Boletín DE OBSERVACIÓN TECNOLÓGICA EN DEFENSA

DIRECCIÓN GENERAL DE ARMAMENTO Y MATERIAL
ARMAMENTO Y MATERIAL

SUBDIRECCIÓN GENERAL DE PLANIFICACIÓN, TECNOLOGÍA E INNOVACIÓN
Boletín de Observación Tecnológica en Defensa n.º 78 • 3.er trimestre de 2023

La permanente transformación cultural, además de digital, para gestionar y compartir datos

Se reinventan los sistemas de suspensión de los vehículos blindados

Notas sobre el contexto legal internacional y de la UE para el uso militar de la inteligencia artificial

X Congreso Nacional de I+D en Defensa y Seguridad (DESEi+D 2023)

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Paseo de la Castellana 109, 28046 Madrid
NIPO 083-15-183-4 (edición en línea)
NIPO 083-15-182-9 (impresión bajo demanda)
ISSN 2444-4839 (edición en línea)
ISSN 2444-4847 (impresión bajo demanda)
Depósito legal M 8179-2009

Autor: Sistema de Observación y Prospectiva Tecnológica (SOPT), Subdirección General de Planificación, Tecnología e Innovación (SDG PLATIN) de la Dirección General de Armamento y Material (DGAM). Paseo de la Castellana, 109, 28046 Madrid; teléfonos: 91 395 52 14 (Dirección), 91 395 52 80 (Redacción); observatecno@oc.mde.es.

Director: Óscar Jiménez Mateo.

Consejo Editorial: José Agrelo Llaverol, Cte. Carlos Calderón. Stte. José María Martínez Benéitez. María Isabel Pérez-Cerdá Herrero.

Asistencia técnica de apoyo a la redacción: Nodo Gestor: David García Dolla, Rosalía Vindel Román; Observatorio de Armamento (OT ARM): Óscar Rubio Gutiérrez; Observatorio de Electrónica (OT ELEC): Yolanda Benzi Rabazas; Observatorio de Energía y Propulsión (OT ENEP): Carlos Garrido Sánchez (OT MAT): Luis Miguel Requejo Morcillo; Observatorio de Defensa Nuclear, Biológica, Química y Radiológica (OT NBQR): Nuria Aboitiz Cantalapiedra; Observatorio de Óptica, Optrónica y Nanotecnología (OT OPTR): Pedro Carda Barrio; Observatorio de Plataformas Navales (OT PNAV): Cristina Mateos Fernández de Betoño, Jaime de la Parra Díaz; Observatorio de Plataformas Terrestres (OT PTER): Pablo Monasterio Albuerne; Observatorio Plataformas Aéreas (OT. PAER) Victoria Maceda; Observatorio de Satélites y Espacio (OT SATE): Ana Belén Lopezosa Ríos; Observatorio de Tecnologías de la Información, Comunicaciones y Simulación (OT TICS): Bernardo Martínez Reif, Isabel Iglesias Pallín.

Portada:
The ultimate game of chess: war games, machine learning, and artificial intelligence.
Fuente: *Defense Visual Information Distribution Service*, dvids-images-the ultimate game of chess war games, machine learning, and artificial intelligence dvidshub.net

El *Boletín de Observación Tecnológica en Defensa* es una publicación trimestral en formato electrónico del Sistema de Observación y Prospectiva Tecnológica orientado a divulgar y dar a conocer iniciativas, proyectos y tecnologías de interés en el ámbito de Defensa. El boletín está abierto a cuantos deseen dar a conocer su trabajo técnico. Los artículos publicados representan el criterio personal de los autores, sin que el *Boletín de Observación Tecnológica en Defensa* comparta necesariamente las tesis y conceptos expuestos. Ningún material publicado en esta revista podrá ser reproducido, copiado o publicado sin el consentimiento por escrito de los autores, legítimos propietarios de los contenidos.

Colaboraciones, suscripciones y dudas:
observatecno@oc.mde.es

Sistema de Observación y Prospectiva Tecnológica (SOPT) (defensa.gob.es)

Catálogo de Publicaciones de Defensa:
https://publicaciones.defensa.gob.es

SOPT
DGAM
Subdirección General de Planificación, Tecnología e Innovación

CONTENIDOS

Editorial

Actualidad

4 ¿Dónde hemos estado?

6 X Congreso Nacional de I+D en Defensa y Seguridad (DESEi+d 2023)

7 Notas sobre el contexto legal internacional y de la UE para el uso militar de la inteligencia artificial

Tecnologías emergentes

12 Se reinventan los sistemas de suspensión de los vehículos blindados

En Profundidad

15 La permanente transformación cultural, además de digital, para gestionar y compartir datos

Protección y seguridad de la investigación tecnológica

La investigación y la innovación en defensa son vitales para sostener la ventaja tecnológica y la capacidad de disuasión, especialmente mirando al medio y largo plazo. Uno de los diversos dilemas a los que se enfrentan está relacionado con la protección de sus resultados en los procesos relativos a su diseminación y explotación o simplemente accesos ilícitos. Vivimos hoy en día en la economía del conocimiento, es un hecho irrebatible. Con ella, el progreso de las sociedades se basa en la generación y compartición de conocimiento y en la inventiva, en contraste con lo que ha venido sucediendo prácticamente en toda la historia de la humanidad, en la que la riqueza se medía por la propiedad de la tierra o de los recursos naturales o, incluso, de los medios industriales y de producción más recientemente. Esta explosión del conocimiento, que ha venido para quedarse, se ve especialmente beneficiada y acelerada por la colaboración internacional en un mundo cada vez más pequeño, aunque no necesariamente más unido. La cruz del dilema se encuentra en el uso malicioso que se puede hacer del conocimiento, tanto en términos de ser usado por rivales geoestratégicos hostiles para amenazar la seguridad de los Estados donde se origina, como por competidores económico-tecnológicos en el ejercicio de prácticas de competencia desleal, de robo de información y de violación flagrante de la propiedad de los autores intelectuales (e industriales) que ha alterado dramáticamente el equilibrio ideal previsto en esa sociedad del conocimiento, etc. Por tanto, hablamos de dos aspectos diferenciados, la seguridad de la información y la propiedad de la información, pero con vidas paralelas en el campo de la defensa.

Frente a este dilema, la Unión Europea (UE) ha planteado para la puesta en marcha, tanto comunitaria, vía Comisión, como de las naciones, vía trasposición de legislación, una serie de restricciones financieras y otras medidas de aplicación a entidades no pertenecientes a la UE o que no se encuentran radicadas en territorios de sus Estados miembros. Por ejemplo, el Reglamento del Fondo Europeo de Defensa, a imagen del Reglamento del Programa Marco Civil de Investigación e Innovación, ha dado unos pasos muy claros en este sentido.

La Agencia Europea de Defensa (EDA), por su parte, utiliza una fórmula similar en la medida en que solo promueve y acoge proyectos de investigación en los que participen entidades de dos o más Estados miembros de la EDA, o de los Estados que tienen suscrito un acuerdo administrativo de colaboración (Noruega, Serbia, Ucrania, Suiza y muy recientemente EE. UU.).

Estas medidas no son suficientes ni pueden ser demasiado tajantes, precisamente en un contexto de globalización en el que la plurinacionalidad del capital de las entidades es un hecho inevitable y hasta necesario para su supervivencia, crecimiento y expansión. Pero se continúan perfeccionando y, por eso, los reajustes normativos son frecuentes.

En el caso de las tecnologías de doble uso, el acceso imprevisto (propiedad, IP) y hasta no autorizado (seguridad) de competidores tecnológico-económicos (propiedad de los derechos de explotación, patentes, etc.) y de rivales geoestratégicos (seguridad), respectivamente, está suponiendo el mayor peligro de pérdida de ventaja en conocimiento. Efectivamente, en estas tecnologías la titularidad del nuevo conocimiento aumenta su proporción en favor de entidades no tradicionales en defensa y, además, de pequeño o muy pequeño tamaño, aquellas a las que resulta imposible, por falta de recursos suficientes de todo tipo, madurar ese conocimiento con alto potencial disruptivo hacia niveles de mercado o de usuario final. En este caso, el acceso imprevisto (protección de la propiedad, IP) y hasta no autorizado (protección de la seguridad de los estados), por medio de capital o de esas otras prácticas ilegales, en el campo de las tecnologías emergentes, de forma tan reiterada en los últimos años, ha disparado todas las alertas y la adopción de las citadas medidas restrictivas.

La OTAN ha sido cronológicamente la primera entidad que ha lanzado una iniciativa, y del más alto nivel, el del secretario general, para apoyo de los innovadores y sus ideas tecnológicas, y su defensa frente a esos accesos ilícitos. Nos referimos a la red de aceleradoras DIANA (*Defence Innovation Accelerator for the North-Atlantic*) y al Fondo de Innovación OTAN (NIF: *NATO Innovation Fund*), dos vías, mismo fin. En la misma línea argumental, algunos aliados y socios ya han puesto en marcha regulaciones nacionales o esfuerzos sistémicos para aprovechar los beneficios de la colaboración internacional en innovación, al tiempo que protegen los resultados sensibles contra los mencionados accesos.

En la reunión de la Junta Directiva de la Organización de Ciencia y Tecnología de la OTAN de este otoño en Helsinki se analizó el caso paradigmático de cómo una colaboración internacional entre un instituto de materiales aeronáuticos de un Estado asiático y el Instituto de Grafeno de la Universidad de Manchester en 2015, que tenía por objeto acelerar la aplicación del grafeno en la industria de la aviación y otros sectores civiles, se ha convertido hoy en una preocupación por la posible aplicación inesperada e indeseada para desarrollar las capacidades militares de ese país rival. Informes elaborados por expertos del mismo sugieren que los blindajes de su helicóptero de ataque más señero en la actualidad fueron desarrollados en el país con información generada en el proyecto con la Universidad de Manchester. Precisamente, esta Universidad también ha reconocido el potencial de doble uso de la investigación conjuntamente con otras universidades del país asiático. La colaboración entre investigadores de las dos universidades, del Reino Unido y del país asiático, condujo a la creación de un nuevo tipo de revestimiento cerámico que podría «revolucionar los viajes hipersónicos con fines aéreos, espaciales y de defensa». Este ejemplo trata de ilustrar los riesgos en las dos esferas arriba citadas: por la propiedad intelectual, los derechos de explotación en el mercado sin apenas esfuerzo entre medias en I+D; y por la seguridad, la exposición a una vulnerabilidad crítica no contemplada en el paradigma mental de la época.

Ha llegado el momento, por tanto, de que se incluya la protección segura de la investigación en las Estrategias de Tecnología e Innovación de los países de nuestro entorno. De hecho, en la misma reunión de la Junta Directiva de la STO se ha planteado empezar por la propia Estrategia de Ciencia y Tecnología de la STO y, por tanto, de la OTAN, por medio del establecimiento de un foro para el intercambio de las mejores prácticas nacionales sobre la orientación que los Gobiernos eligen dar a las instituciones de investigación para lograr el equilibrio más adecuado entre la apertura académica, la innovación abierta, y la seguridad de la investigación e innovación para la defensa de los aliados.

