DIRECCIÓN GENERAL DE ARMAMENTO Y MATERIAL (DGAM)

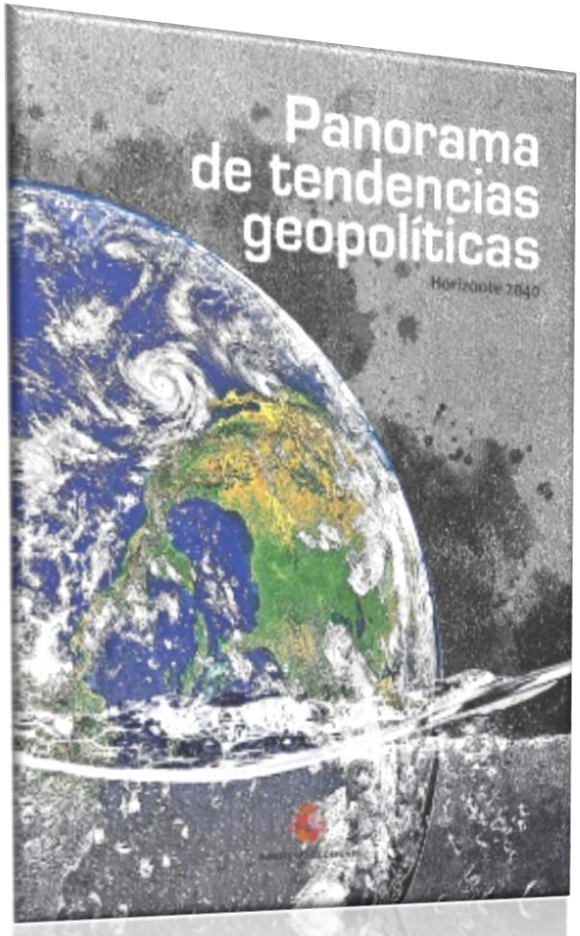
Una evolución de los sistemas de armas con las tendencias actuales en Inteligencia Artificial

Joaquín Catalá Lloret

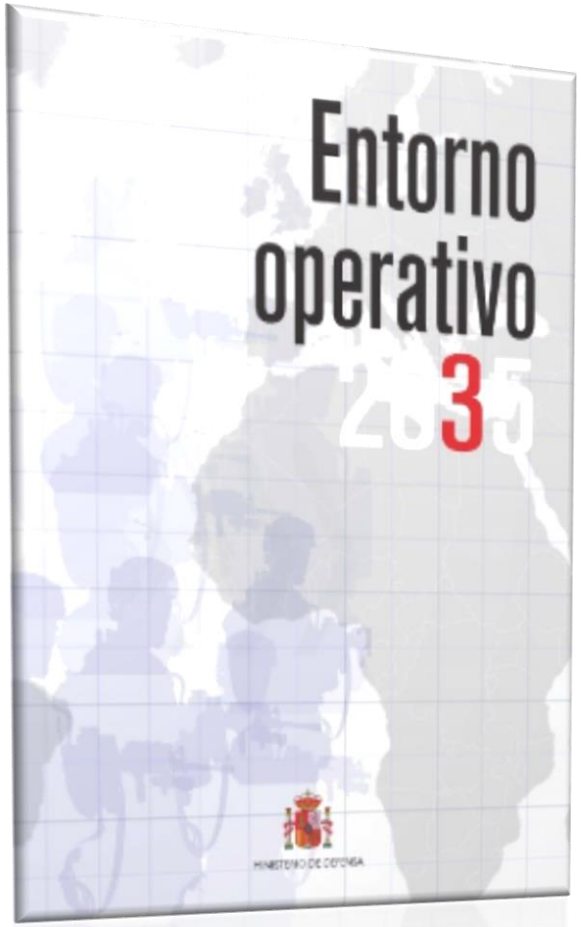
ACAMI, 7 de noviembre de 2019

Contenido

Evolución de los futuros entornos operativos



https://publicaciones.defensa.gob.es/panorama-de-tendencias-geopoliticas-horizonte-2040-libros-papel.html



https://publicaciones.defensa.gob.es/entorno-operativo-2035-libros-papel.html

Cambios en el contexto operativo

- Nuevos dominios de confrontación complementarios a los tradicionales (p.e. ciberespacio, recursos espaciales, percepción a través de medios sociales…).
- Factores potenciadores de riesgos y amenazas (desintegración de sistemas políticos, económicos y sociales; presiones migratorias…)
- Conflictos asimétricos e híbridos, a menudo en entornos urbanos.

