Defensa inteligente en un mundo inteligente

Félix Pérez Martínez

Academia de las Ciencias y las Artes Militares

Sección de Prospectiva de la Tecnología Militar

26 de octubre de 2020

> "El cambio fundamental que traerá la cuarta revolución industrial será que entes autónomos inteligentes irán desplazando a operadores humanos en un espacio de combate cada vez más digitalizado y robotizado**".** Almirante José Manuel Sanjurjo Jul, "La Armada en la Cuarta Revolución Industrial: Algunas Reflexiones", conferencia impartida con motivo del 250 ANIVERSARIO DEL CUERPO DE INGENIEROS DE LA ARMADA.

Un mundo inteligente

En efecto, no se puede dudar que, en la última década, la aplicación de tecnologías y los sistemas inteligentes en prácticamente todos los sectores de actividad está transformando nuestra sociedad en un "mundo" que empieza a ser "inteligente". Son las "ciudades inteligentes", la "salud inteligente", las "energías inteligentes", "los transportes inteligentes", etc.

El fenómeno es consecuencia directa del espectacular crecimiento de la capacidad de computación producida por el incremento de las capacidades de proceso y almacenamiento de información de las nuevas arquitecturas de los sistemas de información y comunicaciones. En los próximos años se acelerará este proceso, permitiendo el tratamiento masivo y eficaz de ingentes cantidades de datos, gracias a la microelectrónica basada en nuevos componentes, como el grafeno, y en nuevas estructuras tridimensionales, así como a las nuevas arquitecturas de computación en el borde y en la niebla (*edge and fog computing*).

Por otro lado, lo que en pocos años convertirá en disruptivas a estas tecnologías inteligentes es que ya se pueden aplicar un conjunto de técnicas de Inteligencia Artificial (IA) gracias al incremento, también exponencial, de la conectividad y la sensorización. Las actuales redes de comunicación tienen coberturas, densidades, velocidades de transmisión y latencias que, junto con el perfeccionamiento y abaratamiento de todo tipo de sensores, permiten la adquisición y tratamiento de

un número ingente de datos –la internet de las cosas (IOT)- y habilitan el entrenamiento de algoritmos de procesamiento muy sofisticados que apenas requieren el modelado y parametrización previos del fenómeno a analizar. Es lo que se conoce como aprendizaje profundo (*deep learning*). Conviene aclarar que la disponibilidad de datos optimiza todas las técnicas de aprendizaje automático (*maching learning*), la diferencia radica en la cantidad mínima de datos necesaria en las diferentes técnicas lo que, hasta ahora, impedía el uso eficaz del aprendizaje profundo.

¿Cómo será este mundo digital inteligente? En el prestigioso informe anual de Gartner, de 2017, sobre tecnologías emergentes

[https://www.gartner.com/en/newsroom/press-releases/2017-08-15-gartner-identifies-three-megatrends-that-will-drive-digital-business-into-the-next-decade]
ya presentaba como una de las tres "megatendencias" que definirían la economía digital en la siguiente década lo que etiquetaba como "INTELIGENCIA ARTIFICIAL EN TODAS LAS PARTES. Sólo tres años después, en el informe de 2020, la