Actualidad

¿Dónde hemos estado?

4 de julio de 2023

Inauguración banco de ensayos

El día 4 de julio se visitaron las instalaciones de la empresa Piedrafita (Paracuellos del Jarama) para asistir a la inauguración y demostración de su nuevo banco de ensayos, con el fin de probar sistemas de suspensión, en el que se puede analizar el comportamiento de los amortiguadores sobre vehículos de hasta setenta toneladas.

5 de julio de 2023

IF CEED TEXTILES

AITEX y la EDA organizaron la reunión final de *Circular Material for Textiles*, dentro del proyecto *Incubation Forum for Circular Economy in European Defence* (IF CEED), en la que participaron expertos del sector de la defensa de distintos países europeos.

En esta iniciativa, representantes de la EDA, del Ministerio de Defensa y de la industria intercambian ideas sobre el reciclaje de los residuos textiles generados por el sector de la defensa y se plantean proyectos de investigación que tienen como objetivo el desarrollo de tecnologías y nuevas metodologías que faciliten este reciclaje.

18 de septiembre de 2023

Visita a *Nigth Laser Vision Spain* (NLVS)

El día 18 de septiembre de 2023 se produjo una visita a las instalaciones de *Nigth Laser Vision Spain* (NLVS) en Alcobendas, Madrid. El objetivo de la reunión fue conocer sus instalaciones y últimos desarrollos, así como sus capacidades actuales, en particular respecto de Sistemas de Visión Nocturna (SVN) y Sistemas Láser.

18 al 29 de septiembre de 2023

DYMS 23 (*Dynamic Messenger* 23)

Tras la participación española en los ejercicios operativos DYMS 22 en la península de Troia (sur de Lisboa), la Armada española, en colaboración con la SDG PLATIN, ha participado en una nueva edición celebrada durante el mes de septiembre del presente año. En esta ocasión el objetivo fue crear un nodo de comunicaciones 5G que permitiera la conexión de las plataformas no tripuladas con sus respectivas estaciones de control embarcadas en el BAM Furor e integradas en el SCOMBA, a través del Sistema NAIAD, así como la transmisión en tiempo real de la información recabada por los mismos en misiones de vigilancia y reconocimiento marítimos.

¿Dónde hemos estado?

19 al 21 de septiembre de 2023

Primera reunión del Plan Complementario de Comunicaciones Cuánticas

Los días 19, 20 y 21 de septiembre tuvo lugar el *kick-off* del Plan Complementario de Comunicaciones Cuánticas, organizado por la UPM de Madrid, donde se reunieron los investigadores y expertos de las entidades nacionales implicadas en cada uno de los nodos que compondrán el mapa nacional de comunicaciones cuánticas: Castilla y León, Galicia, País Vasco, Cataluña, Valencia y Madrid, además del CSIC. El propósito de este Plan es reforzar la ciberseguridad e impulsar la ciencia y la innovación en esta área. El tercer día, denominado *Industry Day*, fue abierto para todos los públicos previa inscripción, y sirvió de encuentro entre investigadores, la industria, startups de comunicación cuántica, instituciones de financiación pública y privada y entidades de *venture capital.*

20 de septiembre de 2023

Diálogos en EOI: Tecnologías disruptivas, una apuesta inevitable

El pasado 20 de septiembre tuvo lugar la segunda jornada de los Diálogos en la EOI, organizado por IDS, en colaboración con la Escuela de Organización Industrial (EOI). Este evento contó con la participación del Ministerio de Defensa, Arquimea y Grupo Oesía. Su objetivo se centró en debatir sobre las tendencias y desafíos que conllevan la adopción de tecnologías disruptivas. Desde la Unidad de Planificación de I+D Nacional (SDG PLATIN – DGAM), el comandante Carlos Calderón expuso la necesidad de una visión de conjunto, dejando claro el apoyo desde el MINISDEF a aquellas iniciativas de las empresas que sirven para retener talento, además de permitir la independencia de terceros.

25 de septiembre de 2023

Taller Ejército-empresas

El día 25 de septiembre se visitaron las instalaciones del Acuartelamiento Capitán Arenas (Guadalajara) para asistir al taller Ejército-Empresas sobre modernización del Leopardo 2E y la transformación del Leopardo 2A4 a carro de zapadores, donde las empresas GDELS, IVECO y KMW expusieron potenciales soluciones para dar respuesta a las necesidades operativas de ET en torno a estos sistemas.

X Congreso Nacional de I+D en Defensa y Seguridad (DESEi+d 2023)

Autor: Rosalía Vindel Román, Nodo Gestor, SDG PLATIN.

Palabras clave:BTID, CUD, dual, universidad, centro tecnológico, empresas.

Áreas ETID relacionadas: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11.

Introducción

La Subdirección General de Enseñanza Militar de la Dirección General de Reclutamiento y Enseñanza Militar (DIGEREM), la Subdirección General de Planificación, Tecnología e Innovación (SDG PLATIN) de la Dirección General de Armamento y Material (DGAM), junto con los Centros Universitarios de Defensa e Isdefe (Ingeniería de Sistemas para la Defensa de España), organizan el X Congreso Nacional de I+D en Defensa y Seguridad (DESEi+d 2023), que este año tendrá lugar en la Escuela de Infantería de Marina General Albacete y Fuster (EIMGAF), ubicada en Cartagena, durante los días 14, 15 y 16 de noviembre de 2023.

La extensa Base Tecnológica e Industrial de Defensa (BTID), formada por los Centros Universitarios de la Defensa (CUD), universidades, centros tecnológicos y empresas, con capacidades tecnológicas de carácter dual, permiten afrontar nuevos retos que se traducen en beneficios tecnológicos, sociales y económicos para las Fuerzas Armadas y los Cuerpos de Seguridad, pero también para toda la ciudadanía. En la línea de las ediciones anteriores, este Congreso se presenta como un foro y punto de encuentro de todos los agentes relacionados con la I+D en el ámbito de la Defensa y la Seguridad, donde tendrá la oportunidad de presentar y difundir los resultados de las últimas investigaciones y trabajos realizados en alguna de sus áreas temáticas, además de permitir poner en común las capacidades, necesidades e intereses para facilitar la necesaria colaboración de la BTID con el fin de afrontar los retos futuros, así como atraer bienestar para la sociedad.

Premios Isdefe I+D+i

En el marco del DESEi+d 2023, Isdefe convoca la séptima edición del Premio Isdefe I+D+i «Antonio Torres», la segunda edición del Premio Estudiante Universitario Isdefe y la primera edición del Premio Desafío Defensa Isdefe (DESEi+d 2023).

Esta edición del Congreso constará de tres premios: a la mejor comunicación general presentada en dicho Congreso; a la mejor comunicación presentada sobre la temática «Sistemas satelitales», ambos premiados con 2.500 €, y un tercero de 1.000 € para la mejor comunicación presentada por estudiantes universitarios.

Más información

En el Portal de Tecnología e Innovación del Ministerio de Defensa se puede encontrar un banner exclusivo para el DESEi+d 2023, con información sobre el programa, que contiene las áreas temáticas y sesiones en las que está dividido el Congreso, cómo y cuándo realizar la inscripción o cómo llegar, entre otros datos de interés.

Notas sobre el contexto legal internacional y de la UE para el uso militar de la inteligencia artificial

Autores: AN Francisco Lamas López, Dr. ingeniero ENPC Paris Tech, Arsenal de Cartagena; Alfonso Peralta Gutiérrez, juez de carrera, Poder Judicial del Reino de España.

Palabras clave: IA confiable, usos militares de la IA, Derecho internacional público, control humano, regulaciones, liderazgo de la UE, Sistemas de Armas Autónomas Letales (LAWS).

Líneas I+D+i ETID relacionadas: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11.

Introducción

El rápido avance de la inteligencia artificial (IA) y la tecnología relacionada plantea desafíos éticos y legales. La Unión Europea (UE) y sus Estados miembros deben garantizar que estas tecnologías se utilicen en beneficio de la humanidad y se ajusten a valores humanistas. Se requiere un marco legal completo que aborde la ética, la responsabilidad y la transparencia, especialmente en tecnologías de alto riesgo potencial en su uso, como las utilizadas en el ámbito militar. La UE debe adoptar una definición común de «IA» y respetar los valores fundamentales y los derechos humanos en su regulación. Esto fomentaría la innovación y la competitividad europea mientras protege estos derechos. La UE debe liderar la gobernanza global de la IA y colaborar con organizaciones internacionales como la ONU y el Consejo de Europa para establecer normas internacionales y abordar cuestiones éticas, legales y de seguridad en este campo.

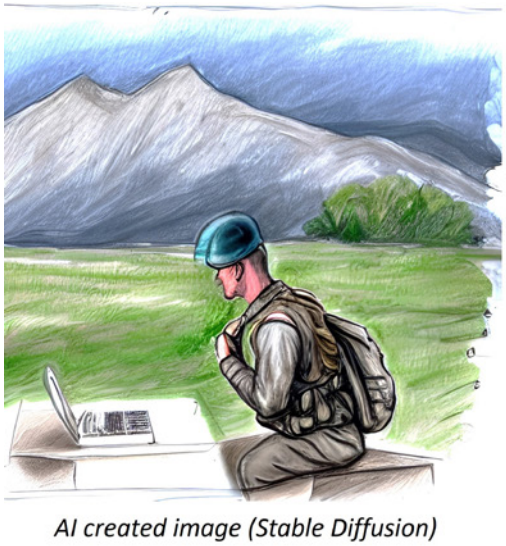
La inteligencia artificial busca imitar funciones cognitivas y conductuales humanas, aplicándose en diversos campos (*European Commission*, 2020) (1) (figura 1). En el ámbito legal, la Comisión Europea promueve su desarrollo con salvaguardias para proteger los derechos fundamentales, respaldadas por la Directiva 2016/679 del Parlamento Europeo y del Consejo (GDPR) (*European Parliament*, 2016) (2).

Además, la UE emitió recomendaciones éticas para la IA, destacando la transparencia y la no discriminación (*European Commission*, 2020). A nivel internacional, las Naciones Unidas han establecido directrices éticas para la IA en su informe *Ética en la Inteligencia Artificial* (*United Nations*, 2019) (3), que incluyen principios generales y aplicaciones sectoriales. La IA, en general, tiene mucho potencial para incrementar las capacidades militares de todas las naciones, pero plantea desafíos legales y éticos que requieren un equilibrio entre la protección de los derechos fundamentales y la promoción de la innovación. Las regulaciones europeas e internacionales deben ofrecer en sus desarrollos futuros un marco seguro para un desarrollo y uso responsables de la IA.

Principios rectores

Según el Grupo de Expertos de Alto Nivel en Inteligencia Artificial (AI-HLEG) de la Comisión Europea, la inteligencia artificial confiable se basa en dos pilares. En primer lugar, debe cumplir con los derechos fundamentales y principios éticos, asegurando un «propósito ético». En segundo lugar, debe ser técnicamente sólida y confiable para evitar daños no intencionados.