Cambios en el contexto tecnológico

- Acelerado ritmo de avance de la tecnología, en particular en ámbitos como la electrónica, los materiales o las TIC.
- Cambios disruptivos que plantean un escenario a futuro muy difícil de prever.
- Pueden traducirse tanto en potenciales ventajas operativas como en nuevas amenazas, dada la creciente facilidad para acceder a la tecnología a nivel global.

Misiones militares actuales y futuras

- Panorama actual y futuro de escenarios y amenazas para la seguridad, caracterizado por su volatilidad, incertidumbre, complejidad o ambigüedad.

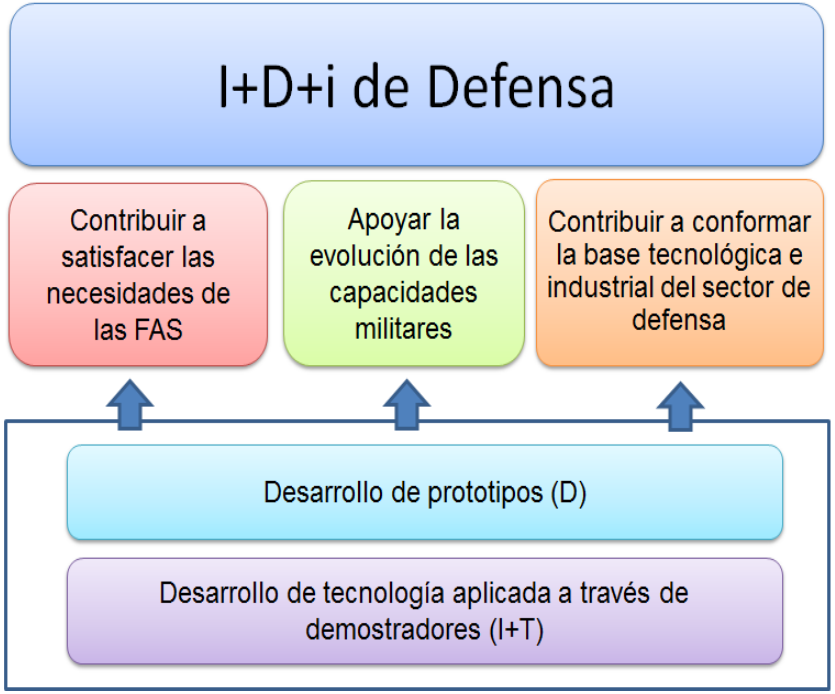
Contexto futuro en el que deberá desarrollarse la IA en defensa

- Como medio para anticiparse a las amenazas se busca disponer de superioridad tecnológica: empleo de sistemas tecnológicamente más avanzados que los de los oponentes.

La IA puede ser una de las principales vías para lograr esa superioridad tecnológica

Política de I+D+i del MINISDEF

- I+D+i como principal vehículo para favorecer la incorporación de tecnologías avanzadas en los sistemas de uso militar que aporten esa superioridad tecnológica.
- I+D+i como medio de mejora de la competitividad y productividad del tejido tecnológico e industrial nacional.