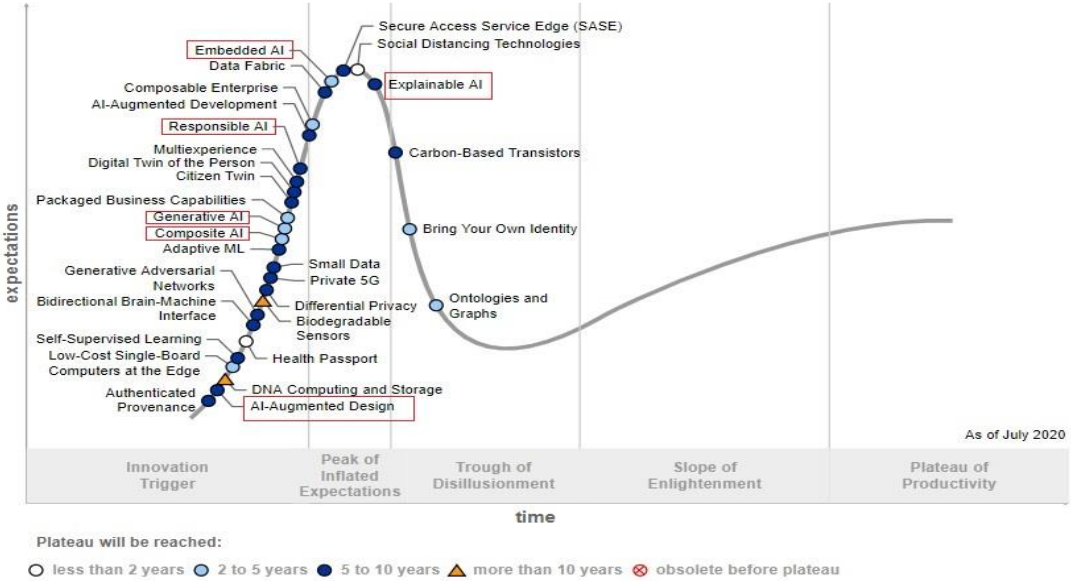

Figura 1 "Hipe-Cycle" deTecnologías emergentes de Gartner en 2020. Fuente: https://www.gartner.com/smarterwithgartner/5-trends-drive-the-gartner-hype-cycle-for-emerging-technologies-2020/

inteligencia artificial se convierte en protagonista indiscutible de las tecnologías emergentes (ver figura)

Por otro lado, el informe permite dibujar los rasgos del futuro mundo digital en las cinco “megatendencias” que destaca [https://www.gartner.com/smarterwithgartner/5-trends-drive-the-gartner-hype-cycle-for-emerging-technologies-2020/]:

- El YO DIGITAL, tecnologías que permiten a las personas interactuar con el mundo digital usando una combinación de modalidades de interacción (voz, visión, gestos, etc.) e incluso alterando directamente nuestro cerebro.

- Las ARQUITECTURAS COMPUESTAS que utilizan datos flexibles donde la inteligencia está descentralizada para asegurar unas organizaciones muy agiles capaces de adaptarse a unas necesidades cambiantes.

- La INTELIGENCIA ARTIFICIAL FORMATIVA que cambiará dinámicamente para responder a variaciones situacionales, en algunos casos generando nuevos modelos dirigidos a resolver problemas específicos.

- CONFIANZA ALGORITMICA. La confianza basada en autoridades responsables está siendo sustituida por modelos de confianza algorítmica para garantizar la privacidad y seguridad de los datos, la fuente de los activos y la identidad de las personas y las cosas.

- MÁS ALLÁ DEL SILICIO. Se reconoce la persistencia de la ley de Moore mediante el desarrollo de otras tecnologías emergentes como ya se ha puesto de manifiesto unos párrafos más arriba y que completa con tecnologías de más largo plazo como son la computación y el almacenamiento cuántico o basado en el ADN.

Obviamente, este enfoque conceptual en la práctica se traduce en el despliegue de técnicas, tecnologías y sistemas concretos que permitirán a las empresas –las destinatarias de estos informes- competir con éxito en la nueva economía digital. A nadie se le oculta que la dimensión ética del impacto que todo esto produce puede acabar siendo una de las principales limitaciones para su desarrollo y que diferentes planteamientos al respecto entre países o culturas puede influir significativamente en el éxito o no en la nueva economía que se está dibujando.

La pregunta es, ¿cómo afectará todo esto al ámbito de la Defensa y la Seguridad?, dedicaremos los siguientes párrafos a tratar de contestarla.

Defensa Inteligente

La OTAN definió, en el año 2011, el concepto de Defensa Inteligente, "*Smart Defence*", como un instrumento para animar a los aliados a cooperar en el desarrollo, la adquisición y el mantenimiento de las capacidades militares para responder a los problemas actuales de Seguridad. Se proponía el intercambio de capacidades adquiridas, el establecimiento de prioridades y la coordinación de esfuerzos para desarrollar las nuevas [https://www.natolibguides.info/smartdefence] . Obviamente es una acepción de la palabra muy alejada del concepto que queremos tratar aquí.

Por el contrario, especialmente en los países de sudeste asiático, también desde hace años se denomina Defensa Inteligente, "*Smart Defense*" o "*Smart National Defense*", a la aplicación de las tecnologías base de la cuarta revolución industrial a la optimización de las actividades de las Fuerzas Armadas y Fuerzas y Cuerpos de Seguridad del Estado a fin de maximizar el potencial de sus componentes y aliviar en lo posible la exposición a los peligros inherentes a sus misiones.

En este contexto, desde hace unos años cada día es más importante la aplicación de las técnicas de extracción y análisis de datos, junto con las técnicas de predicción, para detectar las amenazas a la Seguridad y combatirlas eficazmente. La Defensa Inteligente no solo implica desarrollar nuevas tecnologías para ser una "nación inteligente", también obliga a la selección de aquellas por las que apostar. Un elemento esencial a considerar en esta elección es la dualidad de las tecnologías implicadas, lo que la convierte en una decisión estratégica que debe estar encaminada a apoyar las industrias de defensa nacionales. Así es como se ha planteado en los países que definen así la "*Smart Defense*".

