

La transformación de la inteligencia en la seguridad y defensa de Europa: desafíos y oportunidades en la era digital

Carlos Hugo Fernández-Roca Suárez

Resumen

La inteligencia en seguridad y defensa está experimentando una profunda transformación impulsada por la aceleración tecnológica de la cuarta revolución industrial, caracterizada por avances notables en digitalización, automatización, inteligencia artificial y gestión masiva de datos. Este salto tecnológico, sumado a un escenario geopolítico cada vez más desafiante, sobre todo, tras la agresión rusa contra Ucrania, obliga a Europa a reforzar urgentemente sus capacidades estratégicas de forma coordinada y efectiva.

En este nuevo contexto, la inteligencia artificial emerge como motor fundamental del cambio, revolucionando la obtención, análisis y difusión de inteligencia militar, así como la automatización eficiente de procesos estratégicos y tácticos. Ejemplos internacionales relevantes, como la «guerra algorítmica» del Project Maven en Estados Unidos, ilustran cómo la inteligencia artificial incrementa significativamente la capacidad de anticipación y reacción frente a amenazas actuales y futuras.

La Unión Europea avanza decididamente hacia la consecución de una soberanía tecnológica que garantice plenamente su autonomía estratégica. Con este propósito, iniciativas clave como el programa «Preparación 2030» —inicialmente anunciado como ReArm Europe— y el Fondo Europeo de Defensa impulsan inversiones orientadas al desarrollo de tecnologías emergentes, fortaleciendo así la base industrial europea y reduciendo las dependencias externas en un contexto internacional cada vez más exigente y competitivo.

Palabras clave

Inteligencia artificial (IA), Soberanía tecnológica, Autonomía estratégica, Cuarta revolución industrial y Defensa europea.

The transformation of intelligence in Europe's security and defence: challenges and opportunities in the digital age

Abstract

Intelligence in security and defense is undergoing a profound transformation driven by the technological acceleration of the Fourth Industrial Revolution, characterized by significant advances in digitalization, automation, artificial intelligence, and large-scale data management. This technological leap, combined with an increasingly challenging geopolitical landscape —especially following Russia's aggression against Ukraine— compels Europe to urgently strengthen its strategic capabilities in a coordinated and effective manner.

In this new context, artificial intelligence emerges as a fundamental driver of change, revolutionizing the collection, analysis, and dissemination of military intelligence, as well as efficiently automating strategic and tactical processes. Relevant international examples, such as the «algorithmic warfare» of Project Maven in the United States, demonstrate how artificial intelligence significantly enhances capabilities for anticipation and reaction to current and future threats.

The European Union is decisively progressing toward achieving technological sovereignty that fully guarantees its strategic autonomy. To this end, key initiatives such as the «Preparation 2030» program —initially announced as ReArm Europe— and the European Defence Fund promote investments aimed at developing emerging technologies, thus strengthening Europe's industrial base and reducing external dependencies in an increasingly demanding and competitive international environment.

Keywords

Artificial Intelligence (AI), Technological Sovereignty, Strategic Autonomy, Fourth Industrial Revolution, and European Defence.

1 Introducción

La seguridad y la defensa de Europa están inmersas en una profunda transformación, impulsada por avances tecnológicos sin precedentes en el ámbito digital. La acelerada evolución de la cuarta revolución industrial —caracterizada por avances en digitalización, automatización, datos masivos e inteligencia artificial (en adelante, IA)— está alterando la forma en que se recopila, analiza y emplea la inteligencia en el ámbito militar y estratégico. Estos desarrollos tecnológicos, junto con un entorno geopolítico más desafiante tras acontecimientos como la agresión rusa a Ucrania, han convenido a Europa de la necesidad de reforzar sus capacidades de seguridad y defensa de manera urgente y coordinada (Consejo Europeo, 2022).

Los gobiernos de la Unión Europea (en adelante, UE) han reconocido que invertir en tecnologías emergentes y en la base industrial de defensa es esencial para mejorar la capacidad europea, asumir una mayor cuota de la carga en la seguridad transatlántica y reducir dependencias críticas en materia de tecnología y armamento (Fiott, 2024). En este contexto, instituciones europeas y Estados miembros están emprendiendo reformas y planes ambiciosos para modernizar la inteligencia de defensa, incorporando IA y otras tecnologías disruptivas, al tiempo que promueven la soberanía tecnológica europea como un objetivo común que refuerza, y no contradice, la identidad y los intereses nacionales.

Este artículo analiza dicha transformación de la inteligencia en Europa, abarcando el impacto de la Cuarta Revolución Industrial, el papel central de la IA, las respuestas institucionales —como el plan ReArm Europe—, ejemplos concretos de aplicación tecnológica y la búsqueda de autonomía tecnológica.

2 Impactos de la Cuarta Revolución Industrial en la inteligencia de defensa

La denominada cuarta revolución industrial (en adelante, 4RI) ha sido descrita como un cambio de época de naturaleza disruptiva que difumina las fronteras entre lo físico y lo digital, lo civil y lo militar, la paz y el conflicto (Fojón, 2018). Al igual que revoluciones industriales previas transformaron la conducción de la guerra, la 4RI está introduciendo tecnologías avanzadas —como sistemas autónomos, *big data*, computación en la nube, Internet de las Cosas y aprendizaje automático— que plantean tanto oportunidades como retos para la defensa. En el ámbito de la inteligencia militar y estratégica, estos cambios implican la capacidad de procesar volúmenes masivos de información en tiempo real, provenientes de fuentes cada vez más diversas —sensores remotos, redes sociales, imágenes satelitales comerciales—, así como la automatización de tareas analíticas rutinarias mediante algoritmos.

Las fuerzas armadas y agencias de inteligencia europeas deben adaptarse a este nuevo entorno tecnológico para mantener la superioridad informativa y la capacidad de anticipación. Esto supone transformar doctrinas y procedimientos de inteligencia tradicionales. Por ejemplo, la proliferación de sensores avanzados y plataformas no tripuladas aumenta, de forma exponencial, los datos recabados —señales, imágenes, comunicaciones—, lo que exige nuevas herramientas de fusión de datos y análisis apoyadas en IA para extraer información relevante. A su vez, actores no estatales y potencias rivales también acceden a tecnologías de doble uso asequibles —como drones o software de ciberataque— que «democratizan» el acceso al poder disruptivo, obligando a las agencias europeas a acelerar su innovación (Fojón, 2018). En definitiva, la 4RI está alterando los cimientos de la inteligencia de seguridad y defensa, haciendo obsoletos métodos tradicionales y requiriendo inversiones en nuevas capacidades técnicas, organizativas y humanas.