Figura 1. Conceptos introductorios a la problemática del uso de la IA en contextos militares. (Fuente: propia).



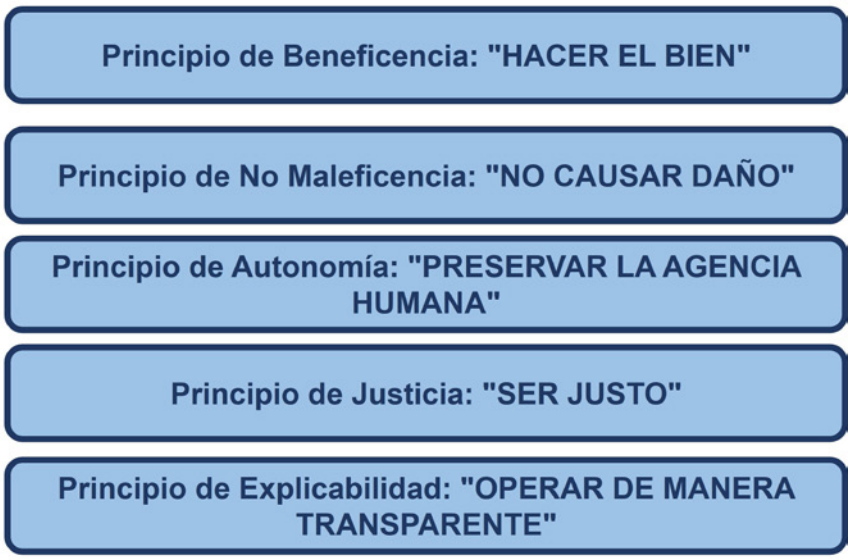


Figura 2. Principios rectores de la IA según el AI-HLEG (2018). (Fuente: propia).

El AI-HLEG destaca varios principios rectores fundamentales (figura 2) relacionados con la IA. Estos incluyen el principio de beneficencia, que establece que los sistemas de IA deben contribuir al bienestar individual y colectivo. También incluye el principio de no maleficencia, que implica que los sistemas de IA no deben causar daño a los seres humanos y deben proteger sus derechos y libertades. El principio de autonomía sostiene que la IA no debe subyugar la autonomía humana sobre los sistemas en ningún caso y que las personas deben tener autodeterminación al interactuar con sistemas de IA. Además, el principio de justicia enfatiza la importancia de prevenir sesgos y discriminación en la IA. La transparencia es clave, tanto en términos tecnológicos como de modelo de negocio, para mantener la confianza en los sistemas de IA.

El AI-HLEG también establece requisitos específicos que se derivan de estos principios, como los mostrados en la figura 3.

Marco jurídico internacional aplicable al ámbito militar

La IA tiene un impacto en diversos campos, incluido el militar, y plantea cuestiones éticas identificadas por el Grupo Europeo sobre Ética en la Ciencia y las Nuevas Tecnologías (AI-HLEG) (*European Commission*, 2020). Estas cuestiones involucran seguridad, prevención de daños, responsabilidad moral humana, gobernanza, regulación, diseño, y toma de decisiones democráticas, así como la explicabilidad y transparencia de la IA y de los sistemas autónomos. En el contexto militar, se destacan los Sistemas de Armas Autónomas Letales (LAWS), donde el AI-HLEG subraya la importancia del «Control Humano Significativo» para la responsabilidad moral (*European Commission*, 2018) (4).

En relación con el uso de armas basadas en inteligencia artificial (IA), se destaca la importancia de tener siempre la capacidad de corregir, detener o desactivar estas armas en caso de comportamiento imprevisto, interferencia externa o adquisición por terceros de esta tecnología. Estas preocupaciones éticas incluyen el riesgo de una carrera armamentista descontrolada y la pérdida de control humano en contextos militares. El derecho internacional, especialmente el humanitario, debe aplicarse rigurosamente a todos los sistemas de armas y operadores. La IA también puede desempeñar un papel en la guerra no convencional (*European Parliament*, 2021) (5).

La IA ofrece oportunidades para fortalecer la seguridad de la Unión Europea (UE) y sus ciudadanos. La UE debe adoptar un enfoque integrado en discusiones internacionales y desarrollar una posición legalmente vinculante para abordar cuestiones éticas y legales, incluyendo el control humano, la supervisión y la responsabilidad, así como la implementación de la ley internacional de derechos humanos, la ley humanitaria internacional y las estrategias militares (*European Parliament*, 2021). La creciente carrera armamentista en sistemas de armas autónomas requiere que la comunidad de investigación en IA integre principios que garanticen el control y la responsabilidad humanas en todos los sistemas de IA militar. La toma de decisiones autónomas no debe eximir a los humanos de su responsabilidad. Se enfatiza la necesidad de un control humano adecuado y unas condiciones uniformes para el uso de IA en conflictos convencionales y no convencionales (*European Parliament*, 2020a) (6). El Parlamento Europeo también evaluó la importancia del control humano en el uso de IA en contextos militares y civiles, destacando la necesidad de tener siempre un humano disponible para corregir, detener o desactivar la IA en situaciones imprevistas. El respeto al derecho internacional público, especialmente el derecho humanitario, es fundamental en este sentido. Se propone que la investigación, desarrollo y uso de IA en la guerra irregular se rija por las mismas condiciones que en conflictos convencionales. Es esencial que la UE adopte un enfoque integrado en futuras discusiones internacionales sobre la inteligencia artificial, destacando que la toma de decisiones autónoma no debe eximir a los seres humanos de su responsabilidad. En cuanto al uso de la inteligencia artificial en el adiestramiento en los ejercicios militares, el informe reconoce su potencial, pero destaca la necesidad de considerar los posibles riesgos, especialmente en

relación con víctimas civiles, lesiones y daños a la infraestructura civil, así como intervenciones no intencionales, manipulación, proliferación y ciberataques.

La UE, junto con la ONU y la comunidad internacional, deberán liderar la promoción de un marco global para el uso de la IA, definiendo la necesidad de sistemas sólidos de monitoreo y evaluación para el desarrollo de tecnologías utilizadas con fines militares (*European Parliament*, 2005) (7). En el desarrollo, despliegue, uso y gestión de la inteligencia artificial, deben respetarse los derechos fundamentales y los valores consagrados en los Tratados de la UE, investigando los riesgos que puedan surgir del uso de la IA por parte de las autoridades estatales y las instituciones de la Unión Europea. Del mismo modo, la UE debe facilitar la investigación y el diálogo sobre las oportunidades de uso de la IA en la ayuda en caso de desastres, prevención de crisis y mantenimiento de la paz, asegurando que los sistemas basados en IA cumplan con principios éticos y legales.

En lo concerniente a los sistemas de armas letales autónomos (LAWS), los sistemas basados en inteligencia artificial no deben reemplazar la toma de decisiones humanas (*United Nations*, 1980) (8). Debe evitarse el desarrollo y uso de LAWS capaces de llevar a cabo ataques sin control humano significativo y se deben iniciar negociaciones para su prohibición internacional. Las LAWS solo son legales si están sujetas a un estricto control humano en todo momento, de acuerdo con regulaciones internacionales. Se enfatiza la importancia de que la inteligencia artificial en contextos militares cumpla con requisitos específicos, incluyendo la distinción entre combatientes y no combatientes y el cumplimiento de los principios del derecho humanitario internacional. Se propone que las LAWS sean incluidas en el Tratado sobre el Comercio de Armas (*United Nations*, 2013) (9) para regular su comercio y prevenir su proliferación incontrolada. Además, se excluye el financiamiento para LAWS sin control humano significativo por parte del Fondo Europeo de Defensa (EDF, por sus siglas en inglés) (*European Parliament*, 2006) (10). En conclusión, es esencial reforzar las regulaciones internacionales para garantizar una regulación adecuada y una mayor transparencia en el desarrollo y uso de LAWS.

Las medidas de seguridad que se deben implementar en estos sistemas incluyen de forma general el uso de materiales no tóxicos y la adición de dispositivos de seguridad tales como sensores y sistemas de parada de emergencia. Como, además, se deben proporcionar instrucciones claras sobre el uso y reparación con seguridad de robots y sistemas autónomos, la Directiva 2006/42/CE del Parlamento Europeo en 2006 establece una serie de requisitos que deben obeceder los robots y sistemas autónomos que cumplen con la definición de «máquina». Las empresas que producen, importan o distribuyen estos dispositivos son responsables de garantizar su seguridad y deben cumplir con las normas y medidas de seguridad establecidas en la Directiva.

La resolución del Parlamento Europeo de 20 de octubre de 2020 con recomendaciones a la Comisión sobre un marco para los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías relacionadas (2020/2012[INL]) (2021/C404/04) (*European Parliament*, 2020b) (11), en la sección de Seguridad y Defensa, evaluó que las políticas de seguridad y defensa de la Unión Europea y sus Estados miembros deben estar guiadas por los principios de la Carta de las Naciones Unidas y por una comprensión común de los valores universales de respeto a los derechos inviolables e inalienables de la persona, la dignidad humana, la libertad, la democracia, la igualdad y el Estado de derecho.

Figura 3. Requisitos de la IA según el AI-HLEG (2018). (Fuente: propia).

Esto fue uno de los resultados tras la aprobación por parte de la Reunión de Altas Partes Contratantes de la Convención de las Naciones Unidas sobre Ciertas Armas Convencionales de 2019 (CCW) (*United Nations* General Assembly, 2019) (12) de once principios rectores para el desarrollo y uso de sistemas de armas autónomas; sin embargo, lamenta la falta de acuerdo sobre un instrumento jurídicamente vinculante que regule las armas autónomas letales con un mecanismo efectivo de cumplimiento.

Se aboga por un aumento de la inversión en inteligencia artificial europea para la defensa y la infraestructura crítica que la sustenta, en vista de los significativos esfuerzos de las potencias militares mundiales en investigación y desarrollo militar e innovación. Igualmente, se subraya que la responsabilidad y la rendición de cuentas por la decisión de diseñar, desarrollar, desplegar y utilizar sistemas de inteligencia artificial deben recaer completamente en los operadores humanos, dado que debe haber una supervisión y control humano significativos sobre cualquier sistema de armas. También se destaca que el control humano debe ejercerse de manera efectiva sobre el mando y control de los sistemas basados en IA, de acuerdo con los principios de la participación, supervisión y control humano, en la conducción de operaciones militares.

La resolución del Parlamento Europeo de 16 de febrero de 2017 con recomendaciones a la Comisión sobre las reglas de derecho civil sobre robótica (2015/2103[INL]) (2018/C 252/25) (*European Parliament*, 2018) (13) reconoce que una nueva era requiere un impulso legislativo e, incluso, una definición generalmente aceptada de robots e inteligencia artificial que sea flexible y no obstaculice la innovación. Ve el potencial de la robótica y de la inteligencia artificial para transformar los estilos de vida y las formas de trabajo, aumentar los niveles de eficiencia, ahorro y seguridad, y mejorar la calidad de los servicios, e incluso acepta la posibilidad de que a largo plazo la inteligencia artificial pueda superar la capacidad intelectual humana, y también reconoce varias preocupaciones sobre sus efectos directos e indirectos en la sociedad en su conjunto. También se determina que la automatización requiere que aquellos involucrados en el desarrollo y comercialización de aplicaciones de inteligencia artificial incorporen características de seguridad y éticas desde el principio.

