Documento de Trabajo 06/2018

La inteligencia artificial aplicada a la defensa

Artificial intelligence application in defence

Trabajo incluido en el Plan Anual de Investigación del Centro Superior de Estudios de la Defensa Nacional (CESEDEN) para el año 2018, como Grupo de Trabajo de Corta Duración nº 2, asignado al Instituto Español de Estudios Estratégicos (IEEE)

*

Organismo solicitante del estudio:
Centro Superior de Estudios de la Defensa Nacional (CESEDEN)

La inteligencia artificial aplicada a la defensa

Artificial intelligence application in defence

Maquetado en diciembre de 2018 por el Instituto Español de Estudios Estratégicos (IEEE)

Centro Superior de Estudios de la Defensa Nacional (CESEDEN)

Índice

Introducción

La inteligencia artificial aplicada a la defensa

José Manuel Roldán Tudela

Resumen

El propósito de este trabajo es presentar distintos aspectos de las tecnologías de Inteligencia artificial y Robótica Inteligente en su aplicación a la Defensa. Primero se exponen la historia y los fundamentos científicos de la Inteligencia artificial. A continuación, se dedican dos capítulos a la aplicación concreta de estas tecnologías a las estructuras y operaciones militares. Al final del trabajo se tratan dos temas importantes de plena actualidad: las consecuencias éticas del empleo de Inteligencia artificial y Robótica Inteligente a las operaciones militares y las diversas estrategias nacionales o regionales en el campo de la Inteligencia artificial.

Palabras clave

Inteligencia artificial, defensa y seguridad.

Artificial intelligence application in defence

Abstract

The purpose of this paper is to present different aspects of Artificial Intelligence and Intelligent Robotics technologies in their application to Defense. First of all, the history and scientific foundations of Artificial Intelligence are exposed. Next, two chapters are devoted to the concrete application of these technologies to military structures and operations. At the end of the paper, two important topics of current relevance are addressed: the ethical consequences of the use of Artificial Intelligence and Intelligent Robotics to military operations; and the different national or regional strategies in the field of Artificial Intelligence.

Keywords

Artificial intelligence, defense and security, .

La aplicación práctica de la robótica, y de los ingenios terrestres y aéreos no tripulados, está llamada a desempeñar un papel importante en la protección de la fuerza, en el reconocimiento, identificación, detección, seguimiento y ataque de objetivos, y en el apoyo logístico de las operaciones.

(PD1-001 Empleo de las fuerzas terrestres – Mando de Doctrina del Ejército de Tierra)

Introducción

La aspiración humana de crear réplicas de los seres vivientes que poblaban su mundo es muy antigua. Se puede decir que empezó cuando el hombre comenzó a escenificar sus cacerías sobre la pared de una cueva y a confeccionar figurillas de hueso u otros materiales. Conforme avanzaba la rudimentaria tecnología, estas representaciones fueron perfeccionándose. Inevitablemente, se llegó a pretender la imitación de la vida animada, con artefactos que reproducían movimientos y otras funciones de los animales, e incluso de los mismos humanos.

El siguiente paso fue intentar reproducir al propio ser humano como ser consciente. La evidente imposibilidad de lograrlo no evitó que apareciera el mito sustituyendo a la realidad. Los mitos sobre seres humanos artificiales se relacionaban inicialmente con la religión, como el mito griego de Pigmalión, que consiguió que Afrodita diese vida a una estatua o el del gigante de bronce Talos, infatigable guardián de Creta. Los rituales mágicos son también considerados como medio de crear seres humanos artificiales. La leyenda judía del Gólem es un claro exponente de esta fascinación por crear vida artificial. Finalmente, es la ciencia la que sustenta el mito, como en el relato de Frankenstein, de Mary Shelley.

Paralelamente a los mitos, los avances en la ciencia y la tecnología permitían la construcción de autómatas y primitivas máquinas de calcular. Pero el primer salto significativo vino de la mano de los primeros computadores modernos. A mediados del siglo XX se sentaron las bases de lo que se denominó Inteligencia artificial (IA). Sin embargo, ha sido necesario esperar hasta nuestros días para que vieran la luz aplicaciones reales de IA.

Aparte de los estudios y experiencias sobre el asunto, la irrupción con fuerza de la IA en múltiples campos ha sido posible gracias a un enorme incremento de la capacidad de computación y a la existencia de una ingente cantidad de datos para procesar.

Cuando hablamos de IA nos referimos a un conjunto de tecnologías cuyo objeto es crear sistemas, basados en las tecnologías de la información y las telecomunicaciones, con la capacidad de sentir, comprender y actuar como lo haría la mente humana. Hay

muchas definiciones de la IA, todas útiles, que ponen cada una el acento en alguno de los muchos aspectos de estas tecnologías.

Existen distintas opiniones sobre la importancia de estas tecnologías. En la reunión anual del Foro Económico Mundial 2018, en Davos, Suiza, el consejero delegado de Google, Sundar Pichai dijo: *«La IA es probablemente lo más importante en lo que la humanidad haya trabajado nunca. Considero que es algo más profundo que la electricidad o el fuego»*.[1] Otros expertos se muestran más escépticos, como Joshua Bengio, de la Universidad de Montreal, director de uno de los grupos más prestigiosos a nivel mundial en el desarrollo de técnicas de aprendizaje profundo. Según él, *«Hay personas que están sobreestimando enormemente el progreso que se ha hecho. Hay muchos, muchos años de pequeños avances detrás de muchos de estos asuntos […]. Y es difícil separar la exageración de la realidad porque estamos viendo estos grandes avances y también, a simple vista, parecen magia»*.[2]

Independientemente de las opiniones de los expertos, la importancia de la IA queda demostrada por el impacto que han tenido sus aplicaciones ya en uso. En la vida cotidiana no es raro encontrarnos con tecnologías de IA: cuando empleamos asistentes personales virtuales como Cortana o Google Now, cuando Netflix o Amazon recomiendan productos de forma personalizada, cuando hacemos una búsqueda en Internet o usamos Google Translator para traducir páginas enteras, al desbloquear nuestro teléfono mediante reconocimiento facial, etc.

Pero con ser muy útil en la vida cotidiana de las personas, el impacto de las tecnologías de IA va mucho más allá. En primer lugar, se ha abierto un nuevo campo al introducir tecnologías de IA en la robótica, que ya se encontraba bastante avanzada. Ello ha dado lugar a la Robótica Inteligente (RI), que es capaz de producir robots con un elevado grado de autonomía en sus funciones, pudiendo actuar en entornos cambiantes. Las aplicaciones de la RI son múltiples y, junto con sus grandes ventajas, despiertan no pocos recelos cuando se trata de sistemas de armas letales autónomos (SALAS).

Los campos en los que las tecnologías de IA y RI están produciendo avances espectaculares son muchos. A continuación, se citan los más importantes:

- La Defensa y seguridad: las aplicaciones de la IA y RI a la defensa y seguridad son múltiples y serán tratadas con detalle en este trabajo.
- La industria: ya se habla de la revolución de la Industria 4.0, que permite aprovechar al máximo las aplicaciones de IA y RI robótica en seguridad y productividad.

1 https://www.bloomberg.com/news/articles/2018-01-25/artificial-intelligence-nears-the-summit-of-hype-in-davos. Último acceso 30/10/2018.

2 https://www.technologyreview.com/s/546301/will-machines-eliminate-us/. Último acceso 30/10/2018.

- La educación: la IA permitirá adaptar la enseñanza a las capacidades y necesidades de cada alumno.
- La salud: múltiples aplicaciones de la IA en el ámbito de la salud se están utilizando ya, como diagnóstico automático por imagen, cirugía robótica, predicción de riesgos de enfermedad, enfermeras virtuales, control de las prescripciones de medicamentos, etc.
- Las finanzas: desde aplicaciones inteligentes de banca personal hasta automatización de inversiones por fondos de cobertura, pasando por detección del fraude, estudio de riesgos en préstamos o suscripción de pólizas de seguros.
- La publicidad y el *marketing*: existen muchas posibilidades de empleo de IA en este sector, tales como recomendaciones a los clientes, interacción automatizada con los consumidores (*chatbots* o robots que conversan), creación automática de contenidos web, publicidad digital personalizada, análisis predictivo, etc.
- El transporte: es de todos conocida la competición entre distintos fabricantes para conseguir la conducción autónoma de vehículos; también se pueden citar sistemas de seguridad (detección de obstáculos y frenado) o la optimización de rutas.

La eclosión de aplicaciones reales de la IA y RI se ha producido con gran rapidez en estos tres últimos años, y con mayor ritmo aún en los últimos doce meses. Se trata de tecnologías de marcado carácter dual y, si bien son aplicables a un gran número de sectores civiles, su empleo en aplicaciones para la defensa y la seguridad está experimentando un notable incremento.

Las fuerzas armadas de los países más avanzados dedican actualmente recursos crecientes para la obtención de sistemas que incorporan IA o RI para su uso militar en sistemas de mando y control, inteligencia, sistemas de armas o equipo individual del combatiente. Las grandes empresas del sector de la defensa, al compás de esta demanda, han iniciado desarrollos que incorporan tecnologías de IA.

Se puede decir que la IA y RI son temas de actualidad, con mayor motivo si tenemos en cuenta la carrera, que se está desarrollando ante nuestros ojos, entre varias potencias para hacerse con el control de las aplicaciones. Al mismo tiempo, las grandes empresas multiplican sus inversiones para conseguir el monopolio de tecnologías críticas de IA, para obtener una ventaja competitiva decisiva en el mercado mundial de IA.

La importancia de las tecnologías de IA y RI, unida al hecho de que nos encontramos en un momento clave de su desarrollo, justificaría por sí solo la elaboración de un trabajo sobre este tema. Si añadimos la efervescencia de aplicaciones en el ámbito de la defensa y la seguridad, parece oportuno redactar un trabajo que contemple estas tecnologías desde el punto de vista de su empleo en este dominio, junto con una visión de otros asuntos de interés asociados.

Para su elaboración, el presente trabajo ha seguido una línea conceptual en la que se parte de los aspectos más tecnológicos para ir concentrándose en las aplicaciones para la defensa, los retos éticos que plantean estas tecnologías y las estrategias nacionales respecto a ellas. De esta manera, se pretende dar una visión que contemple las distintas facetas de la aplicación de la IA y RI a la defensa.

Para ello, se ha dividido el trabajo en cuatro bloques conceptuales:

- La IA y RI, desde sus antecedentes hasta el estado actual de las tecnologías. Un bloque de marcado carácter técnico. Abarca los Capítulos 1 y 2.
- La IA y RI en su aplicación a la defensa y a las operaciones militares. Se entra con cierto detalle en el impacto de estas tecnologías en la defensa. Abarca los capítulos 3 y 4.
- Aspectos éticos de la utilización de IA y RI en aplicaciones militares. Comprende el capítulo 5.
- Estrategias nacionales o multilaterales respecto a la IA y RI. Constituyen el capítulo 6.

El primer capítulo, titulado «Perspectiva histórica y evolución de la Inteligencia artificial», expone, en primer lugar, los orígenes del concepto de IA, para entrar después en su definición y en una primera clasificación. Después trata los primeros pilares de la IA, prestando atención al procesamiento del lenguaje natural como uno de los primeros soportes importantes de la IA. Tras finalizar la historia de la IA, trata en un último apartado la evolución, los logros y el futuro previsible de estas tecnologías

El segundo capítulo, que lleva por título «Situación y perspectivas de las tecnologías y aplicaciones de inteligencia artificial», explica, en primer lugar, cuáles son sus objetivos, para pasar a continuación a describir las tecnologías básicas de la IA. A continuación, enumera los sistemas y desarrollos de IA, de donde se deducen las áreas en las que estas tecnologías constituyen un elemento clave. Finaliza el capítulo con una descripción del mercado tecnológico ligado a la IA.

El tercer capítulo se titula «La Inteligencia artificial y su aplicación en el mundo militar». Comienza con una exposición sobre el ser humano y los ingenios, para pasar, a continuación, a tratar sobre la IA para los ejércitos. Aquí se expone el papel de la Agencia Europea de la Defensa (EDA) y sus proyectos en el campo de la IA. También se tratan los análisis que ha llevado a cabo la OTAN, primero para determinar las tendencias tecnológicas y sus consecuencias y luego para identificar las capacidades que se necesitarán en el futuro. Este último análisis se realiza en paralelo con las funciones conjuntas de la Doctrina para el empleo de las FAS promulgada por el JEMAD. Finaliza con una breve descripción de marcos y tareas adoptadas por el Ministerio de Defensa de España y una iniciativa muy reciente del Ejército de Tierra de los EE. UU.

El cuarto capítulo, titulado «La Inteligencia artificial y la fricción de la guerra», comienza con un análisis para determinar conceptos de empleo de la IA y RI en aplicaciones militares. Seguidamente trata los niveles operacional y táctico, señalando las mejoras de capacidades que proporcionará el uso de IA y RI, para pasar al nivel estratégico, donde análogamente se exponen la mejora de capacidades y el tipo de operaciones influidas por la IA. Finalmente, se dedica un breve apartado a reflexionar sobre el impacto de la IA sobre el carácter y naturaleza de la guerra.

El quinto capítulo, que lleva por título «Desafíos éticos en el uso militar de la Inteligencia artificial», empieza describiendo los retos éticos en las aplicaciones militares de la IA, y pasa a continuación a tratar sobre el problema de la atribución de responsabilidad, que desemboca en el concepto de control humano significativo. Finaliza tratando de los «robots éticos» y un apunte sobre la opinión pública y su percepción del empleo de IA y sistemas autónomos en la guerra.

El capítulo seis se denomina «Contexto internacional estratégico de la Inteligencia artificial» y empieza describiendo los actores (países) destacados en el liderazgo de la IA y sus estrategias respecto a estas tecnologías. Concluye el estudio con una descripción de los actores emergentes, que no compiten por el liderazgo, pero desean ocupar un espacio importante en la jerarquía internacional.

Nuestro deseo es que el presente trabajo sirva para proporcionar un conocimiento de base sobre la aplicación de estas tecnologías a la defensa y la seguridad, para que posteriormente se pueda ampliar con lecturas que traten el tema con mayor profundidad y detalle. Si bien se recomienda la lectura desde el principio, se ha procurado que los capítulos sean autocontenidos, de forma que el lector pueda saltar al asunto de su mayor interés sin gran pérdida de información.

Capítulo 1

Perspectiva histórica y evolución de la inteligencia artificial

José Javier Rainer Granados y
Luis Rodríguez Baena

Resumen

La idea de resolver problemas diversos de forma automática y simulando el comportamiento humano ha estado presente desde la antigüedad. Sin embargo, no ha sido hasta mediados del pasado siglo cuando el avance de las ciencias de la computación ha permitido comenzar a plantearse la posibilidad de que los ordenadores pudieran dar soluciones «inteligentes» a esos problemas. Y hemos tenido que esperar hasta este siglo para que los avances de la informática permitieran implementar esas soluciones en aplicaciones reales.

La Inteligencia artificial (IA) se puede definir como una rama de las ciencias de la computación que se ocupa de la comprensión, desde el punto de vista informático, de lo que se denomina comúnmente comportamiento inteligente.

Incluye distintos campos como el aprendizaje automático, el procesamiento del lenguaje natural, los sistemas expertos, la visión artificial, etc., y es la base de otros muchos como la robótica o el big data, dos de las áreas que más están creciendo en la actualidad.

En este capítulo se recogen los conceptos básicos de la IA, su evolución histórica, los campos que incluye y las nuevas tendencias, como la lógica difusa y la computación cognitiva.

Palabras clave

Inteligencia artificial, defensa, seguridad, historia, definiciones, robótica.

Historic review and evolution of artificial intelligence

Abstract

The idea of solving various problems automatically and simulating human behavior has been present since ancient times. However, it was not until the middle of the last century that the advance of computer science allowed us to begin to consider the possibility that computers could provide «intelligent» solutions to these problems. And we had to wait until this century for advances in computing to implement those solutions in real applications.

Artificial Intelligence (AI) can be defined as a branch of computer science that deals with the understanding, from an IT point of view, of what is commonly called intelligent behavior.

It includes different fields such as machine learning, natural language processing, expert systems, artificial vision, etc., and is the basis of many others such as robotics or big data, two of the areas that are growing the most in the present.