Un ejemplo ilustrativo es el concepto de «guerra algorítmica» desarrollado, inicialmente, por el Departamento de Defensa de EE. UU., donde se emplean algoritmos para multiplicar las opciones y acelerar la toma de decisiones en el campo de batalla (Fojón, 2018). Iniciativas pioneras como el Project Maven estadounidense —que aplica aprendizaje automático para analizar imágenes de inteligencia (IMINT) y detectar objetivos— han servido de referencia sobre cómo la automatización inteligente puede elevar la eficacia de la inteligencia militar. Europa ha tomado nota de estas tendencias: España ha evaluado las lecciones de Maven para considerar aplicaciones similares en nuestras fuerzas armadas (Fojón, 2018). La implantación de herramientas derivadas de la 4RI conlleva también interrogantes éticos y doctrinales —por ejemplo, sobre el grado de autonomía permisible en sistemas de armas inteligentes o la confiabilidad de una decisión tomada por una máquina—, debates que están muy presentes en el entorno europeo, donde impera un enfoque humano-céntrico en el uso de la IA (Csernatoní, 2023).

3 La inteligencia artificial como factor transformador

Entre las tecnologías de la 4RI, la IA destaca como el motor central de transformación de la inteligencia en seguridad y defensa. La IA —entendida, en términos generales, como sistemas informáticos capaces de realizar tareas que normalmente requieren inteligencia humana, aprendiendo de la experiencia (Fiott y Lindstrom, 2018)— se ha convertido en una herramienta estratégica de primer orden en los ámbitos militar y de seguridad (Csernatoní, 2023). Potencias como Estados Unidos y China ya integran la IA en sus doctrinas de defensa, considerándola un elemento clave de superioridad tecnológica y alertando incluso de una posible nueva carrera armamentística en este terreno (Csernatoní, 2023). En Europa, aunque su desarrollo ha

sido más lento, existe una conciencia creciente sobre el potencial revolucionario de la IA en el ámbito de la defensa. Por un lado, puede ofrecer ventajas significativas en inteligencia —como el análisis automatizado de amenazas, la simulación de escenarios o el apoyo a la toma de decisiones—; por otro, suscita preocupaciones éticas y de seguridad —como los sesgos algorítmicos, la autonomía letal o las vulnerabilidades cibernéticas, que exigen un marco normativo equilibrado y adaptado a los desafíos emergentes—.

En el campo de la inteligencia militar, la IA promete acelerar y optimizar todo el ciclo de inteligencia: desde la fase de obtención de datos —mediante algoritmos capaces de rastrear fuentes abiertas o gestionar enjambres de sensores—, pasando por el análisis —que incluye el filtrado inteligente de información relevante, el reconocimiento automático de patrones en imágenes o interceptaciones, y la detección de anomalías—, hasta la distribución y explotación de la inteligencia, a través de sistemas de apoyo a la decisión que ofrecen a analistas y mandos opciones óptimas generadas a partir del procesamiento de grandes volúmenes de datos.

Por ejemplo, algoritmos de aprendizaje profundo aplicados a imágenes satelitales pueden identificar movimientos de equipos militares adversarios con mucha mayor rapidez que analistas humanos, permitiendo alertas tempranas. Del mismo modo, herramientas de procesamiento de lenguaje natural pueden clasificar y traducir automáticamente comunicaciones interceptadas, aumentando la eficiencia de la inteligencia de señales.

Estas capacidades podrían mejorar la detección de amenazas, la protección y la preparación ante riesgos emergentes (Fiott y Lindstrom, 2018), reforzando así la seguridad colectiva europea.

No obstante, los efectos de la IA no son unívocamente positivos ni plenamente conocidos. Existe cierto consenso en que, al menos en el corto plazo, la IA actuará como «facilitador estratégico» más que como sustituto total de la inteligencia humana (Fiott y Lindstrom, 2018). Es decir, la autonomía de los sistemas de IA seguirá siendo limitada y el factor humano continuará siendo crítico en la supervisión de algoritmos y en la toma de decisiones finales.

De hecho, la UE ha subrayado la importancia de mantener «control humano significativo» sobre los sistemas de armas autónomos y la inteligencia artificial militar, atendiendo a consideraciones éticas y legales (Parlamento Europeo, 2020). A medida que la IA avanza, Europa enfrenta el reto de aprovechar sus ventajas sin incurrir en riesgos inaceptables: por ejemplo, asegurar que un sistema de IA no introduzca sesgos o errores sistemáticos en el análisis de inteligencia, o que preserve su integridad operativa ante intentos de manipulación, como los ataques que buscan engañar a los algoritmos de reconocimiento.

Por otra parte, la inteligencia artificial no solo actúa como herramienta, sino que también se está consolidando como un objetivo estratégico y un nuevo campo de confrontación. Su progresiva militarización —que abarca aplicaciones ofensivas como los ciberataques, la desinformación potenciada por IA o los vehículos armados no tripulados— obliga a los servicios de inteligencia europeos a desarrollar capacidades específicas de detección, prevención y respuesta (Csernatoní, 2023). Este dilema refuerza la necesidad de que Europa no se quede atrás en el dominio de la IA aplicada a defensa, pero a la vez lidere su uso responsable y conforme al derecho internacional.

En la actualidad, las instituciones de la UE reconocen que la IA es un arma de doble filo: puede reforzar la seguridad —por ejemplo, en tareas de vigilancia y alerta temprana—, pero también plantea amenazas si se emplea de forma maliciosa o escapa al control humano (Csernatoní, 2023). Por ello, la Unión aboga por una IA «fiable, ética y segura», incluso en entornos militares, integrando estos principios en sus políticas y proyectos de investigación vinculados a la defensa.

4 Respuestas institucionales de Europa: del Plan ReArm Europe a la Estrategia Industrial de Defensa

Conscientes de la magnitud del desafío tecnológico, las instituciones europeas han articulado en los últimos años una serie de respuestas estratégicas e iniciativas políticas para transformar sus capacidades en materia de inteligencia, seguridad y defensa. Un hito importante fue la adopción de la Brújula Estratégica de la UE en marzo de 2022, la cual delineó una visión común de seguridad y defensa para la próxima década, enfatizando, entre otros aspectos, la necesidad de mejorar la inteligencia compartida y anticipativa (Consejo de la UE, 2022).

En concreto, la Brújula destacó la creación de mecanismos como la Capacidad Única de Análisis de Inteligencia (*Single Intelligence Analysis Capacity, SIAC*), orientados a integrar mejor la información procedente de los Estados miembros y proporcionar evaluaciones de amenazas más sólidas a nivel de la UE (Consejo de la UE, 2022). Este enfoque estratégico sentó las bases para posteriores planes más específicos en materia de capacidades y tecnología.

Tras la invasión de Ucrania en 2022, la UE ha dado un paso significativo al reconocer que debía «rearmarse» y fortalecer su postura defensiva de manera acelerada para 2030. La presidenta de la Comisión Europea, Ursula von der Leyen, abogó por movilizar recursos a una escala inédita para dotar a Europa de una disuasión creíble antes del final de la década. Fruto de esta voluntad política, la Comisión presentó el plan conocido, inicialmente, como ReArm Europe, un ambicioso programa dirigido a concentrar y coordinar la

inversión en defensa por parte de los Estados miembros, contando con el apoyo de fondos europeos (Comisión Europea, 2025).

