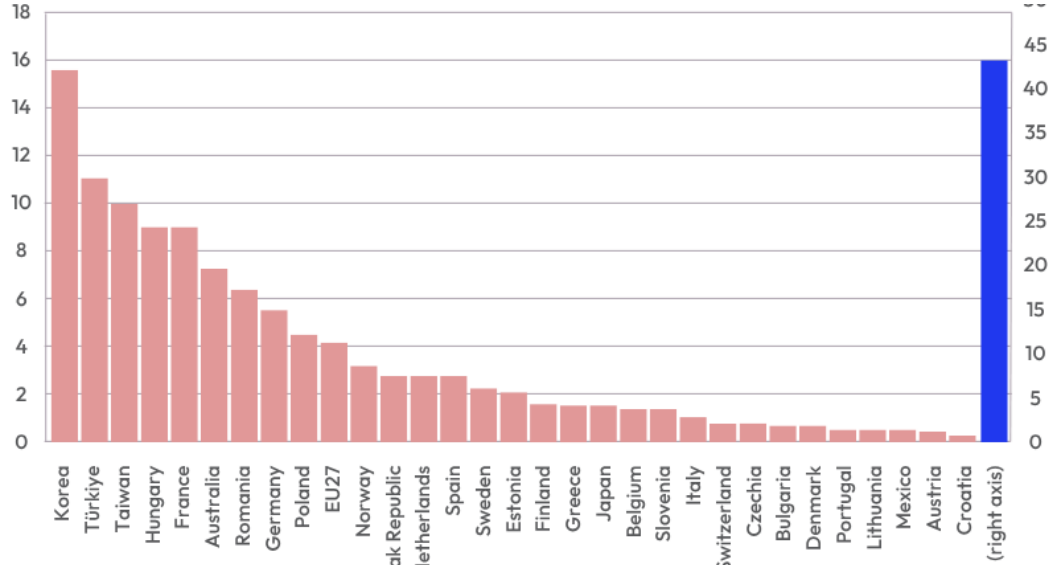


Figura 10. Financiación pública para investigación y desarrollo por país. Fuente: Bruegel (2024) https://www.bruegel.org/policy-brief/european-defence-industrial-strategy-hostile-world

Esta visión abarca el apoyo público a la IA. En Estados Unidos, el 95% de la financiación del gobierno federal para la IA se engloba bajo el título NAICS 54 (servicios profesionales, científicos y técnicos). **El 84% del valor total de la financiación en el marco del 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 manera totalmente direccional las inversiones masivas que ya realiza el sector privado en ese país.

Este patrón es similar al de **China**, donde las inversiones combinan el objetivo de satisfacer las necesidades estratégicas de seguridad al tiempo que impulsan la competitividad del sector industrial. China tiene, en concreto, una *Estrategia de IA para la Defensa y la Seguridad*.

La UE segmenta las inversiones entre instituciones comunitarias y nacionales (incluidas las regionales) y las menos alineadas con los objetivos de seguridad. Por lo tanto, los 1.000 millones de euros anuales declarados en 2018 podrían añadirse a importes comparables en algunos países individuales.

El **capital de riesgo (VC)** ha desempeñado un papel fundamental en el desarrollo y la expansión de la IA en los últimos años, permitiendo a miles de startups y emprendedores llevar la IA de los laboratorios de investigación a aplicaciones concretas. Estas inversiones han acelerado 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 rendimientos son inciertos a corto plazo. El gráfico de la figura 11 muestra la **evolución de la inversión de capital riesgo (VC) en tecnologías de IA por sector industrial**, de 2012 a 2024, sobre la base de datos de la OCDE de 2025.

Áreas como las del **gobierno**, la **defensa** y la **seguridad** han mantenido niveles considerablemente más bajos de inversión, lo que indica una menor prioridad para los inversores privados de capital riesgo en estos campos. El hecho de que se haya incrementado la inversión en seguridad digital e infraestructura computacional de IA es positivo para la defensa. Esta tendencia está cambiando, y **en los últimos dos años han aparecido en la UE nuevos fondos de capital riesgo centrados en la defensa,** con un flujo de acuerdos de inversión cada vez mayor en los Estados miembros.

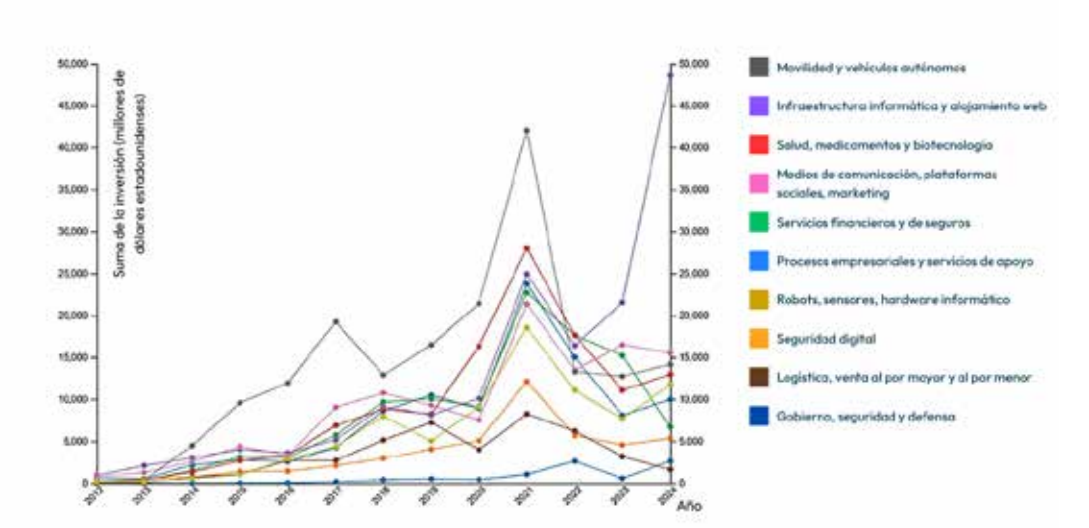


Figura 11. Inversiones de capital riesgo en IA.
Fuente: OCDE (2025): https://oecd.ai/en/data?selectedArea=investments-in-ai-and-data&selectedVisualization=vc-investments-in-ai-by-industry

I+D en IA para la defensa en Europa

El gasto colectivo en investigación y desarrollo en los sectores aeroespacial y de defensa, financiado tanto por la industria como por los gobiernos, alcanzó unos 23.400 millones de euros, según datos de ASD (2025). El **aumento de la asignación de fondos a iniciativas militares** (61% frente al 39% del sector civil) refleja las tendencias mundiales en la priorización de las capacidades de defensa y subraya la importancia de la innovación para mantener una ventaja competitiva y hacer frente a los desafíos cambiantes.

El **Fondo Europeo de Defensa** (*European Defence Fund, EDF)* es un instrumento de financiación gestionado y ejecutado por la Comisión Europea, dotado con 8.000 millones de euros para el periodo 2021-2027, de los que 2.700 millones se dirigen a actividades de investigación y 5.300 millones a desarrollo de sistemas de defensa.

La industria de defensa cuenta con el apoyo para investigación y Desarrollo tecnológico de la **Agencia Europea de Defensa** (EDA). Para garantizar la identificación de brechas tecnológicas y áreas de interés común para la cooperación, la *Agenda Estratégica General de Investigación* (OSRA) que es la herramienta de planificación de investigación y desarrollo de la EDA desarrollada junto con los Estados miembros proporciona una visión compartida de los retos técnicos prioritarios. Desde su creación en 2004, la EDA ha gestionado más de 25O proyectos de I+D, por valor de más de 1.000 millones de euros.

Según un estudio del Parlamento Europeo, los costes en el **ciclo de vida de los equipos de defensa** se dividen en un 10% para I+D, un 30-35% para la inversión (producción y aprovisionamiento) y un 55-60% para la operación, mantenimiento y eliminación, como se indica en la Figura 12. Obsérvese que el ***EDF*** *(European Defence Fund)* se complementa con el Reglamento ***ASAP*** *(Act in Support of Ammunition Production)* y el ***EDIRPA*** (*European defence industry reinforcement through common procurement act*) para apoyar las fases posteriores de los procesos de contratación.

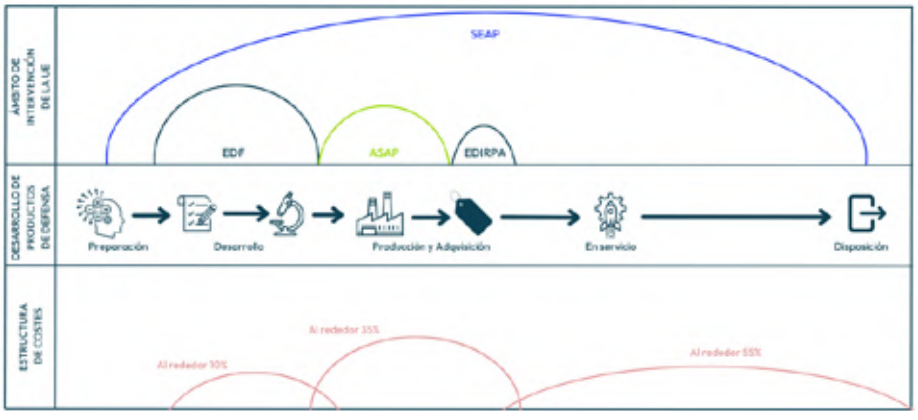


Figura 12. Herramientas y marcos de la UE para prestar apoyo en fases cruciales del ciclo de vida de los equipos de defensa. Fuente: Comisión Europea (2024) https://defence-industry-space.ec.europa.eu/document/download/f1e6ba44-4720-4f14-a991-a3a7f3afb475_en?filename=Staff%20Working%20Document%20on%20EDIP.PDF

Varias empresas españolas han sido importantes beneficiarias de la financiación del Fondo Europeo de Defensa (FED) en diversos proyectos. Estas empresas han participado en proyectos relacionados con la defensa hipersónica, la ciber resiliencia, los sistemas aeroespaciales y las capacidades navales, destacando el papel estratégico de España en el programa. 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.

La **Empresa Común SESAR 3 (SESAR 3 JU)** es una asociación institucional público-privada europea creada para llevar a cabo la transformación digital del tráfico aéreo en Europa (*Cielo Digital Europeo*). Debido a la guerra en Ucrania, SESAR ha iniciado actividades para integrar la gestión del espacio aéreo civil y militar. En el ámbito de los UAS existen sinergias tecnológicas en IA entre los programas SESAR y las aplicaciones militares de este tipo de vehículos aéreos.

En el contexto internacional, destaca el programa **DIANA (OTAN),** con una red de centros de ensayos en países de la Alianza Atlántica que cubrirán los proyectos aprobados en diferentes convocatorias a startups en áreas prioritarias relacionadas con tecnologías emergentes. Uno de ellos relacionado con la IA (*Neurotechnology and AI Test Centre*) se encuentra situado en la Universidad Politécnica de Madrid (UPM).

En España, el objetivo principal del programa **COINCIDENTE** (*Cooperación en Investigación Científica y Desarrollo en Tecnologías Estratégicas*) es aprovechar las tecnologías civiles desarrolladas en el ámbito del *Plan Nacional de Investigación y Desarrollo* para incorporar soluciones tecnológicas innovadoras de interés para el Ministerio de Defensa. En 2024 se añadió un área específica de la IA. La participación de las universidades (40% de los proyectos de investigación y desarrollo) es claramente visible, aunque esta presencia ha disminuido en los últimos años. Las pymes son relevantes en los proyectos de IA, aunque parece que en los últimos años están empezando a aparecer empresas medianas y grandes.

DIMENSIÓN TÁCTICA, OPERATIVA Y ESTRATÉGICA DEL USO DE LA IA EN DEFENSA

Desde esta dimensión se analizan **tres grandes temas** en los que la IA juega un papel esencial en la defensa: la **evolución hacia un campo de batalla inteligente**, el creciente uso de la IA en la llamada **guerra híbrida y cognitiva**, y la importancia de la IA en un dominio dual como es el **espacio**. En todos los temas mencionados, el uso de la IA está evolucionando rápidamente, por lo que se prestará atención a las razones de su progresiva adopción y a las barreras existentes que podrían limitar su uso.

El primero de los temas seleccionados, el **campo de batalla inteligente**, se centra en el papel que juega la IA para disponer de una visión integrada de la situación en el campo de batalla mediante la captura y análisis de datos empleados como base para la **toma de decisiones de forma autónoma o semiautónoma**. El análisis se centra en el uso de la IA en **sistemas de mando y control (C2),** la necesidad de gestionar sistemas integrados de comunicaciones a varios niveles centrados en el concepto de **nube táctica de combate**, y en el uso de **armas autónomas o semiautónomas** y su interacción con sistemas tripulados.