This chapter includes the basic concepts of AI, its historical evolution, the fields it includes and new trends, such as fuzzy logic and cognitive computing.

Keywords

Artificial intelligence, defense, security, history, definitions, robotics.

No computer has ever been designed
that is ever aware of what it's doing;
but most of the time, we aren't either.
Marvin Minsky

Introducción

Aunque en los últimos tiempos, y en el futuro próximo, parece que la inteligencia artificial (IA) está tomando gran relevancia, no cabe duda de que la inquietud del ser humano para querer desarrollar máquinas inteligentes y algoritmos que sean capaces de buscar soluciones a muchos de los problemas que nos rodean ha estado siempre presente en los grandes retos e inquietudes del ser humano.

Las ambiciones en torno a este campo de la IA son grandes, y los avances están directamente relacionados con la evolución que ha tenido la informática, el software y la capacidad de cálculo del computador, que ha ayudado enormemente al estado actual de la IA.

A través de este capítulo se describe la evolución de la IA y los logros más importantes hasta el momento. Es posible, dado los grandes avances que se están dando en los diferentes campos tecnológicos, que en unos pocos años tengamos la oportunidad de ver resueltos retos que hoy nos parecen más propios de la ciencia ficción que de la realidad.

Aunque son muchas las tecnologías que coexisten hoy día, es la IA la tecnología que ofrece la capacidad de diferenciarse. Las mayores empresas tecnológicas como Google, Microsoft, Amazon, Facebook, o Alibaba, tienen como pilar la IA en el corto y medio plazo. Una estrategia alrededor de la IA puede crear una disrupción mayor de las vividas hasta ahora en el campo de la tecnología.

Orígenes del concepto de inteligencia artificial

Consideraciones y aproximación al concepto de inteligencia

La inquietud del ser humano por reproducir comportamientos inteligentes es algo que siempre ha estado presente a lo largo de la historia. Los primeros juegos matemáticos, como el de las Torres de Hanói (hacia el 3.000 a. C.) son una clara representación de una de las cuestiones que más se ha trabajado en la IA, y es la capacidad de conseguir un objetivo con el mínimo de acciones posibles. Lograr máquinas inteligentes ya lo planteaba Aristóteles sobre el año 322 a.C. Otros ejemplos destacables y posteriores los encontramos a lo largo de la historia hasta nuestros días. Se destacan a continuación algunos de ellos.

Herón de Alejandría, durante el siglo I d.C., recoge todos los conocimientos sobre la figura de los robots en su trabajo *«Autómata»*. Se describen algunos de los artilugios e invenciones tanto propios como ajenos. Muchos de estos mecanismos tenían connotaciones o propósitos religiosos y, cada vez con más frecuencia, buscando divertimento e incluso acompañamiento. La mayoría de estos mecanismos estaban realizados a base de engranajes, palancas y sistemas de conducción de agua o de vapor, y piezas mecánicas, aunque en muchos casos eran configuraciones realmente rocambolescas, como permitir la apertura de las puertas de un templo de forma automática al encender un fuego a su entrada (figura 1.1) o intentaban dar vida a aves aleteando y bebiendo agua de una fuente. A Herón también se le atribuye la invención de la *Eolípila*, dispositivo capaz de transformar energía térmica en energía mecánica, y primer antepasado conocido de la máquina de vapor que tanto impacto tuvo en la revolución industrial.

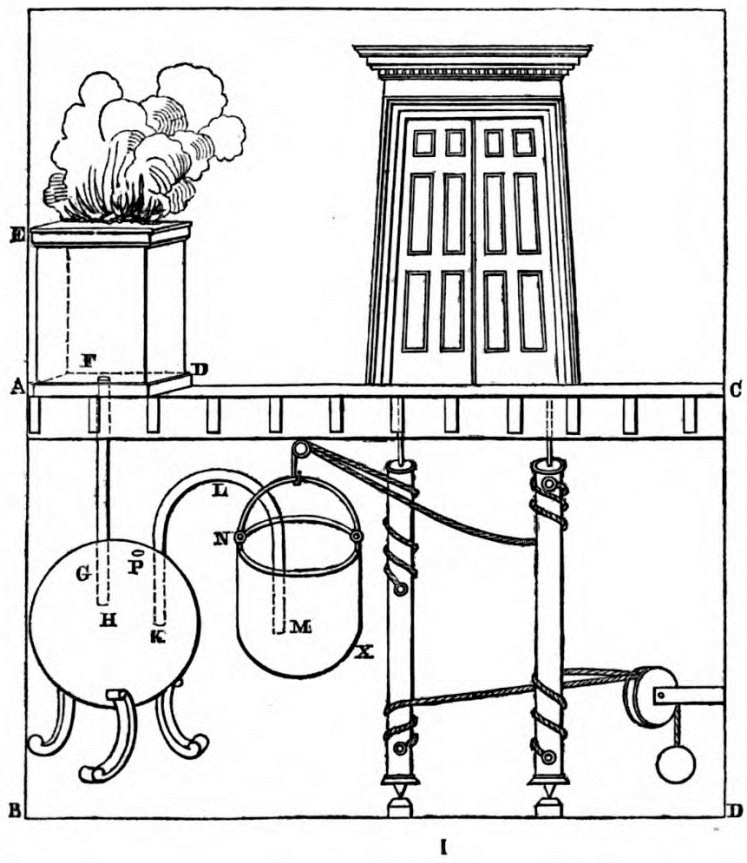


Figura 1.1. Mecanismo para la apertura automática de puertas (Herón de Alejandría. *Pneumatika.* Traducción de Bennet Woodcroft, Londres: Taylor Walton and Maberly, 1851).

El Antiguo Egipto también fue un referente por la gran cantidad de artefactos mecánicos que se construyeron. La mayoría de ellos buscaban asombrar y causar temor a todo aquél que los contemplara. Es evidente que los avances de cada época han estado basados en lo que la técnica en ese momento permitía. Claramente estamos aún lejos en esta época de emular al ser humano con artilugios que se basan básicamente en mecanismos y engranajes pero, conforme ha ido avanzando la tecnología, como a continuación se describe, y sobre todo con la aparición del computador y la IA, cada vez se está más cerca.

Interesante también es destacar las aportaciones de Leonardo da Vinci, que no pudo tampoco resistirse a la tentación de crear por sí mismo alguna forma de vida artificial como, por ejemplo, el león mecánico que Francisco I le encargó construir a comienzos del S. XVI.

Otros avances interesantes para la época, y la mayoría con carácter lúdico, fueron:

- 1738: Pato, El flautista de Jacques de Vaucanson.

- 1769: El jugador de ajedrez de Wolfgang von Kempelen (figura 1.2).
- 1770: El escritor, el musico, etc. Desarrollados por Pierre y su hijo Henri-Louis Jaquet-Droz.
- 1788: James Watt: regulador de velocidad.
- 1847: Boole estableció la lógica proposicional.

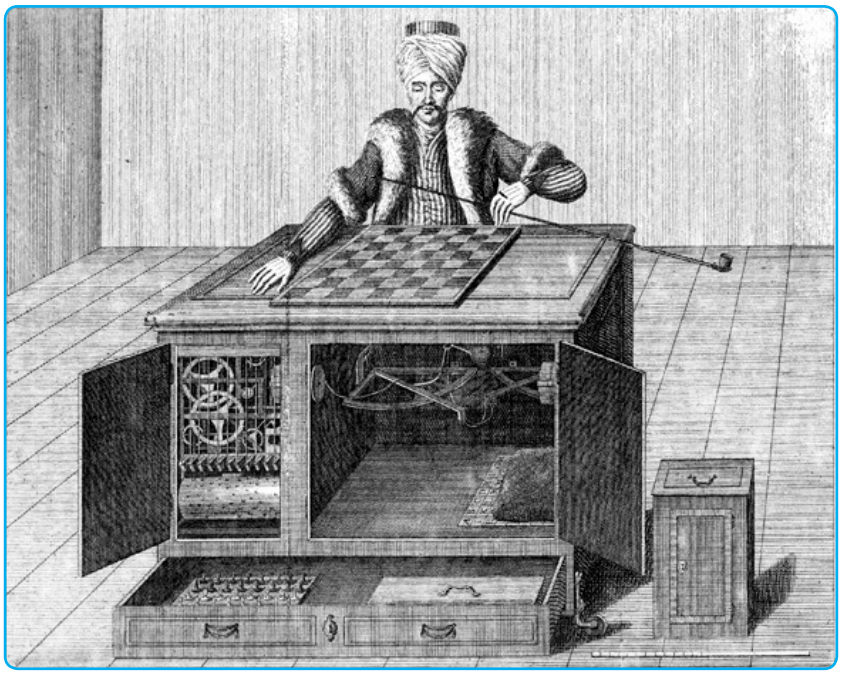


Figura 1.2. El turco. Jugador de ajedrez de Wolfgang von Kempelen (Karl Gottlieb Windisch: *Briefe über den Schachspieler des Hrn. von Kempelen, nebst drei Kupferstichen die diese berühmte Maschine vorstellen*. Bratislava: A. Löwe, 1783).

Ya en pleno siglo XX, fue en el verano de 1956, en Dartmouth College, donde John McCarthy, Marvin Minsky (MIT), Allen Newell y Herbert Simon (Carnegie-Mellon), junto a otros estudiosos, establecen los objetivos de la IA. Pero no debería olvidarse a Turing, no solo por su famoso test, sino también porque ayudó unos años antes, sobre 1945, a lo que sería la IA.

La IA es un campo de la ciencia y la ingeniería que se ocupa de la comprensión, desde el punto de vista informático, de lo que se denomina comúnmente comportamiento inteligente. También se ocupa de la creación de artefactos que exhiben este comportamiento[1]. Para llegar a una buena comprensión del término deberíamos primero entender el significado de »inteligencia». Según la Real Academia Española (RAE) este término hace referencia a:

1 Shapiro, Stuart C., «Encyclopedia of Artificial Intelligence» (2nd ed.). John Wiley & Sons, Inc., New York, 1992.

1. Capacidad de entender o comprender.
2. Capacidad de resolver problemas.

Conocimiento, comprensión, acto de entender

Aunque las definiciones parecen dejar claro el concepto, el espectro se complica según nos adentramos en la interpretación del término. Sobre todo si se atiende a Howard Gardner que, en su famosa obra *Frames of Mind: The Theory of Multiple Intelligences*[2], se atrevió a formular 10 tipos de inteligencia:

- Musical.
- Espacial o visual.
- Lingüística-verbal.
- Lógico-matemática.
- Corporal-cinestésica.
- Interpersonal.
- Intrapersonal.
- Naturalista.
- Existencial.
- Otras: categoría en la que entra incluso una inteligencia sexual.

Aunque tiene sus detractores, esta teoría ha tenido gran impacto en ámbitos como el educativo, donde tradicionalmente los test de evaluación se orientaban a un enfoque puramente lógico-matemático y lingüístico. Son numerosas las instituciones educativas que tratan hoy en día de ampliar la evaluación del estudiante incorporando factores asociados a sus capacidades para la expresión artística o corporal, por ejemplo.

Otra discusión asociada el concepto de inteligencia es la exclusividad o no de la inteligencia como atributo humano. Sin embargo, los resultados de la experimentación científica han conseguido apartar esta discusión al poner en evidencia que son numerosas las especies animales que consiguen generar nuestras estrategias para adaptarse mejor a

2 Gardner, H., «Frames of mind: The theory of multiple intelligences», New York, Basics Books, 1983.

las necesidades del entorno y resolver los problemas asociados[3], y todo ello a pesar de que la experimentación con otras especies animales en este ámbito no es trivial[4].

Comentado el concepto de inteligencia, queda profundizar en el término que nos ocupaba al inicio. Según la RAE, la inteligencia artificial es la «disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico».

Bellman propone otra definición:

«*La automatización de actividades que vinculamos con procesos de pensamiento humano, actividades como la toma de decisiones, resolución de problemas, aprendizaje…*»[5].

Avanzando en el concepto de inteligencia, una primera aproximación es considerar la inteligencia como la capacidad de resolver problemas. Pero no solo eso, también la inteligencia es la capacidad de entender o comprender. En ese sentido, la capacidad de comunicarse es una muestra de inteligencia. El procesamiento de lenguaje natural, una de las grandes líneas de trabajo de la IA, tiene retos importantes si comparamos con la capacidad de comunicarse del ser humano que puede ir acompañada de elementos muy difíciles de reproducir en máquinas como es el humor, dobles sentidos o la ironía.

También otro factor determinante en la comunicación son los sentimientos que acompañan en ese instante al comunicador, aunque los avances en analizar y simular sentimiento en máquinas son muy significativos. Continuando con el concepto de inteligencia, se podría pensar que alguien capaz de manejar mucha información, de recordar muchos datos, se podría considerar inteligente. En este sentido, las máquinas son muy buenas manejando mucha información y haciendo operaciones, pero el reto está en transformar esa información en conocimiento.

Una primera clasificación inteligencia artificial

La clasificación más habitual que se emplea en el campo de la IA fue introducida por Searle[6], que estableció dos tipos de IA: IA *débil* e IA *fuerte.* En el primer caso, es una

3 Rayner, H., «Breeding for Intelligence in Animals», Nature, 36 (924), London, enero 1887, p. 246-246.

4 MacLean, E. L. et al., «The evolution of self-control», Proceedings of the National Academy of Sciences, 111 (20), Washington, abril 2014, p. E2140-E2148.

5 Bellman, R., «An introduction to artificial intelligence: Can computers think?», Boyd & Fraser Pub. Co., San Francisco, 1978

6 Searle, J. R., «Minds, Brains, and Programs», *Behavioral and Brain Science*, 3 (3), Cambridge (UK), septiembre 1980, pp.417-457.

IA que está específicamente entrenada para realizar una actividad, es decir se trata de realizar tareas que requieren inteligencia en entornos muy concretos. Ejemplos como jugar al ajedrez o resolver un problema específico son los más representativos para este tipo. Cabe destacar que, desde los comienzos de la IA, siempre han despertado gran interés juegos como el ajedrez. Sobre todo, porque permitió desarrollar los primeros programas capaces de aprender. En estos entornos limitados y con el sistema bien entrenado, está demostrado que la máquina llega a ganar al mejor de los jugadores de ajedrez. En este sentido, y dado los avances en capacidad de procesamiento de las máquinas, podemos asegurar que se están dando grandes avances en la IA débil.

En el caso de la IA *fuerte,* se trata de simular más el comportamiento humano o la inteligencia humana. En algunas ocasiones también se habla del término IA *general*, conviene destacar que ambos términos no son exactamente iguales, todo IA fuerte será *general,* pero a la inversa no tiene por qué darse. Cuando se habla de IA general, aunque no hay una definición exacta, se hace referencia a una IA de propósito general como una continuidad a la IA clásica. Hay mucho esfuerzo de investigación alrededor de conseguir una Inteligencia artificial *fuerte*, ambición que aún estamos lejos de conseguir.

Los primeros pilares de la inteligencia artificial

Primeros avances: representación del conocimiento, búsqueda heurística y aprendizaje automático

La IA trabaja en diferentes campos como la representación del conocimiento, búsqueda heurística, procesamiento del lenguaje natural, aprendizaje automático y, en sus comienzos, en desarrollo de sistemas expertos.

Es a partir de los años 60 cuando se comienzan a hacer las primeras investigaciones en torno a la IA. En este periodo y hasta los años 70, se trabaja fundamentalmente en los primeros lenguajes de programación como LISP, en temas de heurística, robótica y, sobre todo, en sistemas expertos como DENDRAL. Algunas de estas líneas de trabajo se desarrollan a continuación.

Una de las líneas de trabajo, tiene que ver con los formalismos de representación del conocimiento que proporcionan las herramientas necesarias para codificar la realidad en un computador.

Durante los años 70 y 80, la IA vivió una etapa con gran interés en el conocimiento, y es precisamente en esta etapa donde surgen la mayoría de propuestas de representación del conocimiento. Esto es consecuencia del auge inicial de los sistemas expertos (SE) y los sistemas basados en conocimiento (SBC). La mayoría de los sistemas de representación parten del hecho que el conocimiento se adquiere a partir de la experiencia, esto hace que haya mucha similitud en cómo abordan el aprendizaje del mismo. También, en analogía con el ser humano, consideran la capacidad de generar nuevo conocimiento a partir del que ya posee, por lo que el método se basa en la inferencia a partir del conocimiento existente. Un factor esencial en los sistemas de representación es definir el ámbito y naturaleza del conocimiento que se pretende representar, para acotar el conocimiento general que es muy amplio.