Actualmente, esta iniciativa ha adoptado la denominación «Preparación 2030», debido a las reticencias mostradas por algunos países, entre ellos, España e Italia, respecto al término original, considerado demasiado belicista o sensible desde una perspectiva política y social.

Este plan prevé movilizar más de 800 000 millones de euros en inversión en defensa acumulada hasta 2030. Su objetivo es reducir las divergencias entre los Estados miembros y aprovechar las economías de escala del mercado común. Entre los objetivos concretos de la iniciativa ReArm Europe se encuentran: elevar al 50 % la proporción del gasto en adquisiciones militares destinada a proveedores europeos —fortaleciendo así la Base Industrial y Tecnológica de la Defensa Europea (en adelante, BITDE)— y lograr que, al menos el 35 % de las nuevas capacidades, se adquieran de forma conjunta entre varios Estados miembros, frente al escaso 18 % actual (Fiott, 2024).

Asimismo, se prevé un aumento significativo en el intercambio de armamento y componentes entre países europeos. Si se alcanzan estos objetivos, Europa no solo avanzaría en su autonomía tecnológica, sino que también corregiría deficiencias estructurales de larga data en áreas clave —como las comunicaciones seguras, la vigilancia espacial, la defensa aérea o la ciberdefensa—, muchas de las cuales dependen directamente de capacidades avanzadas de inteligencia. Aunque, a mi juicio, habría que considerar cómo introducir de manera más clara el concepto de soberanía estratégica de las naciones que, en tanto Estados soberanos, conforman Europa.

En paralelo al plan ReArm Europe, la UE ha desplegado instrumentos financieros e industriales para respaldar la innovación tecnológica en defensa. Destaca, particularmente, el Fondo Europeo de Defensa (en adelante, FED), operativo desde 2021, que cuenta con un presupuesto de alrededor de 8000 millones de euros hasta 2027, dedicado a impulsar proyectos colaborativos de investigación y desarrollo militar (Fiott, 2023).

El FED representa la primera vez que la Unión, a través de su presupuesto comunitario, invierte directamente en capacidades de defensa, lo que la convierte ya en uno de los mayores financiadores de I+D en este ámbito a nivel europeo. De ese total, unos 2700 millones se orientan a la investigación innovadora —incluyendo tecnologías disruptivas como inteligencia artificial, microelectrónica, materiales avanzados, entre otras— y 5300 millones al desarrollo de prototipos y a la consolidación de capacidades industriales (Comisión Europea, 2021).

El FED persigue un doble objetivo: fomentar la cooperación entre empresas y Estados miembros en el desarrollo de nuevos sistemas de defensa —evitando la fragmentación de esfuerzos nacionales— y reforzar la Base

Industrial y Tecnológica de la Defensa Europea (BITDE), de modo que Europa pueda abastecerse con medios propios sin depender sistemáticamente de proveedores extracomunitarios.

Este último punto es especialmente crítico: análisis previos revelaban que más del 60 % del gasto en adquisiciones de defensa de los países de la UE entre 2007 y 2016 se dirigió a importaciones militares de fuera de la Unión, principalmente de Estados Unidos (Comisión Europea, 2022). La guerra en Ucrania volvió a poner en evidencia esta dependencia, ya que una proporción aún mayor de las compras urgentes de armamento realizadas en 2022-2023 se efectuaron a proveedores no europeos, especialmente en lo relativo a sistemas de armas y misiles de fabricación estadounidense. Las instituciones comunitarias han advertido que esta situación es insostenible si Europa aspira a una verdadera autonomía estratégica (Comisión Europea, 2022).

Por ello, además del FED, se han puesto en marcha medidas complementarias como el Instrumento Europeo para Compras Conjuntas de Defensa a Corto Plazo (EDIRPA) y propuestas en materia de regulación orientadas a incentivar la adquisición de productos europeos —como, por ejemplo, exenciones fiscales aplicables a proyectos colaborativos dentro del mercado común—.

Otro componente institucional relevante es la Estrategia Industrial de Defensa Europea, publicada en marzo de 2024. Se trata de la primera estrategia integral de la UE centrada en su industria de defensa y surge como respuesta directa a las lecciones de la guerra en Ucrania (Fiott, 2024). Esta Estrategia Industrial pone énfasis en la preparación militar y en el desarrollo de capacidades de nueva generación, muchas de las cuales descansan en tecnologías emergentes.

Entre sus líneas de acción, destacan: la consolidación de la demanda agregada europea —mediante compras conjuntas—, el impulso a la innovación en áreas como la inteligencia artificial, la computación cuántica o el espacio, y la garantía de que la base industrial pueda escalar su producción rápidamente en caso de crisis (Fiott, 2024).

Aunque la estrategia es un paso positivo que demuestra una visión a nivel europeo, expertos señalan que también plantea incógnitas sobre su implementación efectiva y la coordinación con los esfuerzos nacionales (Fiott, 2024). Aun así, refleja la prioridad creciente otorgada a la tecnología de defensa en la agenda europea.

De manera complementaria, la UE y sus Estados miembros han fortalecido la colaboración con la OTAN en materia de innovación, buscando sinergias y división de tareas —por ejemplo, la OTAN ha lanzado su acelerador de innovación en Defensa para el Atlántico Norte y un Fondo de Innovación, mientras la UE se concentra en proyectos industriales y regulación—.

En síntesis, Europa ha pasado, en pocos años, de una posición rezagada a una actitud decididamente proactiva frente a la revolución tecnológica en el ámbito de la defensa. Iniciativas como el plan ReArm Europe, la activación del Fondo Europeo de Defensa y el impulso de nuevas estrategias industriales reflejan una clara voluntad de modernizar tanto las capacidades militares como los sistemas de inteligencia mediante la incorporación de IA y otras tecnologías avanzadas.

Todo ello responde, además, a un objetivo estratégico fundamental: salvaguardar la soberanía tecnológica europea. No obstante, desde nuestra perspectiva, esta aspiración debe ir acompañada de un firme compromiso con el respeto al interés nacional de cada Estado soberano. La construcción de una autonomía tecnológica compartida no puede ni debe producirse a expensas de las soberanías nacionales, sino que ha de sustentarse en formas de cooperación que reconozcan y respeten las prioridades específicas de cada nación.

5 Casos de aplicación tecnológica en inteligencia y defensa

La concreción de esta transformación tecnológica se observa en diversos proyectos y casos prácticos donde la IA y otras innovaciones se aplican ya en el ámbito de la inteligencia de seguridad y defensa europeas. Uno de los ejemplos más directos es el proyecto Artificial Intelligence for Defence (en adelante, AI4DEF), financiado en 2020 bajo el programa europeo EDIDP —Programa Europeo de Desarrollo Industrial de Defensa, precursor del FED—. El AI4DEF es un proyecto multinacional orientado a demostrar los beneficios de la IA en varias funciones militares, sobre todo, en mejorar la conciencia situacional, el análisis de inteligencia, vigilancia y reconocimiento (ISR) y la optimización de la planificación operativa (Comisión Europea, 2021).