En el campo militar, este texto hace solo dos menciones: en su considerando 64 destaca que las restricciones y condiciones establecidas en el Reglamento (CE) N.º 428/2009 del Parlamento Europeo y del Consejo (*European Parliament*, 2009) (14) sobre el comercio de artículos de uso dual (bienes, software y tecnología que se pueden utilizar tanto para aplicaciones civiles como militares o que podrían contribuir a la proliferación de armas de destrucción masiva) deberían extenderse a las aplicaciones de robótica. Por último, pero no menos importante, prohíbe la modificación de robots para su uso como armas.

En el ámbito del Comité Internacional de la Cruz Roja (CICR), se presentó un estudio sobre la Convención sobre Ciertas Armas Convencionales (CCW) en noviembre de 2021 (ICRC, 2021) (15). La CCW y sus Protocolos buscan restringir el uso de armas convencionales que plantean preocupaciones humanitarias, legales y éticas específicas. El CICR emitió opiniones y recomendaciones sobre diversas cuestiones de preocupación humanitaria relacionadas con la CCW, como la adhesión a la CCW, armas como minas que no son antipersonal, armas incendiarias, armas láser cegadoras, restos explosivos de guerra, armas explosivas en áreas pobladas, sistemas de armas autónomas y avances en ciencia y tecnología en relación con nuevas armas.

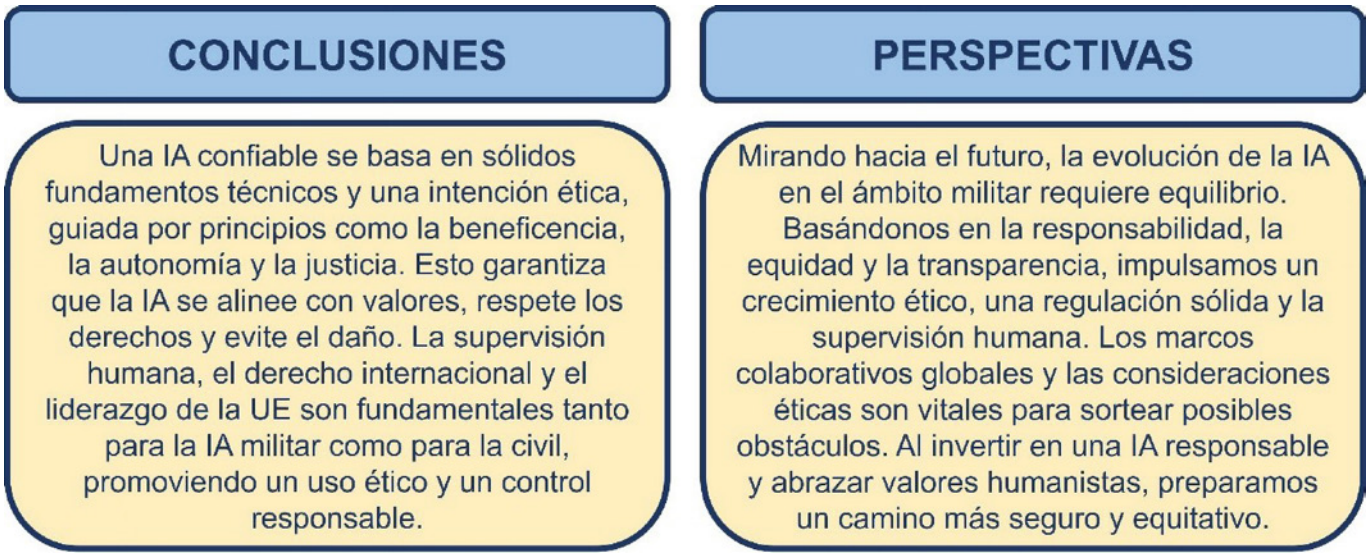


Figura 4. Conclusiones y perspectivas de la nota sobre Marco en la UE sobre usos militares de la IA. (Fuente: propia).

La 6.ª Conferencia de Revisión de la CCW, celebrada en diciembre de 2021 en Ginebra, es crucial para evaluar el papel de la CCW en la minimización del sufrimiento en conflictos armados y asegurar su adecuación a medida que evoluciona la guerra. El CICR aborda los sistemas de armas autónomas, un tema discutido desde 2014 en la CCW y en el actual Grupo de Expertos Gubernamentales (GGE) desde la 5.ª Conferencia de Revisión.

El debate sobre el uso militar de la inteligencia artificial se ha iniciado en la ONU y en la CCW, con varias Altas Partes Contratantes respaldando el principio de «control humano significativo» para sistemas de armas autónomas. El CICR también recomienda que los Estados adopten normas legalmente vinculantes sobre sistemas de armas autónomas para mantener el control y juicio humano en el uso de la fuerza. Esto implicaría prohibir ciertos tipos de sistemas de armas autónomas y regular estrictamente los demás, imponiendo límites en objetivos, duración, alcance geográfico y situaciones de uso, así como requisitos de interacción humano-máquina. El CICR insta a las Altas Partes Contratantes en la Conferencia de Revisión a establecer un camino hacia la adopción de nuevas normas legalmente vinculantes sobre sistemas de armas autónomas, incluyendo un posible nuevo Protocolo del CCW y el fortalecimiento de las normas de derecho internacional humanitario existentes.

Conclusiones y perspectivas

En resumen, la IA confiable se basa en la robustez técnica y el propósito ético, con principios como beneficencia, no maleficencia, autonomía, justicia y explicabilidad. El control humano es clave en contextos militares y civiles, respetando el derecho internacional humanitario (figura 4). La UE y la comunidad global deben promover un marco para la IA y unas regulaciones para sistemas letales de armas autónomas (LAWS), con inversiones en capacitación. Se necesita una estrategia de la UE que refleje valores éticos y asegure el control humano en todas las etapas de desarrollo y uso de la IA, priorizando el respeto a la dignidad y la autonomía humanas.

Bibliografía

[1] *European Commission*. (2020). *White paper on artificial intelligence: A European approach to excellence and trust.* Disponible en: https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

[2] *European Parliament. Council of the European Union*. (2016). *Directive 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union. L 119, 1-88.*

[3] *United Nations*. (2019). *Ethics in artificial intelligence: Report of the Secretary-General.*

[4] *European Commission*. (2018). *High-Level Expert Group on Artificial Intelligence. Draft Ethics Guidelines for Trustworthy AI. European Commission. Directorate-General for Communication. December 18th 2018*. Disponible en: https://digital-strategy.ec.europa.eu/en/library/draft ethics guidelines-trustworthy-AI.

[5] *European Parliament*. (2021). P9_TA (2021)0009 *Artificial intelligence: questions of interpretation and application of international law European Parliament resolution of 20 January 2021 on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (2020/2013[INL])* (2021/C 456/04).

[6] *European Parliament*. (2020a). *European Parliament resolution of 12 February 2021 on a European strategy for artificial intelligence* (2020/2012[INI]).

[7] *European Parliament. Council of the European Union*. (2005). *Directive 2005/36/EC of the European Parliament and of the Council of 7 September 2005 on the recognition of professional qualifications*. *Official Journal of the European Union*. L 255, 22-142.

[8] *United Nations General Assembly*. (1980). *Convention on Certain Conventional Weapons of 10 October 1980.*

[9] *United Nations General Assembly*. (2013). *Arms Trade Treaty, 2 April 2013.*

[10] *European Parliament. Council of the European Union*. (2006). *Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast)*. *Official Journal of the European Union*. L 157, 24-86.

[11] *European Parliament*. (2020b). *Framework for the ethical aspects of artificial intelligence, robotics and related technologies. European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework for the ethical aspects of artificial intelligence, robotics and related technologies* (2020/2012[INL]) (2021/C 404/04).

[12] *United Nations*. (2019). Ethics in artificial intelligence: *Report of the Secretary-General.* Disponible en: https://undocs.org/en/A/74/260

[13] *European Parliament*. (2018). *Civil law rules on robotics.* European Parliament resolution of 16 February 2017 *with recommendations to the Commission on civil law rules on robotics* (2015/2103[INL]) (2018/C 252/25).

[14] *European Parliament*. *Council of the European Union. (2009). Regulation (EC) No 428/2009 of the European Parliament and of the Council of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items (recast)*. *Official Journal of the European Union*. L 134, 1-269.

[15] ICRC. (2021). *Views and Recommendations for the 6th Review Conference of the Convention on Certain Conventional Weapons. Working paper submitted by the International Committee of the Red Cross. 8 November 2021 6th Review Conference of the Convention on Certain Conventional Weapons.*

Se reinventan los sistemas de suspensión de los vehículos blindados

Autora: Juan Sáez, ingeniero jefe; Isabel Ligués, coordinadora de Proyecto y responsable de Estrategia y Desarrollo Empresarial, Piedrafita Systems.

Palabras clave: sellado, cojinetes auto lubricados, hidroneumático.

Líneas I+D+i ETID relacionadas: Subárea 5.1.

Introducción

El actual entorno tecnológico es retador, en rápida evolución y exige la necesidad de desarrollar cada vez más soluciones innovadoras que utilicen tecnologías novedosas.

En el ámbito de la suspensión de vehículos especiales, las soluciones actuales se basan en cilindros hidroneumáticos, en barras de torsión con amortiguador mecánico o hidráulico, o en sistemas de suspensión rotativos accionados por bieletas y basados en cilindros hidroneumáticos.

En las últimas décadas, el constante aumento del peso y los exigentes requisitos de alta movilidad han puesto a prueba las diferentes tecnologías de suspensión. Los amortiguadores rotativos han aumentado notablemente su capacidad de disipación de energía, al pasar de tecnologías basadas en la fricción a amortiguadores rotativos totalmente hidráulicos de alta eficiencia y bajo mantenimiento.

Frente a las soluciones actuales, la tecnología en la que se está trabajando integra tanto un amortiguador rotativo hidráulico (elemento de disipación de energía) como un componente elástico hidroneumático rotativo completo (elemento elástico) en un único sistema.

El estado actual de la técnica no contempla el empleo de sistemas de suspensión totalmente rotativos para vehículos blindados pesados que es lo que, con el fin de mejorar las capacidades de cualquier sistema actual, se propone conseguir este proyecto, por lo que constituye necesariamente una innovación pionera.

Objetivo tecnológico

El proyecto en el que actualmente está trabajando Piedrafita Systems, en un consorcio de trabajo colaborativo junto con la empresa francesa Repack-S y la alemana IB Fischer CFD + Engineering GmbH, se encuentra enmarcado en el programa EDIDP (Programa Europeo de Desarrollo Industrial de la Defensa) 2020. El Proyecto SRB ofrecerá una novedosa suspensión rotativa para blindados, de ahí su acrónimo SRB.