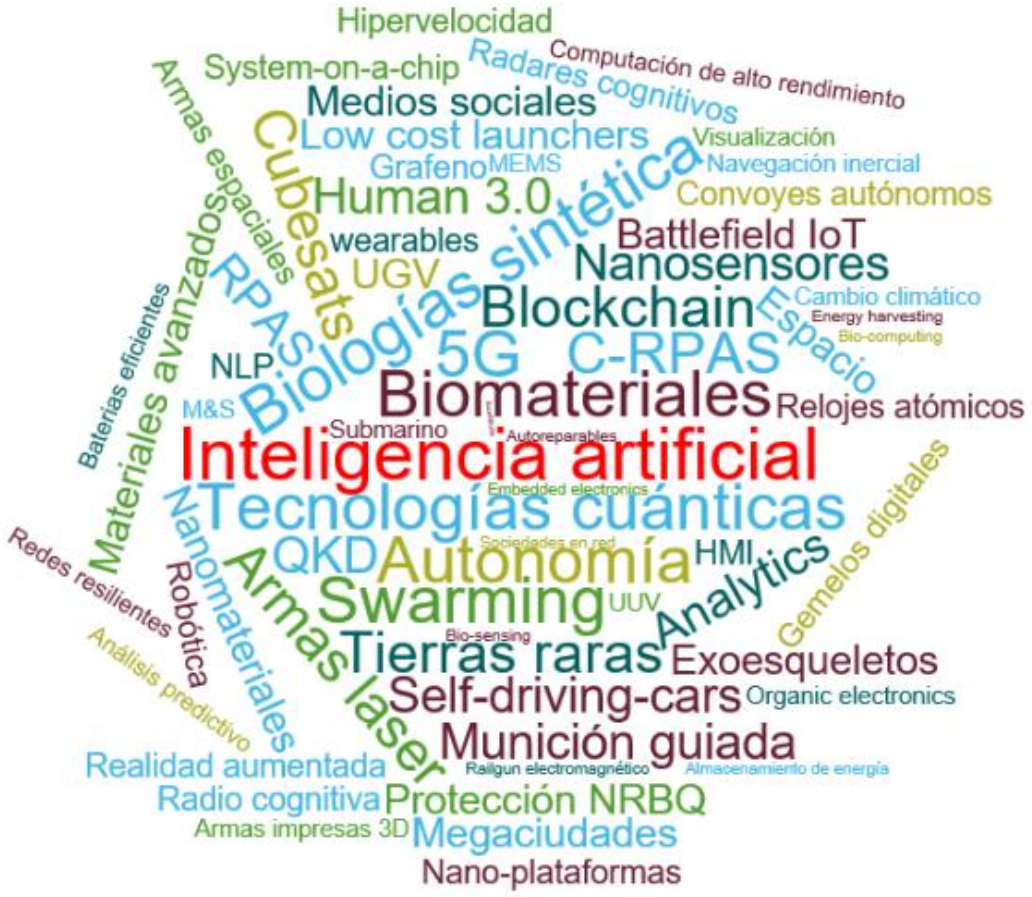


Contenido

- Contexto de aplicación de la IA en defensa
- IA como tecnología disruptivas para defensa
- I+D+i del MINISDEF ante los nuevos retos y oportunidades

¿Va a ser la IA disruptiva?

- Predecir a priori el impacto de una tecnología en defensa es muy complejo.
- Existe cierto consenso respecto al potencial de la IA como habilitador de profundos cambios en la sociedad y en el ámbito militar.



Cambios en los últimos años

- Defensa
  - Alto número de necesidades operativas que requieren soluciones tecnológicas dotadas de mayor inteligencia.
  - Importante proporción de propuestas industriales (p.e. COINCIDENTE) que contemplan elementos basados en IA.
  - Inicio de proyectos que implican IA.

- Ámbito nacional:
  - Muy alta actividad del tejido tecnológico nacional.
  - Grupo de trabajo interministerial sobre IA.
  - Oportunidades a través de los instrumentos del Plan Estatal de Ciencia, Tecnología e Innovación.

- Ámbito internacional:
  - IA aplicada a defensa presente en estrategias tecnológicas, grupos de estudio operativos e industriales, programas de cooperación, llamadas internacionales vinculadas a EDAP, concursos de ideas…

IA aplicada a defensa

- El MINISDEF está apostando por la aplicación de la IA a problemas de Defensa. En particular, en los últimos avances en aprendizaje automático (*machine learning*).

- SOPRENE (2018-2020) - Utilización de redes neuronales como método para mantenimiento basado en la condición en los buques de la Armada

- COINCIDENTE 2018: proyectos en proceso de contratación relacionados con el empleo de técnicas de inteligencia artificial para el mantenimiento de vehículos terrestres, para el apoyo a la vigilancia marítima, para el desarrollo de operaciones terrestres o para ciberdefensa.

Principales aplicaciones en defensa (I)

- Explotación automática de datos de sensores para vigilancia y reconocimiento persistente, empleando redes de sensores desplegados o embarcados en plataformas.
- Explotación inteligente del espectro electromagnético, para aplicaciones tales como radar, guerra electrónica y comunicaciones.
- Adquisición y explotación inteligente de grandes volúmenes de información de fuentes propias y abiertas para aplicaciones militares y lucha contra amenazas contra la seguridad.
- Monitorización y análisis predictivo en ciberdefensa.