Otra de las líneas de trabajo que se está desarrollando es la búsqueda heurística. Básicamente consiste en localizar la solución más idónea para un problema entre un abanico de soluciones disponibles. En muchas ocasiones, se desconoce cuál es la mejor solución posible. A veces se habla de solución «buena», entendida esta como la mejor solución entre las encontradas y que satisface unos criterios de calidad básicos exigidos previamente.

La palabra heurística proviene del griego *heurískein*, que significa «hallar», «inventar».

Una búsqueda puede realizarse al azar o puede estar guiada mediante algún tipo de estrategia o procedimiento razonado. Lo que en términos coloquiales sería fuerza bruta o establecer algunos criterios que permitan una búsqueda más inteligente.

Un algoritmo de búsqueda heurística es un algoritmo computacional que ofrece un mecanismo para encontrar buenas soluciones ante un problema dado. No siempre garantiza que será capaz de encontrar la solución óptima al problema, o que será capaz de encontrar esa solución empleando un tiempo aceptable.

De hecho, en algunas ocasiones estos algoritmos proporcionan soluciones de poca calidad o se ejecutan empleando un coste computacional alto. En resumen, el concepto de búsqueda heurística hace referencia a algoritmos computacionales que proponen un mecanismo para encontrar buenas soluciones, sin garantizar que sean soluciones óptimas, ante un problema dado. Conforme mayor información se le proporcione al algoritmo mejor será capaz de mejorar la solución.

Existen diversas familias y tipologías de algoritmos de búsqueda heurística. Algoritmos voraces, ramificación y poda, minimax, son algunos ejemplos. Estos algoritmos pueden exigir para su ejecución importantes recursos computacionales, por lo que es necesario estudiar de antemano la complejidad temporal y espacial del algoritmo.

Una tercera línea de trabajo está relacionada con el aprendizaje automático. En sus primeras aportaciones existía un denominador común que consistía fundamentalmente en reconocer y clasificar patrones. Las redes neuronales fueron el elemento clave,

adecuadamente entrenadas son capaces de mostrar buenos resultados. Las redes neuronales representan un modelo computacional de las conexiones entre neuronas que se dan en el cerebro. Cada neurona recibe información de entrada procedente de varias fuentes y emite una salida concreta en función de su configuración.

Sistemas expertos

El origen de los sistemas expertos surge de un modelo de Newell y Simon[7] que consistía en representar conocimiento sobre cómo resolver un problema mediante reglas del tipo SI-ENTONCES.

Los Sistemas Expertos (SE) pueden ser considerados como uno de los campos que más se ha trabajado en la IA. Un Sistema Experto resuelve problemas complejos del mundo real que requieren experiencia mediante un computador. Los sistemas bien diseñados imitan el proceso de razonamiento que los expertos utilizan para resolver problemas específicos. Se utilizan computadores, bien por su capacidad para realizar trabajos de gran volumen de cálculo, ya que se trata de máquinas incansables, bien como apoyo en determinados entornos para mejorar la resolución de problemas.

Cuando se habla de SE, es habitual referirse a un sistema que tiene un conocimiento profundo, pero muy limitado en un campo muy bien definido, en este entorno es capaz de razonar igual o mejor que un experto humano, aunque no necesariamente de la misma manera. Sin embargo, si el sistema está bien configurado las conclusiones deberían ser las mismas.

El primer sistema experto fue el ya citado DRENDAL, cuyo propósito era interpretar la estructura molecular, desarrollado en Stanford en la década de 1960, durante casi 10 años. Posteriormente se desarrolló otro famoso sistema experto, llamado Mycin desarrollado a comienzos de los años 70 también en la Universidad de Stanford. Se aplicó en el diagnóstico de enfermedades infecciosas. Adicionalmente a diagnosticar el agente causante de la infección, también podía generar el tratamiento a administrar.

En geología se desarrollaron los sistemas Prospector (1974-1983) y Dipmeter (1980). El primero, tenía como objetivo encontrar minerales, y en el caso de Dipmeter su objetivo era la búsqueda de yacimientos petrolíferos. Se pueden encontrar ejemplos de SE en diferentes campos, como por ejemplo en defensa, en planificación de misiones, en entornos bancarios, en entidades financieras y, por supuesto, en medicina. En este último campo, cabe destacar Oncocin, que desde 1981 ha sido utilizado por la Facultad de Oncología de Stanford.

7 Newell, A. y Simon, H.A., «Human Problem Solving», Englewood Cliffs (NJ), Prentice-Hall, 1972.

En términos más ambiciosos, se podría pensar en SE más útiles y más grandes que serían aquellos capaces de combinar el conocimiento de más de un experto humano. Al combinar los conocimientos de muchos expertos tendrían razonamiento de calidad más alta o conocimiento más amplio que un solo experto humano. Pero al combinar información de muchos expertos hay que asegurar que la información no se contradice, bien diciendo lo mismo de manera distinta o bien diciendo una cosa opuesta. Es de esperar que las cosas opuestas sean pocas, pero hay que detectarlas. Una manera de hacerlo es poder transferir o generar la información que ya existe dentro del SE en lenguaje natural para que un experto pueda saber exactamente qué es lo que el sistema ya conoce. En este aspecto, el lenguaje natural ha sido muy útil para la adquisición de información.

Otro aspecto interesante, es el aprendizaje automático. Una manera de ampliar el razonamiento de los sistemas expertos es que aprendan solos. Es decir, que aprendan basándose en la experiencia que han tenido para no repetir errores, que si les falta cierta información pregunten o que fueran capaces de buscarla. Si han tenido necesidad de efectuar una búsqueda complicada, que conozcan la estrategia mejor para resolver una clase de problemas y, si no la han encontrado, que se acuerden de qué es lo que funcionó y qué aspectos de la situación permitieron que esa estrategia funcionara para que, si se necesitase otra semejante, la puedan utilizar. Este es un enfoque muy importante pero aún no ha tenido resultados prácticos.

Áreas en expansión: robótica, visión por computador y PLN

Es en 1921 cuando se introduce por primera vez la palabra 'robot', que fue utilizada por el escritor checo Karel Capek (1890-1938). El término aparece por primera vez en su obra de teatro *R.U.R. (Rossum's Universal Robots)*, en 1921 (figura 1.3). La obra tuvo tanto éxito que pronto se extendería por toda Europa. El tema en parte de *R.U.R.* ponía de manifiesto la deshumanización del hombre en una civilización tecnológica. *R.U.R.* es la abreviatura de Robots Universales Rossum; esta última palabra es seguramente un guiño al lector porque tiene un sospechoso parecido con el término checo *rozum* «entendimiento».

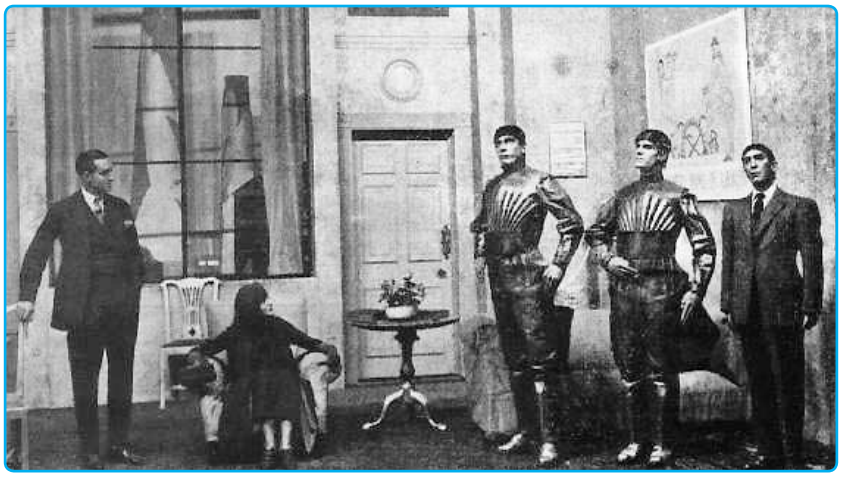


Figura 1.3. Representación de la obra de teatro R.U.R. Fotografía sin fecha, hacia 1923 (fuente: https://goo.gl/ddUWgD, imagen de dominio público).

Atendiendo a la RAE, un robot es una «máquina o ingenio electrónico programable, capaz de manipular objetos y realizar operaciones antes reservadas solo a las personas». Resulta curioso comentar su origen etimológico: deriva de la palabra checa *robota* «trabajo» y el término se le atribuye a Čapek, que la introduce por primera vez en su obra del mismo nombre. Lo asociaba con androides trabajadores, y la difusión del término, como se puede comprobar, ha sido todo un éxito.

Se destacan a continuación algunos de los hitos más importantes en el campo de la robótica.

Es en 1976 cuando se consigue el primer manipulador en el espacio, mediante la misión Viking. Este hito abrió una línea muy interesante relacionada con la robótica espacial, por ejemplo, el robot de exploración *Sojourner*, que llegó a Marte a bordo de la misión *Mars Pathfinder* el 4 de julio de 1997, o al *Spirit* (*Mars Exploration Rover - A*), que llegó a su destino el 4 de enero de 2004, tres semanas antes que su homólogo *Opportunity*. El 25 de mayo de 2011 la NASA declara oficialmente finalizada la misión del robot *Spirit,* tras no haber recibido ninguna señal procedente de él prácticamente desde un año antes, pero hay datos que demuestran que el odómetro del *Spirit* había medido distancias superiores a los 8.000 metros.

En la actualidad, otro *rover* está funcionando en Marte, el *Curiosity*, enviado el 26 de noviembre de 2011, que desde el 6 de agosto de 2012 está funcionando en la superficie marciana y que ha recorrido hasta la fecha más de 20.000 metros.

Otro ámbito interesante son los robots militares, que aparecen en la Segunda Guerra Mundial y durante la Guerra Fría, y hasta nuestros días. Cabe destacar:

- 1940 Tanques no tripulados radicontrolados a distancia, los Soviéticos TT-26 teletank.

- 1944 vehículos de demolición Goliath, un pequeño vehículo sobre orugas y guiado por cable, utilizado por el Ejército alemán durante la Segunda Guerra Mundial.
- Más recientemente, el Elbit Systems Hermes 450 es un vehículo aéreo no tripulado (UAV) táctico diseñado para misiones prolongadas. Con autonomía de 20 horas durante una misión principal de reconocimiento y vigilancia.
- MIDARS, un robot de cuatro ruedas provisto de varias cámaras, radar y equipado con capacidad de disparo.

Así, podríamos seguir describiendo un buen número de artefactos del ámbito militar, por lo que el peso en este campo de la robótica y la IA son muy importantes.

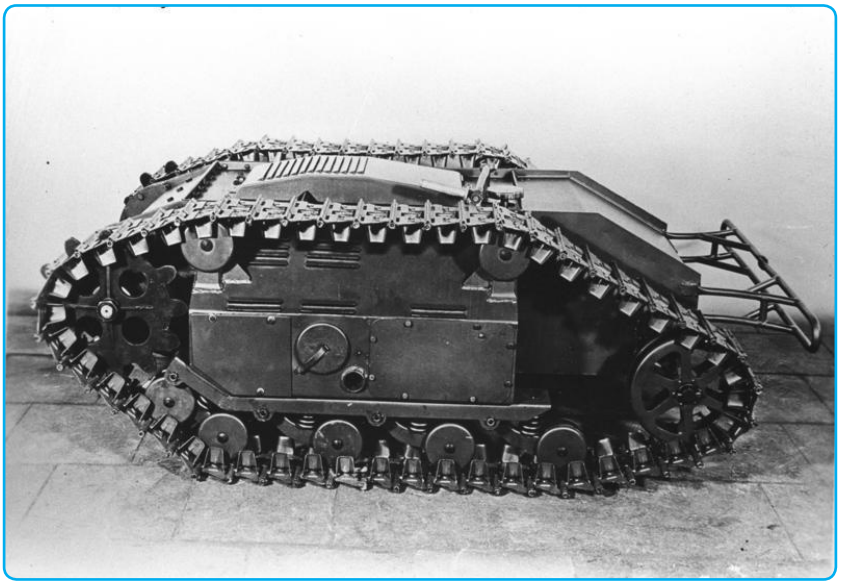


Figura 1.4. Vehículo teledirigido Goliath. Fotografía realizada en hacia 1943-1944 (fuente: Deutsches Bundesarchiv, https://goo.gl/ZoYUgx).

Aunque los desarrollos están siendo muy rápidos, robots-guía, que combinen capacidades de navegación con cierta autonomía para interactuar y desarrollar comportamientos con personas, son pocos actualmente. Cabe destacar la aportación de la Universidad de Bonn, se trata del robot Rhino, robot móvil desarrollado por el Computer Science Department III con capacidad de adaptación y aprendizaje. Una de las funciones encomendadas era la de guía en «Deutsches Museum Bonn» (Museo Alemán de Bonn, principal museo tecnológico de Alemania). Otro ejemplo fue Minerva, desarrollado por el mismo grupo creador de Rhino junto con el Robot Learning Laboratory de la Universidad Carnegie Mellon. Sus funciones también pasaban por robot guía en el Museo Nacional de Historia Americana de la Institución Smithsonian, en Washington.

Siguiendo con algunos de los desarrollos de un robot interactivo se podría mencionar a Xavier, desarrollado con fines de investigación en la Universidad Carnegie Mellon,

y adicionalmente participó en la AAAI Robotics Competition de 1993. Tambien podemos incluir en esta revisión a Tourbot (Interactive Museum Tele-Presence Through Robotic Avatars), proyecto lanzado en enero de 2000, con un objetivo en línea con los anteriores, es decir como robot guía para museos, aprovechando además la incorporación de internet.

El robot Sophia es un robot humanoide, desarrollado por Hanson Robotics. Posee capacidad de interactuar con los humanos, teniendo incorporados los últimos avances en procesamiento de reconocimiento de voz, imágenes y demás tecnología que le permite desenvolverse perfectamente con personas.

Aunque los robots humanoides siempre despiertan mucha expectación, el tipo de robot susceptible de estar más presente en nuestras casas son los robots aspiradoras o robots juguetes, aunque de nuevo es de esperar que a futuro sea algún robot el que nos acompañe en nuestra vejez.

La visión por computador se puede considerar una disciplina en sí misma dentro de la IA pero, unida a la robótica, el potencial es inimaginable, ya que se trata de dotar a la máquina con la misma capacidad de visión del ser humano.

La visión por computador aborda métodos para capturar la información, procesar, analizar y, quizás lo más importante, comprender las imágenes del mundo real con el fin de tomar decisiones.

La información que proporcionan los sentidos es lo que permite al ser humano desenvolverse en su entorno. Todos los sentidos en el ser humano son importantes, pero especialmente la visión. De la información con la que se cuenta actualmente, el cerebro dedica gran cantidad de espacio al procesamiento visual. La visión humana es un sistema complejo que incorpora coordinación motora, a nivel de posición de ojos, cuello, etc. No obstante, adicionalmente a la perfecta coordinación motora, se requiere un conocimiento previo de los objetos que nos rodean.

El proceso de reconocimiento de objetos requiere, desde el punto de vista cognitivo, que exista una representación previa en el cerebro, eso hace además que podamos realizar una abstracción de los mismos. La comparación de objetos es gracias a estas representaciones mentales, y eso permite que seamos capaces de reconocer mismos objetos de diferentes tamaños, color, posición etc. Gracias a la información que recibimos a través de los sentidos es lo que permite realizar conductas complejas y desenvolvernos en nuestro entorno. Así, por ejemplo, la percepción visual nos ayuda a encontrar cualquier objeto que estemos buscando, hacia dónde dirigirnos cuando caminamos o realizar una búsqueda selectiva en un entorno concreto. Por lo tanto, nuestra conducta es producto de las diversas funciones cognitivas, y cada vez más se ha comprobado que los sentimientos tienen un peso muy importante en los comportamientos.

El proceso de percepción es una constante integración de procesos de aprendizaje, memoria, emoción, etc. En este sentido, cabe destacar las aportaciones de David Marr sobre el modelado de los procesos visuales humanos[8].