Se desarrollará un sistema rotativo hidroneumático completo de suspensión, mediante la fusión de un amortiguador rotativo (elemento disipador de energía) y un elemento elástico rotativo (componente elástico).

Este sistema pretende ser la solución de suspensión hidroneumática para la próxima generación de flotas de vehículos blindados (MBT, IFV o APC) y también ser extensivas para la modernización o actualización de plataformas existentes.

El proyecto SRB

El Proyecto SRB, que dará lugar a un sistema rotativo hidroneumático completo de suspensión, cuenta con tres grandes fases, además de una primera fase preliminar de estudio.

La primera gran fase es la de diseño, en la que se proyectan los sellados del elemento elástico, se realiza el cálculo de los fluido dinámicos, su modelado y caracterización, así como el sistema de control de estabilización y altura y todos los demás elementos necesarios para la integración completa del producto.

La segunda fase es la creación de un prototipo y, como tercera y última fase, se realizarán las pruebas del sistema de sellado, la correlación y validación del modelo de fluido dinámico y las pruebas y ensayos de la suspensión completa.

En la actualidad se ha completado la fase de diseño (CDR: Critical Design Review o Revisión Crítica del Diseño). Esta fase ha sido crucial para validar si se pueden superar los retos técnicos presentados en la propuesta EDIDP inicial y para validar que este nuevo amortiguador rotativo hidroneumático se puede adaptar a una amplia gama de carros de combate existentes sin modificaciones significativas sobre los vehículos.

Reto 1: estanqueidad

Es imperativo diseñar una solución de estanqueidad innovadora para garantizar la ausencia de fugas entre fluidos compresibles e incompresibles en el interior del elemento elástico rotativo. Aunque ya existen soluciones para los elementos lineales, no hay ninguna capaz de garantizar el grado de estanqueidad requerido para un elemento rotativo. El desarrollo de esta solución de estanquidad requiere la investigación de materiales, fabricación, geometría, etc. Estos sellados deben ser capaces de soportar muy altas presiones, incrementando el reto tecnológico presentado.

Reto 2: modelo fluido dinámico

Además del diseño de los propios componentes, será de vital importancia disponer de un modelo fluido dinámico del sistema de suspensión, en especial, será de gran importancia poder caracterizar completamente la solución en el sistema de válvulas interno del amortiguador para garantizar la adaptabilidad del producto final. Este modelo fluido dinámico, que habrá que desarrollar para validar el diseño, constituirá un modelo altamente innovador. Asimismo, será necesario para garantizar la posterior modularidad de la tecnología desarrollada y adaptabilidad a diferentes vehículos y tipos de vehículos.

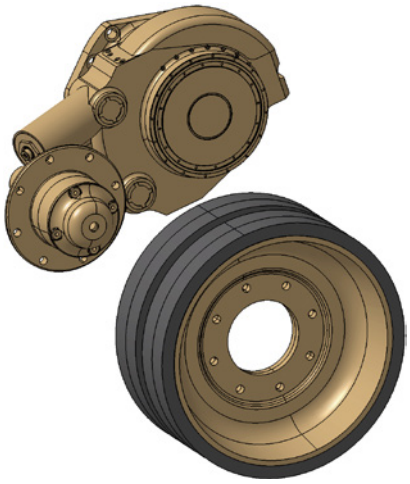


Figura 1. Sistema de suspensión rotativa hidroneumática del Proyecto SRB. (Fuente: propia).

Objetivos específicos del proyecto

- Recorrido vertical de las ruedas: el sistema de suspensión permitirá a los vehículos superar obstáculos más altos que las soluciones actuales.
- Rango de temperaturas de trabajo: el sistema de suspensión será capaz de funcionar bajo temperaturas extremas, que vayan desde el frío extremo hasta temperaturas sumamente elevadas.
- Capacidad de carga del sistema de suspensión: el sistema de suspensión debe ser capaz de proporcionar un par máximo superior al de las soluciones actuales. Un 50 % más de capacidad de amortiguación que la solución actual de última generación.
- Relación muelle/tamaño sin precedentes: mejor rendimiento que el índice de elasticidad de la barra de torsión, en una solución más compacta y sin efecto de fatiga.

Características de esta tecnología

- Mayor movilidad: el sistema de suspensión en el que se está trabajando proporcionará un mayor recorrido de la suspensión, capacidad de degradación energética y control de la altura de la suspensión. Todo ello influirá en gran medida en la movilidad de la plataforma. La capacidad de degradación energética del sistema de suspensión será independiente del recorrido y la posición de la suspensión, y la solución propuesta permitirá una progresividad controlada a lo largo de todo el recorrido.
- Reducción de costes: la facilidad de integración de la solución, así como la modularidad de la misma y la posibilidad de integrar soluciones análogas en diversos vehículos, presenta la capacidad de reducir en gran medida los costes de los vehículos. Desde la mayor facilidad de integración, que puede disminuir los costes iniciales de desarrollo de los vehículos, hasta la drástica reducción del coste de ciclo de vida al tratarse de una solución libre de mantenimiento, pasando por la reducción en el coste de adquisición mediante la posibilitación de la creación de economías de escala al permitir la adaptabilidad para un número mayor de vehículos y, por lo tanto, mayores tiradas de producción.
- Menor o escaso mantenimiento: al emplear tecnología rotativa frente a tecnología de fricción, el sistema eliminará los elementos de desgaste y reducirá así la necesidad de mantenimiento. Se elimina con ello la necesidad de renovar periódicamente los componentes debido a los daños causados por la fatiga, no solo en las barras de torsión, sino también en cualquiera de los muelles helicoidales metálicos empleados actualmente.

  Todo lo anterior garantiza que no será necesario ningún tipo de operaciones de conservación durante la vida útil estimada del sistema. De este modo, se anulan los costes de mantenimiento de la suspensión del vehículo y se aumenta considerablemente su disponibilidad de uso.

  En caso de que fuera necesario efectuar reparaciones debido a daños causados, no por el envejecimiento, sino por factores externos, los costes de mantenimiento seguirían siendo inferiores a los actuales, ya que solo habría que enviar a reparar el vehículo dañado, lo que permitiría al resto de la flota seguir funcionando y aumentar así su disponibilidad y tiempo de funcionamiento.
- Incremento de la protección: el uso de barras de torsión afecta en gran medida a la protección, haciendo que las plataformas sean más vulnerables a los artefactos explosivos improvisados y las minas, por lo que su eliminación supondría automáticamente una mayor protección para el vehículo y su tripulación.
- Fácil integración: al integrar ambos elementos de la suspensión en un único sistema y eliminar así la necesidad de barras de torsión, se facilita la integración del sistema resultante, tanto en nuevas plataformas como en mejoras de movilidad de vehículos actuales, así como en plataformas tripuladas y no tripuladas. Entre los objetivos del proyecto estará la minimización de la demanda de espacio del sistema, con el fin de aumentar la integrabilidad.
- Compatibilidad con todas las plataformas blindadas: de la facilidad de integración de esta solución se deriva que la tecnología desarrollada pueda ser válida para cualquier tipo de vehículo especial, desde ocho hasta setenta toneladas,

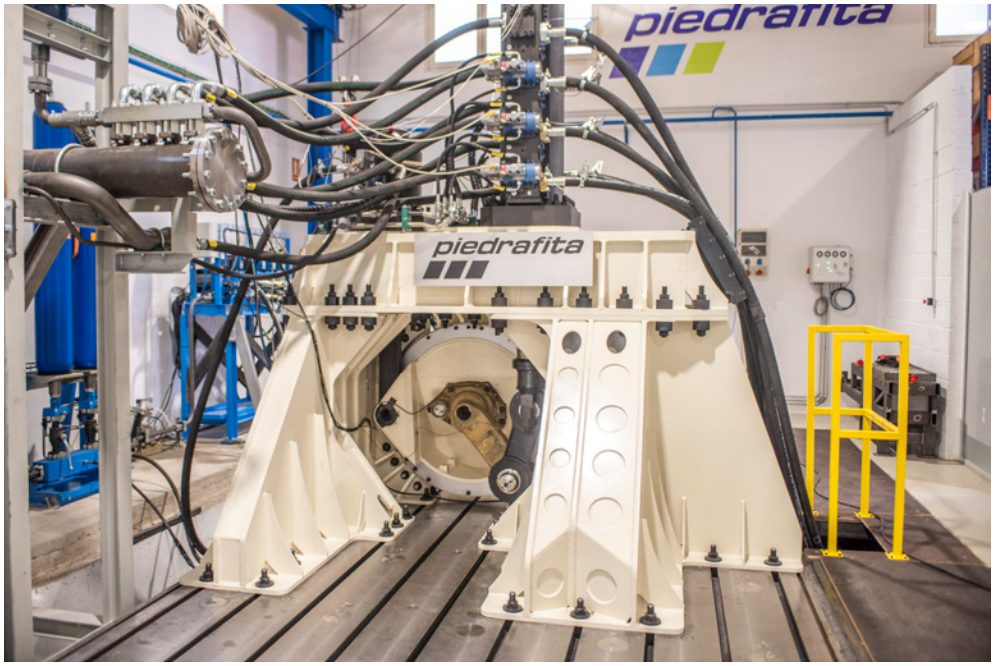


Figura 2. Banco de ensayos en las instalaciones de Piedrafita. (Fuente: propia).

sobre cadenas y sobre ruedas, tripulado y no tripulado; con la necesaria adaptación de la tecnología desarrollada.

Se pretende la total compatibilidad con todas las plataformas blindadas existentes en la actualidad, y no solo en plataformas de nueva generación —modularidad que se estudiará más adelante—, aunque el proyecto actual se centra principalmente en el desarrollo para las plataformas más pesadas, a fin de ser un desarrollo de máximos. De igual manera, se desea que la solución desarrollada sea de valor para España, por lo que se ha puesto un especial énfasis en la integrabilidad con la plataforma española Leopard 2E.

Próximos retos

Una vez completados todos los hitos del diseño, se fabricará un prototipo del sistema de suspensión con el fin de utilizar este para realizar los ensayos y pruebas de validación necesarias para validar su conformidad, tanto con los Initial Common Requirements acordados por los Estados miembros que apoyan el proyecto, como con los requisitos específicos definidos durante la fase inicial de diseño conceptual.

Estas pruebas deberán servir también para permitir la correlación del modelo fluido dinámico desarrollado con el prototipo final, a fin de tener un modelo completo y permitir la mayor escalabilidad posible de cara al futuro. La validación de este modelo será también un primer plazo en el objetivo a largo plazo de permitir la integración con un futuro gemelo digital, ambición que el consorcio tiene intención de continuar desarrollando durante un posible futuro SRB2 bajo el marco de los programas EDF.

Para poder probar esta suspensión, en concreto en su fase de pruebas del prototipo, se ha diseñado un banco de ensayos que permite poner a prueba suspensiones completas de vehículos especiales, y que permite asegurar la calidad y el rendimiento óptimo de los sistemas completos de suspensión.