Imagen: NGA official: Artificial intelligence is changing everything, 'We need a different mentality' (https://spacenews.com/nga-official-artificial-intelligence-is-changing-everything-we-need-a-different-mentality/).

Principales aplicaciones en defensa (II)

- Autonomía en plataformas terrestres, navales y aéreas no tripuladas, incluyendo aspectos de guiado y control, percepción del entorno, navegación en entornos no estructurados y en ausencia de señal GNSS y funcionamiento cooperativo.
- Inteligencia en los sistemas de control de las plataformas militares (p.e. vetrónica, aviónica, gestión energética…) y sus sistemas de misión.
- Mantenimiento predictivo de plataformas militares.
- Logística militar.
- Gestión energética inteligente en bases y campamentos.
- Base logística 4.0.

Imagen: Artificial Intelligence and the Military (https://www.rand.org/blog/2017/09/artificial-intelligence-and-the-military.html).

Principales aplicaciones en defensa (III)

- Monitorización del riesgo NRBQ
- Salud en el campo de batalla
- Interfaces hombre máquina avanzados.
- Man-machine teaming.
- Simuladores para adiestramiento y apoyo a la toma de decisión.
- Etc.

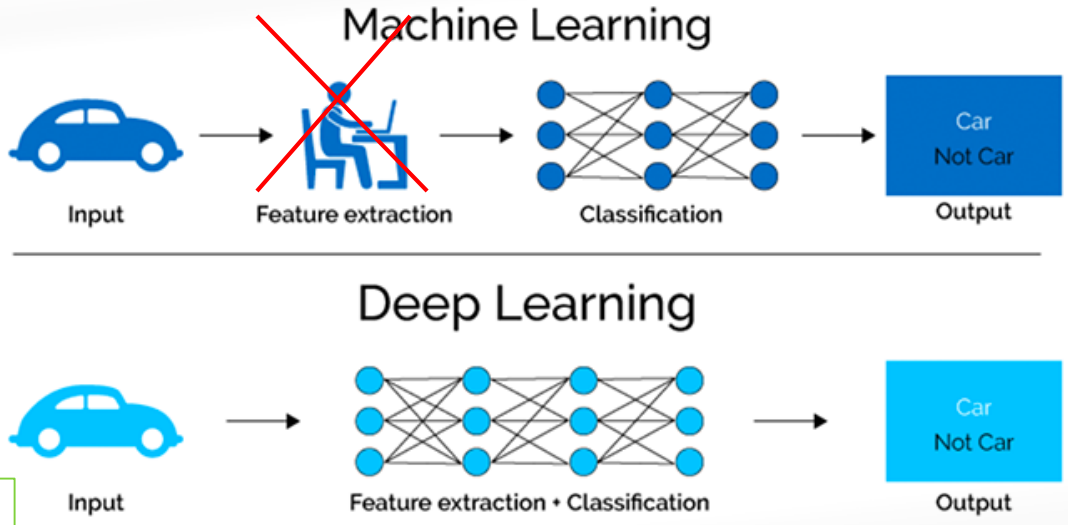
Imagen: Booz Allen: Artificial intelligence is transforming immersive training (https://www.defensenews.com/digital-show-dailies/itsec/2017/12/05/booz-allen-artificial-intelligence-transforming-immersive-training/).

Aprendizaje profundo (*Deep learning*, DL)

- Creciente capacidad para desplegar cientos o miles de sensores interoperables ⇔ Cuello de botella a la hora de explotar esos datos.
- DL tiene el potencial para entrenar algoritmos inteligentes a partir de enormes volúmenes de datos a los que las personas han añadido inteligencia a través de etiquetas ⇨ Explotación inteligente.
- ¡¡¡DISRUPCIÓN!!! ⇨ Muchos problemas hasta ahora inviables utilizando sistemas automáticos pueden llegar a ser abordables.

DoD uses Google's machine learning tools to analyze drone surveillance footage

Google is providing TensorFlow APIs to the Pentagon for Project Maven, which aims to leverage AI to increase drone effectiveness.



Fuente: Insights of The Machine Learning and The Deep Learning

Avances en IA en nuestro radar (II)

Redes antagónicas generativas (GAN)

- Se sigue con preocupación los rápidos cambios de la evolución de este tipo de algoritmos, capaces de crear contenidos (imágenes, audio, video, texto…) falsos con muy alto grado de realismo.
- Potenciales usos disruptivos en defensa y seguridad.
- Interés en los esfuerzos actuales dirigidos a desarrollar tecnología que permita detectar contenidos falsos.