El segundo de los temas seleccionados aborda el **papel que juega la IA en la expansión de la guerra híbrida y cognitiva**. Se presta especial atención a la forma en que el uso de la IA se convirtió en un factor esencial en una gradación de intensidad que va de la amenaza híbrida al conflicto híbrido y, finalmente, a la **guerra híbrida** que combina acciones cinéticas, cibernéticas o de control de la información. También se pretende dar cuenta del creciente uso de la IA en la guerra cognitiva y, especialmente, de la importancia que ha adquirido en la **desinformación y la generación de narrativas** como factor esencial en las guerras híbridas y convencionales cuyo impacto es cada vez mayor.

Por último, con el tercero de los temas seleccionados, el **uso de la IA en el sector espacial de la defensa**, se aborda el uso de la IA en un **dominio eminentemente dual**, dado que muchas de sus plataformas (ya sean las de satélites individuales o formando parte de constelaciones) asumen funciones civiles y militares de comunicaciones, observación y navegación, con independencia de la necesidad de cargas útiles militares específicas y del desarrollo de armas antisatélite (tanto duras como blandas). Progresivamente, el espacio se convirtió en un dominio totalmente integrado junto con los dominios terrestre, marítimo, aéreo, cibernético y cognitivo en el marco del concepto de **operaciones multidominio** que se configura como un elemento clave del uso de la IA en operaciones militares.

Evolución hacia un campo de batalla inteligente

La introducción de sistemas tecnológicos avanzados en el campo de batalla para obtener la superioridad contra el enemigo ha sido una tendencia constante en la historia de la humanidad. Hacerlo a tiempo y de manera eficaz, mediante la adaptación de las tácticas y estrategias militares, si fuese necesario, constituye un **factor clave para el éxito de la incorporación de nuevas tecnologías de defensa** a lo largo del tiempo.

En cada momento histórico, el esfuerzo por poner a disposición de los ejércitos sistemas de combate basados en tecnologías avanzadas, capaces de superar las defensas del adversario, ha presionado a los bandos en conflicto a utilizar la tecnología más avanzada disponible, incluso, aceptando que puedan surgir algunos riesgos derivados de su relativa falta de madurez. En este contexto, **el campo de batalla se comporta como un laboratorio real de experimentación** para madurar sistemas tecnológicos y, en algunos casos, cumple un papel

clave para la difusión de múltiples sistemas civiles en la sociedad. En 2025, emergen tres **características principales** que merecen especial atención al introducir mayor complejidad:

1. **Despliegue más rápido** de la innovación tecnológica en armas y sistemas de defensa en el campo de batalla en comparación con casos históricos anteriores.
2. El **creciente uso de tecnologías duales**, la mayoría de ellas generadas en el ámbito civil y posteriormente adaptadas al ámbito militar para satisfacer necesidades específicas y urgentes.
3. La **necesidad de desplegar soportes automáticos** para la toma de decisiones o para la ejecución de acciones soportadas por algoritmos de IA integrados en sistemas tecnológicos interoperables muy complejos.

Los sistemas impulsados por IA están cambiando profundamente la forma en que se conciben e implementan las operaciones militares al mejorar la toma de decisiones, el conocimiento de la situación en el campo y la asignación dinámica de recursos. Desde el punto de vista técnico, las principales áreas de defensa en las que los sistemas de IA están teniendo un papel destacado son las siguientes:

- **Soluciones basadas en la gestión de grandes volúmenes de datos históricos y en tiempo real**. Por ejemplo, la IA se aplica a la logística y al mantenimiento predictivo para maximizar el uso de los recursos materiales.

- **Guerra Electrónica (EW).** Se refiere al uso de tecnologías digitales para interrumpir o inhabilitar los sistemas informáticos, las redes de comunicaciones y la infraestructura enemigas, mediante el lanzamiento de ciberataques inteligentes, la anticipación de amenazas y operaciones encubiertas.

- **Inteligencia, vigilancia y reconocimiento (ISR**): Implica el uso de sensores, drones, satélites y otras plataformas para recopilar y analizar datos sobre posiciones y movimientos de las fuerzas enemigas. Los sistemas impulsados por IA podrían analizar un gran volumen de datos y extraer conclusiones de datos imprecisos a una velocidad mucho mayor que la que pueden tener los operadores humanos.

- **Visión artificial**: Se refiere a la captura y análisis de datos visuales de imágenes y videos para detectar, reconocer y rastrear objetos, reconocimiento facial, comprensión de escenas y elaboración automática de mapas topográficos. La información y las instrucciones relevantes podrían enviarse a robots, drones o cualquier otro sistema autónomo.

- **Interfaz hombre-máquina (HMI)**: Permiten a los humanos interactuar con los sistemas de IA reduciendo la carga cognitiva, mejorando el conocimiento de la situación y facilitando la toma de decisiones rápidas en entornos de alto estrés. Entre esas técnicas, se están utilizando sistemas de procesamiento de lenguaje natural e inferencia a partir de

modelos de lenguaje grandes (LLM) para facilitar una interacción fluida entre los humanos y los sistemas de armas sofisticados.

- **Sistemas autónomos**: se refieren a cualquier tipo de vehículo no tripulado, dron o robot, para poder operar sin interacción humana. Por lo general, están diseñados para realizar tareas de reconocimiento y vigilancia complementando o sustituyendo a los humanos o integrados en otros sistemas tripulados.

- **Inteligencia de enjambre**: algoritmos de IA diseñados para coordinar el comportamiento de múltiples sistemas autónomos que cooperan para lograr un objetivo común. Esta área está relacionada con las técnicas de inteligencia grupal y la forma en que el comportamiento individual contribuye a la inteligencia de enjambre.

- **Mando y control (C2)**: Utilización de sistemas basados en IA para el análisis y la gestión en tiempo real de grandes volúmenes de datos y su presentación visual al operador humano.

- **IA en el borde (*edge AI)***: Implica el uso de algoritmos de IA para el procesamiento en tiempo real de datos en el extremo (borde) de la red (por ejemplo, dispositivos como sensores o terminales), para reducir la latencia y mejorar la toma de decisiones en aplicaciones con sistemas autónomos y de guerra cibernética.

La **explosión del uso de la IA generativa** en los últimos años con multitud de aplicaciones para los usuarios finales también ha llegado al sector de la defensa. La cuestión básica a la hora de adoptarlo en el entorno militar es determinar si se puede confiar en los sistemas de IA generativa en los que el entrenamiento depende del uso de datos (gran parte de ellos clasificados) que no pueden verificarse externamente.

A causa de estos **riesgos potenciales**, los ejércitos de las principales potencias militares han puesto en marcha procesos internos de **experimentación y validación de técnicas de IA generativa antes de su adopción generalizada**. El *Departamento de Defensa* de los Estados Unidos (DoD) creó un grupo de trabajo especial llamado "*Task Force Lima*" en agosto de 2023 para **analizar y evaluar el uso de la IA generativa en temas de seguridad nacional**, así como recomendar su uso responsable y proporcionar implementaciones seguras en todas las unidades del DoD.

Como ejemplo de estos esfuerzos de adopción de la IA generative, el DoD en Estados Unidos ha desarrollado un LLM específico para uso militar llamado ***Defence Llama***, construido sobre el LLM *Llama 3* de *Meta* para poder responder a preguntas y escenarios relacionados con la defensa. Recientemente, el DoD ha puesto en marcha una plataforma de IA generativa llamada "*Army Enterprise Large Language Model Workspace*" para agilizar la comunicación, mejorar la eficiencia operativa e impulsar la innovación. Un paso más en la dirección de la adopción real de la IA es el programa *"Thunderforge"*, cuyo objetivo es ofrecer un **eco-**

sistema de planificación unificado en el que los agentes de IA simulen juegos de guerra y planifiquen escenarios.

Todos estos esfuerzos anticipan, si los resultados de estos proyectos son los esperados, una **aceleración en el uso de sistemas militares basados en agentes de IA apoyados en técnicas de IA generativa** en diversos ámbitos de la planificación y la toma de decisiones como complemento al proceso de toma de decisiones basado en humanos.

Uso de la IA en operaciones multidominio

El **masivo incremento en el desarrollo y despliegue de sensores aéreos, terrestres o marítimos terrestres, fijos o móviles, de bajo coste**, que capturan información detallada del terreno, combinados con su procesamiento automatizado en tiempo real para alimentar la toma de decisiones y su interacción con sistemas robóticos, está acelerando un proceso de **cambio disruptivo en el campo de batalla**.

Estos elementos conducen gradualmente a la existencia de un **campo de batalla "transparente"** en el que no es posible ocultar los movimientos de tropas o equipos militares a mediana o gran escala durante períodos prolongados de tiempo. La "transparencia" en el campo de batalla se refiere a la capacidad de un adversario para obtener información detallada y casi en tiempo real sobre las actividades y movimientos del enemigo mediante la combinación de información de comunicaciones, inteligencia y capacidades de vigilancia. Como resultado, las tácticas de combate empleadas han evolucionado en poco tiempo en respuesta a la necesidad de **aumentar la movilidad con unidades ligeras y autosuficientes**.

La información que debe tenerse en cuenta en un sistema de decisión militar es muy voluminosa y cambia rápidamente con el despliegue de multitud de sensores. Por esta razón, **la interpretación de los datos**, exclusivamente por operadores humanos, **es muy difícil**. Se pueden identificar algunas tendencias en el uso de la IA:

- **Mayor uso de la IA en la identificación y selección automática de objetivos** basada en la integración y el análisis de datos históricos y de otro tipo obtenidos en tiempo real de múltiples sensores.

- Introducción de **algoritmos de IA en plataformas de apoyo a la decisión** tanto a nivel personal (en forma de asistente automatizado) como en sistemas de mando y control a diferentes niveles organizativos.

- Uso de **sistemas de armas letales**, aislados o en enjambre, autónomos o semiautónomos, con diversos grados de inteligencia.

- Integración de **sistemas inteligentes de guerra electrónica** en múltiples sistemas militares.

Sistemas de armas inteligentes

En tan solo unos años se han incorporado múltiples **sistemas de armas inteligentes o sistemas de armas autónomos** con diversas soluciones basadas en IA, junto a sistemas microelectrónicos, sensores y actuadores de todo tipo, en una carrera tecnológica en busca de la supremacía entre grandes potencias. La idea básica es **delegar parcial o totalmente la toma de decisiones en algoritmos de IA** (ya sea con o sin intervención del operador humano) para acelerar el proceso de decisión y poder manejar grandes volúmenes de datos que un operador humano no podría analizar.

Se trata de un **enfoque progresivo**. Desde el nivel en el que el sistema informático no tiene ninguna función y es el operador humano el que toma todas las decisiones, hasta el nivel máximo en el que es el sistema impulsado por IA el que toma todas las decisiones y el humano ninguna, existen muchos niveles intermedios que implican **aceptar progresivamente una mayor responsabilidad por los algoritmos del sistema informático**; por ejemplo, permitiendo la aprobación, el veto temporal, o proporcionando información a tiempo al operador humano para la toma de medidas alternativas o deshacer la acción iniciada. En todos estos casos, se puede decir que "*el ser humano está en el bucle*".

Los **niveles más altos de automatización corresponden al uso de algoritmos que toman la decisión por ellos mismos**. Los seres humanos pueden o no ser informados de ello, dependiendo del nivel considerado, pero está fuera del ciclo de decisión. Otra categoría que se utiliza mucho más hoy en día es la de los sistemas de armas semiautónomos. La diferencia básica es que, en el caso de armas totalmente autónomas, la decisión la toman solo los algoritmos de IA incorporados en el sistema, una vez que el sistema ha sido entrenado para identificar objetivos predefinidos, y en los sistemas semiautónomos un operador humano da la orden final de atacar o no atacar a un objetivo identificado.

Los sistemas autónomos utilizados como armas que pueden tener graves impactos en las personas son denominados por las Naciones Unidas **"Sistemas de Armas Autónomas Letales" (SALA)**. Una definición común de los SALA es: *"sistemas de armas que utilizan inteligencia artificial (IA) para identificar, seleccionar y atacar objetivos sin intervención humana".* En los últimos años, países como Estados Unidos, Reino Unido, India, Israel, Irán, Corea del Sur, Rusia y Turquía han invertido mucho en la integración de la IA en el desarrollo de SALA. Actualmente, los ejércitos de todo el mundo utilizan más de **130 sistemas de armas que pueden rastrear y atacar a sus objetivos de forma autónoma**.

Como ejemplo de estas capacidades, los **drones avanzados** se lanzan, a menudo, en "cápsulas" desde muy lejos; Una vez liberados, pueden volar a distancias cortas y atacar sin intervención humana. Las mejoras en la tecnología de las cámaras y la IA hacen posible que estos drones identifiquen y se centren en objetivos específicos utilizados en su proceso de entrenamiento. Para hacer frente a esos desafíos, ***Replicator***, un nuevo programa militar de

Estados Unidos se basa en el uso de modelos LLM tanto para drones kamikaze como para defensas anti-drones, centrados en la creación de sistemas para responder rápidamente a los ataques de los aviones no tripulados y contramedidas a los aviones no tripulados kamikaze. Como cambio relevante de las prácticas comunes, el programa ***Replicator*** depende en gran medida (75%) de nuevas empresas y proveedores innovadores que no participan en las cadenas de suministro de defensa habituales, buscando la introducción rápida de innovaciones radicales.