Con capacidades para ensayar vehículos de hasta setenta toneladas, este banco de ensayos es capaz de simular perfiles muy exigentes, como el paso de cadenas de vehículos pesados por las irregularidades del terreno, reproduciendo altos niveles de vibración. Esta función es esencial para evaluar la resistencia y el rendimiento de las suspensiones en condiciones desafiantes y extremas.

Digitalización de la suspensión

Una vez que se haya validado y probado el prototipo de este sistema rotativo hidroneumático completo de suspensión, el siguiente paso por el que se apuesta es la digitalización de los sistemas de suspensión. Este desafío se refiere no solo a la capacidad de sensorizar y digitalizar únicamente las suspensiones, sino cualquier sistema de suspensión existente en las flotas de vehículos, en plataformas nuevas o legadas.

Esta digitalización, en la que ya se está trabajando, permite registrar el uso real del vehículo y hacer un cálculo de la vida útil restante de sus componentes. Es capaz de realizar una trazabilidad automatizada de los mismos gracias a que el vehículo está totalmente monitorizado. De esta forma se favorece la capacidad de realizar un mantenimiento predictivo de cada vehículo de la flota, realizando predicciones basadas en el uso.

Mediante la implantación de un DSC (*Digital Suspension Controller*) que se prevé desarrollar e integrar en la solución durante el proyecto SRB2, se sentarán las bases para permitir la realización del mantenimiento predictivo de las suspensiones, ayudando también con la información proporcionada al avance del desarrollo del mantenimiento predictivo, mediante la integración con los sistemas de los integradores de vehículos y soportando los avances de los propios usuarios finales.

Objetivo último de esta tecnología

Ofrecerá una mayor competitividad y autonomía al potenciar las capacidades industriales europeas. La naturaleza patentable del producto, así como sus destacadas ventajas tecnológicas, podrían conducir al establecimiento de una hegemonía europea en sistemas de suspensión.

El Proyecto SRB contribuirá en gran medida a la mejora general

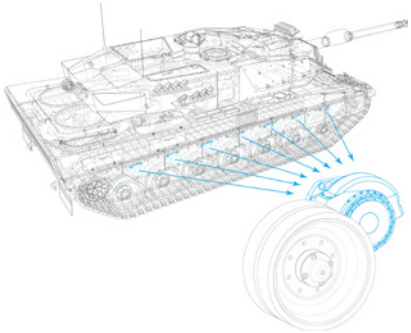


Figura 3. Simulación de integración en plataforma existente. (Fuente: propia).

de la industria europea de defensa al abordar varias prioridades de desarrollo de capacidades, preocupaciones europeas en materia de seguridad del suministro (tanto generales como específicas de varios Estados miembros), prioridades tecnológicas definidas por la Agencia Europea de Defensa (EDA), bloques de construcción tecnológica (TBB) y el desarrollo y estímulo de competencias clave relacionadas con la defensa.

El proyecto SRB ahora prevé su avance hacia SRB2, implementando importantes mejoras tecnológicas (como la miniaturización del sistema de control de altura, la digitalización de la suspensión y el análisis de viabilidad de la sustitución de materiales PFAS contaminantes por materiales que supongan un menor impacto en el medioambiente) y con la ambición de cualificar y validar la solución mediante la integración completa de un vehículo Leopard 2 del Ejército español. El Consorcio prevé avanzar también hacia la industrialización de la solución y los estudios de modularidad para garantizar la adaptabilidad de la tecnología a la mayor cantidad de plataformas posibles.

Este proyecto ha recibido financiación del Programa Europeo de Desarrollo Industrial de la Defensa (EDIDP) en virtud del acuerdo de subvención n.º EDIDP-SME-2020-064-SRB. Este artículo refleja únicamente la opinión del autor, la Comisión Europea no es responsable de la información que contiene.

Cofinanciado por la Unión Europea

En Profundidad

La permanente transformación cultural, además de digital, para gestionar y compartir datos

Autor: Cap. D. Manuel Ángel de Pedro Cibanal (CIETO EA - TEL), Ministerio de Defensa, Secretaría de Estado de Defensa, Dirección General de Asuntos Económicos, Subdirección General de Contratación, Grupo de Estimación de Costes.

Palabras clave: gestión de datos, arquitectura de referencia única para la gestión de la información y del conocimiento del Ministerio de Defensa, AR GIC, transformación digital, *Nato Architecture Framework* versión 4, NAFv4.

Líneas I+D+i ETID relacionadas: Área 11.

Introducción

Podemos afirmar que todas las organizaciones son cada vez más conscientes de la importancia del análisis de sus datos. De hecho, en el actual contexto de incertidumbre y cambio constante, es crucial tanto para el Ministerio de Defensa como para la Alianza Atlántica tomar decisiones basadas en datos para la consecución de sus objetivos de una manera ágil y eficiente, no solo en el entorno operativo, también en sus aspectos de gestión interna. Este artículo trata de plantear una reflexión sobre modos y maneras al respecto.

Sin embargo, dar el salto para que personas y algoritmos de inteligencia artificial (IA) utilicen datos de calidad que asistan en la toma de decisiones, operativas o funcionales, requiere reevaluar el modelo de organización desde sus cimientos para ser, de verdad, Data Centric. Este término significa poner los datos en el centro de todas las actividades, otorgarles el protagonismo que merecen y abordar un cambio cultural en su gestión para poder compartirlos de manera automática con personas y «máquinas».

Para conseguirlo es imprescindible contar con capacidades analíticas que capturen datos de calidad. Estos datos son el resultado de nuevas actividades de gestión desarrolladas en entornos que protegen los activos de información, sin que dicha protección afecte a su transmisión o tratamiento.

La gestión de datos

La gestión de datos (o *data management*) es la solución a las nuevas necesidades y permite poner a disposición conjuntos de datos (*datasets*) precisos, auténticos y fiables en cualquier momento de su ciclo de vida. Además, sus procesos facilitan la flexibilidad necesaria para que los usuarios autorizados, ya sean humanos o algoritmos, puedan acceder a los datos en formato digital de manera segura y ágil, en el momento y lugar adecuados (concepto de superioridad en la información).

Figura 1. La gestión de datos: origen de datos de calidad para su explotación por analistas e inteligencia artificial. (Fuente: *Food-For-Thought Paper on A Data-Centric Reference Architecture for the Alliance. NATO C3B Data Management Capability Team*).

Según la «Estrategia de desarrollo, implementación y uso de la Inteligencia Artificial en el Ministerio de Defensa», hemos entrado en una era en la que los *datasets* para el entrenamiento, junto con los modelos algorítmicos de IA, se deben convertir en activos estratégicos totalmente gestionados para su reutilización y puesta en valor.

Cualquier científico de datos puede corroborar las siguientes expresiones: «No confío en el análisis de datos de baja calidad porque no arroja resultados fiables», o «El 80 % de mi tiempo lo dedico a limpiar datos para poder utilizarlos y solo un 20 % lo destino al entrenamiento y análisis de modelos». Por lo tanto, es más necesario que nunca establecer no solo infraestructuras técnicas seguras para la gestión de *datasets*, sino también procesos de gestión previos al entrenamiento de cualquier modelo algorítmico, con el fin de facilitar el trabajo de los científicos de datos y de los analistas tradicionales.

Para evitar los problemas mencionados anteriormente, existen marcos de referencia de buenas prácticas de gestión de datos aceptados internacionalmente y que debemos aplicar cuanto antes. El Ministerio de Defensa ya ha dado cuando menos un primer paso al elaborar un documento llamado *Arquitectura de Referencia única para la Gestión de la Información y del Conocimiento (AR GIC v1.0)*. Este documento, en formato de Arquitectura OTAN NAFv4, reúne las mejores prácticas en gestión de datos *(Data Management Book of Knowledge - DMBoK)* y en el uso de infraestructuras tecnológicas que faciliten el movimiento de grandes conjuntos de datos

Figura 2. Capacidades GIC del MDEF. (Fuente: Vista C1 del Documento NAFv4 «Arquitectura de Referencia Única para la Gestión de la Información y del Conocimiento»).

Figura 3. Índice NAFv4 "Arquitectura de Referencia Única para la Gestión de la Información y del Conocimiento. (Fuente: Vista A2 del Documento NAFv4 «Arquitectura de Referencia Única para la Gestión de la Información y del Conocimiento»).

para su explotación (NIST *Big Data Interoperability Framework*).

Asimismo, esta primera versión del documento establece una hoja de ruta para alcanzar las once capacidades necesarias (con sus principios, procesos, productos de información y requisitos del *software* que apoyarán a dichos procesos) para lograr la adecuada gestión de los datos, la información y el conocimiento del Ministerio de Defensa.

Estas once áreas guían la gestión de datos remarcan la importancia de actividades como el mantenimiento de datos maestros y de referencia, la medición de indicadores de calidad de los datos, el uso correcto de datos estructurados o no estructurados, la aplicación de reglas de integración de datos, el uso de platillas estandarizadas para la generación de documentos y/o analíticas (información), el uso de etiquetas de seguridad para la distribución segura y cifrada, la aplicación de protocolos de manipulación según qué tipo de dato, el meta datado semántico (no solo estructural) con esquemas de metadatos documentales y de diferentes comunidades de interés, el mantenimiento del linaje de datos que se van generando, la aplicación de procedimientos de acceso o la gobernanza de las taxonomías, términos y ontologías de las familias funcionales establecidas por la Estrategia de la Información del MDEF.

Características del documento y aspectos a mejorar AR GIC:

Las Arquitecturas NAFv4 (como la AR GIC), tienen un índice en formato de tabla para facilitar su lectura. Dentro de cada área se usa un meta modelo que relacionan todas las entidades, garantizando la representación de conocimiento de la materia desde diferentes puntos de vista en un lenguaje común. No es el único documento de este tipo, ejemplos de esta nueva manera de redactar son las arquitecturas promocionadas por la Política CIS/TIC del MDEF, las Arquitecturas Operativas redactadas con la metodología NATO *Mission Thread* y la documentación de las Redes de Misión FMN (*Federated Mission Networking*) de la OTAN.

Este formato, en apariencia de fácil compresión, no lo es para muchos roles clave del Ministerio. Los motivos: la inercia de documentar de manera tradicional, la reticencia a la aplicación de nuevos estándares y la reciente novedad del uso del Marco de Arquitecturas OTAN (NAFv4) para redactar documentos interoperables dentro de la Alianza.

También se observa, en esta primera versión de la AR GIC, que el documento no se vincula del todo con las buenas prácticas de Gestión de la Información de la OTAN y sus normas homólogas de Gestión de Documentos Electrónicos de la AGE y del MDEF, junto con sus respectivos esquemas de metadatos publicados (ver bibliografía).