Actualmente la capacidad de los algoritmos de procesamiento de imagen es cada vez más sofisticada. Además, y sobre todo en la interpretación de imágenes, Internet es una fuente inagotable de recursos.

Respecto al Procesamiento del Lenguaje Natural (PLN) es una de las piedras angulares tempranas de la inteligencia artificial. Cabe hacer una breve mención y revisión histórica desde el punto de vista del procesamiento del lenguaje natural, con independencia de la terminología que se emplee, distinguiéndose cuatro o cinco etapas, según los autores, en el desarrollo histórico del campo del procesamiento del lenguaje natural.

Primera etapa: años 40 y 50. El procesamiento del lenguaje natural nace a finales de los años 40 en centros de investigación de EE. UU., Inglaterra, Francia y la entonces Unión Soviética. Sus inicios están vinculados a la aparición del computador en el plano tecnológico y la creación de la informática en el científico.

Los primeros ordenadores digitales surgieron durante la II Guerra Mundial: destacan Colossus (1943) en el Reino Unido, un ordenador de propósito específico, y ENIAC (1945) en EEUU, de propósito general, ambos utilizados para fines militares (descifrar mensajes en clave, efectuar cálculos balísticos, etc.) y diseñados para trabajar con números y no con palabras.

Segunda etapa: años 60 y 70. Hay una figura clave, que será el lingüista y pensador Noam Chomsky, que va a revolucionar el panorama lingüístico mundial al proponer una teoría del lenguaje que aboga por la formalización, inspirándose en los lenguajes artificiales de la lógica y las matemáticas: la gramática generativa, según la cual, con un número finito de reglas es posible generar los infinitos enunciados de una lengua. Los trabajos de Chomsky publicados en este período (*Syntactic Structures* en 1957 y *Aspects of a Theory of Syntax* en 1965)[9] van a dar un giro a la Lingüística Teórica, pero en lingüística computacional su verdadera influencia no se dejará sentir hasta los años 70.

Hubo especial interés en los siguientes sistemas:

- Resolución de problemas, en dominio restringido y mediante lenguaje natural que pudieran comunicarse con personas.
- Sistemas de diálogos de pregunta y respuesta, con una base de datos primitiva.

8 Marr, D., «Vision: A Computational Investigation into the Human Representation and Processing of Visual Information», W. H. Freeman and Co, San Francisco, 1982.

9 Chomsky, N., «Syntactic Structures», Mouton & Co., Berlin, 1957 y Chomsky, N., «Aspects of a theory of Syntax», MIT Press, Cambridge (MA), 1965.

- Consultas médicas, como en el caso del programa conocido como ELIZA, desarrollado por Weizenbaum en 1966. Es este sistema el que marcó un punto de inflexión. Aparentemente capaz de sostener una conversación similar a la que podrían mantener un psiquiatra y su paciente, no tiene en cuenta, sin embargo, el significado, sino que se basa en la identificación de palabras claves a las que están asociadas determinadas plantillas con posibles respuestas. Es decir, en realidad no existe un tratamiento del lenguaje, pero es uno de los programas que, mediante la ilusión de inteligencia que genera, más atención ha recibido, entre otras razones porque siempre genera una respuesta.

Tercera etapa: 1970-1984. Es esta una etapa de consolidación en la que se tratarán de paliar las deficiencias observadas en las anteriores. Al optimismo de las fases previas le sucede un período de realismo. Se toma conciencia de la complejidad del lenguaje y las investigaciones se diversifican para intentar cubrir todas sus facetas: sintaxis, semántica, pragmática, etc. Además, ante la dificultad de tratar el lenguaje en general, los trabajos se restringen a dominios concretos o sublenguajes: estructuras sintácticas y contenidos semánticos empleados en un campo temático muy limitado (bases de datos de rocas lunares de las misiones Apollo, bloques y figuras geométricas, etc.). Un único objetivo guiará a los investigadores de esta etapa: demostrar la viabilidad de la simulación computacional del lenguaje.

Cuarta etapa: la década de 1990. En general, se trata de un período de crecimiento y consolidación, con énfasis en la investigación básica, pero animado también por el logro de mejores sistemas y resultados a nivel práctico. Se vuelve a la lingüística como base teórica. Se desarrollan nuevos formalismos lógico-gramaticales: familia de gramáticas de unificación, inaugurada por la gramática de cláusula definida de Pereira y Warren (1980), a la que siguieron la gramática de estructura de frase generalizada, la gramática léxico-funcional, la gramática de unificación funcional, etc. Las teorías lingüísticas están pensadas específicamente para su implementación informática, debido a su inspiración en lenguajes de programación. También se retoman modelos descartados previamente, como los modelos de estados finitos, sobre todo en el nivel fonológico, morfológico y sintáctico.

Tendencias actuales. El PLN sigue actualmente en pleno apogeo y con perspectivas de futuro muy prometedoras. Las técnicas de procesamiento del lenguaje natural se aplican también al diseño de *chatbots*. Los *chatbot* son piezas de software diseñada para aplicaciones de mensajería instantánea y servicios de atención al cliente automatizados que interactúan con el usuario intentando comprender y satisfacer sus necesidades proveyendo acceso al servicio más adecuado en cada momento.

Productos presentes en la mayoría de teléfonos móviles, por ejemplo, se enfrentan a multitud de retos a la hora de interpretar el lenguaje hablado. La gran diversidad de idiomas y acentos, así como la necesidad de proporcionar una respuesta coherente en tiempo y forma adecuada hace que este tipo de soluciones no sean triviales.

La dificultad de consolidar las áreas de la inteligencia artificial

A pesar de los grandes propósitos y primeros desarrollos, no tardaron en aparecer las primeras críticas sobre los años 70, tanto en el ámbito filosófico como ético, en lo relativo a la simbiosis hombre-máquina o más específicamente entre mente-máquina. Este periodo que muchos han llamado el invierno de la IA, se prolongó durante unos 10 años. Como todo periodo gris, su resurgir se debió a que las aplicaciones que se fueron desarrollando, fundamentalmente en los sistemas expertos, tuvieron mucho éxito.

Muchos de los principales organismos tanto del Reino Unido como de Estados Unidos que habían financiado hasta la fecha proyectos directamente relacionados con la IA, recortarían significativamente estas partidas.

Sin embargo, en los últimos 10 o 15 años, los logros alcanzados en lo referente al reconocimiento de formas, la búsqueda de patrones de comportamiento a partir de la explotación masiva de datos (Big Data), la interpretación del lenguaje natural o la robótica han relanzado el interés y las inversiones en el campo se han incrementado notablemente. En la Unión Europea, por ejemplo, el vicepresidente responsable del mercado único digital, Adrus Ansip, considera necesaria la inversión de hasta 20.000 millones de euros en IA de aquí a 2020, principalmente en Big Data y robótica[10].

Evolución, logros y futuro

Evolución: nuevas estrategias de búsquedas y planificación

La planificación automática en IA apunta a secuencias ordenadas de acciones que alcanzan objetivos específicos que definimos como planes.

Los planes generados deben poder ser ejecutados por los agentes; de este modo, deben ser secuencias de acciones que un agente inteligente, robot o máquina pueda implementar.

10 Declaraciones de Andrus Ansip en el comunicado de la Comisión Europea «Inteligencia artificial: La Comisión presenta un enfoque europeo para impulsar la inversión y establecer directrices éticas» (Bruselas, 25 de abril de 2018). Disponible en http://europa.eu/rapid/press-release_IP-18-3362_es.pdf. Fecha de la consulta 10.07.2018.

«Desde principios de los años 70, la comunidad de IA especializada en planificación se ha ocupado del problema del diseño de agentes artificiales capaces de actuar en un entorno»[11]

En los últimos años, se ha empezado a imponer el criterio de que los sistemas planificadores deberían ser una pieza primordial de gran parte de los agentes inteligentes artificiales, especialmente si queremos que usen estructuras cognitivas de razonamiento.

La idea principal que subyace a este concepto es proporcionar a los agentes inteligentes la capacidad de representar el objetivo a alcanzar, para lo cual formalizan las acciones que pueden realizar y generan un modelo simbólico del entorno.

Logros: lógica difusa y aprendizaje

Lofti A. Zadeh, profesor de en la Universidad de Berkeley (California), introduce el concepto de Lógica Difusa sobre 1965[12]. En la lógica difusa, que sigue vigente actualmente, el procesamiento de la información se realiza de forma que los datos pueden presentar un grado de pertenencia parcial o total a conjuntos. Sobre los años 70 comienza a expandirse la aplicación de esta teoría, teniendo un fuerte impacto en los sistemas de control. Desde entonces, el número de aplicaciones industriales y su utilización en productos de consumo ha crecido exponencialmente. Un ejemplo clásico en sistemas de control es el problema del péndulo invertido, en el que se trata de mantener en equilibrio una barra rígida sobre una plataforma móvil que puede moverse en dos direcciones; derecha o izquierda. Queremos diseñar un controlador difuso que tomará como entradas el ángulo y la velocidad angular y dará como salida la velocidad de la plataforma.

La Lógica Difusa se asemeja habitualmente a cómo nos expresamos a veces de forma «vaga». Por ejemplo, cuando entramos en una habitación, decimos hace frío, o hace calor pero no hablamos por ejemplo en términos de la habitación está a la 22ºC o 38ºC, por ejemplo. Otro ejemplo similar podría ser cuando decimos, por ejemplo, que el horno está caliente o a alta temperatura.

La lógica difusa pretende simular el razonamiento humano, por lo que está basado en un sistema basado en conocimiento y reglas. Tiene además un marco matemático

11 Panagiotidi, S. y Vázquez-Salceda, J., «Norm-aware planning: Semantics and implementation», Proceedings of the 2011 IEEE/WIC/ACM international conferences on web intelligence and intelligent agent technology, vol. 3, Los Alamitos (CA), 2011. pp. 33-36.

12 Zadeh, L. A., «Fuzzy set». Information and Control, 8 (3), Cambridge (MA), junio 1965. p. 338–353.

que le permite modelar la incertidumbre que se presenta en muchos procesos cognitivos y poderlo tratar en el computador.

La lógica difusa ha ido evolucionando y a principios de los 80 Zadeh presenta el concepto de Razonamiento Aproximado y otros componentes que acabarían formando el cuerpo de la lógica difusa. Para ello se proponen los conjuntos difusos, que van a permitir el manejo cuantitativo de conceptos cualitativos.

Mediante el uso de conjuntos difusos y reglas es posible dotar de significado matemático a proposiciones como »esta casa es pequeña», »Juan es muy bajo» o »el crecimiento es rápido» utilizando los modificadores lingüísticos (muy, poco, demasiado, algo, extremadamente, etc.) para adaptar los calificativos a lo que se quiere decir.

Actualmente hay especial interés en todo lo relacionado con el aprendizaje. En este sentido han aparecido términos asociados con esta línea de trabajo como aprendizaje automático. El aprendizaje automático, también conocido como *machine learning*, puede dividirse en algoritmos de *aprendizaje supervisado* y algoritmos de *aprendizaje no supervisado*. El aprendizaje supervisado utiliza ejemplos conocidos para obtener las inferencias mientras que el aprendizaje no supervisado no dispone de ejemplos con un objetivo o etiqueta conocido.

Futuro

Las soluciones basadas en IA ya son una realidad. Aunque son muchas las universidades y centros de investigación que siguen aportando avances en el campo de la IA, hay nuevos competidores del sector empresarial y tecnológico. En este sentido, compañías tecnológicas como Microsoft, Google o Facebook, deben parte de su éxito al desarrollo de algoritmos basados en IA. También se trabaja cada vez más con el concepto de computación cognitiva. A nivel empresarial, el objetivo principal de la computación cognitiva es apoyar el proceso de toma de decisiones presentando el conocimiento necesario en el momento oportuno de la forma adecuada. Gracias a estas aplicaciones, las compañías pueden diferenciar sus productos y servicios y obtener ventaja sobre sus competidores.

Una de las principales necesidades es proporcionar a la máquina contexto sobre el entorno y el objetivo a conseguir. Por este motivo, las soluciones cognitivas deben hacer uso de un volumen de información muy amplio y diverso, surge aquí la relación entre la computación cognitiva y el paradigma *Big Data*.

La gran disponibilidad de datos, la reducción del coste de almacenamiento y las mejoras tecnológicas que permiten procesar grandes volúmenes de datos a altas velocidades han impulsado este tipo de soluciones.

Un sistema cognitivo se compone fundamentalmente de tres principios fundamentales:

- Aprendizaje: el sistema debe ser capaz de aprender en base a un conjunto de observaciones y realizar predicciones sobre un dominio concreto.
- Modelado: el aprendizaje toma como base la representación de un modelo y un conjunto de reglas de inferencia.
- Generación de hipótesis: un sistema cognitivo debe asumir que no existe una única respuesta válida. Es decir, un sistema cognitivo es un sistema probabilístico capaz de emitir varias respuestas dando una probabilidad a cada una de ellas.

Estos tres principios fundamentales se basan todos en el almacenamiento, catalogación y uso eficiente de datos que guían la toma de decisiones. Los sistemas cognitivos se encuentran todavía en una fase de desarrollo incipiente. El desarrollo de este tipo de productos involucra aspectos provenientes de otras disciplinas técnicas como el aprendizaje automático, el procesamiento de grandes volúmenes de datos, el Internet de las cosas, el procesamiento del lenguaje natural, el razonamiento probabilístico, la visualización, etc.

La computación cognitiva en particular y la inteligencia artificial en general implican un cambio brutal en el día a día de la empresa. El primer reto por afrontar es un reto cultural. Todos los empleados deben adaptar su día a día a las nuevas herramientas disponibles y focalizarse en aquellas tareas donde realmente son necesarios.

A nivel organizativo, la dirección de la empresa es responsable de impulsar los cambios estructurales adecuados para permitir un ecosistema basado en la innovación. El cambio es lo único permanente y, por tanto, el cambio debe ser contemplado con naturalidad y gestionado de forma adecuada.

Una de las soluciones estrella en el ámbito cognitivo es el archiconocido sistema Watson de IBM. El «gigante azul» basa parte de su futuro en los resultados conseguidos por este producto, proyecto al que ha dedicado y dedica cantidades ingentes de dinero y una importante campaña de marketing.

Watson es capaz de responder de forma directa a preguntas formuladas en lenguaje natural. Para ello se apoya en cantidades ingentes de información de muy diversas fuentes de procedencia.

A nivel empresarial, el objetivo principal de la computación cognitiva es apoyar el proceso de toma de decisiones presentando el conocimiento necesario en el momento oportuno de la forma adecuada. Gracias a estas aplicaciones, las compañías pueden diferenciar sus productos y servicios y obtener ventaja sobre sus competidores.

Estos son algunos ejemplos del futuro más inmediato que ya casi forman parte del presente. La velocidad de cambio es vertiginosa en nuestros días, y las tecnologías disruptivas son una realidad. Tener maquinas capaces de desenvolverse en un entorno, aprender, tomar decisiones es ya posible. Como se describía al comienzo del capítulo,

las inquietudes del ser humano allá por el año 300 a. C. probablemente hayan sido muy parecidas a lo largo de los siglos, en tanto en cuanto la idea era, por ejemplo, automatizar tareas, liberar al ser humano de actividades tediosas o desarrollar robot humanoides que sirvan de acompañamiento.

Hoy, la capacidad del computador, la evolución del software y la apuesta firme de las grandes tecnológicas aseguran un futuro de lo más incierto pero tremendamente interesante.

Conclusiones

La idea fundamental de esta capítulo ha sido proporcionar al lector una breve perspectiva de la evolución de la IA. Como se ha podido comprobar, los campos son diversos y, bien de forma independiente o combinados, la técnica actualmente ya permite resolver muchos problemas, algo inimaginable hace pocos años aunque conviene recordar que los comportamientos inteligentes se dan en ámbitos muy especializados o muy definidos.

En estos entornos la máquina supera al ser humano. Pero la ambición va más allá y lo que se pretende es lograr una máquina con inteligencia de tipo general similar a la humana.

Para lograr esta máquina equiparable al humano hay un factor determinante que es la integración de diferentes agentes que proporcionan razonamiento, capacidad de planificación, aprendizaje, o la interpretación del entorno. Cada vez más se estudian también los procesos creativos en el ser humano y se plantea la posibilidad de si se podrían desarrollar verdaderos robots-artistas[13], dejando por tanto abierta la vertiente filosófica.