La **evolución tecnológica hacia "enjambres de drones inteligentes"** basados en cientos o miles de drones aéreos, terrestres o marítimos en los que cada uno de ellos puede identificar objetivos en tiempo real y comunicarse con sus drones vecinos supondrá un cambio cualitativo con impactos relevantes en las tácticas militares. El éxito en la misión de un enjambre de drones requiere integrar las capacidades de los drones individuales para lograr un comportamiento colectivo. Se pueden establecer **tres enfoques básicos para la coordinación de enjambres**:

- **Enfoque 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.

- **Enfoque descentralizado semiautónomo**. 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 nivel inferior podrían ser realizadas de forma autónoma por drones individuales.

- **Enfoque descentralizado totalmente autónomo**. No hay un operador humano. Cada dron intercambia información con todos o algunos de los drones cercanos para decidir los próximos movimientos y acciones siguiendo comportamientos para los que sus algoritmos de IA han sido entrenados. Este enfoque podría apoyar enjambres heterogéneos donde los drones podrían diferir en tamaño y capacidades.

Todas las grandes potencias mundiales están trabajando en el desarrollo de enjambres de drones con fines militares. Esta tecnología no solo está en manos de grandes potencias tecnológicas como Estados Unidos o China. Se pueden mencionar algunas **empresas europeas con enfoques innovadores para el control de enjambres** (lista no exhaustiva): *Saker* (Ucrania), *Quantum Systems* (Alemania), *Thales* (Francia), *Helsing* (Alemania), *BlueBear AI* (Reino Unido), *Swarming Technologies & Solutions* (España). Es relevante indicar la creación de múltiples startups por Ucrania que han introducido soluciones en el campo de batalla en los dos últimos años.

El anuncio efectuado en julio de 2024 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**.

Estas innovaciones representan **avances notables en la tecnología de los drones**, pero las revoluciones tecnológicas en asuntos militares requieren 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 esto requiere acumular experiencia derivada de su uso real.

Relevancia de la IA en la Guerra híbrida y cognitiva

El papel y la relevancia de la IA han crecido en los **conflictos asimétricos** y, especialmente, en la denominada **"guerra híbrida".** Se pueden distinguir **tres tipos de situaciones "híbridas"** (amenaza, conflicto y guerra) que aluden a una gradación en la intensidad y en el impacto social y la participación militar que conllevan. Estas son:

- ***Amenaza híbrida***: Fenómeno resultante de la interconexión de diferentes elementos que, en conjunto, constituyen una amenaza más compleja y multidimensional para las sociedades.

- ***Conflicto híbrido***: Una situación en la que las partes se abstienen del uso abierto de la fuerza (armada) y actúan combinando la intimidación militar (sin llegar al umbral de un ataque convencional) y la explotación de las vulnerabilidades económicas, políticas, tecnológicas y diplomáticas a través de acciones planificadas y sincronizadas.

- ***Guerra híbrida***: Situación en la que un país recurre al uso abierto de la fuerza (armada) contra otro país o contra un actor no estatal, junto con el uso de otros medios de coerción (por ejemplo, económicos, políticos o diplomáticos) combinados con operaciones encubiertas o no encubiertas de menor intensidad.

Un factor decisivo para alcanzar el éxito es la **sincronización y escalada de acciones**, tanto desde una perspectiva de *escalada horizontal* entre diferentes dominios de poder (militar, político, económico, civil o de información) como de *escalada vertical* con diferentes niveles de intensidad y visibilidad de la acción híbrida en la población. La figura 13 muestra varias **herramientas de poder** en las que se deben sincronizar las acciones de guerra híbrida: militar, política, económica, civil e informativa.

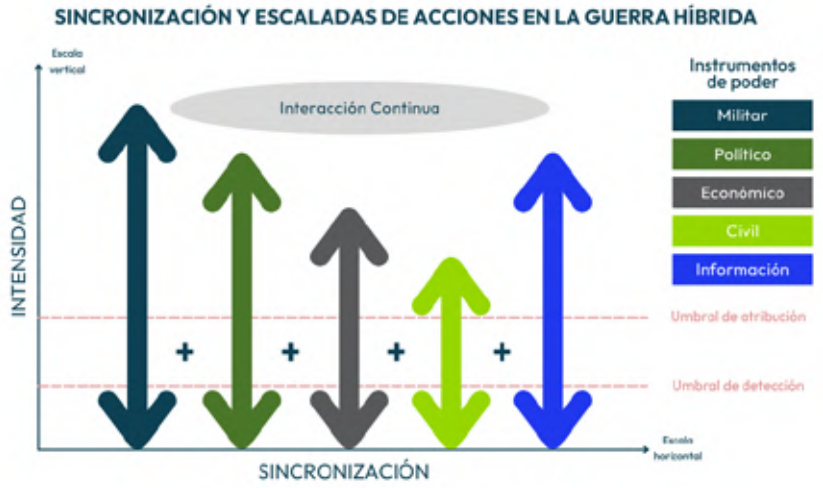


Figura 13. Sincronización y escalada de acciones en la guerra híbrida. Fuente: adaptado de: https://assets.publishing.service.gov.uk/media/5a8228a540f0b62305b92caa/dar_mcdc_hybrid_warfare.pdf

En la figura 13 se ha indicado dos **umbrales de visibilidad** que son relevantes para entender la intensidad del conflicto:

- **Umbral de detección**: nivel mínimo de intensidad de acción híbrida que permite a un gobierno detectar que se está produciendo una amenaza, conflicto o guerra híbrida.

- **Umbral de atribución**: nivel mínimo de intensidad que permita convencer a la atribución (una vez detectada) de quién es el actor que la provoca para poder realizar acciones con solidez y no refutables.

La **guerra híbrida** se desarrolla como un proceso temporal en el que el *nivel de escalada* (aumento de la intensidad del conflicto) fluctúa, no es lineal y está marcado por diversas acciones de "crisis" y "desestabilización" a lo largo del tiempo. Esta calificación depende de una decisión estratégica sobre el nivel de confrontación que se desea alcanzar con estas acciones en respuesta al impacto obtenido y la potencial respuesta del adversario. Luego, tanto los umbrales de atribución como los de detección evolucionan con el tiempo.

Para el "*Hybrid-CoE Centre of Excellence*", **la tecnología es uno de los principales impulsores de la guerra híbrida** y de las teorías de la guerra híbrida. Un análisis del *Hybrid-CoE* identificó tres tipos de tecnologías:

- Tecnologías que tienen como objetivo **manipular el acceso radio a la información utilizando técnicas de guerra electrónica** para interferir la señal de radio, suplantación de identidad u otros ataques cibernéticos.

- Tecnologías orientadas a la **manipulación de la información y su narrativa** actuando sobre los servicios que ofrecen las plataformas digitales generando "desinformación" a través de la generación de noticias falsas o tendenciosas.

- Tecnologías emergentes como las **neurotecnologías**, los **sistemas autónomos**, la **realidad extendida** o, en el futuro, la interacción con las **tecnologías cuánticas**.

El **impacto potencial de los ataques híbridos** se ve acelerado por el uso de sistemas automatizados debido al uso de sistemas de IA capaces de analizar múltiples datos contextuales en un volumen tal que es imposible para los analistas humanos utilizarlos. **Con el uso de la IA, entramos en una zona de explosión de la capacidad de "guerra cognitiva"**, superpuesta a acciones de carácter híbrido (véase figura 14) cuyo objetivo es el dominio de la información para la construcción y difusión de narrativas orientadas a la consecución de objetivos políticos.

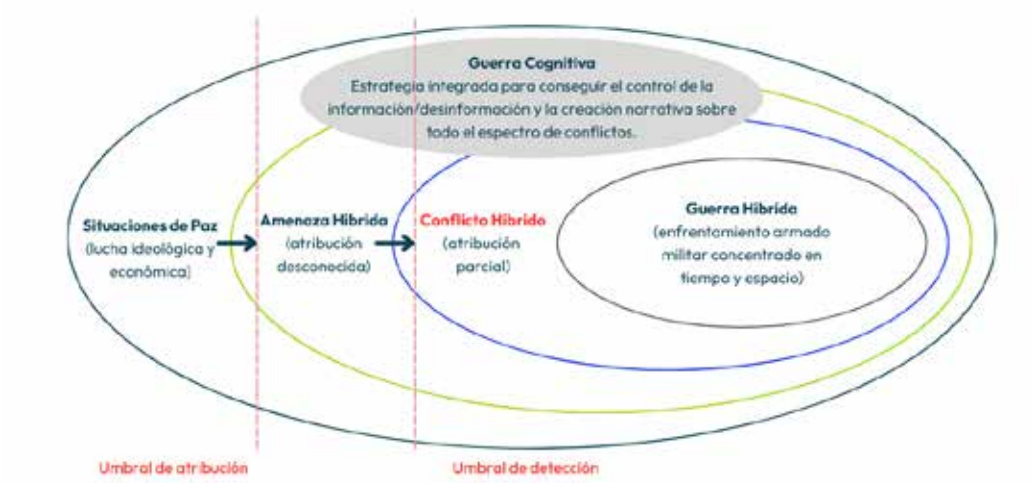


Figura 14. Amenazas, conflictos y guerra híbrida, y guerra cognitiva. Fuente: elaboración propia

No habría sido posible lograr el impacto de la guerra cognitiva en la situación actual sin el **uso de las redes sociales como "arma"**, y el lanzamiento (automatizado) de sofisticados ciberataques con la ayuda de herramientas de IA (por ejemplo, a través de la generación automática de mensajes multimedia personalizados con bots empáticos, la distorsión de la realidad y su difusión masiva en grupos de población objetivo). Sin embargo, la forma en que se aborda depende del país considerado, como han demostrado los casos de Rusia y China.

- **Rusia** complementa la guerra en Ucrania con ciberataques y campañas de desinformación contra objetivos de la UE. Por lo tanto, la UE reforzó en 2024 las sanciones a las personas y entidades que participan en acciones respaldadas por Rusia contra la UE.

- En **China**, la guerra cognitiva adopta el término **"guerra cognitiva algorítmica"**. El objetivo es aprovechar al máximo la combinación de algoritmos de análisis de datos y recomen-

daciones de redes sociales para influir de manera efectiva en el comportamiento de un individuo. Aprovecha las grandes cantidades de datos disponibles sobre el comportamiento de las personas y las entidades para entrenar algoritmos de IA.

Un **modelo de guerra cognitiva** debe centrarse en la cognición a la que se subordinan los rendimientos físicos en el campo y, por el lado de la información, vincularse a la difusión de narrativas en el dominio cognitivo a nivel nacional e internacional. Para abordarlo sistémicamente, se utilizan **cinco tipos de dimensiones instrumentales**:

- Herramientas que explotan los sesgos cognitivos y la percepción.
- Herramientas relacionadas con la neurociencia y la biología.
- Herramientas que explotan la psicología social y las dinámicas de grupo.
- Herramientas que emplean aplicaciones tecnosociales.
- Herramientas de tecnología de la información.

Un elemento básico para implementar la guerra cognitiva es el dominio de las **campañas de desinformación**. Su éxito depende de tres condiciones: **narrativas** que transmitan de manera efectiva y persuasiva el mensaje diseñado para un objetivo específico; la **difusión del mensaje** a un público objetivo para influir en las decisiones políticas a nivel nacional o institucional; y **persuasión efectiva** a una proporción suficiente de personas de la veracidad y pertinencia del mensaje para generar una cadena de reacciones que logren el objetivo.

El **aumento de la desinformación, respaldado y potenciado por el desarrollo de la IA**, ha penetrado en gobiernos, instituciones y ciudadanos con un efecto desestabilizador. La *Asamblea General de las Naciones Unidas* ha expresado su preocupación por la proliferación de la desinformación y la necesidad de promover la cooperación internacional en la lucha contra la desinformación.

En la actualidad, conseguir el **dominio de las plataformas digitales impulsadas por la IA** forma parte de las estrategias de las grandes potencias tecnológicas para influir en la opinión pública de 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. Desde el punto de vista del interés político, el tratamiento de esta información personal también permite **analizar o introducir sesgos** hacia determinadas ideologías, partidos políticos, miembros del gobierno, representantes o candidatos en elecciones políticas.