Source: NVIDIA

Fuentes y referencias:

- How to Generate Fake Videos with Generative Adversarial Networks (DeepFake)
- The Defense Department has produced the first tools for catching deepfakes
- The US military is funding an effort to catch deepfakes and other AI trickery

Avances en IA en nuestro radar (III)

Aprendizaje por refuerzo profundo (*Deep reinforcement learning*)

- El futuro en defensa demandará un alto número de sistemas remotamente tripulados, capaces de adaptarse al entorno y a los cambios.
- Se tiene interés en los prometedores avances de las tecnologías de aprendizaje por refuerzo, en particular por su potencial para dotar de autonomía a las plataformas no tripuladas.

(a) Atlas: Walk

(b) Atlas: Run

(c) Atlas: Backflip

(d) Atlas: Spinkick

Imagen: DeepMimic: Example-Guided Deep Reinforcement Learning of Physics-Based Character Skills. Peng et al. University of California, Berkeley (https://xbpeng.github.io/projects/DeepMimic/2018_TOG_DeepMimic.pdf)

Limitaciones y riesgos (I)

- Se requieren enormes cantidades de datos etiquetados ⇨ En muchos casos no están disponibles.
- Muchas de estas tecnologías son cajas negras, cuyas salidas no pueden ser explicadas, despertando dudas sobre su fiabilidad y derivas ⇨ Importancia de investigaciones como la de DARPA: Explainable Artificial Intelligence (XAI)

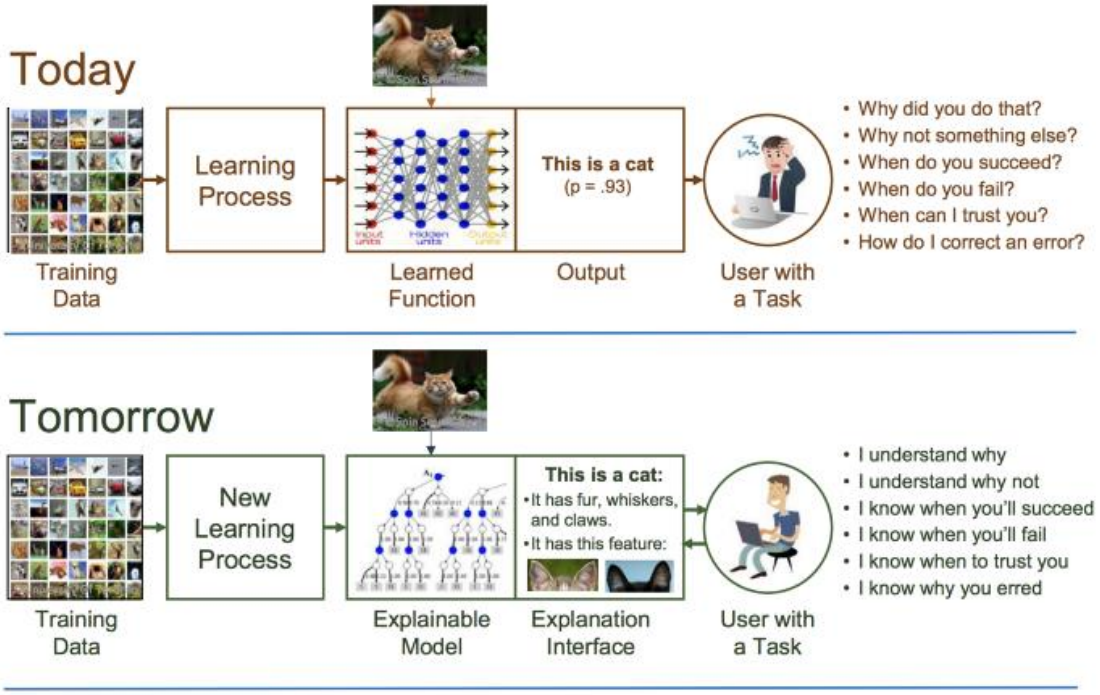


Imagen: Explainable Machine Learning — 5 Must Read Papers (https://medium.com/@raeidsaqur/explainable-machine-learning-5-must-read-papers-95660d9f0c72).