Concretamente, AI4DEF está desarrollando una plataforma en la nube que integra algoritmos de inteligencia artificial para, por ejemplo, analizar en tiempo real imágenes captadas por vehículos aéreos no tripulados (UAV) e identificar objetivos de interés. Este proyecto ilustra cómo la IA puede tener un enfoque integrado y adaptable en el ámbito de la defensa, aplicándose en los dominios terrestre, aéreo y marítimo a desafíos como la detección automatizada de amenazas móviles, la segmentación tridimensional del terreno para operaciones urbanas o la fusión inteligente de datos procedentes de sensores heterogéneos (Comisión Europea, 2021).

Otra aplicación tecnológica clave se da en el procesamiento avanzado de imágenes satelitales y de reconocimiento. La UE cuenta con el Centro Satelital de la Unión Europea (en adelante, SatCen), ubicado en España, que proporciona análisis geoespacial a los Estados miembros y misiones de la Política Común de Seguridad y Defensa. Ante el creciente volumen

de imágenes de observación terrestre disponibles —incluyendo las del programa Copernicus de la UE y proveedores comerciales—, SatCen y la Agencia Europea de Defensa han impulsado estudios para integrar IA en los procesos de Imagery Intelligence (IMINT), a fin de automatizar la identificación de objetos, el cambio detectado en infraestructuras y la vigilancia de fronteras. Por ejemplo, los algoritmos de visión por computador pueden analizar miles de imágenes satelitales en busca de patrones —como concentraciones inusuales de vehículos o indicios de preparación militar— con una velocidad y precisión muy superiores a las de un equipo humano, lo que permite centrar los esfuerzos analíticos únicamente en aquellas alertas con mayor probabilidad de relevancia. Este tipo de herramientas ha cobrado especial importancia en conflictos recientes como el de Ucrania, donde la inteligencia de fuente abierta (OSINT) y las imágenes satelitales comerciales han desempeñado un papel fundamental en la monitorización de movimientos militares. A partir de esta experiencia, las agencias europeas aspiran a dotarse de plataformas basadas en inteligencia artificial capaces de filtrar el ruido informativo y extraer conocimiento útil y accionable a partir del vasto volumen de datos abiertos disponibles.

Asimismo, países europeos han comenzado a aplicar IA en apoyo a la inteligencia contra el terrorismo y el crimen organizado. Un caso es el uso de algoritmos para analizar comunicaciones en Internet y redes sociales con el fin de detectar señales precoces de radicalización o planificación de ataques. Existen proyectos piloto, a menudo en colaboración con agencias de seguridad interior, que combinan procesamiento de lenguaje natural en múltiples idiomas con técnicas de análisis de redes sociales para identificar perfiles potencialmente peligrosos, siempre respetando las leyes de protección de datos. Aunque se trata de un ámbito sensible, el uso de inteligencia artificial en funciones predictivas podría permitir a las unidades europeas de inteligencia priorizar investigaciones y prevenir actos violentos a partir de indicios que, de otro modo, quedarían ocultos entre enormes volúmenes de datos. Organismos como Europol ya han explorado herramientas de este tipo para cribar contenidos extremistas en línea, y a nivel nacional varios servicios de inteligencia están invirtiendo en capacidades avanzadas de análisis masivo de datos (*big data*). Esta evolución tecnológica ilustra cómo las fronteras entre la seguridad interior y exterior tienden a desdibujarse, una dinámica reconocida por la Brújula Estratégica (Consejo de la UE, 2022) y que demanda una cooperación interagencias cada vez más estrecha.

En el ámbito de los ejércitos de las naciones europeas, la adopción de tecnologías 4RI también es palpable. La robotización y los sistemas no tripulados son cada vez más comunes en misiones de reconocimiento e inteligencia. Por ejemplo, varios países de la OTAN desplegados en la región del Sahel han empleado minidrones para vigilancia aérea táctica, reduciendo el

riesgo para el personal y obteniendo inteligencia en tiempo real sobre movimientos insurgentes. En entornos urbanos complejos, donde los GPS pueden fallar y abundan obstáculos, se investigan soluciones de IA para mejorar la navegación autónoma de drones: En 2018, Francia financió, a través del organismo CEA/LIST —especializado en IA—, varios proyectos orientados a resolver la localización tridimensional precisa de vehículos aéreos no tripulados (UAV) en entornos urbanos densamente edificadas, mediante la combinación de visión artificial y aprendizaje profundo (Ministère des Armées, 2019).

Este tipo de desafíos técnicos —como detectar y esquivar obstáculos en calles estrechas o identificar figuras humanas ocultas entre edificios— está siendo abordado mediante algoritmos entrenados para interpretar imágenes de vídeo en tiempo real. Los avances obtenidos no solo fortalecen las capacidades de reconocimiento militar, sino que también presentan un notable potencial de aplicación dual, por ejemplo, en la gestión de desastres o en la seguridad civil.

Cabe destacar, además, el ambicioso proyecto franco-germano-español del Sistema de Combate Aéreo del Futuro (FCAS), concebido como un «sistema de sistemas» que integrará un caza tripulado de sexta generación con enjambres de drones de combate y una «nube de combate» (*combat cloud*) que conectará sensores y operadores en tiempo real. Aunque todavía en fase conceptual, el FCAS incorpora de forma explícita el uso de IA y tecnologías de computación en la nube para facilitar la fusión masiva de datos y la asignación dinámica de objetivos entre plataformas.

Este programa, liderado por Francia, ejemplifica cómo la visión europea de superioridad aérea hacia 2040 y más allá depende estrechamente del aprovechamiento de capacidades avanzadas de IA —para la gestión cooperativa de sistemas no tripulados, la guerra electrónica cognitiva, entre otros— y de garantizar la plena interoperabilidad de sistemas autónomos. Si el FCAS tiene éxito, dotará a Europa de una arquitectura de inteligencia y mando distribuido altamente sofisticada, reduciendo significativamente su dependencia operativa de activos estadounidenses en escenarios futuros.

En suma, los casos citados —AI4DEF, SatCen con IA, análisis big data antiterrorista, drones autónomos o FCAS— demuestran la amplitud de ámbitos en que la tecnología está cambiando el quehacer de la inteligencia y la defensa europeas. Desde el nivel táctico hasta el estratégico, la IA, la robótica y las herramientas digitales están amplificando el alcance y la rapidez con que Europa puede obtener y explotar información de valor militar.

No obstante, esta revolución tecnológica requiere de una visión política y estratégica que garantice su viabilidad, lo que enlaza con el concepto de soberanía tecnológica discutido a continuación.