Como ya se ha indicado, el elemento disruptivo en los próximos años es la aparición de una inteligencia artificial habilitadora de unas tomas de decisión mucho más eficientes que las del operador humano, al menos en términos de velocidad de respuesta y, lo que es peor, utilizando criterios no conocidos ni explicados, en algunos casos "decisiones ciegas", como puede ocurrir con las técnicas de aprendizaje profundo.

La sustitución del operador humano – lo que por otra parte han estado haciendo de modo acelerado las TIC durante cuarenta años- hasta los niveles de decisión más críticos y en las condiciones indicadas en el párrafo anterior produce vértigo y dispara todas las alarmas. A pesar de ello, los futuros planes de modernización de los sistemas de defensa se caracterizan por la irrupción de la Inteligencia Artificial

en los nuevos sistemas, en mayor grado cuanto más desarrollado está la correspondiente industria nacional en el ámbito TIC. De hecho, los más avanzados en la aplicación de estos conceptos posiblemente sean países como Singapur, Australia o Taipei.

En España la preocupación por el impacto de la IA en los asuntos de Defensa se ha incrementado notablemente en los últimos años. La monografía 79 del CESEDEN, "La inteligencia artificial, aplicada a la defensa" [https://publicaciones.defensa.gob.es/la-inteligencia-artificial-aplicada-a-la-defensa-n-79-libros-pdf.html], en el que se describe la problemática con generalidad y se aborda los diferentes aspectos de la misma, es un buen ejemplo; como lo son el creciente número de actividades y documentos que abordan el tema. Sin embargo, lo cierto es que el desarrollo concreto de algoritmos y sistemas está muy retrasado en nuestro país respecto de los de nuestro entorno, tanto en el ámbito académico como industrial.

Por ahora se apuesta por unirnos a iniciativas de la Comunidad Europea que en el año 2019 fijó entre sus prioridades para el período 2019-2024 el preparar a Europa para la era Digital y anunció el inicio del debate sobre una IA centrada en las personas, definiendo posteriormente unas directrices éticas para una IA adaptada a los valores éticos europeos…, una IA confiable… todo demasiado complejo.

Obviamente, en el ámbito de la Defensa y la Seguridad estas consideraciones éticas son muy importantes, el ejemplo más evidente son los sistemas de armas autónomos letales. No es fácil permitir que la IA tome decisiones de forma totalmente autónoma sobre el uso de fuerza letal, en el complejo campo de batalla del presente y del futuro. La solución empleada, la supervisión humana en algún momento del lazo de decisión, no es fácil de implementar en un escenario en el que combaten aplicaciones de IA desarrolladas por las fuerzas contendientes.

Posiblemente estas consideraciones éticas junto con las dificultades de estandarización y certificación de muchas de estas técnicas -algo esencial en el ámbito de la Defensa- serán los frenos del desarrollo de las aplicaciones militares de la IA. Es un error que países como el nuestro no se pueden permitir. Permítaseme por ello que finalice esta contribución con algunas reflexiones y propuestas.

Propuestas

- El desarrollo y despliegue acelerado de la IA en el ámbito militar es imparable y un elemento esencial para el cumplimiento de las misiones de las Fuerzas Armadas y las Fuerzas y Cuerpos de Seguridad del Estado.
- Los sistemas de mando y control y los sistemas de armas serán los primeros en hacerse inteligentes, pero será una revolución que afectará al resto de actividades: ciberdefensa, guerra electrónica, transporte, logística…
- Se debe apoyar el desarrollo en el país de algoritmos, aplicaciones y sistemas basados en IA mediante mecanismos de ayudas a la industria de la Defensa con subvenciones, uso de la compra Pública innovadora, etc. Las tecnologías que soportan la IA son completamente duales por lo que las sinergias con otros sectores son imprescindibles.
- Se requieren estrategias específicas para formar, retener y captar talento, así como administrar las limitaciones y dependencias tecnológicas para asegurar la capacidad de responder ante necesidades propias.
- Se precisa concienciar a la ciudadanía para que no se convierta en un freno al desarrollo de estas tecnologías para lo que se precisa superar uno de sus principales retos: la seguridad de los sistemas y su robustez y resiliencia de sus aplicaciones.

En definitiva, en los próximos años se producirá una brecha digital en la IA entre los países que dispongan de una “Defensa Nacional Inteligente” potente -con unos sistemas militares dotados de IA, personal capacitado para diseñarlos, producirlos y operarlos, y recursos invertidos en su despliegue- y otros que no. Las decisiones que se tomen ahora definirán a que grupo se pertenecerá en el futuro… y también su peso en la nueva economía digital