Limitaciones y riesgos (II)

- Comportamiento imprevisible de los sistemas si se intentan utilizar ante nuevos problemas para los que no han sido entrenados.
- Los sistemas basados en IA (implican software) pueden ser hackeados o su entrenamiento puede ser corrompido con ruido en los datos.
- Futuro: complejidad al desplegar un largo número de sensores y sistemas de armas que incorporen componentes de IA en diferentes subsistemas (posibles errores en cascada).

Imagen: Teaching AI Systems to Adapt to Dynamic Environments (https://www.darpa.mil/news-events/2019-02-14).

Contenido

- Contexto de aplicación de la IA en defensa
- IA como tecnología disruptivas para defensa
- I+D+i del MINISDEF ante los nuevos retos y oportunidades

Incorporación de tecnologías de IA a defensa (I)

Existen importantes retos que condicionan el aprovechamiento por defensa de las ventajas de la IA. Se apuntan algunos:

- Disponibilidad de datos etiquetados.
- Instrumentos adaptados a las particularidades de defensa y de la IA.
- Gestión del cambio y los avances.
- Capacidad de financiación de la I+D+i de aplicación a defensa.

Disponibilidad de datos etiquetados

- Muchas de las técnicas de IA requieren enormes cantidades de datos etiquetados con descriptores inteligentes que reflejen el conocimiento humano ⇨ Importante tarea de recopilación, revisión y etiquetado de datos para disponer de *datasets* que permitan aprovechar en el futuro las ventajas de esta tecnología.
- Múltiples dominios en defensa que requieren ser estudiados y trabajados para habilitar la introducción de estas tecnologías.
- Implicación de usuarios finales (conocen el problema) y expertos en IA (conocen la tecnología).

Instrumentos adaptados a las particularidades de la IA

- El empleo de unas técnicas de IA frente a otras es muy dependiente del problema específico que se debe resolver y de los datos disponibles.
- Amplio conjunto de entidades nacionales con capacidades en este ámbito ⇨ dificultad en saber quien va a poder proporcionar la mejor solución.
- En el ámbito civil se utilizan concursos competitivos abiertos para generar las mejores soluciones ⇨ problema de la sensibilidad de los datos en defensa.
- Necesidad de adaptar los instrumentos existentes o de crear nuevos instrumentos adecuados a estas particularidades.

Gestión del cambio y los avances

- Aplicar técnicas de IA resulta complejo y a menudo las soluciones basadas en IA no son mejores que las obtenidas por técnicas clásicas ⇨ Necesidad de aceptar el riesgo de fracasar en los proyectos.

- Las soluciones basadas en IA generalizan mal y a menudo son poco flexibles: deben evolucionar con las circunstancias y cambios del contexto.
- Mayor complejidad en la gestión del ciclo de vida de sistemas con elementos basados en IA.

Financiación de la I+D+i de defensa

- Progresiva reducción en la última década de la financiación pública dirigida a I+D+i de aplicación a defensa.
- Efectos muy negativos tanto para el desarrollo de capacidades militares como para la competitividad y supervivencia de la base tecnológica e industrial de defensa.
- Barrera real para lograr mayores avances en todos los ámbitos tecnológicos, y en particular en la introducción de tecnologías de IA en defensa.
- Necesario aumentar la financiación pública dirigida a I+D+i de aplicación a defensa.

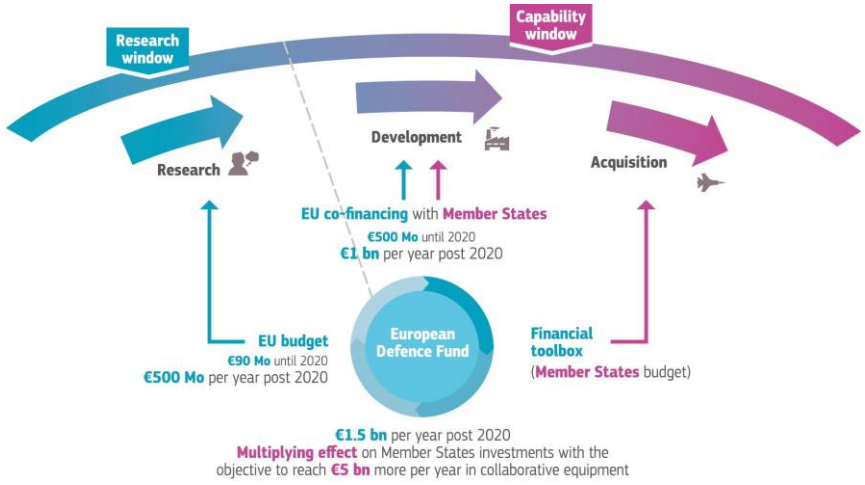
Incorporación de tecnologías de IA a defensa (II)