Este documento (no solo en su contenido, sino en su formato), comienza a hablar de conceptos con los que muchos actores internos del Departamento están todavía en fase alineación. Ya no se dejará a la interpretación lo que hay que hacer, y se deberá completar cada área del índice interrelacionándola con la normativa ya elaborada para generar una única fuente de verdad (del anglicismo *Single Source of Truth -SSOT-*). Para lograrlo, a partir de ahora existirán más roles que los tradicionales elaboradores, propietarios delegados y custodios (normalmente de documentos). Los nuevos roles como son el Oficial Jefe de la Información (CIO), el Oficial Jefe del Dato (CDO), las Autoridades Coordinadoras de Datos por Familia Funcional, los Arquitectos de Datos, los Custodios de Datos, los Curadores de Datos, etc. tendrán nuevas tareas y los antiguos roles tendrán que adaptar ciertos procesos de trabajo. Sus nuevas actividades diferirán significativamente de las tareas que venían llevando a cabo hasta ahora en relación con la gestión de datos (y de documentos electrónicos) y sus jefes orgánicos deberán de ser conscientes de que estos procesos serán la prioridad absoluta en muchos casos.

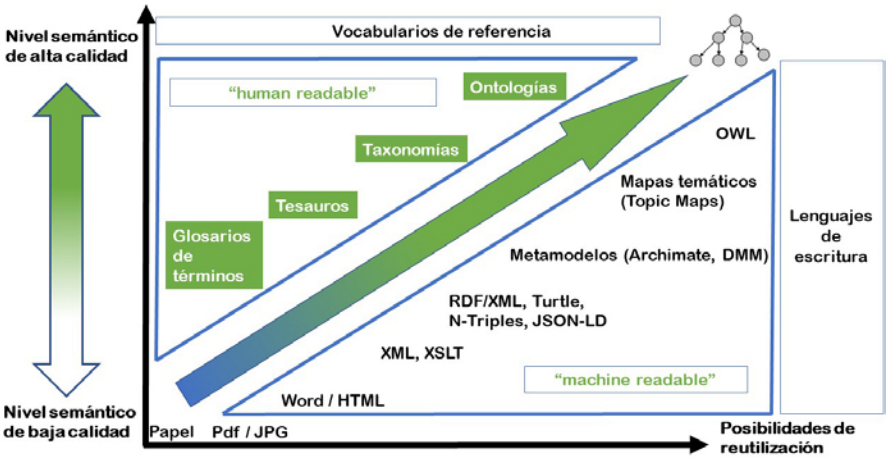


Figura 4. Evolución de la madurez semántica de los datos, la información y el conocimiento. (Fuente: propia).

Hay que añadir que la AR GIC es un documento estructurado, con vocabularios de referencia para ser leído por personas, pero la base de algo a lo que aún no estamos acostumbrados: *un documento machine readable,* formado por *Building Blocks (BB),* análogos a los de las Taxonomías OTAN C3 y cuyos conceptos parten del estándar TOGAF de Arquitectura Empresarial (modelo que representa el negocio para determinar y gestionar la tecnología que lo apoya en una organización). Estos BB representan taxonomías de términos entrelazados (*Linked Data*) y meta datados semánticamente (*Web* Semántica), y su objetivo es la creación de un mismo lenguaje para que todas las partes interesadas puedan entenderse (única fuente de verdad para una comunicación que evite interpretaciones erróneas).

Quizá esta primera versión de la AR GIC debería haber sido escrita mejor en un lenguaje estandarizado de modelos empresariales como ArchiMate® (uno de los lenguajes de escritura que sugiere la documentación OTAN NAFv4), con las relaciones definidas entre sus entidades para facilitar su reutilización por otras personas y por herramientas de gestión de datos y algoritmos de IA. Este nuevo «documento electrónico», junto con otros, se integrará en el Modelo Semántico Digital del Ministerio de Defensa, formado por diferentes ontologías, según una de las actuaciones del Plan de Acción para la Transformación Digital del MDEF. Entender los anteriores puntos tiene sus dificultades sin la adecuada «evangelización» y pudiera ser fuente de incomprensión e indiferencia hacia la AR GIC. Sin ser perfecto, este documento está adelantado a su tiempo y requerirá un periodo de aprendizaje para que las personas de la organización avancen de forma lo más fluida posible en su aplicación.

De manera adicional, los estándares anteriormente nombrados requieren ser usados por todo el Departamento (como ya ha empezado a hacer la OTAN), para un mejor entendimiento y facilitar la interoperabilidad. Pero como toda novedad, el esfuerzo adicional para aprender nuevas formas de trabajar/documentar hace necesaria una adecuada gestión del cambio para el fomento de su aplicación y la comunicación de las ventajas que surgen de esta nueva manera de hacer las cosas.

Por lo tanto, y por lo anteriormente expuesto, será lógico que el Grupo de Trabajo colaborativo de Gestión de la Información y del Conocimiento (GIC) y de Transformación Digital inter-ámbitos, cuyas bases han sido establecidas por la Instrucción de Coordinación para la GIC y el Plan de Acción para la Transformación Digital, mejore en futuras versiones los aspectos antes mencionados para generar datos en forma de *Building Blocks* accesibles y compartidos.

La AR GIC v1.0 tiene la ventaja de ser una «combinación de conocimientos». Ahora tendrá que seguir evolucionando para facilitar su comprensión en futuras versiones y madurar semánticamente.

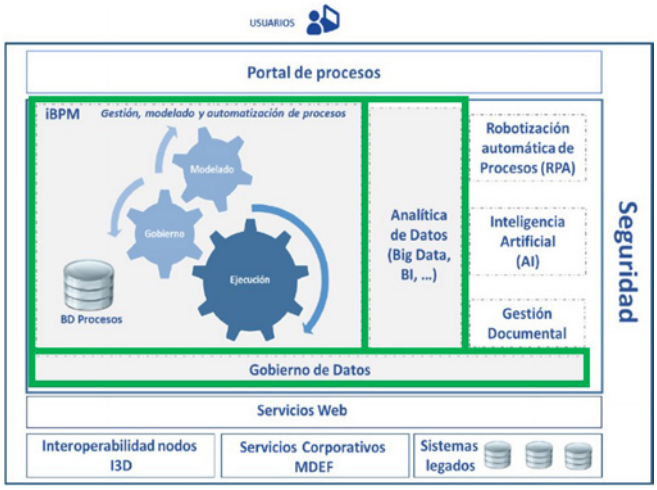


Figura 5. Primeros lotes licitados de la plataforma ARGO en verde. (Fuente: Grupo de trabajo inter-ámbitos del MDEF de Trasformación Digital y GIC).

De manera adicional, y de ahí otro de los puntos importantes del documento, gracias a la hoja de ruta definida en la AR GIC v1.0, se están juntando las primeras piezas que ayudarán a gobernar los datos en la Plataforma de Armonización para la Gestión de la Organización (ARGO), donde el Departamento ha puesto grandes esperanzas de uso. Estas piezas son herramientas que forman parte del ya adquirido IBM *Cloud Pack 4 Data*, y que habilitarán a las aplicaciones (nuevas y legadas) del MDEF, a las nuevas herramientas analíticas de IA y a las personas un acceso seguro a los datos, siempre garantizando la accesibilidad a la información, de una manera gobernada e interoperable.

Necesario un trabajo previo

Las empresas han analizado la necesidad del Departamento para su «modernización digital» y se están presentando a los diferentes lotes de ARGO. Gracias a ello, se están adquiriendo las herramientas más avanzadas en apoyo a los procesos de gestión de datos. De hecho, para ellas resulta muy sencillo vender las ventajas tecnológicas, el software avanzado y los beneficios de los tratamientos automatizados de datos que no requieren autorizaciones continuas (característica típica de organizaciones muy jerarquizadas).

Sin embargo, el Ministerio de Defensa no es ni una empresa, ni civil, ni al uso, y sus datos aún no están preparados para ser compartidos con otras personas o con agentes inteligentes de IA, sobre todo debido a la gran compartimentación orgánica que existe. Además, en estas primeras fases, y principalmente por este motivo, el uso de las nuevas herramientas tendrá un valor limitado, aunque ayudarán a iniciar, operar y completar un cambio de paradigma.

Bajo la ilusión de soluciones «todo en uno», las nuevas herramientas no accederán a ninguna base de datos si los creadores no quieren o no habilitan mecanismos, para que todo potencial consumidor acceda a «sus aplicaciones legadas o silos de información».

En otras palabras, por parte de la institución y de sus miembros sería clave gestionar los datos de una manera más adecuada y perfeccionada desde el inicio (aplicando las once áreas clave citadas de la AR GIC) con el fin de aprovecharlos y compartirlos de manera más eficiente. Pero de todo se aprende y se abre un nuevo mundo de oportunidades en el que es importante destacar que hay que tener en cuenta las necesidades de múltiples comunidades de interés generadoras de datos. De ahí la importancia del cambio cultural y de establecer mecanismos de gobernanza, para compartir y adoptar un nuevo modelo de organización, que aproveche al máximo todos sus datos y las nuevas herramientas que vayan llegando.

Beneficios

Sin entrar en la necesidad inevitable de alcanzar la Superioridad en la Información, para conseguir la Superioridad en el Enfrentamiento de las FAS (en el entorno multi dominio y en el *Combat-Cloud* a través de la interconexión de los datos de todo tipo originados por sistemas de armas), está demostrado que los nuevos tratamientos analíticos disponibles desde cualquier parte de la organización pueden agregar aún más valor. La fusión y análisis de diferentes fuentes de datos heterogéneas, que antes estaban separadas tanto tecnológica como organizativamente, van a servir para mejorar aspectos de funcionamiento de todo el Departamento.

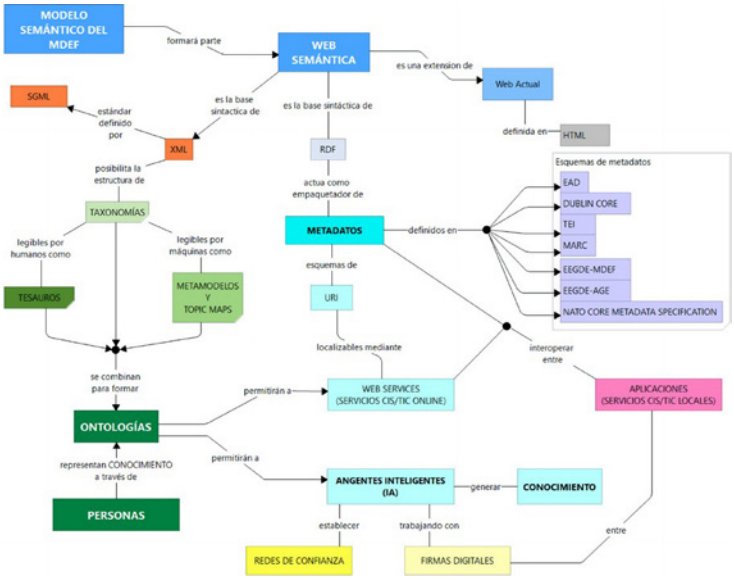


Figura 6. Esquema de la Web Semántica (Web 3.0). (Fuente: propia GIC).