Además, **el uso de herramientas especializadas en IA ha permitido crear automáticamente campañas de desinformación** con realidades sintéticas difíciles de contrarrestar. La **IA generativa multimodal** (capaz de clonar no solo la imagen, sino también la voz y el lenguaje corporal en vídeos hiperrealistas) se combina con otro tipo de herramientas como la realidad virtual (con la generación de modelos 3D realistas) para permitir ataques cognitivos basados en un área creciente como es la **manipulación emocional** aprovechando entornos

de realidad virtual que han demostrado su capacidad para inducir emociones negativas. El uso de herramientas de IA ofrece mejoras a los diferentes actores involucrados en la guerra cognitiva para lograr el efecto deseado. Concretamente:

- El contenido que se publica y comparte puede analizarse utilizando técnicas de inteligencia artificial (IA) como el **procesamiento del lenguaje natural** (*Natural Language Processing, NPL*).
- 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 o manipuladas, por ejemplo, buscando rastros dejados por los sistemas utilizados para capturar imágenes alteradas.
- Las aplicaciones de IA también pueden entrenarse para **detectar información falsa** (*fake news*) en las redes sociales y emitir advertencias. Al analizar bloques de datos de intercambios en redes sociales como *Facebook*, *X* o *Telegram*, las herramientas de IA pueden reconocer elementos estilísticos típicos de las noticias falsas.
- También se les puede capacitar para **identificar contenido potencialmente problemático** y ayudar a los operadores a comprender por qué se ha marcado.

Siendo plenamente consciente de la gravedad de esta situación, **la estrategia de la UE se basa en el refuerzo de un ecosistema integral de resiliencia frente a la guerra híbrida** que implique la coordinación y el intercambio de información entre diferentes tipos de actores. Se basa en el ***Sistema de Alerta Rápida*** (*Rapid Alert System*, SAR), cuyo objetivo es desarrollar un marco y una metodología exhaustivos para la recopilación sistemática de incidentes facilitados por el *Centro de Análisis e Intercambio de Información* (FIMI, ISAC) que aumente la resiliencia de Europa frente a las injerencias externas.

En el contexto de la guerra cognitiva, las **habilidades cognitivas de los seres humanos** son las más relevantes. Por este motivo, la **neurotecnología** como tecnología de doble uso ha despertado el interés de las agencias de investigación en defensa por converger con la IA en un avance disruptivo con **impacto en la guerra híbrida**.

La mejora cognitiva de los seres humanos afecta a la recopilación, análisis y uso de datos de actividad cerebral, en los que los algoritmos de IA juegan un papel relevante. **La mejora del rendimiento cognitivo se puede "entrenar"**. También se puede utilizar la evolución tecnológica de las prótesis externas, como los **cascos de monitorización y estimulación cerebral** equipados con sensores que permiten obtener información sobre la actividad cerebral, o las prótesis internas como los **implantes cerebrales**. Más lejos en el tiempo, se están considerando **mejoras cognitivas basadas en terapias génicas** mediante técnicas como CRISPR y que podrían suponer un salto adelante en el futuro.

En ese contexto, la emergencia de una nueva generación de **armas cognitivas** estará progresivamente a disposición de las grandes potencias. Probablemente, en la próxima década se desplieguen algunas de ellas.

Las ***neuroarmas*** se refieren a las tecnologías utilizadas para mejorar o dañar las capacidades cognitivas y/o físicas de un combatiente u objetivo, o para atacar a individuos o infraestructuras críticas de la sociedad. El objetivo es alterar el comportamiento de un soldado influyendo en la atención, la toma de decisiones y la reacción. Disponer de **personal militar con un mayor rendimiento físico y mental** facilitará que la **guerra cognitiva** se extienda al campo de batalla de las redes sociales.

La IA en el sector especial de la defensa

El **dominio y la explotación del sector espacial** se ha convertido en un factor decisivo desde el punto de vista de la defensa. Un elemento clave para entender la relevancia geopolítica alcanzada por el sector espacial es que **la tecnología espacial tiene un carácter dual**, históricamente ligado a la confrontación entre grandes potencias, con la implicación de las Fuerzas Armadas y la industria de defensa. Como dato relevante, el 70% de los satélites que orbitaron la Tierra en 2023 fueron militares o de doble uso. Solo en 2023, se lanzaron 107 satélites militares, lo que eleva el número total a más de 900 y se estima que habrá 2.500 satélites militares en los próximos diez años.

En la Figura 15 se identifican los **principales impulsores del uso de la IA en el espacio**. En la parte central, se han señalado dos *meta impulsores* vinculados a la necesidad de reducir el costo 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 espaciales.

Figura 15. Impulsores del uso de la IA en el espacio. Fuente: elaboración propia

En la parte superior de la figura se indican **tres retos tecnológicos**:

- **Aumentar las capacidades de procesamiento a bordo** del satélite o la nave espacial para obtener sistemas espaciales más inteligentes para la gestión de plataformas y cargas útiles.
- **Reducir la transferencia de datos capturados a las estaciones terrestres** con el objetivo de reducir la dependencia de los enlaces por satélite y la ventana de visibilidad hacia las estaciones terrenales.
- **Proteger los sistemas de comunicación frente a ciberataques** provocados para inutilizar el funcionamiento del satélite.

En la parte inferior de la figura, se identifican **cuatro desarrollos tecnológicos relacionados con la IA como "facilitadores"** frente a los desafíos señalados:

- **Desarrollo de chips de alto rendimiento, bajo consumo y adaptados al espacio** para el (re)entrenamiento de modelos de IA y la extracción de inferencias.
- **Generación de gemelos digitales ciberfísicos** para acelerar el diseño rápido de sistemas espaciales basados en un modelo digital preciso del sistema a desarrollar.
- Uso de **herramientas de IA generativa** basadas en el uso de grandes modelos de lenguaje (LLM) adaptados a las necesidades de espacio y defensa.
- Uso de **robótica inteligente** en el espacio basada en brazos robóticos o robots autónomos.

Los avances en estas áreas tecnológicas proporcionaron las **bases para la aplicación de la IA en el sector de la defensa espacial**. Las áreas de aplicación más relevantes son las siguientes:

- **Mejora del conocimiento del dominio espacial (SDA).** Comprender y gestionar los activos espaciales ubicados en el espacio y su posición real para identificar objetos cercanos, amenazas derivadas y reducir los riesgos operativos.
- **Defensa de la navegación satelital**. Implementar métodos que permitan saber si la señal de navegación GNSS está alterada o es imposible de obtener, ofreciendo técnicas de navegación alternativas para no depender de la señal satelital.
- **Análisis inteligente de imágenes satelitales**. Procesamiento de imágenes impulsadas por IA tomadas por el satélite, ya sea en el propio satélite o en estaciones terrestres para identificar objetos específicos de interés y alimentar la toma de decisiones en plataformas específicas.
- **Ajustes automáticos de la órbita para evitar colisiones**. Conocimiento de la distancia y la órbita de los satélites con respecto a las estaciones terrenas o por el propio satélite si tiene suficientes sensores y capacidad de procesamiento para evitar impactos con otros objetos en el espacio (por ejemplo, desechos espaciales o asteroides).
- **Mantenimiento predictivo de satélites**. Uso de algoritmos de IA para planificar procesos de mantenimiento de satélites basados en el análisis de series temporales de datos combinados con otros datos capturados en tiempo real

- **Optimización de las comunicaciones espaciales militares**. Uso de la IA para lograr comunicaciones de banda ancha robustas, inmunes a las interferencias naturales o provocadas por el hombre en el entorno espacial.
- **Ciberseguridad espacial**. Sistemas de defensa contra ciberataques de datos hacia o desde satélites, ya sean datos generados por cargas útiles a bordo (por ejemplo, imágenes) o señales de control como parte de redes de navegación o comunicaciones.
- **Robótica espacial inteligente**. Robots autónomos fijos (por ejemplo, brazos robóticos) o robots móviles (por ejemplo, antropomórficos o que no cooperan con humanos, vehículos de explotación espacial) para realizar múltiples misiones sin intervención humana.
- **Marcos comunes para la simulación y la interoperabilidad de datos espaciales**. Garantizar la interoperabilidad de los datos espaciales para compartir datos entre las fuerzas armadas aliadas y tener sistemas y aplicaciones de múltiples fuentes y proveedores.
- **Integración de la IA con las tecnologías cuánticas**. Analizar cómo se puede integrar la IA con el uso de tecnologías cuánticas (comunicaciones, sensores o computación) en aplicaciones espaciales.

Este listado de **aplicaciones espaciales basadas en IA** está evolucionando muy rápidamente al explotarse la disponibilidad de procesadores integrados más potentes y versiones más ligeras de sistemas LLM.

DIMENSIÓN ÉTICA Y REGULATORIA DE LA IA EN DEFENSA

El **objetivo 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 legítimo en su iniciación, desarrollo y consecuencias. Este tema ha cobrado **relevancia con el uso de la IA en la toma de decisiones y el papel que pueden jugar los humanos**. Los sistemas basados en IA han demostrado su capacidad para ayudar a los humanos a mejorar su actividad a través de los llamados **"agentes inteligentes"** que asumen funciones que hasta hace poco solo realizaban los seres humanos. Se está experimentando con el uso de **agentes inteligentes militares** que pueden formar parte de sistemas de armas autónomas letales (SALA) o como una mejora de las prestaciones de otras armas convencionales.

La **posición de las Naciones Unidas** desde 2018 ha sido que los SALA son "*políticamente inaceptables y moralmente repugnantes"* y, por lo tanto, ha pedido reiteradamente que se **prohíban en virtud del derecho internacional**. En la *Resolución de la Asamblea General* de 24 de diciembre de 2024 se incluyó un área sobre "*La inteligencia artificial en el ámbito militar y sus consecuencias para la paz y la seguridad internacionales*". China propuso en 2022 la necesidad de distinguir entre "*sistemas de armas autónomas aceptables e inaceptables*"; De todos modos, aún no hay consenso, y el debate continúa.

El uso de la IA en el ámbito de la defensa debe abordarse con un marco ético y regulatorio equilibrado. En la figura 16 se muestran todos los elementos implicados. A falta de un marco jurídico específico, el tratamiento de la IA en el ámbito militar está subordinado al derecho internacional.

Figura 16. Relaciones entre el marco ético y el regulatorio. Fuente: elaboración propia

Las *Cumbres* al máximo nivel celebradas entre Estados (en 2023 en los Países Bajos, en 2024 en Corea del Sur, y la próxima prevista en 2025 en España) denominadas **IA Responsable Militar (REAIM)** tienen como objetivo establecer límites éticos al uso militar de la IA. No implican la creación de un marco legislativo, sino el establecimiento de acuerdos sobre acciones "voluntarias" basados en la discusión y la experiencia a través de la implementación de un plan de acción. Sin embargo, no hay garantía de que, en caso de un conflicto militar agudo, los contendientes los cumplan cuando su supervivencia esté en juego.

El **Reglamento de la UE sobre la IA**, publicado el 13 de junio de 2024, no es aplicable en este ámbito porque **excluye explícitamente la seguridad nacional, la defensa y los fines militares**. De hecho, durante las negociaciones, algunos Estados miembros presionaron para que se establecieran exenciones con el fin de preservar la autonomía estratégica de Europa, garantizando restricciones mínimas a la IA en defensa y seguridad. El Reglamento introduce una **clasificación de las aplicaciones de IA basada en el riesgo que su uso puede implicar**, imponiendo obligaciones de cumplimiento a los proveedores que podrían transferirse al ámbito militar.

Un paso más en la puesta en marcha de la Regulación de IA de la UE se ha producido en julio de 2025 con la publicación de las **directrices voluntarias para su desarrollo y despliegue** (*General-Purpose AI Code of Practice*). Definidas por un grupo de expertos y miles

de opiniones externas, aborda temas de transparencia, copyright y seguridad buscando el **equilibrio entre la innovación y la salvaguarda de los intereses públicos**.

En una línea más dura, el *Parlamento Europeo* ha instado sistemáticamente al Consejo a que impida el desarrollo y el uso de los SALA que operen sin un **control humano significativo** y a que presione para que se prohíban en todo el mundo. Destaca la **importancia de las directrices éticas, la transparencia y la rendición de cuentas en el despliegue de la IA**, especialmente en las áreas que afectan a las operaciones militares.

De cara al futuro, la **convergencia entre la IA y la neurotecnología** ha generado un nuevo marco para los debates éticos y regulatorios sobre el desarrollo y el uso de tecnologías de aumento cognitivo y social. Hay dos **preocupaciones éticas principales**: la **privacidad mental** y el **albedrío humano**. Aunque hoy en día la tecnología cognitiva no está lo suficientemente madura como para controlar la privacidad mental y el albedrio humano, está evolucionando muy rápidamente por lo que el debate es oportuno.

- La **"privacidad mental"** se refiere a la aceptación de que los contenidos de la mente de una persona solo son conocidos conscientemente por esa persona. Con la tecnología disponible, no es posible acceder a ese contenido, a menos que la persona decida compartirlo con otros hablando, escribiendo, dibujando o utilizando el lenguaje corporal para expresarlo y comunicarlo a los demás.
- El **"albedrío humano"** se refiere a la libertad y autonomía de una persona. La neurotecnología en combinación con drogas se puede utilizar para influir en su comportamiento, pensamientos, emociones o recuerdos, aumentando o inhibiendo algunas habilidades cerebrales.

Es evidente la **relación existente entre estas dos preocupaciones éticas y las neuroarmas** mencionadas en el capítulo anterior alrededor de la Guerra híbrida por lo que su relevancia será creciente.