6 La búsqueda de la soberanía tecnológica europea

El impulso europeo por incorporar IA y tecnologías emergentes en defensa está estrechamente vinculado con la aspiración de lograr una mayor soberanía tecnológica. Este concepto se refiere a la capacidad de Europa para decidir y actuar de forma autónoma en el terreno tecnológico, controlando las cadenas de suministro críticas y reduciendo dependencias excesivas de potencias externas en ámbitos estratégicos (Ministère des Armées, 2019). En los últimos años, «soberanía tecnológica» y «autonomía estratégica» se han convertido en ejes discursivos centrales en la UE, impulsados por desafíos como la rivalidad comercial y geopolítica entre EE. UU. y China, las disrupciones en suministros —por ejemplo, Semiconductores— y la citada dependencia europea en defensa de proveedores extracomunitarios.

En materia de seguridad y defensa, la soberanía tecnológica implica que Europa pueda desarrollar y producir sus propias tecnologías críticas —desde IA y ciberseguridad hasta satélites, plataformas militares avanzadas o redes 5G seguras— sin verse sometida a vetos o vulnerabilidades externas. Ursula von der Leyen ha defendido esta idea en su mandato al frente de la Comisión, alineándola con la visión de una «Comisión Geopolítica» capaz de dotar a la UE de las herramientas para ser un actor estratégico por derecho propio (Csernaton, 2023). La búsqueda de soberanía tecnológica ha motivado iniciativas como la identificación de «proyectos importantes de interés común europeo» (IPCEI) en campos como la microelectrónica y la nube, el Acta Europea de Chips para fomentar la producción de semiconductores en Europa, o la ya mencionada movilización de inversiones en defensa para fortalecer la BITDE. En defensa, en concreto la Declaración de Versalles de marzo 2022 —firmada por los jefes de Estado y de Gobierno de la UE— explicitó la necesidad de reforzar la base industrial y tecnológica de defensa europea y corregir dependencias estratégicas, listando sectores clave donde Europa debe garantizar el control.

La IA se considera precisamente uno de esos sectores críticos. El Gobierno francés llegó a afirmar en su Revisión Estratégica de Defensa y Seguridad Nacional 2017 que la pericia en IA sería una cuestión de soberanía en el futuro (Ministère des Armées, 2019). En línea con ello, Francia y otros países han abogado por que la UE trate a la IA militar y a las tecnologías profundas —*deep tech*— como un dominio de inversión prioritaria, para no quedar rezagados frente a Estados Unidos o China.

El discurso de la soberanía tecnológica también permea la narrativa sobre datos e inteligencia: se insiste en que Europa debe poder almacenar, procesar y extraer valor de sus datos —incluidos los datos de inteligencia— en infraestructuras seguras europeas, evitando dependencias de servicios en la nube extranjeros que podrían suponer riesgos de acceso o interrupción. Este es un argumento a favor de iniciativas

como (GAIA-X) —infraestructura de datos abierta— o de reforzar las capacidades propias en cifrado cuántico y ciberseguridad.

No obstante, lograr la soberanía tecnológica no significa aislarse: la UE reconoce que cooperar internacionalmente sigue siendo importante. Por ejemplo, se busca un equilibrio en el que Europa pueda «caminar con sus propios pies» en tecnología de defensa, pero a la vez interoperar plenamente con aliados de la OTAN. Tampoco todos los países de la UE comparten el mismo énfasis en la autonomía; mientras Francia, tradicionalmente, empuja una visión de «Europe puissance» capaz de actuar de forma autónoma, otras naciones ven esta autonomía de manera complementaria —no sustitutiva— con la alianza transatlántica. En cualquier caso, el concepto de soberanía tecnológica ha servido para orientar políticas concretas: la UE ha condicionado la financiación del FED a la participación mayoritaria de industrias de países miembros —evitando control de empresas desde el exterior—; igualmente, se están mapeando vulnerabilidades en suministros —por ejemplo, Europa importa drones de reconocimiento de proveedores israelíes o estadounidenses, lo que ha motivado proyectos para fabricar drones europeos—. El discurso estratégico europeo ahora liga claramente la superioridad tecnológica a la independencia estratégica: quien controle las tecnologías críticas, controlará en buena medida su destino en seguridad y defensa.

Frente a esta apuesta, surgen algunas dificultades. Desarrollar tecnologías punteras requiere enormes inversiones, coordinación y atracción de talento, en un contexto donde Europa compite con ecosistemas de innovación más dinámicos como Silicon Valley o Shenzhen. De igual modo, imponer «Buy European» en defensa puede elevar costes o retrasar capacidades si la industria europea no produce cierto equipamiento al ritmo requerido —por ejemplo, drones armados, donde hasta hace poco no había alternativa europea consolidada—.

Por ello, la soberanía tecnológica se plantea como un objetivo a alcanzar de forma gradual, combinando la cooperación entre los Estados miembros de la UE —para ganar masa crítica— con una colaboración externa selectiva allí donde sea necesario. En este contexto, el papel de Francia ha sido crucial, como se desarrollará en la siguiente sección, ya que ha actuado como catalizador de la autonomía tecnológica europea, impulsando proyectos industriales comunes y dando ejemplo mediante políticas nacionales ambiciosas en IA y defensa.

7 Aspectos normativos en la transformación digital de la seguridad y defensa en Europa

La transformación digital de la seguridad y la defensa europeas requieren un marco jurídico estructurado que regulen tanto los desarrollos tecnológicos disruptivos como la protección de las infraestructuras estratégicas.

La UE ha desplegado en los últimos años una serie de instrumentos normativos que buscan establecer un entorno regulado, coherente y seguro para la digitalización de servicios esenciales, incluidos aquellos con implicaciones en materia de inteligencia y soberanía tecnológica.

Uno de los desarrollos más relevantes es la Directiva (UE) 2022/2555¹, conocida como NIS 2.0, que sustituye y amplía la Directiva NIS original (2016/1148/UE). Este nuevo marco normativo establece requisitos más exigentes para entidades de sectores clave —entre ellos, el transporte, la energía, la Administración Pública y determinadas infraestructuras digitales—, e introduce obligaciones en materia de gestión de riesgos y notificación de incidentes. Aunque las actividades estrictamente relacionadas con la defensa nacional quedan excluidas de su ámbito de aplicación (art. 2.3), la directiva afecta indirectamente a operadores estratégicos que pueden colaborar con el sector de defensa o manejar información sensible.

Entre las novedades más significativas figura la creación de la Red Europea de Organizaciones de Enlace para Crisis Cibernéticas (EU-CyCLONe), prevista en su artículo 16, que facilita la coordinación operativa entre Estados miembros en caso de incidentes graves de ciberseguridad con posibles efectos transfronterizos. La aplicación efectiva de esta directiva depende de su transposición por parte de los Estados miembros. En el caso de España, esta adecuación encuentra una base ya avanzada en el Real Decreto 311/2022, que reforma el Esquema Nacional de Seguridad² (ENS) y anticipa principios de protección activa, supervisión continua y respuesta ante amenazas, en línea con los estándares comunitarios.