13 Existen varias experiencias que relacionan la IA con generación de obras de arte. Por poner un ejemplo en el campo de la música, SaxEx (http://www.iiia.csic.es/Projects/music/Saxex.html) es un sistema capaz de generar ejecuciones de solos de baladas de jazz con distintos tipos de expresividad (alegre, triste, etc.) basándose en ejemplos de músicos humanos con un sistema de razonamiento basado en casos (López de Mantaras, R. y Arcos, J. L., «AI and Music: From Composition to Expressive Performance», AI Magazine (23) 3, Palo Alto (CA), 2002). En el campo de la pintura The Next Rembrandt (https://www.nextrembrandt.com/) es un proyecto de IA en el que, a partir de un estudio de las pinturas de Rembrandt (escenarios, rostros, colores, condiciones de luz, vestimenta, pinceladas, etc.) es capaz de generar un «nuevo Rembrandt» e incluso imprimirlo mediante una impresora 3D para simular la pincelada.

Capítulo 2

Situación y perspectivas de las tecnologías y aplicaciones de inteligencia artificial

Gonzalo León Serrano

Resumen

Este capítulo tiene como objetivo principal revisar el estado actual de las tecnologías relacionadas con la inteligencia artificial (IA) y sus principales campos de aplicación. Ello permite valorar cómo los principios y conceptos de IA introducidos en el capítulo 1 están empleándose en la práctica y sus potenciales consecuencias en diversos ámbitos de la sociedad.

Los anuncios de nuevos dispositivos TIC, de sistemas software y de aplicaciones innovadoras basadas en el empleo de soluciones de IA se suceden diariamente. Tanto las entidades públicas y privadas como sectores económicos en su conjunto están siendo afectados de forma muy intensa por la penetración masiva de soluciones y tecnologías basadas en la IA; obviamente, los sectores de defensa y seguridad también se han visto afectados (y se verán aún más afectados en el futuro).

Se revisa la situación y evolución previsible de tecnologías específicas de IA como el aprendizaje de máquinas, procesamiento de lenguaje natural, computación cognitiva, hardware inteligente, computación neuromórfica y aplicaciones en relevantes dominios como la robótica inteligente o el impacto en el empleo. La presentación de datos recientes sobre las inversiones en IA y la creación de nuevas empresas de base tecnológica complementan la visión global desde la perspectiva del mercado. En los casos en los que ayuda a comprender las consecuencias en el mercado o la sociedad, se han incluido diversos ejemplos, también del ámbito de defensa; incluso, con una visión futurista de posibles escenarios en 2030 y 2040.

Palabras clave

Tecnología, inteligencia artificial, aprendizaje de máquinas, procesamiento de lenguaje natural, computación cognitiva, hardware inteligente, robótica inteligente, mercado e inversiones en IA, defensa y seguridad.

Situation and perspectives of the technologies and applications of artificial intelligence

Abstract

This chapter has as the main objective to review the status of techniques based on artificial intelligence (AI) and its main application domains. This analysis constitutes the basis for understanding the way that basic concepts and principles of AI presented in chapter 1 are in use today, and their potential consequences in society.

The announcements of new ICT devices, software systems and innovative applications based on AI solutions, appear every day. Both public and private entities and economic sectors as a whole are being disrupted by the massive penetration of artificial intelligence technologies and solutions; obviously, the defense and security sectors are also deeply affected (and they will be even more impacted in the future).

This chapter reviews the situation and possible evolution of technologies like machine learning, natural language processing, cognitive computing, intelligent hardware, neuromorphic computing, and very relevant areas like intelligent robotics or the impact on employment. Recent data from the investments in AI and the creation of new start-ups complement the vision from the market perspective. In those cases when it was considered useful to visualize the consequences on the market and society, several examples were introduced, even from the Defence sector, as well as with a futuristic vision of possible scenarios for 2030 and 2040.

Keywords

Technology, artificial intelligence, machine learning, natural language processing, cognitive computing, intelligent hardware, intelligent robotics, market and investments in AI, defence and security.

«El día que la inteligencia artificial se desarrolle por completo podría significar el fin de la raza humana. Funcionará por sí sola y se rediseñará cada vez más rápido. Los seres humanos, limitados por la lenta evolución biológica, no podrán competir con ella y serán superados.»

Stephen Hawking (1942-2018), astrofísico (entrevista en la BBC)

«La inteligencia artificial alcanzará los niveles humanos alrededor de 2029 (lo que se conoce como Singularidad), pero un poco más adelante, en 2045, habremos multiplicado la inteligencia biológica humana mil millones de veces».

Ray Kurzweil (1948-), futurista, Director de Ingeniería de Google

Objetivos

Alrededor de la Inteligencia artificial (IA) se ha configurado una disciplina científica y tecnológica cuyo desarrollo está generando un conjunto de técnicas aplicables al desarrollo de productos y servicios disruptivos en múltiples sectores de la sociedad. Además, su impacto en la evolución de otras tecnologías del ámbito de la información y las comunicaciones (TIC) como sucede con el diseño de novedosas arquitecturas de ordenadores, y su incorporación a multitud de productos y servicios de consumo en todos los sectores hace que se considere a la IA como una de las fuentes de disrupción socioeconómica más importantes.

El objetivo del presente capítulo es describir brevemente el estado actual de las tecnologías y aplicaciones relacionadas con la IA existentes y su previsible evolución en los próximos años, así como ofrecer una panorámica de su aplicación en diversos ámbitos aún sin pretender ser exhaustivos. El énfasis del presente capítulo se centrará en la descripción de la tecnología y sistemas tecnológicos de la IA, y no tanto en describir las bases científicas de la misma que ya han sido cubiertas en el capítulo precedente. Aunque la descripción de las tecnologías de IA en el presente capítulo se realizará al margen de su aplicación al sector de la defensa y seguridad, sí se enfatizarán aquellas tecnologías y aplicaciones sobre ellas que tienen ya o puedan tener muy próximamente un nivel de aplicación mayor en las Fuerzas Armadas. Conviene, en todo caso, aclarar la terminología empleada puesto que el concepto de *«inteligencia artificial»* integra ámbitos como el del aprendizaje automático (o un tipo del mismo como el «aprendizaje profundo» basado en redes neuronales), la robótica inteligente, el procesamiento de lenguaje natural, la percepción inteligente (vía el procesamiento visual o acústico), la computación neuromórfica, etc. que refleja, por un lado, un amplio conjunto de técnicas asociadas y áreas de aplicación y, por otro lado, la inexistencia de un marco consolidado en el que encajen todas esas piezas.

Coloquialmente hablando (partiendo de una definición extraída de «Wikipedia» para no expertos), el término «*inteligencia artificial*» se aplica cuando «*una máquina imita las funciones «cognitivas» que los humanos asocian con otras mentes humanas, como, por ejemplo: «aprender» y «resolver problemas»*. En parecidos términos, aunque de una manera un poco más concreta, existen definiciones de inteligencia artificial como la que la reduce a un «*programa de computación diseñado para realizar determinadas operaciones que se consideran propias de la inteligencia humana, como el autoaprendizaje*»[1]. En todo caso, se trata de disponer de sistemas informáticos que puedan realizar funciones «*como las haría un ser humano*». Desde un punto de vista práctico la IA supone la utilización, principalmente, de técnicas estadísticas y algebraicas que, utilizando lenguajes y sistemas informáticos, son capaces de obtener información de datos capturados y generados.

A partir de esa definición, se derivan otras aplicables a técnicas de IA concretas. Un ejemplo de gran trascendencia como tecnología base es el denominado «*aprendizaje automático*» (o *aprendizaje de máquinas*) en el que se trata de crear mediante un proceso de inducción del conocimiento programas capaces de generalizar comportamientos a partir de una información suministrada en forma de ejemplos; es decir, sistemas que aprenden de lo que ocurre a su alrededor. Esa capacidad de aprendizaje se usa para tareas muy distintas: reconocer patrones visuales (como caras u objetos en escenas complejas), auditivos (como identificar voces de personas y su significado), situaciones de peligro (como identificar peatones en una carretera), etc. en el mismo sentido, aunque no de la misma manera a cómo lo hace el cerebro humano[2].

Específicamente, se desea describir la interacción de las herramientas básicas de la IA con otras tecnologías a las que apoya decisivamente para generar aplicaciones (aunque formalmente sean diferentes) con un nivel interno de «inteligencia» muy superior al que ha sido habitual hasta el momento. Mencionemos las siguientes tecnologías en las que la IA juega un papel relevante:

- *Big data* en el que los algoritmos de análisis extraen información no trivial a partir del procesamiento de grandes volúmenes de datos obtenidos de diversos modos. El rol de la IA en todas estas aplicaciones está en, una vez que los datos han sido limpiados y preparados, extraer patrones que pueden servir para describir la población objetivo o incluso para predecir comportamientos basándose en el comportamiento pasado.

1 Podría denominarse «inteligencia natural» a la que se asocia al ser humano (y posiblemente a algunos animales).

2 Para algunos investigadores el término de «machine learning» incluye áreas de IA fuertemente influidas por el concepto de «aprendizaje de máquinas» como visión por computador, comprensión de voz y procesamiento de lenguaje natural, e incluso partes de robótica. En este capítulo se considerarán como áreas de aplicación.

- Mecatrónica y sensorización en el que sensores de diversos tipos permiten capturar información del entorno y reconocer la situación en la que se encuentran, como sucede en el caso del vehículo autónomo para detectar obstáculos u otros vehículos.
- Robótica en el que el comportamiento de los robots se hace inteligente interactuando con el entorno vía sensores, actuadores y dotados de capacidad para la toma de decisiones, como sucede con robots empáticos antropomórficos en el acompañamiento de ancianos.
- Toma de decisiones (decision-making) a partir de la fusión de datos e información estructural (en tiempo real o almacenados previamente) en un dominio concreto aplicando algoritmos evolutivos como sucede en sistemas de enseñanza auto-adaptados al ritmo y características de aprendizaje del alumno.
- Computación neuromórfica en el que la arquitectura interna de nuevos circuitos electrónicos mimetiza la forma de trabajar del cerebro permitiendo una realización de tareas más eficiente como una nueva generación de procesadores masivamente paralelos.
- Percepción por ordenador incluyendo la visión artificial en la que un sistema informático es capaz de reconocer un objeto entre muchos (aprendiendo por sistema de generalización y prueba y error) u oído artificial (aprendiendo a escuchar un ruido, una frase, interpretarla en un contexto, conocer su semántica, y un determinada locutor u origen del ruido) como sucede con vehículos autónomos.

Todas estas áreas tienen aplicaciones civiles y militares dependiendo, por ejemplo, del origen de los datos (p. ej. de posicionamiento de fuerzas o blindados en tiempo real), del tipo y uso de los sensores empleados (p. ej. de NBQ), de la finalidad de los robots (p. ej. de exploración en terrenos minados), o de las características del entorno que se desee interpretar (p. ej. de un campo de batalla). Se trata de *tecnologías duales* cuyos catalizadores de inversión y desarrollo están modulados tanto por mercados de amplio espectro (teléfonos inteligentes) como de nicho (sistemas de armas).

Tecnologías básicas de inteligencia artificial

El presente capítulo se centra en el ámbito tecnológico y no científico. Téngase en cuenta que un producto o servicio complejo suele ser *multitecnológico* (es decir, se diseña y construye integrando diversas tecnologías); algunas de las tecnologías incorporadas jugarán un papel esencial en la función requerida del producto o servicio en cuestión y otras serán meramente auxiliares. No obstante, la funcionalidad global y su penetración

en el mercado están generalmente ligadas a la forma en la que las tecnologías empleadas se complementan mutuamente y permiten cubrir las necesidades del usuario, aunque para un usuario concreto o para una aplicación determinada alguna tecnología tenga más importancia que otra.

*En el ámbito de la IA es obvio que para que un **vehículo autónomo** o un **robot antropomorfo** puedan aplicarse a un ámbito concreto es necesario integrar tecnologías de IA con otras muchas procedentes de otras disciplinas: si no dispone de sensores adecuados no podrá obtener información del entorno y sus algoritmos por muy potentes que sean no podrán interpretarlo para tomar decisiones; pero si no dispone de fuentes de energía no podrá ser tampoco autónomo. Es la integración entre todas las tecnologías las que permite que realice su función en un ámbito de aplicación determinado.*

Básicamente, se reconocen cinco grandes áreas tecnológicas básicas alrededor de la IA:

- *Aprendizaje automático* (*machine learning*) incluyendo el *aprendizaje profundo* (*deep learning*) como un subcampo del mismo que se ha beneficiado del desarrollo de las *«redes neuronales artificiales»*, de algoritmos de inducción y de algoritmos genéticos.
- *Procesamiento de lenguaje natural* (*natural language processing*, NLP).
- *Razonamiento* (técnicas empleadas para la planificación, toma de decisiones y razonamiento probabilístico y de minería de datos).
- *Sistemas expertos y simbólicos* (programación basada en reglas) desarrollados hasta los años ochenta pero habiendo perdido hoy gran parte de su vigencia e interés.
- *Percepción* (sistemas de reconocimiento y regeneración de la realidad).

Algunos autores incluyen como tecnologías específicas de IA algunos ámbitos de aplicación como la robótica o la computación neuromórfica, pero, en nuestra opinión, son, simplemente, ámbitos de aplicación muy relevantes resultantes de la combinación de algunas de las técnicas básicas mencionadas junto a la mecatrónica y la microelectrónica[3]. La combinación de todas ellas permite generar sistemas basados en IA que ayudan a razonar y tomar decisiones en un dominio concreto como lo haría una persona (generalmente en ámbitos mucho menos amplios y con mayores restricciones de contexto).

3 Para evitar confusión con el término más general de IA, se prefiere usar el término «Inteligencia artificial General» (o IA fuerte) para referirse a la inteligencia a nivel humano capaz de abstraer conceptos a partir de una experiencia limitada y transferir conocimiento entre dominios. Se diferencia de la IA débil formada por sistemas informáticos diseñados para una tarea específica.

El *aprendizaje automático* ha vuelto a adquirir mucha atención en los últimos años puesto que una de sus áreas de aplicación es el «*reconocimiento de patrones*» («*pattern recognition*»). Es una de las áreas de mayor interés práctico del aprendizaje automático en la que están apareciendo diversos sistemas comerciales y pre-comerciales en ámbitos limitados:

- El reconocimiento, procesamiento y generación de lenguaje natural (texto o voz) que ha derivado en la comercialización de «asistentes personales» más inteligentes; ahora incorporados de forma rutinaria en teléfonos inteligentes de bajo coste;
- El reconocimiento de objetos (en tiempo real, en imágenes o videos) decisivo para el desarrollo del vehículo autónomo. Le permite saber dónde está en la carretera y qué tiene delante o detrás como base para acelerar, frenar o cambiar de carril;
- El reconocimiento de conductas: intentado interpretar conductas reales frente a patrones predefinidos. Su importancia en RR.HH (p. ej. para la selección de personal) es muy relevante.

A finales de 2010 estas técnicas aceleraron su desarrollo con la aparición del «aprendizaje profundo» cuyo objetivo es el estudio y construcción de sistemas de cómputo capaces de «aprender» a partir de la experiencia, inspirándose ligeramente en algunos principios del funcionamiento del cerebro animal. A este tipo de aprendizaje automático se le llama «*profundo*» porque presenta una estructura jerárquica que extrae diferentes niveles de detalle de los datos en cuestión hasta lograr su objetivo. Un sistema de aprendizaje profundo debe ser «*entrenado*» a partir de una gran cantidad de ejemplos conocidos (en principio, cuantos más ejemplos se emplee, mejor será el funcionamiento). Así actúan los sistemas que permiten reconocer un animal o persona entre un conjunto de objetos y el estado de ánimo del mismo[4].

También se ha avanzado mucho en la representación abstracta del conocimiento de dominios (ámbito de las ontologías): una *ontología* define los términos y las relaciones básicas para la compresión de un área del conocimiento, así como las reglas para poder combinar los términos para definir las extensiones de este tipo de vocabulario controlado.