SOBERANÍA TECNOLÓGICA DE LA UE EN IA PARA LA DEFENSA

Niveles de soberanía tecnológica

En un momento en el que **la UE ha decidido aumentar su autonomía estratégica** para poder tomar sus propias decisiones sin depender en la medida de lo posible de otros, **conocer el nivel de soberanía tecnológica alcanzable desde una posición realista** se convierte en un elemento básico para la adopción de políticas públicas concretas y efectivas.

El **análisis de la soberanía tecnológica** se puede realizar utilizando un modelo como el que se muestra en la Figura 17, que representa el grado de autosuficiencia tecnológica alcanza-

ble (de 0 a 100%) en diversos ámbitos de intervención política en **tres niveles diferentes.** El **primer nivel** se refiere al acceso a los recursos naturales y a las infraestructuras para el procesamiento y el transporte de materiales. El **segundo nivel** se refiere a las capacidades de investigación e innovación y a los recursos humanos capacitados, así como a la fabricación de componentes y sistemas industriales. Por último, el **tercer nivel** está relacionado con la estructura del mercado, el marco regulatorio y los principios y valores compartidos.

Figura 17. Niveles de soberanía tecnológica. Fuente: Elaboración propia.

Desde una perspectiva cualitativa desarrollada por el Grupo de Trabajo, la figura 18 ejemplifica la situación de la **soberanía tecnológica de la UE en relación con la IA**.

- El **acceso a los recursos naturales** en la UE está condicionado por la necesidad de fabricar semiconductores utilizados en la IA y disponer de fuentes de energía a costes reducidos para alimentar los centros de datos utilizados en el entrenamiento de algoritmos de IA o para la extracción de inferencias. En ambos ámbitos, la UE tiene una posición débil dependiendo de importaciones.

- Las **infraestructuras de procesamiento y transporte** de las materias primas o de los componentes necesarios para el desarrollo y uso de los sistemas de IA obligan a la UE a garantizar el suministro desde países lejanos, mitigado por la diversificación de proveedores en países amigos o acercándolos físicamente a la UE. Influye también la debilidad de la UE en disponer de grandes cables submarinos transatlánticos de fibras ópticas en manos de empresas no europeas.

- La **fabricación de componentes y sistemas de IA** está condicionada en la UE por la falta de grandes fundiciones para la fabricación de chips de IA, aunque se le da bien desarro-

llar máquinas de *fotolitografía extrema (EUV)* capaces de fabricar chips de IA. También es necesario mejorar la soberanía tecnológica en superordenadores y grandes centros de datos para la IA.

- La **investigación, la innovación y la formación de recursos humanos** en actividades de IA que ya lleva a cabo la UE son notables. Sin embargo, debe redoblar los esfuerzos para formar más recursos humanos en tecnologías de IA, retenerlos y aprovechar las oportunidades para atraer a investigadores de otros países.

- La **estructura del mercado europeo de IA** presenta una **fuerte dependencia de grandes empresas y plataformas de IA no europea**s que ofrecen productos y servicios de IA en la nube, con pocas empresas emergentes de IA muy valoradas en la UE.

- La **situación regulatoria de la UE en IA** tiene dos debilidades: 1) la necesidad de conciliar la regulación y la innovación en las mismas o mejores condiciones que las existentes en otros países y 2) la necesidad de que la regulación evolucione con la tecnología de IA.

- Un elemento clave de la regulación y evolución del mercado es el conjunto de **principios y valores compartidos en relación con el desarrollo y uso de la IA** con los que la UE desea verse reflejada en el mundo.

Figura 18. Evaluación cualitativa de la soberanía tecnológica de la UE en tecnologías de IA. Fuente: elaboración propia.

La figura 19 ofrece una **visión cualitativa complementaria de la soberanía tecnológica europea en IA** atendiendo a las capas técnicas (*stack model*) del desarrollo de sistemas de IA desde el hardware a las aplicaciones finales, y sus posibles impactos en el sector de la defensa.

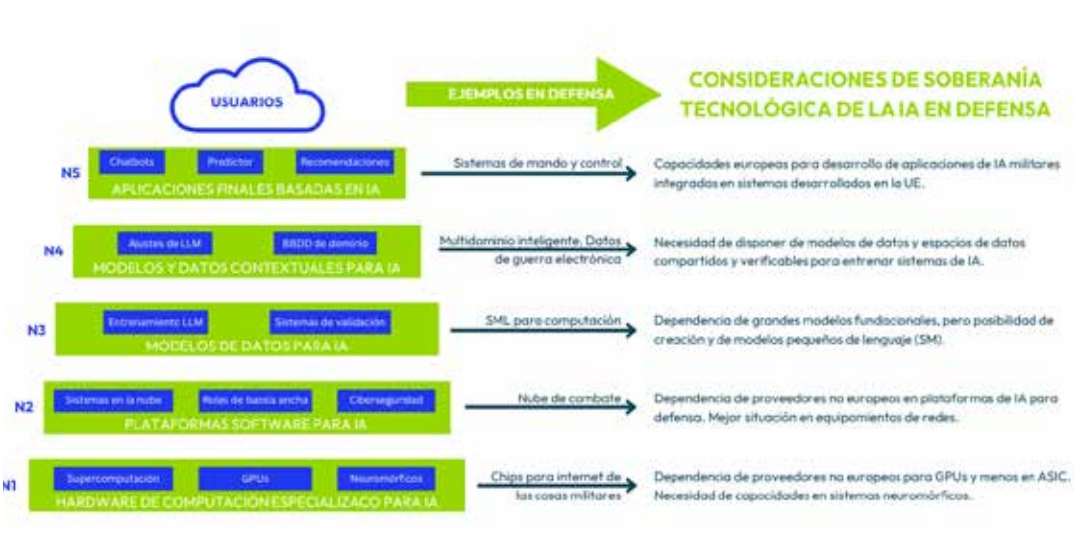


Figura 19. Consideraciones sobre la soberanía de la tecnología de IA en defensa en un modelo por capas. Fuente: elaboración propia

Dado que **la tecnología de semiconductores es dual**, no hay nada que impida que los esfuerzos indicados anteriormente para mejorar la soberanía tecnológica en semiconductores no puedan beneficiar su aplicación en defensa, incluidos los **chips diseñados para las necesidades de IA, como las GPU y los aceleradores de inferencia**. Sin embargo, hay dos aspectos relevantes que influyen en la toma de decisiones: un **volumen de mercado limitado** en términos de número de chips que es mucho menor y **consideraciones de coste menos relevantes** que las que se aplican a las aplicaciones civiles con chips de IA integrados en millones de productos (como los teléfonos inteligentes impulsados por IA).

Para **mejorar la soberanía tecnológica en IA**, la *Comisión Europea* propuso en abril de 2025 un **Plan de Acción** basado en un conjunto de acciones sobre infraestructura informática, datos, formación, desarrollo y adopción de algoritmos, y simplificación regulatoria. Este plan de acción afecta también a la industria europea de defensa, que debería **concentrarse en equipos militares que incorporen IA** con vistas a su desarrollo en los Estados miembros de la UE y, si es posible, con modelos comunes de desarrollo y contratación que reduzcan las dependencias externas.

Interacción entre la geopolítica y las plataformas digitales para la IA

La UE debe intentar en los próximos años adoptar **alternativas europeas** que vayan desde el desarrollo de dispositivos semiconductores clásicos hasta dispositivos de computación neuromórfica para la ejecución de algoritmos de IA, el desarrollo de LLM europeos, la adopción de plataformas basada en IA para la toma de decisiones, y la integración de todos ellos en múltiples sistemas militares.

El **aumento de los recursos de la UE asignados a la industria de defensa**, así como un mayor esfuerzo hacia las tecnologías duales como la IA, pueden servir de base para condicionar a los Estados miembros a comprar sistemas y plataformas europeos. La industria europea debería plantearse una estrategia para acceder a un mercado dual que es global; única forma de recuperar la inversión.

De aquí a 2030, las **sinergias de la IA con otras tecnologías facilitadoras emergentes**, incluidas las **tecnologías cuánticas** y la **neurotecnología**, abren un amplio abanico de posibilidades que la UE debería estar dispuesta a aprovechar ahora para garantizar un nivel suficiente de soberanía tecnológica de la UE en un ámbito emergente de doble uso muy relevante.

CONCLUSIONES Y RECOMENDACIONES

Del informe elaborado se ha extraído un conjunto de las **conclusiones más relevantes sobre el uso de la IA en la defensa**. A partir de ellas, se proponen un **conjunto de recomendaciones de actuación** para mejorar el posicionamiento de la UE en el uso de la IA en el ámbito de la defensa y su posible traslado a la situación de la defensa española y su mejora en los próximos años.

Hacer realidad las recomendaciones propuestas en el ámbito de la defensa es un proceso complejo que requiere **voluntad política**, **inversiones sostenidas en el tiempo** y la **participación de todos los actores** en los diferentes ámbitos de la sociedad, desde la industria de defensa, a las fuerzas armadas de los Estados miembros y las universidades y centros de investigación para llevarlo a cabo.

Conclusiones

Sobre la dimensión científica y tecnológica de la IA

Las siguientes conclusiones reflejan los **avances o barreras actuales en el desarrollo tecnológico 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 de la IA se ha entrado en una **nueva fase del proceso de digitalización** que complementa, desarrolla y construye sobre las fases anteriores desde las últimas décadas del siglo XX con un impacto creciente en la sociedad.

Se trata de un **proceso acelerado y continuo de digitalización** que también afecta al sector de la defensa, tanto para las empresas que generan productos y servicios de uso militar en los procesos de desarrollo y fabricación como para su uso final por parte de los propios ejércitos en el ejercicio de sus misiones.

2. El camino para **conseguir una IA general** no se asume como un hecho cierto a medio o largo plazo, existiendo diferencias significativas en las opiniones de los expertos sobre si ello será posible o no.

Lograr **disponer de una IA que supere a los humanos en todas las facetas requeriría avances disruptivos**, no previsibles en este momento. Lo que sí es posible es obtener mejoras incrementales múltiples y continuas de sistemas de IA específicos centrados en abordar muchos tipos de problemas; En muchos de ellos, ya superan el rendimiento del ser humano medio y ese proceso continuará en el futuro.

3. La IA actúa como una **tecnología habilitadora de carácter dual** en todos los ámbitos socioeconómicos con múltiples interacciones cruzadas entre el ámbito civil y el militar, pero en la que el volumen de las inversiones y el tamaño del sector civil actúan como un motor clave.

El principal motor del desarrollo de la ciencia y la tecnología de la IA en las últimas dos décadas ha residido en las inversiones realizadas en el sector civil por entidades públicas y privadas. Sin embargo, en el sector de la defensa, el punto de partida es la adaptación de un producto o servicio en el mercado civil para su uso en el sector de la defensa o viceversa para aprovechar el esfuerzo realizado.

4. La **integración progresiva de algoritmos de IA** para proporcionar funcionalidades clave de casi todos los productos y servicios utilizados por las fuerzas armadas hará que **su uso en defensa sea más transparente para el usuario final**.

La integración transparente de la IA para obtener funcionalidades clave en los sistemas militares hace que el usuario final sea menos consciente de sus implicaciones. En ese caso, la formación del personal militar y el establecimiento de normas y procedimientos claros para su utilización deberían ser un requisito previo para su adopción.

5. La **necesidad de gestionar volúmenes masivos de datos específicos estadísticamente significativos** para el entrenamiento de modelos fundamentales de IA 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 computacionales que deben ser cubiertas por hardware especializado.

Este factor **afecta al uso de las técnicas de aprendizaje automático** como el aprendizaje profundo, incluida la IA generativa basada en el aprendizaje supervisado. El **aprendizaje por refuerzo** solo se puede aplicar en entornos altamente controlados, lo que los hace inutilizables en situaciones de combate, aunque sí sean válidos para el entrenamiento.

6. Los **sistemas multiagente**, formados por múltiples agentes de IA coordinados entre sí abordando problemas reales orientados a apoyar a los seres humanos para el desarrollo

de funciones complejas, acelerarán y extenderán **el uso de la IA** en la sociedad al abordar la resolución de problemas reales con importantes ventajas derivadas de su uso.

Su uso implica el **despliegue acelerado de agentes de IA en todos los niveles operativos de las fuerzas armadas**, lo que implica la modificación de muchos de los procesos, tácticas y estrategias utilizados actualmente, lo que, a su vez, explica el aparente retraso en su adopción en comparación con las áreas civiles.

7. La **creciente importancia del hardware especializado para IA**, tanto para el desarrollo de sensores inteligentes 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.

Necesidad de asegurar que la industria de defensa posea los **conocimientos necesarios para desarrollar circuitos integrados avanzados y sensores** o acuerdos estables a través de proveedores fiables en otros países fuera de la UE, y que las Fuerzas Armadas tengan la capacidad de adoptarlos.

8. La **fabricación de los modelos más avanzados de unidades de procesamiento gráfico (GPU)** se ha convertido en un factor crítico en la IA generativa; Su disponibilidad surge como un **potencial cuello de botella** y está ligada a múltiples restricciones y condiciones para exportarlos a determinados países.