La visión de sistemas aislados y usuarios exclusivos, pertenece al pasado. En la actualidad, todos los sistemas deben coexistir y compartir, aprovechando las nuevas oportunidades que ofrecen los flujos de datos a través Servicios CIS/TIC (como los llaman las FAS siguiendo las taxonomías de *Building Blocks*/Términos C3 de la OTAN).

Por ello, hay que incidir en que los procesos de integración e interoperabilidad de los nuevos repositorios compartidos se conseguirán a través de metadatos semánticos, no solo estructurales, como resultado de la aplicación de la gestión de datos. Gracias a estos metadatos se facilitará exponencialmente la Ciencia de Datos, habilitando a los repositorios como fuentes de datos para entrenar algoritmos de calidad, sin sesgos, auditables y con reglas comunes, y la integración de nuevas aplicaciones orientadas al usuario basadas en la web semántica. De esta manera, los Servicios CIS/TIC accederán fácilmente a diferentes tipos de bases de datos (nuevas o legadas), a repositorios de información (documentos electrónicos) y a ficheros *machine readable* llenos de conocimiento (ontologías).

La nueva analítica de la IA solo podrá avanzar si los datos se estructuran como activos permanentes y compartidos, y sería interesante que el Departamento siguiera, el ejemplo de la Alianza para ser *Data Centric a través de* los Objetivos VAULTIS: datos visibles (*Visible*), accesibles (*Accesible*), comprensibles (*Understandable*), vinculados (*Linked*), fiables (*Trustworthy*), interoperables (*Interoperable*) y protegidos (*Secure*). Esto supone un desafío cultural para los siete ámbitos del Departamento (SUBDEF, SEDEF, SEGENPOL, EMAD, ET, AR y EA) y para toda la orgánica que hay detrás. Los datos ya no son «tus datos», son datos del Ministerio de Defensa y son «los datos que se van a compartir» para satisfacer las necesidades que surjan en cualquier ámbito, orgánica o comunidad de interés (*Community of Interest, CoI*) a través de una adecuada gobernanza.

De esto deriva que existirán nuevos usuarios que podrán utilizar datos para obtener nuevas visiones temporales y agregadas de los hechos a lo largo del tiempo con datos sin aparente relación. No solo eso, podrán compartirlos para contrastarlos y sugerir cambios para mejorar y «optimizar» toda la organización. Este es el objetivo último de una organización centrada en el conocimiento y las personas (Knowledge Centric Organization, KCO), dar a sus componentes la oportunidad de aportar y documentar su conocimiento para que no se pierda y para que contribuya a mejorar la organización de la que forma parte, para que se «transforme», para que sea más ágil y eficiente.

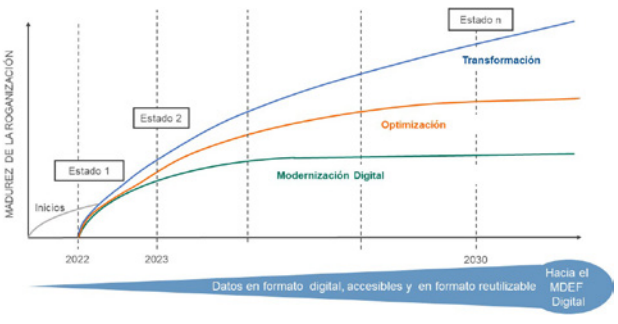


Figura 7. Hoja de ruta de la Transformación Cultural y Digital del MDEF. (Fuente: Presentación II Jornadas de IA del Ejército del Aire 2022, elaboración propia).

Cambio cultural

Todo lo anterior supone un cambio cultural importante, pasando de la necesidad de conocer (el famoso *need to know*), al deber de compartir de una manera segura (el nuevo *duty to share*). Todo ello dejando atrás la antigua práctica de restringir el acceso a los datos, fruto del pensamiento desactualizado de que «la información es poder y no la comparto».

Se considera necesario aplicar las mejores prácticas de gestión de datos, incorporando desde ya esas nuevas actividades que antes pudieran no considerarse necesarias o no eran realizadas de una manera estandarizada. El objetivo que se propone es avanzar más aún en convertir los datos en un activo estratégico y compartirlos para su uso de manera segura a través de la Infraestructura Integral de Información para la Defensa (I3D).

Llevará tiempo, pero forma parte del proceso de transformación permanente del Ministerio de Defensa (o de cualquier entidad en nuestros días) asimilar y aplicar plenamente las nuevas actividades de gestión de datos. Algunos objetivos que este autor ve positivos en la línea del artículo serían, por ejemplo, que el Departamento dispusiera de alguna forma de espacios de datos abiertos para compartir y reutilizar información de gestión entre diferentes ámbitos, universidad e

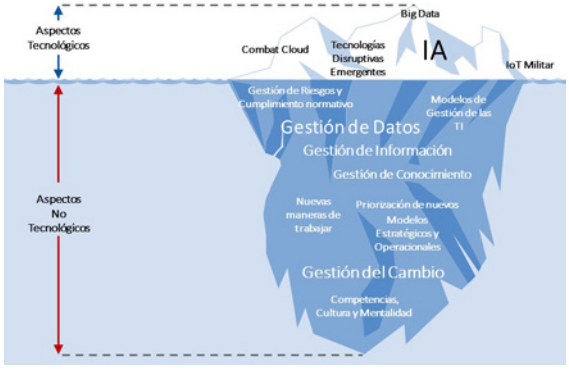


Figura 8: Aspectos tecnológicos y no tecnológicos de la Transformación Cultural y Digital del MDEF. (Fuente: Presentación II Jornadas de IA del Ejército del Aire 2022, elaboración propia).

industria para permitir descubrir cómo mejorar procesos internos, respetando sus peculiaridades, también compartidas a través de los modelos, meta dados y ontologías generadas por cada comunidad de interés; y de manera adicional abrir dentro la institución repositorios de datos operativos, para facilitar la interoperabilidad entre organismos de las FAS y aliados en ejercicios/zonas de operaciones.

Por último, seguir trabajando en la mejora de la agilidad, eficacia y eficiencia y en avanzar en la constante transformación del Ministerio de Defensa en una entidad que progresa basándose en el conocimiento aportado por las personas (ya sean actores internos o externos). Este es el principal recurso del Departamento y se debe aprovechar al máximo a través de las nuevas tecnologías digitales, no solo para lograr la debida adaptación al cambio, sino para estar siempre en vanguardia.

Bibliografía

[1] ArchiMate Standard®. Disponible en: https://pubs.opengroup.org/architecture/archimate3-doc/

[2] Arquitectura de Referencia única para la Gestión de la Información y el Conocimiento en el Ministerio de Defensa (AR GIC). Disponible en: http://calderon.cud.uvigo.es/items/9b6d30af-090b-4d75-aa64-51e77474aa48/full

[3] Data Management Book of Knowledge – DMBoK. Disponible en: https://www.dama.org/cpages/body-of-knowledge

[4] Departament of Defense Data Strategy. Disponible en: https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF

[5] Estudio y propuesta de uso del lenguaje «ArchiMate®» para generación de arquitecturas NAFv4 en el Ministerio de Defensa. Disponible en: http://calderon.cud.uvigo.es/items/ec7a5337-375f-4907-8831-a4ced9dbad3d

[6] Instrucción 58/2016, de 28 de octubre, del secretario de Estado de Defensa, por la que se aprueba la Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio. En: Arquitectura global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa (AG CIS/TIC). Disponible en: https://publicaciones.defensa.gob.es/arquitectura-global-de-sistemas-y-tecnologias-de-informacion-y-comunicaciones-del-ministerio-de-defensa-ag-cis-tic.html

[7] Linked Data. Disponible en: https://datos.gob.es/es/noticia/linked-data-como-modelo-de-datos

[8] NATO Architecture Framework v4. Disponible en: https://www.nato.int/cps/en/natohq/topics_157575.htm

[9] NATO C3 Taxonomy. Disponible en: https://www.nato.int/cps/en/natohq/topics_157573.htm#:~:text=The%20C3%20Taxonomy%20is%20a%20model%20that%20represents,connecting%20NATO%27s%20Strategic%20Concept%20and%20Political%20Guidance%20

[10] NATO Core Metadata Specification. NATO Information Management Authority (NIMA). Disponible en: https://nima.reach.nato.int/SitePages/Home.aspx

[11] NATO Information Management Policy. NATO Information Management Authority (NIMA). Disponible en: https://nima.reach.nato.int/SitePages/Home.aspx

[12] NIST Big Data Interoperability Framework. Disponible en: https://www.nist.gov/

[13] Orden DEF/1196/2017, de 27 de noviembre, por la que se establece la Estrategia de la Información del Ministerio de Defensa. Disponible en: https://boe.es/diario_boe/txt.php?id=BOE-A-2017-14417

[14] Orden DEF/2639/2015, de 3 de diciembre, por la que se establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa. Disponible en: https://publicaciones.defensa.gob.es/politica-de-los-sistemas-y-tecnologias-de-la-informacion-y-las-comunicaciones-del-ministerio-de-defensa.html

[15] PAe. *Metadatos*. Esquema de metadatos para la gestión del documento electrónico. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Archivo_electronico/pae_Metadatos.html

[16] Plan de Acción del Ministerio de Defensa para La Transformación Digital. Disponible en: https://publicaciones.defensa.gob.es/plan-de-accion-del-ministerio-de-defensa-para-la-transformacion-digital-libro-pdf.html

[17] Política de Gestión de Documentos Electrónicos de la AGE. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/Archivo_electronico/pae_Politica-de-gestion-de-documentos-electronicos.html

[18] Política de Gestión de Documentos Electrónicos del MDEF. Disponible en: https://publicaciones.defensa.gob.es/politica-de-gestion-de-documentos-electronicos-del-ministerio-de-defensa.html

[19] Real Decreto 521/2020, de 19 de mayo, por el que se establece la organización básica de las Fuerzas Armadas. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-5190.

[20] Resolución 11197/2023, de 29 de junio, de la Secretaría de Estado de Defensa, por la que se aprueba la Estrategia de desarrollo, implantación y uso de la Inteligencia Artificial en el Ministerio de Defensa. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/2/0/20230706.pdf.

[21] Resolución 420/17058/2018, de 7 de noviembre, de la Secretaría General Técnica, por la que se da publicidad al Esquema de Metadatos para la Gestión del Documento Electrónico en el ámbito del Ministerio de Defensa. Disponible en: https://publicaciones.defensa.gob.es/esquema-de-metadatos-para-la-gestion-del-documento-electronico-ministerio-de-defensa-eemgde-mdef-version-1-0.html

[22] The Open Group Architecture Framework. Disponible en: https://www.opengroup.org/togaf

Boletín de Observación Tecnológica en Defensa

Disponible en

http://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Contenido/Paginas/Publicaciones.aspx?cat=BOLETINES TECNOLÓGICOS

https://publicaciones.defensa.gob.es/

SOPT

SISTEMA DE OBSERVACIÓN Y PROSPECTIVA TECNOLÓGICA

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL

9 772444 483008 78023