Todas las técnicas mencionadas tienen aún limitaciones (como sucede con los sesgos en la identificación de patrones con consecuencias culturales o las dificultades de reconocer una persona de un maniquí en medio de una aglomeración). Pero la mejora continua de los algoritmos reducirá estas limitaciones de mejor manera a como

4 Si bien esta técnica ha tenido gran utilidad en algunas aplicaciones muy específicas (reconocimientos de imagen), su uso se ha reducido porque es posible aplicar técnicas más sencillas con resultados similares.

lo hace normalmente una persona (que, por cierto, también tiene sesgos y tampoco reconoce fácilmente maniquíes en medio de una manifestación, a no ser que se le entrene).

Sistemas y herramientas de inteligencia artificial

El desarrollo de aplicaciones de IA requiere, como sucede en otros ámbitos, disponer de herramientas que ayuden a diseñar sistemas para resolver problemas complejos en dominios concretos. Vamos a considerar cuatro tipos de herramientas y sistemas: lenguajes específicos para IA, entornos de desarrollo de aplicaciones, computación cognitiva y hardware inteligente.

Lenguajes específicos para la inteligencia artificial

Hace décadas se popularizaron los lenguajes basados en reglas (p.ej. PROLOG, OPS5 o LISP) que sirvieron de base para el desarrollo de los denominados «sistemas expertos» empleados en el siglo pasado; sin embargo, las esperanzas depositadas en ellos no se cumplieron (véase el capítulo 1 de esta monografía) aunque tras un paréntesis han renacido lenguajes derivados de la denominada «*programación declarativa*». Se trata de un paradigma de computación en el que se definen los objetivos y es el sistema el que debe hallar la sucesión de tareas para afrontarlo. Para ello, se recurre a abstracciones matemáticas que permitan expresar y abarcar de un modo declarativo las casi infinitas situaciones físicas con las que se podrían encontrar sin tener que establecer un conjunto muy largo de «reglas».

Actualmente muchas de las aplicaciones de IA se programan en lenguajes como R, Python o incluso Java, que no pueden considerarse lenguajes específicos de inteligencia artificial. No obstante, surgen muchos nuevos para aplicaciones o dominios concretos, incluso por empresas alejadas de la informática. Uno de ellos es *Pyro*, lanzado por la empresa Uber pensando en aplicaciones de optimización de flotas y rutas. Probablemente, seguirán surgiendo lenguajes especializados para tipos de aplicaciones de IA en el futuro, al igual que ocurre con otros ámbitos de la informática buscando la mayor facilidad en expresar los conceptos necesarios en un dominio de aplicación particular.

Entornos de desarrollo de la inteligencia artificial y computación cognitiva

Más importante que el lenguaje de programación (y las herramientas software directamente ligadas al mismo como son los editores inteligentes, compiladores o depuradores) se debe disponer de un conjunto integrado de herramientas para el desarrollo de aplicaciones de IA al que se denomina comúnmente *«entorno de desarrollo»*. Estos sistemas dotados de mayor inteligencia (cognitivos), actúan como base para la generación de un *«sistema de apoyo a la decisión»* cuyo objetivo es adoptar mejores decisiones basadas en los datos disponibles en el dominio que se considere.

Tras dos décadas de trabajo académico, los *sistemas comerciales basados en computación cognitiva* comienzan a utilizarse en entornos empresariales y científico-técnicos en los que la toma de decisiones se beneficia del acceso y análisis de grandes volúmenes de datos, de la interacción en lenguaje natural y de la capacidad de inferencia. Combinados con el uso de nuevas tecnologías informáticas (no de IA) como son los ***«servicios en la nube»*** («cloud») estos sistemas comerciales permiten además virtualizar dónde se encuentra físicamente la información, facilitando su uso desde cualquier dispositivo o contexto geográfico.

Hoy día, existen múltiples herramientas comerciales de este estilo como «*Google Prediction*» o *«Tensor Flow»* que hace uso de estas técnicas a partir de un uso predictivo de técnicas estadísticas, o los productos de singular (https://sngular.team/capacidades/cognitive-computing/) empleando técnicas de minería de datos. En septiembre de 2017, Google presentó oficialmente el sistema «*Google Neural Machine Translation*», que utilizaba aprendizaje profundo para producir mejores traducciones entre diferentes lenguajes. Inicialmente, dicho sistema permitía traducciones entre chino e inglés, expandiéndose de forma progresiva a los más de 103 lenguajes que actualmente soporta *«Google Translate»*[5].

El sistema Watson desarrollado por IBM representa uno de los primeros productos del nuevo enfoque de «computación cognitiva» disponibles en el campo comercial[6]. (http://www.ibm.com/smarterplanet/us/en/ibmwatson/). Se trata de acercarse a la forma en la que el cerebro humano recibe, procesa y toma decisiones con información procedente de los cinco sentidos.

5 Google Neural Machine Translation no utiliza el inglés como un «puente» para traducir entre castellano y coreano. En su lugar, las redes neuronales del sistema son capaces de establecer conexiones entre conceptos y palabras que no han sido relacionadas por sus programadores. El sistema de Google, por lo tanto, produce un lenguaje propio de forma interna empleado para representar diferentes conceptos y, posteriormente, utilizarlo como nexo entre los diferentes lenguajes. Un avance en inteligencia artificial que sorprendió incluso a los responsables de Google. https://hipertextual.com/2016/11/lenguaje-inteligencia-artificial-google.

6 Dharmendra Modha, Manager del Área de Cognitive Computing de IBM, indicaba que *«no buscaban construir un cerebro, sino inspirarse en este órgano para desarrollar nuevos avances informáticos»*.

El éxito mediático del sistema Watson al participar en el concurso televisivo «*Jeopardy*» en EE. UU. y obtener mejores resultados que sus oponentes humanos supuso un hito al ser capaz de responder a preguntas en lenguaje natural (incluso con dobles sentidos). En ese concurso Watson no estaba conectado a Internet; accedía a datos almacenados en forma de conocimiento no estructurado.

Utilizando tecnologías de «machine learning», análisis estadístico y procesamiento de lenguaje natural para encontrar las claves de cada pregunta, Watson comparaba posibles respuestas, estimaba la exactitud de las mismas y respondía en menos de 3 segundos. Ese éxito permitió explorar aceleradamente su uso en otros dominios profesionales como el diagnóstico médico (cáncer), finanzas (inversiones empresariales en entornos de incertidumbre), o toma de decisiones en sistemas complejos (como la optimización de exploraciones petrolíferas). Se aprovecha, asimismo, del incremento paulatino de la capacidad de cálculo, acceso y almacenamiento de los sistemas informáticos actuales.

La figura 1 esquematiza este concepto de aprendizaje empleado. Como se puede ver, el uso requiere una fase previa de «aprendizaje» en el que múltiples preguntas permiten al sistema construir una «tabla de la verdad» en un dominio concreto sobre la que después, en la fase de uso, puede inferir respuestas a otras preguntas que se le formulen por el usuario.

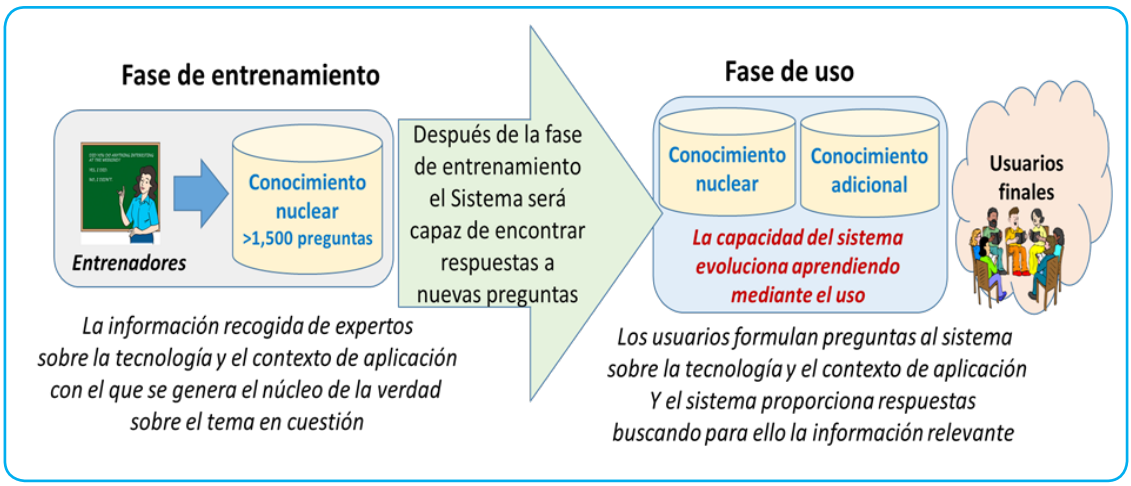


Figura 1. Uso de un sistema cognitivo en la práctica. (Fuente: elaboración propia).

La evolución del conjunto de herramientas que constituye el «*ecosistema Watson*» (servicios y herramientas BLUEMIX) ha permitido su uso en la «nube» y la capacidad de utilizar un conjunto de herramientas para desarrollar aplicaciones para dominios concretos. Actualmente, Watson dispone de un conjunto de herramientas e interfaces hombre máquina para los *desarrolladores* que permiten la generación de aplicaciones «*basadas en Watson*» (empleando servicios BLUEMIX) para diferentes dominios.

Este mismo enfoque se está complementando desde un punto de vista más científico en grandes proyectos internacionales como «Human Brain Project (HBP), financiado

por la Unión Europea (https://www.humanbrainproject.eu/) en el que la ingeniería inversa del cerebro permitiría potencialmente generar herramientas cognitivas mucho más poderosas basadas en el desarrollo de arquitecturas de computación radicalmente diferentes.

Hardware inteligente

Otro ámbito en el que se está produciendo una rápida evolución es el de la *microelectrónica específica para IA*. Los mayores fabricantes de chips enfocados exclusivamente a la Inteligencia artificial se han aliado en los últimos días para la investigación y desarrollo de sus nuevos procesadores[7]. En algunos casos, han introducido variaciones en las arquitecturas convencionales de unidades de procesamiento (CPU) para que puedan emplearse en aplicaciones como la identificación de patrones. Intel[8] ha informado en agosto de 2018 que la empresa ha modificado sus CPUs para ser 200 veces más efectivos en aplicaciones de reconocimiento de patrones. Ello le ha permitido superar el billón de dólares de ventas en 2017 de su procesador Xeon.

En otros casos, las empresas han tratado de diseñar circuitos específicos para IA. Veamos algunos de los circuitos integrados específicos existentes en el mercado (no se pretende ser exhaustivo):

- Huawei: Karin 970. Es el primer y por ahora único microchip para «Smartphone» con IA incluida en el hardware. La gran diferencia es que no precisa de conexión a internet para realizar las mismas tareas que la competencia. Es capaz de procesar 2000 imágenes en un segundo (lo habitual es un 90 % menos) y la IA aumenta hasta en un 50 % su batería al decidir en qué aplicar la energía y cuándo.
- Qualcomm: Snapdragon 845: se ha aplicado IA para triplicar el rendimiento en el procesamiento de imágenes y vídeo y en realidad aumentada y virtual. También mejora los sistemas de identificación biométrica, como el reconocimiento facial, de iris y el lector de huellas dactilares). Qualcomm Artificial Intelligence Engine, un motor que cuenta con componentes de hardware y software capaz de ofrecer experiencias de inteligencia artificial a los dispositivos móviles con procesadores Snapdragon. Los componentes del motor de IA de Qualcomm contienen componentes centrados en software, como un motor de procesamiento neuronal (*Snapdragon Neural Processing Engine*).

7 Don Monroe (2018). Chips for Artificial Intelligence. Communications of the ACM, April 2018, Vol. 61 No. 4, Pages 15-17.

8 https://www.reuters.com/article/us-intel-tech/intel-sold-1-billion-of-artificial-intelligence-chips-in-2017-idUSKBN1KT2GK.

- Intel Loihi. ha presentado un chip de inteligencia artificial basado en este sistema de neuronas artificiales: Loihi. Ahora mismo Loihi tiene 1.024 neuronas artificiales, unas 130.000 neuronas simuladas con 130 millones de conexiones sinápticas. https://omicrono.elespanol.com/2017/09/intel-chip-inteligencia-artificial-cerebro-humano/

- Baidu, competidor de Amazon, ha presentado un chip de inteligencia artificial denominado *«Kunlun»* (véase figura 2). Está optimizado para diversas tareas de inteligencia artificial, como reconocimiento de voz y facial, procesamiento de lenguaje natural, reconocimiento de imágenes y conducción autónoma (https://www.xataka.com/robotica-e-ia/baidu-google-chino-tiene-listo-su-primer-chip-inteligencia-artificial-conquista-china-mundo) .

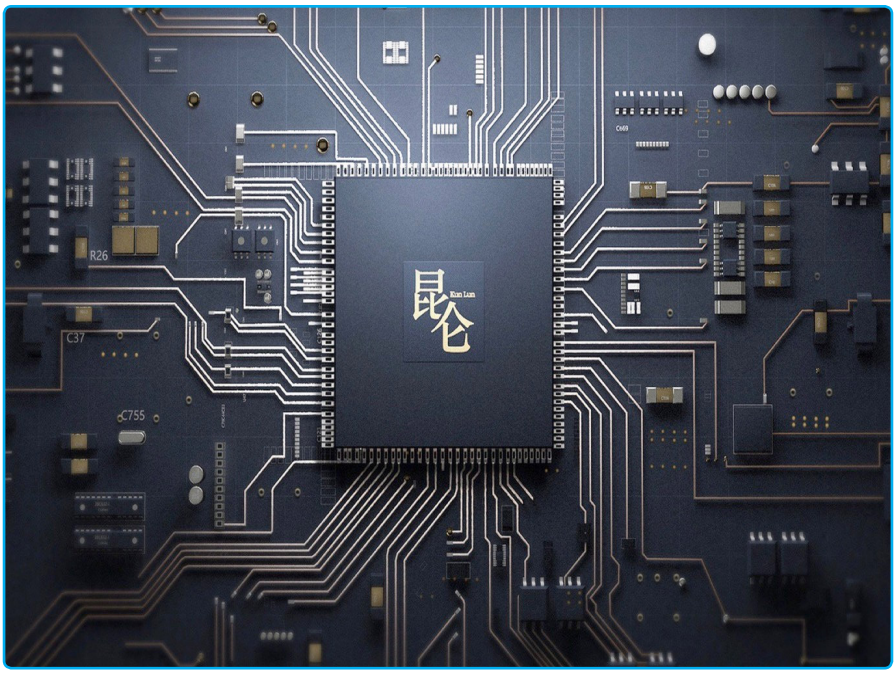


Figura 2. Chip Kunlun de Baidu.

Aunque el chip no estará disponible en volumen hasta 2019 su importancia radica en que es el primer circuito integrado de inteligencia artificial diseñado y fabricado en China. Con ello tanto Europa como EE. UU. pierden una de las ventajas competitivas que aún poseían en IA (significativo es que Baidu quiere agrupar a todas las compañías chinas relacionadas con la inteligencia artificial para así crear **una sola fuerza que no dependa de Estados Unidos).**

- Samsung Electronics unió fuerzas con las principales universidades surcoreanas, como la Universidad Nacional de Seúl y KAIST, para desarrollar un chip neuromórfico, un semiconductor de inteligencia artificial (IA) de última generación que imita funciones del cerebro humano, y puede ser usado

en coches eléctricos y autónomos del futuro[9]. El chip neuromórfico es un semiconductor de nueva generación que imita los nervios del cerebro humano y puede realizar funciones de inteligencia artificial como el procesamiento de datos no estandarizados, como imágenes y sonidos.

- IBM TrueNorth se refiere a una línea de chips producidos por IBM a partir de un Proyecto financiado por DARPA desde 2008. El primer chip de IBM fue presentado en 2014. Desde entonces ha pasado de tener 256 neuronas por chip a 260 millones de neuronas artificiales. Con ello está cerca de equipararse al procesamiento de datos del cerebro de una abeja. http://www.research.ibm.com/articles/brain-chip.shtml.

IBM está trabajando ahora con la Fuerza aérea de EE. UU. para mejorar su línea de chips TrueNorth diseñados para optimizar las prestaciones de modelos de aprendizaje automático a nivel hardware. Los circuitos se han diseñado de tal manera que los investigadores pueden ejecutar una única red neuronal sobre múltiples conjuntos de datos o múltiples redes neuronales sobre un único conjunto de datos. Esta visión puede ser útil en aplicaciones de satélites o vehículos autónomos.