Se asiste a **mejoras continuas e incrementales** en las prestaciones de los algoritmos de IA en chips especializados (GPUs, FPGAs y ASICs). A finales de la década se dispondrá de potentes **chips neuromórficos** con una potencia mucho menor, adaptados a la ejecución de **algoritmos de redes neuronales**.

9. La **IA generativa multimodal** ha madurado muy rápidamente, siendo capaz de generar información a partir de datos, texto, voz, imagen o vídeo muy difícil de distinguir de la realidad, hecho que alimenta las campañas de desinformación e incrementa las 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 en el caso de la guerra híbrida y la guerra cognitiva**. Este uso se da en un contexto de alto crecimiento de los ciberataques y del lanzamiento de campañas de desinformación provocadas por actores estatales o paraestatales.

10. Persisten problemas técnicos relevantes en el uso de sistemas de IA derivados del **problema de la "caja negra" de algoritmos**, de los **sesgos** y las **"alucinaciones"** en los procesos de inferencia de la IA generativa en aplicaciones derivadas del uso de grandes modelos de lenguaje (LLM), lo que dificulta su uso en aplicaciones de defensa.

Los problemas mencionados representan una **barrera para su uso en defensa** que debe ser evaluada antes de su adopción en sistemas de decisión crítica en los que es necesario conocer las razones que llevan a una determinada respuesta del sistema; especialmente, en aquellos con consecuencias potencialmente letales.

11. La **necesidad de reducir el consumo energético y computacional** necesario para el entrenamiento de modelos y 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 específicos, como algunos de naturaleza dual o con restricciones contextuales como el espacio.

La proliferación de modelos pequeños de lenguaje (SML) ofrece oportunidades para el entrenamiento con datos de interés militar. Este proceso también implica reducir las necesidades computacionales y energéticas de los centros de procesamiento de datos relacionadas con el entrenamiento de modelos de IA o para la ejecución de algoritmos preentrenados en dispositivos finales de usuario.

12. La **integración de la IA con la neurotecnología está todavía en pañales**, ya que se trata de una tecnología inmadura, pero se producirá con posibles disrupciones en la sociedad durante la próxima década y con una progresiva aplicación en el sector de la defensa.

La convergencia de la IA con la neurotecnología ha avanzado considerablemente en la última década, **aunque su uso fuera del ámbito médico aún es limitado**. El potencial para facilitar el aumento de las capacidades cognitivas humanas y su aplicación en personas sanas le otorga una relevancia potencial en el campo de la defensa, donde ya se están aplicando todas las tecnologías.

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 todavía maduras, será necesario disponer de **programas experimentales** que permitan evaluar su utilidad potencial y, a través de ellos, acelerar el proceso de maduración de los productos duales multitecnológicos emergentes. Esta integración combinada con la IA forma parte de la futura **“guerra cuántica inteligente”.**

Conclusiones sobre la dimensión socioeconómica de la IA

1. El **mercado global de IA sigue creciendo** a una tasa compuesta anual muy alta; especialmente en áreas como el aprendizaje automático, la IA generativa y los sistemas de agentes inteligentes.

El dominio de la IA y su convergencia con otras tecnologías emergentes es parte de la batalla por la supremacía tecnológica entre las grandes potencias. Estas tasas de crecimiento son elevadas en el sector de la defensa, y se acelerarán en los próximos años.

2. El **liderazgo en el desarrollo y uso de la IA** con influencia global en la economía occidental sigue en manos de Estados Unidos, tanto en términos de volumen de mercado alcanzado como en términos de valoración bursátil de sus grandes empresas digitales en todos los eslabones de la cadena de valor.

En sectores donde la dualidad sea un factor clave, es probable que se consolide una **fragmentación del mercado de la IA en bloques o áreas de influencia de las grandes potencias**, e incluso de los espacios de datos utilizados para el entrenamiento de modelos.

3. En muy poco tiempo, **China se ha convertido en uno de los países líderes en el desarrollo de la ciencia y la tecnología de la IA**, ya sea medido en el porcentaje de patentes, en el crecimiento de las publicaciones científicas o en el volumen del mercado alcanzado; todo ello, en conjunto, implica la reducción gradual de la brecha con Estados Unidos.

China ha alcanzado a Estados Unidos en varias áreas de la IA, como el **reconocimiento de imágenes** y el **desarrollo de modelos de lenguaje eficientes**, respaldado por la aparición de múltiples startups con enfoques disruptivos financiados por fondos gubernamentales. El potencial de doble uso de prácticamente todos los productos generados está alineado con el **concepto de fusión militar-civil** que China ha estado propugnando durante años.

4. Las **sanciones y restricciones impuestas a China por Estados Unidos** para la exportación de equipos de fabricación de semiconductores o circuitos integrados utilizados en el entrenamiento de grandes modelos de lenguaje o para la generación de inferencias han impulsado y acelerado el desarrollo de la tecnología propia de IA en China.

En respuesta a la imposición de sanciones a la exportación e importación de productos tecnológicos, se ha estimulado el **desarrollo de capacidades internas**. Las empresas chinas han conseguido obtener resultados muy apreciables en comunicaciones móviles, formación LLM o sistemas de armas sin necesidad de utilizar las versiones más potentes de chips de IA.

5. **Las empresas de defensa han abrazado la naturaleza dual de la IA** y están acelerando su inclusión en multitud de productos militares colaborando con empresas digitales, adaptando productos civiles y compitiendo y colaborando con empresas del resto del mundo.

Las empresas europeas están siguiendo la misma tendencia, aunque creciendo lentamente, y manteniendo la dependencia de componentes y subsistemas de IA de otros países, lo que ha llevado a un replanteamiento del marco de alianzas estratégicas de la UE con

el objetivo de mejorar la resiliencia de su cadena de suministro de IA y la generación de capacidades propias.

6. La **adopción de la IA en el sector de la defensa** está empezando a extenderse no solo por parte de las grandes empresas digitales que aprovechan la dualidad de uso para su integración en productos y servicios digitales, sino también por el papel que juegan multitud de empresas emergentes altamente especializadas.

La **aparición de startups con soluciones disruptivas de IA** que están siendo probadas y adaptadas por las Fuerzas Armadas de muchos países está actuando como un **factor acelerador del proceso de innovación dual** basado en la IA.

7. **El esfuerzo de la UE en la adopción de la IA generativa es creciente**, pero no parece ser suficiente para garantizar un papel de liderazgo a nivel mundial en los próximos años si no se aceleran fuertemente las inversiones y la disponibilidad de recursos humanos**.**

La UE mantiene importantes deficiencias en la cadena de valor de la IA, junto con otras en el sector de los semiconductores. Además, su esfuerzo inversor global es menos extenso y más fragmentado en comparación 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 los usuarios de todo el mundo frente a sus competidores mucho más grandes y fuertemente apoyados por sus respectivos gobiernos.

La actual **debilidad europea en la fabricación avanzada de semiconductores** se extiende a los **circuitos integrados específicos de IA** (como GPU, FPGA y ASIC), la disponibilidad de **plataformas de software en la nube** y la disponibilidad de **grandes modelos de lenguaje (LLM)** con importantes cuotas de mercado global que sirven de base para el 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 para las startups europeas en el campo de la IA es que sean **adquiridas por otras grandes empresas no europeas o migren para continuar su proceso de escalado en Estados Unidos**. Además, dependen de las estrategias de retorno de inversión de fondos de inversión especializados, muchos de ellos no europeos, que han entrado en su

capital. Esta situación es especialmente preocupante para quienes desarrollan productos o servicios basados en IA para la defensa.

10. **El valor de los ecosistemas europeos de innovación centrados en la IA está creciendo** con la participación de las grandes empresas y las administraciones públicas nacionales y de la UE como motores que asumen la necesidad de aumentar la **interacción estable entre los actores** a través de políticas, programas e instrumentos de financiación adecuados.

Este proceso es menos evidente debido a las **connotaciones de seguridad y a una menor apertura de miras de las empresas y las administraciones públicas**, aunque están empezando a surgir núcleos de ecosistemas innovadores específicos apoyados por programas de contratación militar y de investigación y desarrollo de uso dual en diversas partes de la UE, aunque con una perspectiva nacional.

11. A pesar de que **Estados Unidos sigue siendo el país en el que residen los fondos de inversión en defensa mejor dotados**, en varios países europeos están creándose o adaptándose nuevos fondos especializados en defensa y seguridad, tanto en la fase de puesta en marcha como en fase de escalado de nuevas empresas tecnológicas.

Esta situación también se ha comenzado a observar en España con una fuerte **implicación de las agencias públicas de financiación junto con el capital privado en las rondas iniciales de financiación**. Esta situación se apoya en grandes fondos de inversión, ya sean nuevos o con la implementación 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 técnicas de ingeniería digital centradas en datos** como en la **simulación** (por ejemplo, con el empleo de gemelos digitales) utilizando la IA como factor esencial para aumentar la funcionalidad y flexibilidad de sus productos.

El uso acelerado de **técnicas integradas de gestión de datos** y el uso más incipiente de **gemelos digitales** y **fabricación aditiva 3D** para reducir los ciclos de desarrollo y facilitar los ciclos posteriores de operación y mantenimiento se han extendido entre todos los grandes contratistas de programas de defensa.

13. Las **limitaciones de tamaño de la industria española de defensa** pueden impedirle desempeñar un mayor protagonismo en los grandes programas de defensa que se pondrán en marcha en la UE 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 aumentar los recursos para el desarrollo y la adquisición de sistemas de defensa que cubran las lagunas identificadas representan una oportunidad en los próximos años para fortalecer la industria europea de defensa y su competitividad en los mercados globales apoyada en 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 esta cuestión en las convocatorias y licitaciones públicas de las administraciones públicas cuya normativa debe adaptarse para acelerar el ciclo de innovación.

El proceso de elaboración del nuevo Programa Marco de Investigación e Innovación de la UE, el del programa sucesor del actual Fondo Europeo de Defensa, las prioridades de la Agencia Europea de Defensa y la Agencia Espacial Europea son grandes oportunidades para **cubrir los gaps identificados y mejorar la soberanía tecnológica europea en IA** si se incrementasen significativamente los recursos y las sinergias entre ellos.

15. El papel de los **estándares y normas industriales para los productos de IA**, así como los procesos de **certificación de sistemas basados en IA**, es clave para lograr una rápida expansión del mercado de sistemas de defensa inteligentes interoperables a nivel internacional.

Todavía estamos en una fase no consolidada en la que no hay muchos estándares específicos relacionados con la IA militar o de organismos internacionales. En 2024, en la Estrategia de IA revisada de la OTAN, se decidió establecer un panorama de *pruebas, evaluación, verificación y validación de IA (TEV&V)* en toda la Alianza para garantizar la adopción responsable de la IA.

Conclusiones sobre la dimensión táctica, operativa y estratégica del uso de la IA por parte de las Fuerzas Armadas

1. Se está produciendo una **evolución gradual hacia un campo de batalla inteligente** en el marco de un proceso continuo de digitalización que seguirá siendo muy rápido e intenso a lo largo de esta década.

Su despliegue en el sector de la defensa está siendo más lenta en que en las áreas de uso civil, dada la **relativa inmadurez de las tecnologías involucradas para delegar funciones críticas en ellas**, y la necesidad de asegurar la coexistencia con muchos otros sistemas militares preexistentes.

2. La **búsqueda de la superioridad en las fuerzas de combate** para experimentar con soluciones tecnológicamente inmaduras y acelerar la innovación tecnológica, requiere

mantener una estrecha interacción entre las Fuerzas Armadas, las empresas y 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 uso de soluciones de IA en múltiples áreas, respaldadas por la **captura y el análisis de datos casi en tiempo real** procedentes de múltiples sensores y el uso de datos sintéticos cuando sea necesario.

3. El **uso de sistemas de IA autónomos o semiautónomos dentro de cadenas de armas letales** es tecnológicamente viable, ya sea en el caso de que su uso se limite al proceso de identificación y selección de objetivos o en su neutralización directa o indirecta.

Este uso parece acelerarse durante la década actual con la aparición o continuación de conflictos militares de alta intensidad en los que el uso de la IA en sistemas autónomos o semiautónomos se ha convertido en un factor clave para asegurar la superioridad en 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 es impulsada por las administraciones públicas o grupos de empresas que crean los llamados "***espacios de datos compartidos***". Sin embargo, en el sector de la defensa, muchos de los conjuntos de datos relevantes para el entrenamiento de sistemas ML o LLM están clasificados y no se comparten fuera de las organizaciones militares. Por esta razón, los datos sintéticos se han generalizado. El envenenamiento de datos y las vulnerabilidades en el dominio del ciberespacio se suman a su complejidad.

5. **El papel del ser humano en el bucle de decisión se ha convertido en un factor clave** desde el punto de vista técnico y táctico de los sistemas de IA en defensa, independientemente de las consideraciones éticas y las reglas de enfrentamiento que su uso pueda implicar o motivar.