Pero existen oportunidades que favorecen ese aprovechamiento por defensa de las ventajas de la IA:

- Oportunidades europeas para el desarrollo de la industria de defensa.
- Cooperación nacional en I+D+i.
- Nuevos enfoques estratégicos de la I+D+i de defensa y nacional.

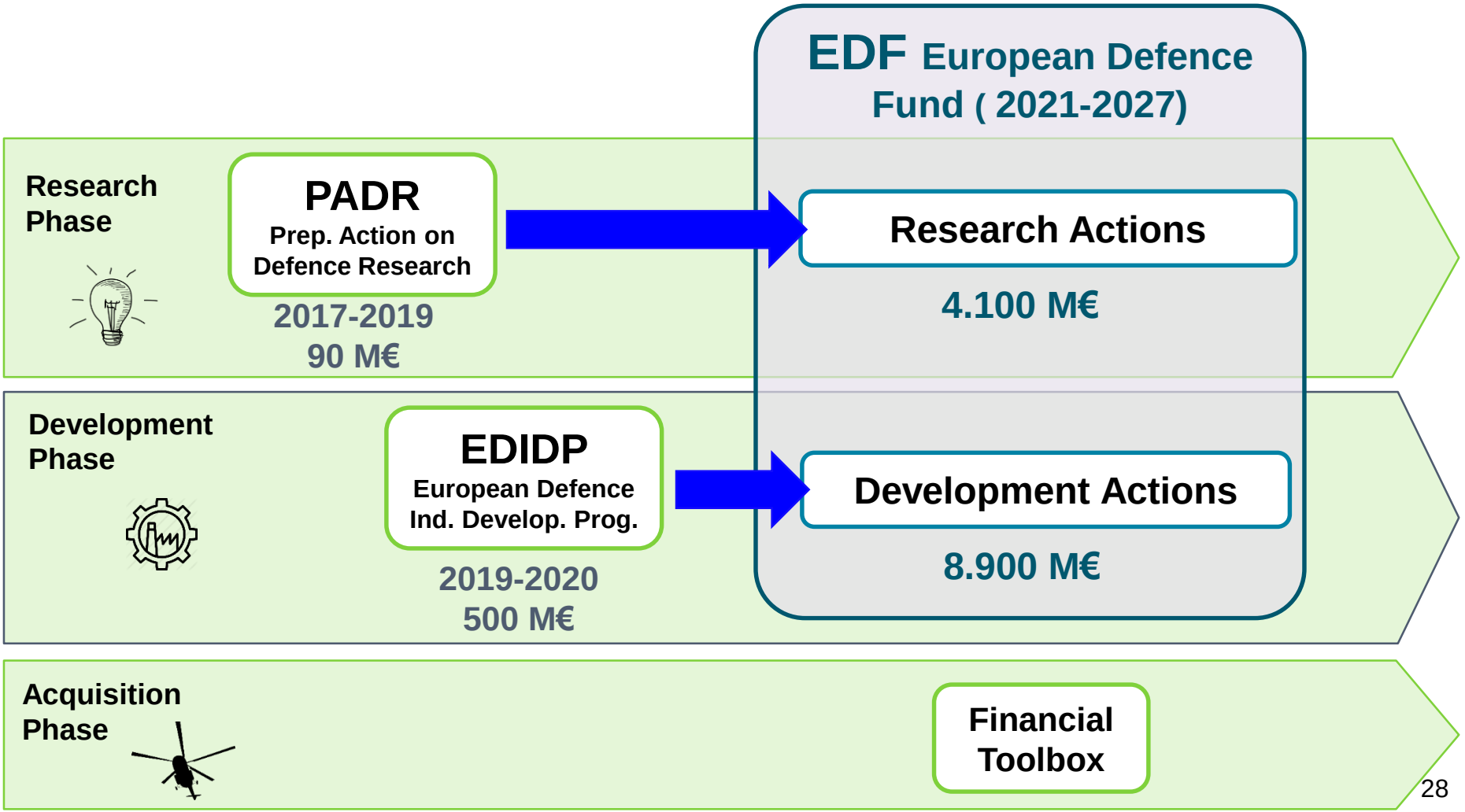
Financiación europea de la I+D+i

- El Fondo Europeo de Defensa proporciona nuevos instrumentos de financiación para desarrollar I+D+i de defensa en cooperación internacional.
- Principal reto: ser capaces de lograr la máxima participación del tejido tecnológico e industrial nacional en proyectos de I+T y la cofinanciación europea de proyectos prioritarios para las FAS.



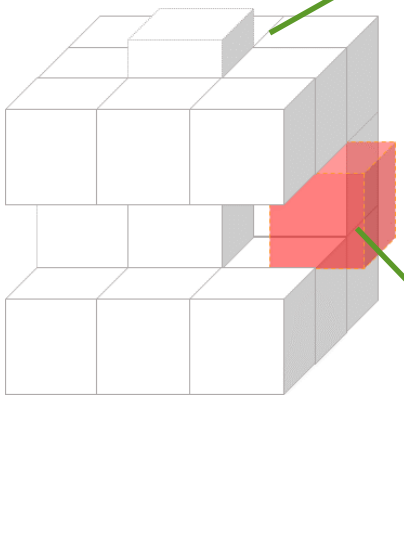
Fondo Europeo de Defensa

- La IA aplicada a defensa ya está tomando un papel destacado en las llamadas tanto de PADR como de EDIDP.



Cooperación nacional en I+D+I

Estrategia Española de Ciencia y Tecnología y de Innovación (2013 – 2020)



I+D+i nacional

Plan Estatal de Investigación Científica y Técnica y de Innovación (2017-2020)

Reto de Seguridad, Protección y Defensa

I+D+i sectorial de defensa

Estrategia de Tecnología e Innovación para la Defensa (ETID - 2015)

- La ETID se alinea con los principios incluidos en la Estrategia Española de Ciencia y Tecnología y de Innovación (2013 – 2020)
- Existe comunalidad entre el MINISDEF y otros organismos nacionales financiadores de la I+D+i en cuanto a políticas de apoyo a la capacitación del tejido tecnológico nacional.