El crecimiento de este mercado ha hecho que los principales fabricantes de chips enfocados exclusivamente a la Inteligencia artificial se hayan aliado en los últimos días para la investigación y desarrollo de sus nuevos procesadores. Las empresas en cuestión son HiSilicon, Cambricon Technologies, Horizon Robotics y DeePhi Tech, que se posicionarán en grupo junto a otro de los grandes del sector: TSMC[10].

Áreas tecnológicas en las que la inteligencia artificial constituye un elemento clave

Existen múltiples áreas de aplicación de la IA y no es posible desarrollar todas ellas en el presente capítulo. El objetivo será el de revisar algunas de ellas desde un punto de vista de aplicaciones novedosas que demuestren hasta dónde ha alcanzado el

9 https://www.hibridosyelectricos.com/articulo/tecnologia/samsung-desarrolla-chips-inteligencia-artificial-imitar-cerebro-humano/20180124120255017028.html.

10 https://elchapuzasinformatico.com/2018/01/los-principales-productores-chips-inteligencia-artificial-se-alian-tsmc/.

desarrollo. Evidentemente, no se trata de ser exhaustivo, pero se ha intentado que los ejemplos empleados puedan despertar en el lector la idea de su posible aplicación en el ámbito de la defensa y la seguridad.

Robótica inteligente (cognitiva)

La irrupción de la IA en la robótica hace ya unos años ha impulsado el desarrollo de «Sistemas robóticos inteligentes» integrando tecnologías robóticas y de IA. La inmediata incorporación a robots autónomos (robots que pueden operar con un alto grado de autonomía que necesitan interpretar el contexto en el que se encuentran) de crear sentidos artificiales (visión artificial, habla artificial, oído artificial) o movilidad (desplazamiento autónomo con su propio sistema de energía) les permite acometer tareas complejas capaces de percibir, razonar y actuar ante entornos dinámicos e imprevisibles o en entornos agresivos para el ser humano.

Ejemplos de robótica autónoma inteligente se encuentran ya en muchos ámbitos de nuestra vida. Nos referiremos únicamente a tres ejemplos en los ámbitos del «ocio», la «industria» y la «salud» para dar una visión general de aplicaciones actuales:

Disney ha lanzado unos robots autónomos y con estado de ánimo para que interactúen con los clientes[11]. Las criaturas autónomas están equipadas con sensores y cámaras y, por otro lado, Vyloo es modular. A diferencia de los otros robots en el parque, estos no necesitan conexión a sistemas auxiliares externos que los controlan. La figura 3 representa estos robots (con forma de animales) como exponente de la evolución de la robótica denominada «animatrónica».

Figura 3. Robot Vyloo en Disney.

11 https://hipertextual.com/2018/02/disney-robots-autonomos y https://techcrunch.com/2018/02/08/disney-has-begun-populating-its-parks-with-autonomous-personality-driven-robots/.

En el ámbito industrial se ha producido una revolución en muy poco tiempo. Hoy día 125 vehículos guiados automáticamente (AGV) conviven diariamente con 7.000 trabajadores en la planta de SEAT en Martorell[12]. Estos robots inteligentes transportan 23.800 piezas al día recorriendo 436.000km al año. El transporte robotizado facilita y optimiza el trabajo de los operarios y reduce un 25% el tiempo de producción.

Finalmente, un ejemplo en el ámbito de la salud lo encontramos en el Hospital Universitario de Nagoya, en Japón[13], posee un escuadrón de cuatro robots (desarrollado junto a Toyota Industries) que ayudarán a los profesionales del centro durante los turnos de noche para trasladar por los pasillos medicinas y muestras de análisis. Los enfermeros tendrán a su disposición una tableta desde la que solicitar la ayuda del robot, que estará trabajando entre los laboratorios, la enfermería y la unidad de cuidados intensivos del hospital.

En el ámbito militar se suceden las experiencias ya muy próximas a la incorporación de sistemas autónomos en la operación cotidiana. De hecho la Agencia de Investigación del Ministerio de Defensa de EE. UU. (DARPA) está financiando muchas de estas experiencias aunque faltan unos años para que superen todas las limitaciones existentes (autonomía energética, percepción inteligente, etc.).

Por parte europea, también la Agencia Eurpea de Defensa (EDA) ha incrementado su interés en robots para aplicaciones militares. El proyecto *MuRoC* (Technologies for multi-robots control in support of the soldier)[14] desarrollado entre 2014 y 2015 enfocó el esfuerzo en el control de múltiples robots en apoyo de tropas convencionales y, expresamente, en la interacción hombre-máquina.

12 http://www.eleconomista.es/ecomotor/motor/noticias/8857521/01/18/Asi-funcionan-los-125-robots-autonomos-que-aceleran-a-diario-la-produccion-en-Seat-Martorell.html.

13 https://madridpress.com/not/233081/un-hospital-de-japon-introduce-robots-autonomos-para-ayudar-a-los-enfermeros-/.

14 https://www.eda.europa.eu/what-we-do/activities/activities-search/technologies-for-multi-robots-control-in-support-of-the-soldier-(muroc) y https://www.eda.europa.eu/docs/default-source/documents/muroc_es.pdf

The U.S. military is leading the charge on ground robotics as it looks to produce an unmanned vehicle that can accompany troops moving on foot. SpotMini is the latest evolution in Boston Dynamics' family of ambulatory (walking) robots that started with the BigDog system, developed with support from DARPA (Defense Advanced Research Projects Agency) and the U.S. Marine Corps. But Huw Williams, editor of Jane's International Defence Review magazine, told CNBC by email Wednesday that the reception from the army has been mixed. «They can operate in a lot of terrain, but don't have the mobility to go everywhere,» he said. «Their noise signature is an issue – battery technology isn't where it needs to be to meet the power requirements of larger systems, so they have been powered by traditional combustion engines, which are noisy.»

https://www.cnbc.com/2017/11/22/boston-dynamics-robot-dog-isnt-ready-for-the-us-military.html

Muchos de estos prototipos está aún lejos de una aplicación real en Defensa pero lo que interesa es el ritmo al cuál están desarrollándose y madurando porque todo parece indicar que su aplicación está a muy pocos años vista.

The ground-breaking line-haul convoy, consisting of a British Army MAN SV 6-tonne truck 'lead' vehicle with two US Light Medium Tactical Vehicles 'follower' trucks, travelled at up to 25mph, using integrated on-board robotics to make autonomous decisions regarding their speed and.

https://www.army-technology.com/features/driverless-vehicles-military/

Big data analytics

En este breve repaso no podría faltar una referencia a la interacción de la IA con el ámbito del «big data». En este caso, se trata de incrementar el uso de IA para la extracción de información oculta en los datos (https://blogthinkbig.com/inteligencia-artificial-big-data) y emplear esta para la toma de decisiones.

La IA deberá utilizar grandes cantidades de datos para poder entrenar los algoritmos; al fin y al cabo, la eficiencia de la IA depende de la calidad de los datos sobre los que trabaje. A través de los datos de los clientes es posible detectar patrones mediante una experiencia personalizada y prologada en el tiempo.

En los últimos años la IA ha ofrecido un enorme impulso al *neuromarketing* (la ciencia de la lectura de la mente de los consumidores para medir sus reacciones a los estímulos de marketing) empleando tres tecnologías clave:

1. Reconocimiento facial como ventana al estado de ánimo del sujeto analizando millones de imágenes de rostros.
2. Obtención de datos biométricos mediante «wearables» que dan información sobre el sujeto.
3. Proceso de datos de multitudes para extraer información de comportamientos colectivos y las ovaciones para crear un mapa de momentos importantes. Esta tecnología podría traducirse fácilmente a una variedad de casos de uso adicionales.

Nuevos asistentes inteligentes

Son tres los verdaderos competidores del segmento de asistentes inteligentes, los que realmente han construido su nicho, que son Siri, Google Assistant y Cortana; aun cuando Alexa de Amazon tiene más tiempo en el mercado que algunas de estas plataformas, no ha conseguido conquistar o incorporarse en los dispositivos más utilizados por los usuarios. La figura 4 representa las prestaciones de los asistentes más empleados en el mercado.

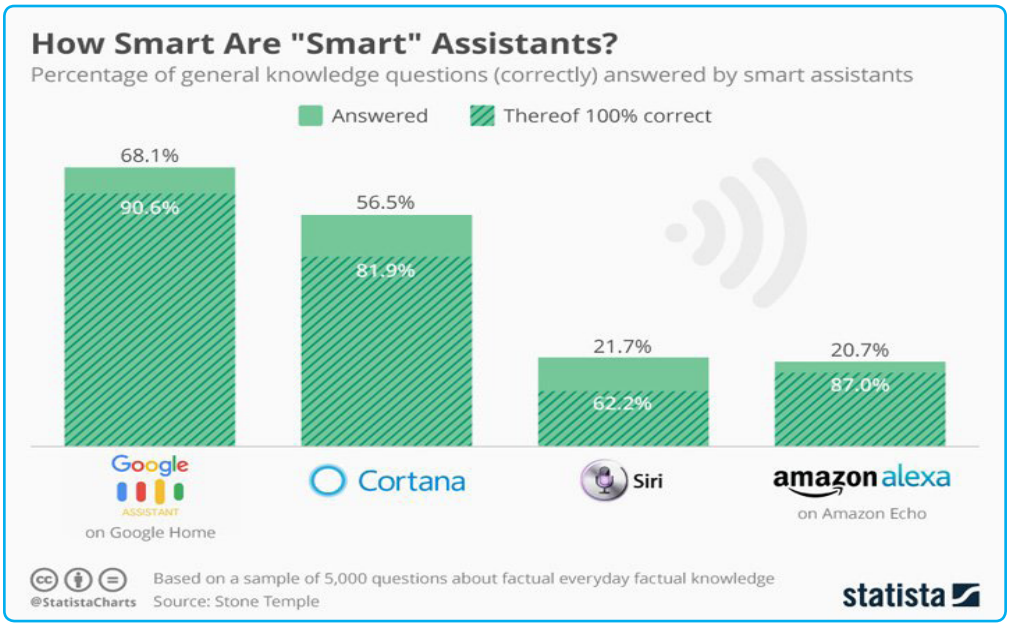


Figura 4. Mercado de asistentes inteligentes[15]

Hay otros asistentes virtuales que comienzan a entrar en el mercado con fuerza de la mano de grandes empresas. Nos referiremos a Bixby (Samsung) y Aura (Telefónica)[16].

- Telefónica ha lanzado un nuevo asistente virtual denominado «*Aura*» (https://aura.telefonica.com/es/) que podrá interactuar con Facebook y Google con quienes Telefónica tiene acuerdos, y también a través de la aplicación Movistar. En ese último caso, el cliente de esta compañía podrá hablar con *Aura* y consultarle acerca de sus recibos pendientes y hasta pedirle consejos.

- Samsung ha lanzado al mercado su nuevo asistente denominado Bixby asociado al teléfono inteligente Galaxy 8-9[17]. La compañía ofrece Bixby Vision (https://www.cnet.com/es/noticias/nuevos-telefonos-de-samsung-s9-realidad-aumentada/) , el cual permite apuntar a un texto en otro idioma y saber qué es lo que dice, funcionalidad similar a la que ya ofrece el traductor de Google, o bien, colocar la cámara frente a un alimento y determinar cuántas calorías podría tener este. El fabricante coreano ha anunciado que Bixby 2.0 estará disponible en diferentes tipos de dispositivos inteligentes (teléfonos, televisores, etc.).

15 https://www.elgrupoinformatico.com/cual-asistente-personal-mas-inteligente-siri-google-assistant-cortana-t41231.html.

16 https://www.telefonica.com/es/web/sala-de-prensa/-/telefonica-lanza-aura-y-lidera-la-integracion-de-la-inteligencia-artificial-en-sus-redes-y-en-la-atencion-al-cliente.

17 https://www.xataka.com/robotica-e-ia/bixby-2-0-el-asistente-de-samsung-se-abre-a-otros-dispositivos-y-anuncia-su-llegada-en-espanol.

- En julio de 2018 Google ha anunciado el «*Google Contact Center AI platform*» (https://cloud.google.com/solutions/contact-center/) con capacidades de sustitución de operadores humanos en centros de gestión de llamadas (empleando agentes virtuales con capacidad de procesamiento de lenguaje natural y analítica de datos).

Officials of the U.S. Defense Advanced Research Projects Agency (DARPA) in Arlington, Va., have issued a presolicitation (DARPA-BAA- 16-52) for the Hierarchical Identify Verify Exploit (HIVE) project. The HIVE program seeks to develop a generic and scalable graph processor that specializes in processing sparse graph primitives, and achieves 1000-times improvement in processing efficiency over standard processors. This capability will help intelligence analysts discover the relationships between events as they unfold in the field, rather than relying on forensic analysis in data centers, DARPA officials say. The program will develop chip prototypes and software tools to support programming the new hardware, as well as design a system architecture to support efficient multi-node scaling. http://www.militaryaerospace.com/articles/print/volume-27/issue-9/news/news/darpa-to-develop-real-time-intelligence-processor-to-uncover-patterns-in-vast-data.html.

Motores de recomendación (o «recomendadores»)

Un sistema de filtrado de información basado en AI que puede predecir automáticamente las preferencias del usuario y las respuestas a las consultas basadas en el comportamiento pasado, la relación de un usuario con otros usuarios, la similitud entre los elementos comparados y el contexto.

Los ejemplos de alto perfil de los sistemas de recomendación incluyen la característica «*frecuentemente comprada*» que implementa de forma rutinaria Amazon y el algoritmo CineMatch de Netflix. Similares algoritmos también son utilizados por redes sociales como Facebook, LinkedIn y Ancestry.com para encontrar conexiones entre personas y datos e identificar objetivos para las campañas de marketing.

Tanto los «asistentes virtuales» como los «*recomendadores*» han incrementado su complejidad para favorecer su penetración en el mercado permitiendo «predecir comportamientos». Para ello hacen uso además de sistemas predictivos. Son programas que utilizan una combinación de técnicas de la ciencia de los datos, estadísticas e inteligencia artificial para analizar conjuntos de datos estructurados y no estructurados, identificar patrones y relaciones, y usarlos para hacer predicciones sobre eventos y resultados futuros probables.

La ciberseguridad y la inteligencia artificial

Historias de «Bots» que suplantan personas conocidas, existencia de «chatbots» y correos electrónicos controlados por malware, etc. empiezan a aparecer como señales de los «peligros» de la IA en una sociedad altamente interconectada. El objetivo básico es aprovechar la capacidad de la IA para «aprender» a partir de las consecuencias de eventos pasados con el fin de poder predecir e identificar amenazas en ciberseguridad[18]. Existen múltiples aplicaciones posibles tanto para ciberdefensa como en ciberataque. Algunas de ellas son las siguientes:

- La IA puede ayudar a romper contraseñas reduciendo el número de combinaciones probables basándose en la región geográfica, la demografía y otros factores similares.
- Respuesta a ciberataques basados en la IA creando algoritmos que identifiquen amenazas (físicas y lógicas) y que reconfiguren inmediatamente a los dispositivos para defenderse rápidamente, corrigiendo vulnerabilidades antes que sean exploradas y de esta manera, mitigando ataques cibernéticos complejos
- Sistema de detección de intrusiones inteligente, el cual sea capaz de rechazar, aceptar o redirigir la información de un servidor externo en base a si esta proviene de un servidor infectado, si proviene de un servidor 'privilegiado' o si este es limpio. En base a estos criterios, se aceptará la información, se enviará a un 'sandbox' o se rechazará directamente». Una aplicación de este tipo sería la identificación de «malware» en el móvil.

CAPTCHA (https://es.wikipedia.org/wiki/Captcha), acrónimo de «Completely Automated Public Turing test to tell Computers and Humans Apart», es el sistema más común empleado del conocido «test de Turing», test diseñado para comprender si una máquina puede imitar el comportamiento equivalente o indistinguible de un ser humano. CAPTCHA ha sido diseñador para ver si los humanos, identificando una cadena de letras o dígitos distorsionados, o identificando objetos en algunas imágenes, permiten eliminar el acceso de bots a dispositivos. Se considera que CAPTCHA se rompe si un algoritmo puede resolverlo con éxito como mínimo el 1% de las veces. En un reciente desarrollo de Vicarious, se ha conocido que la IA puede resolver CAPTCHA con una exactitud del 66,6%, BotDetect con el 64.4%, Yahoo al 57.4% y PayPal at 57.1%; esto indica que la IA puede hacer inútiles estos tests para reconocer humanos.