La aceleración del desarrollo tecnológico de los sistemas de armas autónomas letales (SALA) permitiría su incorporación acelerada a los ejércitos de todos los Estados miembros de la UE, lo que, de ocurrir, implicará profundas modificaciones en la forma en que se llevan a cabo las operaciones militares y en su impacto en la población.

6. En el ámbito de la **guerra electrónica**, la IA desempeña un papel cada vez más importante. 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 superpuestos a los conflictos militares convencionales.

La **creciente complejidad de los potenciales ataques a la información radioeléctrica transmitida de interés militar** (señales de navegación, información de mando y control, datos satelitales, etc.) hace necesario el desarrollo de nuevas y más sofisticadas técnicas inteligentes de guerra electrónica capaces de detectar señales en todo el espectro de frecuencias.

7. La **generación automática de campañas de difusión de desinformación y narrativas** dirigidas a entidades o sectores específicos de la población a partir de herramientas de IA se ha extendido y está en manos de actores estatales o no estatal.

Esta situación proviene 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. Cada vez es mayor el uso de herramientas de IA generativa para su generación y difusión en redes sociales.

8. La UE y sus Estados miembros cuentan con herramientas y procedimientos impulsados por la IA para **detectar y contrarrestar las noticias falsas y las narrativas intencionadas de otros países**.

El uso de herramientas y procedimientos de IA está ligado a la **necesidad de los gobiernos de contrarrestar el crecimiento de la injerencia y la manipulación de otros países**, lo que ha obligado a la creación de unidades y procedimientos especializados para el intercambio de información entre gobiernos aliados y protocolos de alerta y respuesta rápida.

9. **El sector espacial se configura como un sector dual** en el que tanto los usuarios públicos como los privados pueden compartir plataformas satelitales, sistemas de lanzamiento y seguimiento, datos obtenidos, así como herramientas específicas de IA.

Las plataformas o constelaciones de satélites individuales se utilizan en aplicaciones civiles y militares de observación, comunicaciones y navegación. Aunque su estructura puede ser dual, puede requerir el **desarrollo de cargas útiles especializadas para cada uno de los dominios**. El uso para aplicaciones militares, como demuestra el uso de *Starlink* en Ucrania, las ha convertido en activos esenciales para todos los gobiernos y, con ello, han adquirido relevancia estratégica para todos los países.

10. **La IA tiene un valor cada vez mayor en la gestión eficaz de un dominio espacial más poblado**, en términos de objetos y fragmentos espaciales, especialmente en órbitas bajas, que pueden utilizarse como objetivo militar contra activos de otros países.

Las herramientas de IA para un mejor conocimiento de la situación en el dominio espacial permiten **reducir o gestionar los riesgos de colisión** con desechos de satélites u otros elementos naturales, las **interferencias** causadas o no en la navegación por satélite y la **protección de los activos espaciales**.

11. **El desarrollo y adopción de sistemas hardware de IA especializados en la operación de activos espaciales** con el objetivo de reducir el consumo y aumentar la flexibilidad ha aumentado fuertemente. Esta evolución permite tener una mayor capacidad de procesamiento a bordo y la ejecución autónoma de funciones más complejas.

El espacio es un dominio dual de creciente relevancia en el que **la automatización de las operaciones espaciales implica la necesidad de aumentar la capacidad de procesamiento a bordo** para la ejecución de algoritmos de IA, el análisis y filtrado de los datos recopilados, y su transferencia a las estaciones terrenas.

12. **La UE y España se encuentran en una buena posición para explotar el sector espacial** mediante el desarrollo de aplicaciones basadas en IA que exploten los datos generados por los activos espaciales y mejoren así la soberanía tecnológica europea en la nueva generación de plataformas espaciales.

La experiencia acumulada por la Agencia Espacial Europea y diversas agencias espaciales nacionales de los Estados miembros, junto con una profusión de nuevas empresas del sector espacial con la integración de soluciones de IA, permitirá mejorar la seguridad europea si se les dota de recursos suficientes. España es un jugador relevante en el dominio especial.

Conclusiones sobre la dimensión ética y regulatoria de la IA

1. **No existe una regulación específica para el uso de la IA en defensa**. Solo existen directrices voluntarias de uso basadas en el uso responsable de la IA en el ámbito militar propuestas por diversos organismos, pero sin una aceptación global por todos los países.

Las regulaciones de IA para aplicaciones civiles tampoco están acordadas y muchos países tienen diferentes enfoques basados en sus visiones histórico-culturales y su posicionamiento tecnológico en los mercados globales. Sin embargo, el Reglamento de la UE sobre IA podría utilizarse como base para el desarrollo de sistemas duales de IA.

2. La **creciente disponibilidad de sistemas inteligentes automatizados sin necesidad de que un ser humano tome las decisiones necesarias** que ya permite el desarrollo de la IA implica asumir considerables riesgos éticos, especialmente en el caso del uso de **sistemas de armas letales autónomos o semiautónomos** (SALA).

La UE debe ser consciente de que las normativas para el uso de los SALA deben ser consensuadas en la medida de lo posible a nivel global, estableciendo limitaciones a su desarrollo y uso. De no ser así, como ocurre actualmente, se corre el riesgo de que se produzcan enfrentamientos asimétricos en su uso que pueden alcanzar no sólo a los ejércitos estatales, sino también a otros grupos armados cuyas normas de uso son imprevisibles o no están sujetas al cumplimiento de normas internacionales.

3. El **desarrollo de productos basados en tecnologías duales por parte de empresas ajenas al sector de la defensa** ha generado problemas derivados de la aceptación de proyectos de potencial utilidad militar por parte de su personal técnico, ya que se consideraba que no existía una aceptación previa explícita y que 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 signifique 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 de apoyo a la toma de decisiones militares basados en IA no pueden analizarse como sistemas aislados, sino por el **papel que asumen en la integración en cadenas letales, 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.

5. Aunque se han realizado muchos **esfuerzos por parte de organizaciones internacionales para lograr un uso responsable de la IA**, 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 estos acuerdos vayan más allá de la aprobación de un conjunto de **directrices de implementación voluntaria** que los países firmantes acepten, pero sin la existencia de organismos internacionales que garanticen su cumplimiento, como sí es el caso de las armas nucleares.

6. **Encontrar el equilibrio entre una regulación que proteja al usuario y apoye la innovación no es fácil**, y ese debate sigue abierto en el contexto de la Unión Europea en el proceso de implementación de su regulación de IA diseñada solo para aplicaciones civiles y no militares.

La UE deberá adoptar un enfoque flexible durante la aplicación del Reglamento, garantizando interpretaciones coherentes en todos los Estados miembros y adaptando periódicamente la normativa sobre IA a los avances tecnológicos para garantizar su pertinencia.

7. La **progresiva convergencia de la IA con la neurotecnología** abre el camino a una nueva fase de conflictos militares con problemas éticos específicos como los de privacidad y libre albedrío en el contexto de la discusión de los neuroderechos y su aplicación en la defensa.

El campo de la neurotecnología aplicada a la mejora de las capacidades cognitivas humanas, más allá del uso médico, tiene enormes **implicaciones éticas derivadas de la alteración de las capacidades cognitivas de la especie humana**. Su desarrollo en el campo de la defensa se lleva a cabo con poca transparencia por parte de las potencias más avanzadas, conscientes de su potencial relevancia futura.

8. Un factor que condicionará el desarrollo y uso de la IA en las operaciones militares es el posible **enfrentamiento militar entre adversarios con diferentes marcos éticos y morales en el uso de sistemas autónomos.**

Este factor puede condicionar la autolimitación en el uso de ciertas armas inteligentes para no estar en desventaja frente al adversario, lo que significa que el uso de la IA en estos contextos debería limitarse, al menos, a alcanzar compromisos de "*no primer uso*", como ya ocurre en ciertos países con el uso de armas nucleares.

9. Las **tecnologías para aumentar las capacidades cognitivas**, más allá de lo que la especie humana permite en su biología, a través de la convergencia entre la neurotecnología y la IA, es todavía un tema lejano en términos de adopción masiva, pero que, en vista de su acelerado desarrollo, implicará anticipar medidas éticas.

La **viabilidad tecnológica de la convergencia de la neurotecnología con la IA** está más cerca en el tiempo. El uso de técnicas de biología sintética en tejido neuronal y su convergencia con la neurotecnología y la inteligencia artificial también está avanzando rápidamente. Este proceso de convergencia multitecnológica nos obliga a pensar en las **consecuencias éticas y regulatorias** que se derivarían de convertirse en una realidad en los próximos años.

Conclusiones sobre la soberanía tecnológica europea en IA

1. Dada la relevancia estratégica de la tecnología, **el objetivo de la UE de alcanzar su tan ansiada autonomía estratégica pasa por aumentar su soberanía tecnológica**.

Este objetivo debe perseguirse, incluso aceptando la imposibilidad de alcanzar la autarquía en la IA, para lo cual será necesario contar con aliados fiables a largo plazo.

2. Los Estados miembros de la UE dependen de múltiples sistemas de defensa que incorporan **funcionalidades de IA desarrolladas localmente o desde otros países cuya transferencia de conocimiento desde el proveedor es parcial.**

El equipamiento militar no desarrollado localmente de 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 de uso 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.

3. El **desarrollo futuro de sistemas militares de IA con un alto grado de soberanía tecnológica europea** requerirá el establecimiento y la financiación significativa de programas comunes público-privados respaldados por una voluntad política sostenida con prioridades a largo plazo.

Este será un proceso largo y complejo ya que las principales competencias en política de defensa residen en los Estados miembros, más allá de la coordinación y utilización de los recursos relacionados con la política industrial que se puedan coordinar y financiar desde el presupuesto de la UE.

4. 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 incorporan, de forma relevante, módulos de inteligencia artificial.

La velocidad a la que se está desarrollando la tecnología relacionada con la IA dificulta que la industria de un solo Estado miembro posea todas las capacidades necesarias para el desarrollo autónomo de sistemas militares inteligentes. Por esta razón, **la cooperación tecnológica estable entre los agentes de la industria de defensa en un mercado único debe ser un objetivo político prioritario**.

5. Una parte significativa del **continuo aumento de la inversión en sistemas de tecnología de defensa** en relación con el PIB acordado por los Estados miembros de la OTAN pertenecientes a la UE debe asignarse a las **inversiones en sistemas 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.

6. Las **startups con productos de IA disruptivos** tienen dificultades para experimentar con soluciones en bajos estados de madurez (TRL 5-6 o menores) junto a los ejércitos 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 debería pasar por la creación de instrumentos específicos para la contratación pública de tecnología por parte del Gobierno, y las modificaciones reglamentarias e interpretativas necesarias por parte de la UE y los Estados miembros. Las medidas propuestas por la UE para promover el **emprendimiento deep-tech** constituyen contribuciones útiles desde esta perspectiva.

7. La **estrategia de simplificación administrativa** impulsada por la UE tendrá que adaptarse rápidamente al sector de la defensa para reducir drásticamente los plazos de los contratos de adquisición y mantenimiento de nuevos sistemas armamentísticos que impliquen el uso de fondos de la UE.

Aunque esta situación no es exclusiva de la IA y también afecta a otras tecnologías emergentes, se manifiesta claramente en el desarrollo y adquisición de sistemas autónomos en los que el avance en su implementación real es muy rápido, como demuestra la experiencia de Ucrania.

A partir de las conclusiones extraídas del análisis realizado en este informe, **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 garantizar su rápida adopción por parte de sus fuerzas armadas. Otras grandes potencias tecnológicas con las que compite han asumido esta realidad y han priorizado el desarrollo y uso de la IA, conscientes del **papel esencial que juegan en la búsqueda de la supremacía militar**.

Posibles escenarios de la soberanía tecnológica europea en IA

Sobre la base de las conclusiones obtenidas, se han identificado y evaluado **tres posibles escenarios para la UE en materia de IA en defensa en el horizonte de 2030**. Somos conscientes de que se trata de escenarios básicos para promover un debate abierto y poder analizar en detalle, si se desea, la situación en el conjunto de la UE o en algunos de los Estados miembros. Los tres escenarios identificados han sido denominados el escenario **"optimista"**, el escenario **"realista"** y el escenario **"pesimista"**. En las siguientes subsecciones se describen con más detalle.

Escenario optimista para 2030

El escenario optimista supone que la UE se convierte en una potencia tecnológica mundial en materia de IA, liderando junto a Estados Unidos y China el desarrollo y el uso de la IA en defensa.

Este escenario se caracteriza por las siguientes características definitorias.

- Creación de un mercado único europeo de defensa que reduzca significativamente la fragmentación actual y maximice los resultados. Esto hará necesario realizar las modificaciones reglamentarias necesarias 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.

- Lograr una elevada soberanía tecnológica en IA aplicada a la defensa, desde la capacidad de diseñar y fabricar hardware específico de IA hasta el desarrollo de aplicaciones integradas en sistemas militares.

- Lanzamiento de grandes programas comunitarios de investigación y desarrollo en defensa, haciendo hincapié en la aplicación de la IA plenamente integrada en los programas nacionales.