En paralelo, la UE ha formulado un enfoque jurídico integral para la regulación de la IA, mediante la Propuesta de Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial, conocido como Artificial Intelligence Act³. Este reglamento, aún en tramitación parlamentaria, introduce una clasificación basada en el nivel de riesgo del sistema de IA, estableciendo restricciones proporcionales según su impacto potencial en el marco del ejercicio de derechos fundamentales, seguridad pública o integridad institucional.

Los sistemas de inteligencia artificial clasificados como de alto riesgo —como los empleados en infraestructuras críticas, vigilancia biométrica o administración de justicia— deberán cumplir estrictas obligaciones en

¹ Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a medidas para garantizar un elevado nivel común de ciberseguridad en toda la Unión (DOUE L 333/80, 27.12.2022).

² Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. BOE n.º 106, de 4 de mayo de 2022.

³ Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (COM/2021/206 final).

cuanto a la calidad de los datos, la documentación técnica, la supervisión humana y la trazabilidad. Si bien el reglamento excluye formalmente de su ámbito de aplicación los usos militares y de defensa (art. 2.3), su impacto es significativo en contextos de doble uso o cooperación civil-militar, en especial, en relación con sistemas utilizados por autoridades públicas o contratistas que operan en entornos sensibles.

El reglamento prevé, asimismo, la creación de una Oficina Europea de inteligencia artificial, concebida como un órgano de supervisión y coordinación responsable de garantizar la correcta aplicación de la norma en todo el territorio de la Unión. Este organismo se configura como un elemento clave para asegurar el desarrollo ético y controlado de las tecnologías automatizadas, incluidas aquellas que pueden incidir directamente en funciones estatales esenciales.

En conjunto, el marco normativo europeo refleja una arquitectura legal orientada a garantizar un entorno digital controlado, conforme a estándares técnicos elevados y principios fundamentales del Derecho europeo. La interacción entre normativas como la NIS 2.0, el futuro Reglamento de IA y las propuestas sectoriales en materia digital, constituye un eje esencial para la evolución estratégica de las capacidades de inteligencia y defensa en la era tecnológica.

8 Escenarios prospectivos hacia 2040: el futuro de la inteligencia digital europea

Mirando hacia 2040, pueden vislumbrarse varios escenarios posibles para la inteligencia y la seguridad europea en función de cómo se gestionen las oportunidades y los riesgos actuales. A continuación, se plantean tres escenarios prospectivos que ilustran futuros plausibles del rol de la inteligencia digital en Europa, considerando variables tecnológicas, geopolíticas y normativas.

8.1 Escenario primero: autonomía e inteligencia europea integrada

En este futuro, la UE logra materializar con éxito sus planes de transformación. Para 2040, Europa dispone de una infraestructura digital de defensa plenamente interoperable y soberana: satélites europeos de próxima generación proporcionan vigilancia ubicua; redes seguras europeas de 5G/6G conectan sensores y centros de mando en tiempo real; y los Estados miembros comparten inteligencia a través de una plataforma común, robusta y protegida, evolución de la actual SIAC.

Este avance ha sido posible gracias a un enfoque que respeta y contempla la soberanía de las naciones. Los Gobiernos han sabido construir un futuro en el que los intereses nacionales no se diluyen, sino que convergen

y se refuerzan mutuamente en el marco de una cooperación voluntaria. Lejos de suponer una cesión de soberanía, la colaboración europea se ha convertido en una herramienta para fortalecer las capacidades nacionales y proyectarlas con mayor eficacia en un entorno internacional complejo.

La IA, desarrollada conforme a estos principios éticos, se emplea rutinariamente para anticipar crisis, detectar campañas de desinformación hostil y coordinar despliegues multinacionales. La UE ha establecido un Centro de Inteligencia Europeo permanente, donde analistas de todos los países trabajan juntos con acceso a bases de datos comunes, respetando los niveles de clasificación.

Gracias a la inversión sostenida en I+D, Europa ha mitigado sus dependencias estratégicas, produciendo localmente chips y sensores críticos, compitiendo en condiciones de igualdad con EE. UU. y Asia en áreas como ciberseguridad, robótica e IA militar (Csernatoní, 2023).

Desde el punto de vista político, la UE gana peso normativo y logra que su enfoque de «IA fiable» sea adoptado a nivel mundial en el ámbito armamentístico, contribuyendo así a evitar una carrera descontrolada hacia el desarrollo de armas autónomas. En este escenario, la inteligencia digital europea actúa como un multiplicador de seguridad: anticipa amenazas híbridas, facilita respuestas rápidas ante crisis y respalda la autonomía estratégica europea en la toma de decisiones internacionales.

Las iniciativas actuales, como la Brújula Estratégica y PESCO, se implementan con éxito, fortaleciendo la solidaridad entre los Estados miembros frente a amenazas externas y consolidando a la UE como un actor clave en la seguridad internacional.

8.2 Escenario segundo: dependencia persistente

En este escenario, los esfuerzos de integración en materia de defensa avanzan de forma limitada, en parte porque varios Estados miembros optan por reafirmar su soberanía en el ámbito de la seguridad y la defensa. Tras la crisis en Ucrania, se impone una lógica de acción nacional, en la que cada país fortalece sus capacidades con arreglo a sus propias evaluaciones estratégicas, estableciendo alianzas bilaterales y contratando directamente con proveedores internacionales según sus necesidades particulares.

Para 2040, la inteligencia europea permanece estructurada principalmente en torno a capacidades nacionales y la UE no ha conseguido consolidar un núcleo operativo común. La SIAC mantiene una función simbólica y de coordinación básica, pero no evoluciona hacia una plataforma plenamente integrada. Esta configuración permite a los Estados conservar el control sobre su información sensible, aunque dificulta respuestas colectivas rápidas ante crisis compartidas (Csernatoní, 2023).

En el plano tecnológico, Europa ha avanzado de manera prudente en el desarrollo de inteligencia artificial aplicada al ámbito militar, en parte debido a un enfoque excesivamente cauteloso en materia ética, lo que le resta competitividad frente a potencias como China, que se perfila para alcanzar la supremacía en IA militar hacia 2035 (Csernatoní, 2023).

Esta situación ha reforzado la dependencia estratégica respecto a Estados Unidos, limitando la capacidad de Europa para ejecutar operaciones complejas de forma plenamente autónoma. Como consecuencia, su margen de maniobra diplomática se ve reducido y ciertas vulnerabilidades persisten frente a actores internacionales con agendas más asertivas (Csernatoní, 2021).

8.3 Escenario tercero: cooperación condicionada

Este escenario, el más probable, sitúa a Europa en una posición intermedia. Para 2040, la UE ha alcanzado avances notables en integración tecnológica y de inteligencia, aunque persisten ciertas limitaciones estructurales. La seguridad común se sostiene mediante mecanismos como la Brújula Estratégica, renovada cada cinco años, si bien Europa continúa dependiendo parcialmente de importaciones en tecnologías críticas.