Cooperación nacional en I+D+I

- Recientemente se ha firmado un Protocolo General de Actuación entre el MINISDEF, MICIU, CDTI y AEI para coordinar esfuerzos en I+D+i.
- Marco apropiado para abordar una parte importante de los retos y barreras existentes para lograr un mayor uso de las tecnologías de IA en problemas de defensa y seguridad.

Estrategia de Tecnología e Innovación para la Defensa (ETID)

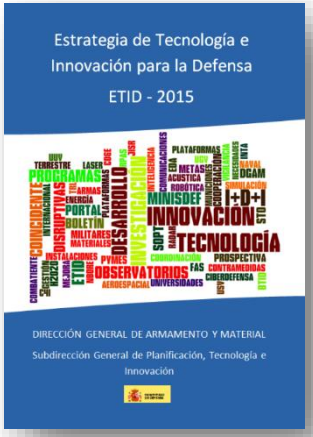
- Se está trabajando en la revisión de la ETID para adaptarla a los nuevos retos y oportunidades, en particular los vinculados al uso de la IA en defensa.
- Coordinación con la elaboración de la siguiente Estrategia Española de Ciencia y Tecnología y de Innovación.

POLITICA I+D+i DEL MINISDEF

Orientación Tecnológica

Coordinación de Actores

Tecnologías dirigidas a cubrir las necesidades actuales y futuras de las FAS



http://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Contenido/Paginas/detallepublicacion.aspx?publicacionID=205

Conclusiones

- El empleo de soluciones basadas en IA es esencial para incrementar la superioridad tecnológica y libertad de acción de las FAS frente a las nuevas amenazas y retos del mundo actual.
- Existen importantes retos asociados al uso de IA en defensa.
- Énfasis en aprovechar las oportunidades de cooperación internacional y nacional.
- Se está trabajando en una nueva versión de la ETID, adaptada a estos nuevos retos.

MUCHAS GRACIAS POR SU ATENCIÓN

¿PREGUNTAS?