- Aparición de grandes empresas europeas de IA en defensa que se han convertido en líderes mundiales en algunas de las áreas de aplicación.

Escenario realista para 2030

El escenario realista supone que **la UE se convierte en una potencia tecnológica relevante en el desarrollo y uso de la IA en defensa**, con liderazgo en algunas áreas técnicas específicas, pero dependiente de otras potencias en el resto de las áreas tecnológicas relevantes en IA.

Este escenario se caracteriza por las siguientes rasgos definitorios.

- La creación de un mercado único europeo de defensa no ha cumplido todos sus objetivos, pero se ha producido una **mayor sinergia de acciones con la reducción significativa de la fragmentación actual** en algunas áreas prioritarias de defensa.

- Se han introducido algunas modificaciones normativas para facilitar la adopción de acuerdos conjuntos en el ámbito de la defensa a través de esquemas de cooperación reforzada coordinados con la OTAN.

- Se ha avanzado hacia una **soberanía tecnológica limitada en la IA aplicada a la defensa** con capacidades mejoradas de diseño de chips específicos de la IA y el desarrollo de aplicaciones integradas en sistemas militares, **aunque persiste la dependencia de proveedores externos de componentes y fabricación**.

- Implementación de **programas comunitarios de investigación y desarrollo 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 de las grandes empresas nacionales de IA en el ámbito de la defensa** que ha permitido garantizar el liderazgo mundial en algunas áreas de aplicación de la IA.

Escenario pesimista en 2030

El escenario pesimista supone que **la UE no se convierte en una potencia tecnológica global en el desarrollo y uso de la IA en defensa**, consolidando su dependencia de otros países.

Este escenario pesimista, que supone una continuidad de la situación actual, se caracteriza por los siguientes rasgos:

- 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.

El escenario realista podría lograrse para 2030 si se asignaran los recursos necesarios y existiera una voluntad política consensuada a largo plazo. A ello contribuirá el convencimiento de los Estados miembros de que la conflictiva situación global obligará a la UE a coordinar mucho mejor sus acciones de defensa y a hacer más viables los acuerdos para alcanzar este escenario. El siguiente apartado pretende ofrecer, a partir de las conclusiones extraídas, un conjunto de recomendaciones de actuación para que el escenario realista presentado pueda convertirse en una realidad en 2030.

Recomendaciones para la acción

A partir de las conclusiones realizadas, se propone un **conjunto reducido de recomendaciones de actuación** para la regulación, el desarrollo y el uso avanzado de la IA en los sistemas de defensa con el fin de aumentar su uso responsable en el contexto europeo y alcanzar el escenario realista descrito en el apartado anterior. **Las recomendaciones de acción propuestas no son totalmente inconexas**; de hecho, lograr un alto impacto en el funcionamiento de las Fuerzas Armadas de los estados miembros de la UE a través de ellas

puede hacer aconsejable la implementación de varias de ellas de manera simultánea y coordinada. Las recomendaciones de acción propuestas son las siguientes:

Recomendación R1. Priorización de la IA en los programas de I+D, defensa y contratación militar de los Estados miembros con visión de uso dual.

La UE y los Estados miembros deben **intensificar sus esfuerzos sobre el doble uso de la IA** estableciendo prioridades específicas en sus programas públicos de investigación y contratación pública y facilitando el uso de sus resultados tanto en el mercado civil como en el militar.

Esta recomendación debe tenerse en cuenta en el proceso de negociación del Programa Marco de Investigación e Innovación de la UE **HE 2028-2034** y del futuro **Fondo Europeo de Defensa** financiado en el futuro marco *financiero plurianual de la UE (2028-2034).*

Recomendación R2. Necesidad de crear un marco regulador común para el desarrollo y el uso de la IA en la defensa, en consonancia con los principios y valores europeos.

Es necesario establecer lo antes posible un **marco regulador común para el uso de la IA en la defensa** basado o no en el Reglamento sobre IA vigente. Aunque las regulaciones están 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 su 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.

Recomendación R3. Facilitar la experimentación acelerada 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 para evaluar la eficacia y los riesgos que puede conllevar su uso en aplicaciones vinculadas a la toma de decisiones.

La experiencia adquirida en Ucrania permite una reducción drástica de los tiempos de desarrollo si se incorpora al ciclo de vida la experimentación en condiciones reales. Su aplicación podrá implicar la creación de espacios de datos físicos y de defensa compartidos en los Estados miembros, pero accesibles a terceros en condiciones preestablecidas. Sería

posible aprovechar la red de centros de pruebas del programa DIANA desplegados en los estados miembros de la OTAN que tengan una relación con la IA.

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.

La ampliación de la *Ley del Chip* con recursos adicionales para incluir diversas acciones destinadas a disponer de circuitos integrados de IA específicos para los sistemas de defensa con el mayor grado posible de soberanía tecnológica europea. España podría impulsar una línea piloto de chips de IA para defensa.

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 relacionada con la IA y su convergencia con otras tecnologías emergentes, la UE tendrá que redoblar sus esfuerzos para atraer, retener y formar a especialistas en IA que puedan ser empleados por la industria de defensa y las Fuerzas Armadas para acelerar su adopción en Europa.

La UE debe reducir la escasez de especialistas en IA mediante la creación de programas de formación conjuntos entre varios países, apoyados por la Comisión Europea y la industria de defensa, para actualizar los conocimientos. Las prioridades de formación deben estar en consonancia con las lagunas de la UE identificadas en el *Libro Blanco de la Defensa*. Desde un punto de vista instrumental, una opción posible es aprovechar las redes universitarias europeas y la creación de un programa transversal específico con acciones en HE 2028-2024 alimentado con recursos de la UE y de los Estados miembros de la UE.

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 el fortalecimiento de ecosistemas nacionales de IA en defensa se entiende como un requisito previo para la **creación de un "ecosistema europeo" flexible y suficientemente integrado** para mejorar el posicionamiento europeo en un contexto global altamente competitivo.

Los ecosistemas nacionales deben centrarse en los ámbitos de la IA aplicada a la defensa en los que exista un fuerte tejido industrial y favorecer el desarrollo de grandes proyectos de interés común europeo en los que la IA sea una tecnología clave. Una opción es apro-

vechar el esfuerzo ya realizado por la Comisión Europea con las llamadas *fábricas de IA*, evolucionar algunas de ellas con un enfoque dual, asegurando su relación e interacción con las Fuerzas Armadas y la industria de defensa.

Recomendación R7. Poner en marcha una aceleradora europea de la defensa basada en la 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 doble naturaleza 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.

El objetivo es **evitar o limitar una fragmentación del proceso de aceleración**. Una opción para implementar la aceleradora es su integración futura en el Consejo Europeo de Innovación (EIC) a partir de 2028, aunque con las especificidades del sector de defensa, redefiniendo su desempeño en TRLs bajos, e incrementar la coordinación con las aceleradoras del programa DIANA de la OTAN, una de ellas ubicada en España.

Recomendación R8. Actualizar la Estrategia Tecnológica de Defensa de España 2020 (ETID 2020) 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.

Actualizar la ETID 2020 del Ministerio de Defensa para alinearlo con las prioridades de "*Preparación 2030*" de la Comisión Europea, el Programa Europeo de Defensa, el programa Horizonte Europa 2028-2034, las prioridades de la OTAN en relación con la IA y los programas españoles de defensa y seguridad relacionados.

La actualización debería llevarse a cabo lo antes posible para competir mejor con otros países y contar con un marco nacional de apoyo que aumente la participación y el liderazgo español en el futuro Programa Marco de Investigación e Innovación de la UE Horizonte Europa HE 2028-2034.

Recomendación R9. Alinear la estrategia europea con escenarios realistas para lograr la soberanía tecnológica en IA para la defensa.

El análisis pormenorizado de la soberanía tecnológica europea y española en IA para uso militar debe estar **alineado con los escenarios factibles hacia 2030** que se van a impulsar conjuntamente desde una posición realista de la situación europea.

Se considera que el **escenario realista** indicado anteriormente es adecuado para España y debe ser alcanzado. En cualquier caso, se considera necesario **reevaluar periódicamente la**

situación de la soberanía tecnológica europea en IA utilizando para ello indicadores sintéticos 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. Este alineamiento debe contemplar la actualización de las prioridades establecidas para la defensa en áreas relacionadas con la IA.

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.

Se considera necesario crear un ***Observatorio de IA en Defensa*** para evaluar la evolución desde las dimensiones científico-tecnológicas, socioeconómicas, tácticas y operativas en los ejércitos, y éticas y regulatorias. No se trata, por tanto, de una cuestión de vigilancia tecnológica, sino también de mercados, usuarios y el contexto en el que se utiliza.

Este *Observatorio* podría ser **coordinado por la Comisión Europea**, junto a la industria europea de defensa y con la participación de expertos externos. El Observatorio también debería coordinar sus actividades con la OTAN y, en temas específicos, con las existentes en otros países aliados con los niveles necesarios de confidencialidad. Parte de la documentación generada podría considerarse como clasificada.

Observación final

Este informe ha presentado un **escenario muy dinámico del uso de la IA en defensa**, impulsado por objetivos de supremacía de las grandes potencias y limitado por los riesgos geopolíticos. Los intensos conflictos militares actuales están actuando como impulsores del desarrollo y despliegue de sistemas basados en IA en el campo de batalla, lo que acelera la toma de decisiones. Por este motivo, la tecnología, la economía, el ejército, las perspectivas ética y regulatoria están profundamente entrelazadas,

En este contexto, **la UE se enfrenta a un reto urgente y profundo para poder desempeñar un papel relevante en la carrera mundial para el dominio de la IA en el sector de la defensa.** Para abordarlo, la UE debe reducir la fragmentación, proporcionar abundantes recursos, tanto humanos como materiales, llevar a cabo cambios regulatorios inteligentes y una voluntad política sostenida. Todos ellos deben ser compilados e integrados para concurrir con éxito en el panorama global de la inteligencia artificial y su uso en defensa.

COMPOSICIÓN DEL GRUPO DE TRABAJO

El **grupo de trabajo** estuvo integrado por las siguientes personas[02]:

- **Gonzalo León** (Coordinador) (FEI y catedrático emérito de la UPM).
- **Luis Fernando Álvarez-Gascón** (FEI y CEO Secure eSolutions GMV).
- **Txema Báez Cristóbal** (FEI y NOVADAYS).
- **Juan Carlos Dueñas** (Catedrático de la UPM).
- **Ángel Gómez de Agreda** (Coronel (R) del Ejército del Aire y del Espacio y de Europa-via Middle East).
- **Asunción Gómez-Pérez** (Catedrático de la UPM).
- **Luis Guerra** (FEI y Oesia Group).
- **José María Insenser Farré** (FEI, y AMETIC IPCEI Chip).
- **Juan Bosco Morales de los Ríos** (CTO Grupo Amper).
- **David Ramírez Morán** (Analista IEEE-CESEDEN, Ministerio de Defensa).
- **Luis Vázquez Martínez** (FEI y catedrático emérito de la UCM).

Soporte técnico y colaboración de:

- **Aureliano da Ponte** (Investigador de la UCM y consultor en defensa).
- **José Sousa** (AMPER Portugal).

Durante las reuniones del Grupo de Trabajo, se ha invitado a las siguientes personas a mejorar las perspectivas del análisis:

- **Manuel Pérez Cortés** (Director del Área de Defensa de GMV).
- **Ricardo Sáenz** (Director de Programas de Defensa y Seguridad de GMV).
- **GD Guillermo Ramírez Altozano** (Director de Sistemas de Información, Telecomunicaciones y Asistencia Técnica (JCISAT) del Ejército de Tierra, Ministerio de Defensa.
- **GB (R) Roberto Villanueva** (Anterior director of Ciberseguridad del CESTIC, Ministerio de Defensa).
- **Claudio Feijoo** (Catedrático de la UPM. Responsable de la Cátedra Jean Monnet de Diplomacia Tecnológica y Soberanía Digital).
- **GD (R) Juan Antonio Moliner** (Vicepresidente de la Academia de las Ciencias y las Artes Militares, ACAMI).

Carmen Vela (Presidenta FEI) y **Pedro Morenés** (Presidente Grupo Amper) también han participado en algunas reuniones del Grupo de Trabajo.

---

02 En la versión completa del informe se pueden encontrar currículos más extensos de los miembros del Grupo de Trabajo y de los expertos invitados.

Versión resumida del informe final

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

septiembre 2025


ABB


aertec
SOLUTIONS


AIRBUS


AIRBUS
DEFENCE & SPACE


AMADIX


ANTOLIN


ayming


CCOO


Fundación
Caja Rural
de Asturias


Fundación
General CSIC


FUNDACIÓN
Parque Científico
de Madrid


gmv
INNOVATING SOLUTIONS


IENAI [SPACE]


innovaIrv


MERCK


MSD
INVENTING FOR LIFE


Poile
ingenieros s.l.


sacyr


SAVANA
The AI + RWE Company


Smart
Agrifood


tecnalia


Talgo


uc3m
Parque
Científico