El desarrollo de la IA en Europa avanza principalmente en aplicaciones defensivas, evitando una carrera incontrolada hacia el armamento autónomo. Este enfoque es posible gracias a acuerdos internacionales promovidos por la propia UE, que han logrado establecer una regulación estricta sobre estas tecnologías (Calderón y Pedemonte, 2023).

La cooperación transatlántica se mantiene sólida, aunque adaptada a un nuevo equilibrio: EE. UU. sigue aportando inteligencia estratégica a escala mundial, mientras Europa contribuye con estabilidad regional y capacidades especializadas en inteligencia local. La OTAN, por su parte, incorpora estándares éticos europeos en el desarrollo de IA, lo que refuerza la confianza operativa entre aliados (Calderón y Pedemonte, 2023).

En el ámbito industrial, aunque EE. UU. conserva la supremacía en sectores clave, empresas europeas lideran nichos estratégicos como la ciberseguridad o los drones inteligentes no letales. En este contexto de competencia contenida, la UE ejerce una influencia significativa en la regulación internacional de la IA, contribuyendo a prevenir conflictos accidentales derivados de algoritmos no supervisados.

Europa, en definitiva, será más fuerte que en 2025, aunque seguirá manteniendo ciertas dependencias selectivas. Su inteligencia digital habrá alcanzado un nivel de eficacia considerable, si bien aún requerirá del respaldo de aliados para consolidar una soberanía plena.

Estos escenarios —aproximaciones analíticas— ponen de relieve que el futuro de la inteligencia europea dependerá en gran medida de las decisiones que se adopten hoy. La forma en que los Estados miembros equilibren cooperación y autonomía, inversión conjunta y prioridades nacionales, será decisiva para definir la dirección de ese futuro.

La variable determinante será la voluntad política de los Estados para sostener la inversión, preservar sus principios y articular formas de cooperación que sean compatibles con sus intereses nacionales. La inteligencia digital podrá convertirse en un factor de fortalecimiento o de exposición en materia de seguridad, según cómo se gestione. Por ello, imaginar estos futuros no es un ejercicio meramente especulativo, sino una herramienta estratégica para el presente: Europa no debe resignarse a que otros definan su destino, sino asumir con determinación la responsabilidad de construirlo desde la soberanía de sus naciones.

9 Conclusiones

La transformación de la inteligencia en la seguridad y defensa europea en la era digital es un proceso complejo y dinámico que responde directamente a los desafíos impuestos por la Cuarta Revolución Industrial y a la creciente sofisticación de amenazas híbridas y convencionales. La adopción generalizada de la IA, el *big data* y los sistemas autónomos está redefiniendo las capacidades y procedimientos operativos de las fuerzas armadas y agencias de inteligencia europeas, brindando oportunidades excepcionales para mejorar significativamente la eficacia, velocidad de reacción y precisión en operaciones.

Tanto la UE como sus naciones soberanas han identificado claramente estos beneficios potenciales, pero también reconocen plenamente los desafíos tecnológicos, éticos y políticos involucrados. Esto se ha traducido en la implementación de múltiples iniciativas estratégicas y programas de inversión, entre los que destacan la Brújula Estratégica, la Estrategia Industrial de Defensa, el Fondo Europeo de Defensa y proyectos clave como ReArm Europe, Eurodrone y el Sistema de Combate Aéreo Futuro (FCAS). Estos esfuerzos buscan consolidar la autonomía estratégica europea, reduciendo su dependencia tecnológica y operativa de países terceros, especialmente en áreas críticas como IA, ciberdefensa, tecnologías satelitales y vehículos no tripulados.

No obstante, Europa continúa enfrentando desafíos decisivos. Las diferencias entre naciones soberanas —resultado de trayectorias históricas, estructuras estratégicas y prioridades nacionales legítimas— constituyen una realidad estructural que influye directamente en la manera en que se articula la cooperación en materia de seguridad y defensa. Lejos de ser

un impedimento, puede convertirse en un factor de solidez si se gestiona desde el respeto mutuo y la voluntad de colaboración. No se trata de imponer uniformidad, sino de fomentar la cooperación desde el respeto a la soberanía nacional.

Hoy en día, la UE aún no ha logrado articular una doctrina clara y coherente sobre el uso militar de tecnologías emergentes como la inteligencia artificial, lo que amenaza con generar estrategias dispersas, ineficaces y condicionadas por lógicas burocráticas alejadas de las realidades nacionales. En un entorno tecnológico que evoluciona con rapidez, se impone la necesidad de una respuesta ágil y coordinada entre Estados soberanos, guiada por el interés nacional y no por agendas ajenas, para garantizar la defensa y la seguridad desde una auténtica Europa de las naciones.

Asimismo, será fundamental gestionar adecuadamente las relaciones estratégicas con aliados clave como Estados Unidos. La autonomía estratégica que Europa persigue no debe interpretarse como un distanciamiento, sino como una búsqueda de equilibrio, fortaleciendo capacidades propias que complementen las de la OTAN. Este enfoque implica un diálogo constante, una cooperación estrecha y reforzar la influencia europea en la regulación ética y el marco normativo internacional sobre el uso de la IA militar.

Europa dispone de activos fundamentales para afrontar estos retos con solidez: cuenta con talento científico de primer nivel, empresas tecnológicas competitivas, un mercado común consolidado y una tradición significativa de cooperación en materia de seguridad y defensa. El compromiso político y la implicación activa de países como Francia, Alemania, Italia y España constituyen una base firme para seguir impulsando esta transformación, a partir de capacidades nacionales que, al sumarse de forma voluntaria y coordinada, fortalecen el conjunto.

De cara a 2040, la inteligencia digital podría adquirir una relevancia estratégica equiparable al papel desempeñado por las armas nucleares en el siglo xx, redefiniendo equilibrios de poder y estrategias mundiales. Europa aspira a que esta inteligencia digital sirva como herramienta efectiva para salvaguardar la paz, promover valores democráticos y evitar convertirse en un instrumento de control totalitario o conflicto descontrolado. Para ello, será crucial mantener un enfoque centrado en las personas, asegurando mecanismos de control democrático y transparencia, en la mayor medida posible sin comprometer las necesidades legítimas de seguridad.

En definitiva, esta transformación —enmarcada en la era digital— constituye una oportunidad excepcional para fortalecer tanto la seguridad colectiva como la autonomía estratégica de las naciones soberanas europeas. Si bien persisten desafíos considerables, los avances alcanzados

evidencian una Europa en constante evolución, donde la cooperación se construye sobre la base del respeto a la soberanía nacional. Si se mantiene la voluntad política, se garantizan inversiones sostenidas en investigación y desarrollo y se consolida una visión común sobre el uso responsable de la tecnología, Europa estará en condiciones de llegar a 2040 con capacidades de inteligencia significativamente reforzadas, preparada para proteger de forma eficaz a sus ciudadanos, así como sus principios y valores, en un entorno internacional cada vez más dinámico e incierto.

Referencias bibliográficas

- Ash Center. (2024). *AI, Digital Sovereignty, and the EU's Path Forward: A Case for Mission-Oriented Industrial Policy*. Harvard Kennedy School. [Consulta: 2025]. Disponible en: <https://ash.harvard.edu/resources/ai-digital-sovereignty-and-the-eus-path-forward-a-case-for-mission-oriented-industrial-policy/>
- Calderón, I. y Pedemonte, C. (2023). NATO's AI strategy focuses on responsible use: AI chief. *NATO News*. [Consulta: 2025].
- Comisión Europea. (2021). EDIDP 2020 – Artificial Intelligence: Project AI4DEF (Factsheet). Bruselas, DG DEFIS. [Consulta: 2025]. Disponible en: https://defence-industry-space.ec.europa.eu/system/files/2021-06/EDIDP2020_factsheet_AI_AI4DEF.pdf Defence Industry and Space
- Comisión Europea. (2021). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (COM/2021/206 final). [Consulta: 2025]. Disponible en: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206>
- Comisión Europea. (2022). *Joint Communication to the European Parliament and the Council on Defence Investment Gaps Analysis and Way Forward* [JOIN (2022) 24 final, 18 de mayo de 2022]. [Consulta: 2025]. Disponible en: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022JC0024EUR-Lex+1EUR-Lex+1>
- Comisión Europea. (2025). *White Paper on European Defence – Readiness 2030 (ReArm Europe Plan)*. Bruselas, Comisión Europea. [Consulta: 2025]. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_793 European Commission+1 European Commission+1
- Consejo de la Unión Europea. (2022). Brújula Estratégica para la Seguridad y la Defensa. Bruselas, Consejo de la Unión Europea. [Consulta: 2025]. Disponible en: <https://www.consilium.europa.eu/es/policies/strategic-compass/Consilium>

- Consejo Europeo. (2022). *Declaración de Versalles, 10-11 de marzo de 2022*. Bruselas, Consejo Europeo. [Consulta: 2025]. Disponible en: <https://www.consilium.europa.eu/es/press/press-releases/2022/03/11/the-versailles-declaration-10-11032022/Consilium>
- Csernaton, R. (2021). *Security 2040: Perils and Promise Over the Near Horizon*. Carnegie Europe. [Consulta: 2025]. Disponible en: <https://carnegieeurope.eu/2021/03/25/security-2040-perils-and-promise-over-near-horizon-pub-84124>
- Csernaton, R. (2023). *Weaponizing Innovation? Mapping Artificial Intelligence-enabled Security and Defence in the EU. Non-proliferation and Disarmament Papers*. Estocolmo, SIPRI. 84. [Consulta: 2025]. Disponible en: <https://www.sipri.org/publications/2023/eu-non-proliferation-and-disarmament-papers/weaponizing-innovation-mapping-artificial-intelligence-enabled-security-and-defence-euSIPRI>
- Finabel. (s.f.). *A Shift Towards Sovereign EU Military Capabilities? The Eurodrone Project Awaits Final Signature*. The European Land Force Commanders Organisation. [Consulta: 2025]. Disponible en: <https://finabel.org/a-shift-towards-sovereign-eu-military-capabilities-the-eurodrone-project-awaits-final-signature/finabel.org>
- Fiott, D. (2021). The European Front-Runners: France, Germany, Italy and Spain in PESCO. *European Foreign Affairs Review*. 26, pp. 87-110.
- Fiott, D. (2023). *Investing and Innovating? Spain and the European Defence Fund*. Real Instituto Elcano. [Consulta: 2025]. Disponible en: [https://www.realinstitutoelcano.org/en/analyses/investing-and-innovating-spain-and-the-european-defence-fund/Real Instituto Elcano](https://www.realinstitutoelcano.org/en/analyses/investing-and-innovating-spain-and-the-european-defence-fund/Real%20Instituto%20Elcano)
- Fiott, D. (2024). *¿Más allá de la estrategia? Estrategia industrial y futuro de la defensa europea*. Real Instituto Elcano. [Consulta: 2025]. Disponible en: [https://www.realinstitutoelcano.org/analisis/mas-alla-de-la-estrategia-estrategia-industrial-y-futuro-de-la-defensa-europea/Real Instituto Elcano](https://www.realinstitutoelcano.org/analisis/mas-alla-de-la-estrategia-estrategia-industrial-y-futuro-de-la-defensa-europea/Real%20Instituto%20Elcano)
- Fiott, D. y Lindstrom, G. (2018). *Artificial Intelligence: What Implications for EU Security and Defence?* París, Instituto de Estudios de Seguridad de la UE. 18. [Consulta: 2025]. Disponible en: <https://www.iss.europa.eu/publications/briefs/artificial-intelligence-what-implications-eu-security-and-defenceiss.europa.eu>
- Fojón, E. (2018). *La cuarta revolución industrial, el «algoritmo de guerra» y su posible aplicación a la Defensa española*. Real Instituto Elcano [en línea]. [Consulta: 2025]. Disponible en: <https://www.realinstitutoelcano.org/analisis/la-cuarta-revolucion-industrial-el-algoritmo-de-guerra-y-su-posible-aplicacion-a-la-defensa-espanola/>

- Global X. (2023). *Rearming Europe Boosts Defense Tech*. [Consulta: 2025].
- Gobierno de España. (2022). Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. *Boletín Oficial del Estado*. 4 de mayo, núm. 106.
- Ministère des Armées (Francia). (2019). *L'intelligence artificielle au service de la défense – Rapport de la Task Force IA*. París, Ministerio de las Fuerzas Armadas.
- Ministerio para Europa y Asuntos Exteriores. (2022). *A Strategic Compass to Strengthen the Security and Defence of the European Union by 2030*. [Consulta: 2025].
- OpenAI. (2024). *ChatGPT (modelo GPT-4)* [El texto ha sido revisado con apoyo de herramientas basadas en inteligencia artificial para mejorar la claridad y coherencia]. [Consulta: 2025]. Disponible en: <https://chat.openai.com/>
- Parlamento Europeo. (2020). *Report on Artificial Intelligence in a Digital Age – Civil and Military* [2020/2266 (INI), 19 de abril de 2021]. Bruselas.
- PESCO. (s.f.). *Joint EU Intelligence School (JEIS)*. [Consulta: 2025].
- Politico. (2023). Brussels Rebrands “Rearm Europe” After Backlash from Italy and Spain. *Politico*. [Consulta: 2025].
- SpringerLink. (2023). *Waking Up Slowly: Defense AI in Spain*. [Consulta: 2025].
- Unión Europea. (2022). Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a medidas para garantizar un elevado nivel común de ciberseguridad en toda la Unión. *Diario Oficial de la Unión Europea*. 27 de diciembre, L 333/80.