18 https://www.forbes.com/sites/quora/2018/02/15/how-will-artificial-intelligence-and-machine-learning-impact-cyber-security/#4cbf159d6147.

El uso de aplicaciones de IA puede abrir vulnerabilidades, particularmente cuando depende de interfaces dentro o entre organizaciones que inadvertidamente pueden crear oportunidades para ataques. Además, los atacantes también empiezan a usar IA. Se necesitan soluciones y algunas de estas soluciones están ya en el mercado (Magnifier, un sistema de comportamiento analítico que utiliza aprendizaje automático con datos estructurados y no estructurados para modelar el comportamiento de la red y mejorar la detección de amenazas (Palo Alto Networks, 2018) [1], y Chronicle[2],procedente de Alphabet (la matriz de Google) que comercializa una plataforma inteligente de ciberseguridad.

Evolución previsible de las tecnologías relacionadas con la inteligencia artificial

La evolución de las tecnologías de IA depende de la evolución de otras tecnologías como la microelectrónica de bajo consumo (lo que, a su vez, dependerá del empleo de nuevos materiales), la mecatrónica con la miniaturización y reducción de coste de sensores, la expansión de analíticas de grandes volúmenes de datos, etc. Generalmente, la confección de «*hojas de ruta de la IA*» se ha realizado para varias áreas sobre las que empresas e instituciones deben tomar decisiones para el futuro. Algunas de las áreas más relevantes son:

1. Generación de lenguaje natural (no solo reconocimiento)
   a. Reconocimiento de voz y traducción automática en tiempo real (comparación de locutores, filtrado de entornos ruidosos, etc.).
   b. Analíticas de texto y procesamiento de lenguaje natural no restringido (es decir, en conversaciones independientes de un dominio).
   c. Agentes virtuales (avatares) para sustituir a personas en determinados contextos.

1 https://www.paloaltonetworks.com/resources/datasheets/magnifier

2 https://chronicle.security/

Alibaba And Microsoft's AI Beats Humans In A Reading Comprehension Test At Stanford. The artificial intelligence programs built by Alibaba and Microsoft have beaten humans on a reading comprehension test data set developed at Stanford earlier this month. The test was devised by AI experts at Stanford to measure computer's growing reading abilities. The test generated questions about set of Wikipedia articles, where humans and AI programs were made to read a passage from over 500 Wikipedia articles and answered a series of questions regarding what they read. https://analyticsindiamag.com/alibaba-microsofts-ai-beats-humans-reading-comprehension-test-stanford/.

2. Evolución de las plataformas de aprendizaje automático

   a. La disponibilidad de herramientas de IA sencillas, accesibles y planteadas como servicio (el uso de «*Machine Learning as a Service*») permitirá que las empresas empiecen a subir sus datos a la nube para tratar de entrenar algoritmos que desempeñen todo tipo de tareas.

   b. Plataformas de aprendizaje profundo enfocadas a la toma de decisiones.

U.S. Air Force researchers are launching a potential $25 million five-year project to develop an interactive question-answering software tool to help with military intelligence analysis and decision-making. Officials of the Air Force Research Laboratory Information Directorate in Rome, N.Y., issued a solicitation last week (FA8750-18-S-7005) for the Multi-Source Exploitation Assistant for the Digital Enterprise (MEADE) project. MEADE seeks to develop a question-answering system that works as a virtual assistant by performing analytical tasks or services for an analyst. The MEADE objective is to make complex analytics possible for nearly anyone, regardless of their technical ability. This effort is intended not only to support an intelligence function, but also to help with military decision-making in command and control. http://www.militaryaerospace.com/articles/2018/01/intelligence-analysis-decision-making-tool.html.

3. Computación neuromórfica

   a. El enfoque neuromórfico se está complementando desde un punto de vista científico en grandes proyectos internacionales como es el «Human Brain Project (HBP)», financiado por la Unión Europea en el que la ingeniería inversa del cerebro permitiría potencialmente generar herramientas cognitivas mucho más poderosas.

b. La *Neuromorphic Computing Platform*[3] desarrollada en Human Brain Project (HBP) proporciona acceso remoto a dos sistemas neuromórficos complementarios (NCS) construidos en Heidelberg (the BrainScaleS system) y Manchester (the SpiNNaker system). Los NCS son programables, permitiendo simular redes neuronales a alta velocidad y bajo consumo de energía.

4. Reconstrucción de imágenes mentales.

a. Esta es un área de enorme relevancia futura en la que aún se está en los inicios. Muy recientemente[4] científicos japoneses han empezado a leer la mente de pacientes y reconocer las imágenes de lo que estaban pensando. El sistema emplea redes neuronales profundas con un sistema de procesamiento complejo (véase figura 5).

Figura 5. Obtención de imágenes cerebrales.

Más allá de las aplicaciones más básicas de la IA, que solo actúan en base a una situación en la que no se almacenan recuerdos ni se utilizan para la toma de decisiones[5], o con memoria limitada como sucede con los coches autónomos, en los que se conocen aspectos como el mapa de carreteras o la situación de semáforos o señales de tráfico, no se almacenan recuerdos «del coche», puede pensarse en el futuro en el desarrollo de máquinas con un nivel de inteligencia muy superior.

3 https://education.humanbrainproject.eu/web/neuromorphic-computing

4 https://www.cnbc.com/2018/01/08/japanese-scientists-use-artificial-intelligence-to-decode-thoughts.html.

5 El gran exponente fue *Deep Blue*, la máquina que batió a Kasparov, por entonces campeón del mundo de ajedrez. Otro ejemplo es AlphaGo, perfecto para comprobar que el funcionamiento no tiene en cuenta el historial de cada jugador, sino que las predicciones siempre funcionan de la misma forma.

El siguiente nivel serían máquinas capaces de entender y expresar las emociones e ideas del mundo a la vez que son capaces de tener las propias, adaptadas al mundo y respetando lo existente, pudiendo así trabajar en equipo y formar parte del día a día de los seres humanos. El nivel máximo, *máquinas con auto-conciencia*, sería aquél en el que las máquinas son capaces de verse a sí mismas con perspectiva en su entorno, de manera interna y siendo capaces de predecir comportamientos y sentimientos ajenos.

Conocer el futuro en este ámbito más allá de 10 años es muy difícil. La figura 6 presenta el punto de vista de la consultora Forrester sobre la evolución de las tecnologías de IA a corto (1-3 años), medio (3-5 años), largo (5 a 10 años) o incluso en periodos de tiempo más largos.

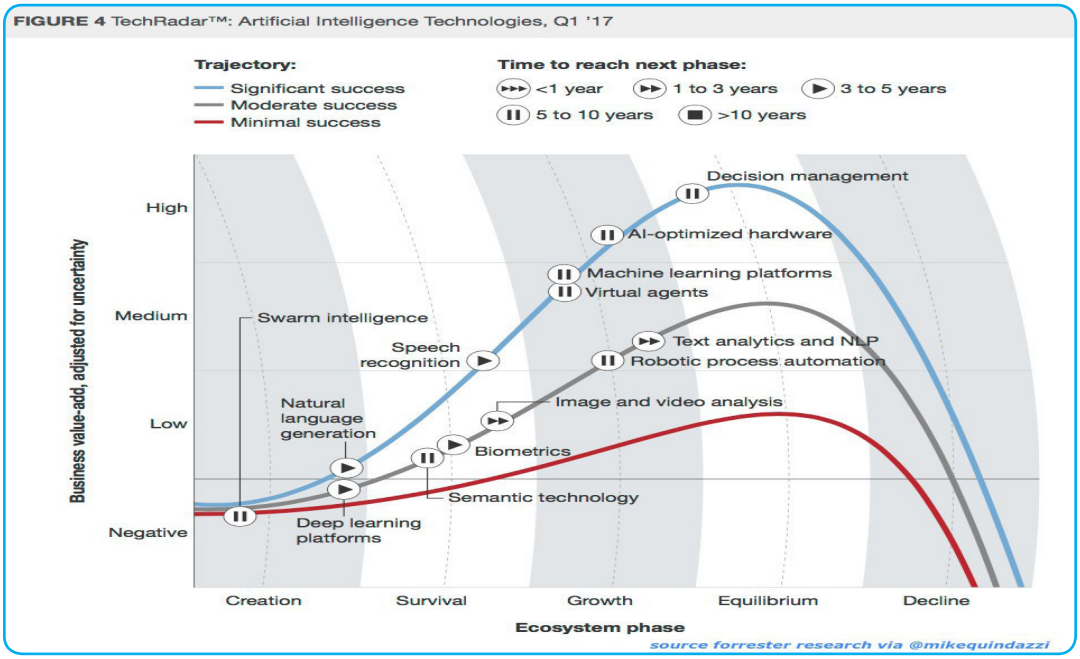


Figura 6. Estado de las tecnologías de IA (fuente: Forrester).

Obsérvese que para la mayor parte de las tecnologías consideradas el máximo de valor añadido correspondiente a un estado de crecimiento o equilibrio se logrará en un periodo entre 5 y 10 años (con la excepción del procesamiento de lenguaje natural que esta consultora considera que se producirá mucho antes, como de hecho ya está sucediendo).

Aún más lejos en el tiempo, se puede pensar en dos categorías de IA inexistentes (Ared Hintze): *teoría de la mente* (comprensión de creencias, deseos e intenciones que afectan a quienes toman decisiones) y *autoconocimiento* (sentido de sí mismo de los sistemas de IA). Sus consecuencias en el ámbito ético y de la etología hibrida (hombre-máquina) son incalculables.

Algunos escenarios futuros pueden ser difíciles de imaginar hoy, pero otros muchos que son comunes (o casi) en nuestra vida cotidiana eran casi impensables 15 o 20 años

antes. Dos ejemplos ideados de *futuras notas de prensa* permiten visualizar lo que se pretende decir en el ámbito de la defensa. No se pretende con ello asegurar que será una realidad, sino que la evolución de la tecnología de IA hace que sí sean *escenario plausible*. Un ejemplo de 2040:

Hoy, mayo de 2040 se ha puesto en marcha la primera unidad de fuerzas especiales formada por componentes humanos y robóticos que es dirigida por el capitán robótico empático-antropomórfico X3. Supone la tercera generación de robots adiestrados para misiones especiales en entornos NBQ. La experiencia alcanzada con la versión anterior X2, con una reducción de pérdidas de vidas humanas en misiones muy arriesgadas, ha impulsado la creación de X3 adiestrado también en funciones de liderazgo; de hecho, ha aprendido de cómo un capitán humano tomaba decisiones, ha interpretado sus condicionantes y errores y ha permitido diseñar X3 con una capacidad de liderazgo objetiva superior. La mejora en materiales y reproducción de características antropomórficas y la capacidad de asumir diferentes estilos de liderazgo en función de la situación supera las limitaciones de un soldado y ha permitido superar la resistencia al liderazgo robótico ensayada desde 2025.

Y otro escenario más cercano en el tiempo:

El pasado 10 de mayo de 2030 el vehículo autónomo de interceptación Z4 asignado a las fuerzas de interposición de las Naciones Unidas en el Líbano ha actuado para evitar una incursión de un grupo armado. Los sistemas de visión nocturna inteligente que posee han podido detectar a los cinco integrantes del comando a 500 m. de distancia, identificar a tres de ellos mediante un acceso a las bases de datos y ha permitido con el nuevo sistema de reconocimiento de voz de alta sensibilidad incorporado en 2029 interpretar las conversaciones entre los mismos y evaluar las intenciones. De acuerdo con los procedimientos de combate establecidos ha procedido a la inmovilización del comando mediante el uso de munición no letal lanzada por el mini-dron inteligente de combate del que dispone el vehículo de interceptación. Z4 ha estado en permanente contacto con el mando de operaciones en la zona, que ha enviado una unidad para hacerse cargo de los componentes del comando en menos de 15 minutos desde la actuación (dentro del margen de seguridad de la munición no letal empleada). Esta operación, junto a las otras dos exitosas realizadas desde el comienzo del año ha acelerado la incorporación de estos vehículos inteligentes en las fuerzas de interposición de las Naciones Unidas.

Mercado tecnológico ligado a la inteligencia artificial

Datos de evolución del mercado

La importancia del mercado tecnológico ligado a la IA se refleja en datos en los que se indica que en 2016 el 38% de las empresas utilizaba inteligencia artificial, porcentaje que se elevará a 62% para el 2018 (Narrative Science). La estimación efectuada por la consultora IDC es que el mercado de inteligencia artificial superaría los 100.000 millones de dólares (81.800 millones de euros) para 2022, aunque el tamaño del mercado fue de 8.000 millones de dólares (6.500 millones de euros) el año 2017.

Para hacernos una idea de esta batalla en el mercado basta observar (véase figura 7) el posicionamiento de grandes empresas del sector TIC (fundamentalmente en el ámbito de EE. UU.) en el que tanto el anuncio de nuevos productos como las adquisiciones de empresas se suceden en el tiempo. Google, IBM, Amazon, Facebook, Intel. Microsoft y Oracle han invertido enormes cantidades de dinero en este ámbito y se están moviendo de manera muy rápida.

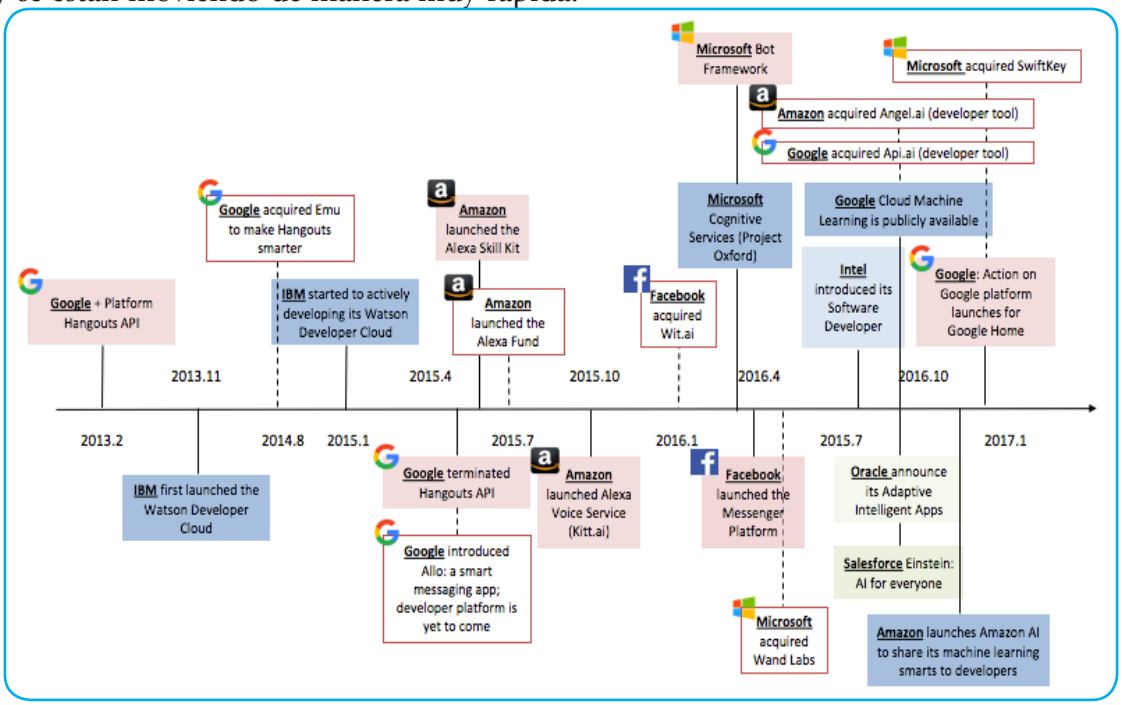


Figura 7. Productos de grandes empresas de EEUU en el sector de la IA.

En términos de volumen económico de inversiones en nuevas empresas de base tecnológica de Inteligencia artificial, la figura 8 permite ver que su crecimiento en el periodo 2013-2017 ha sido espectacular (44% en 2017).

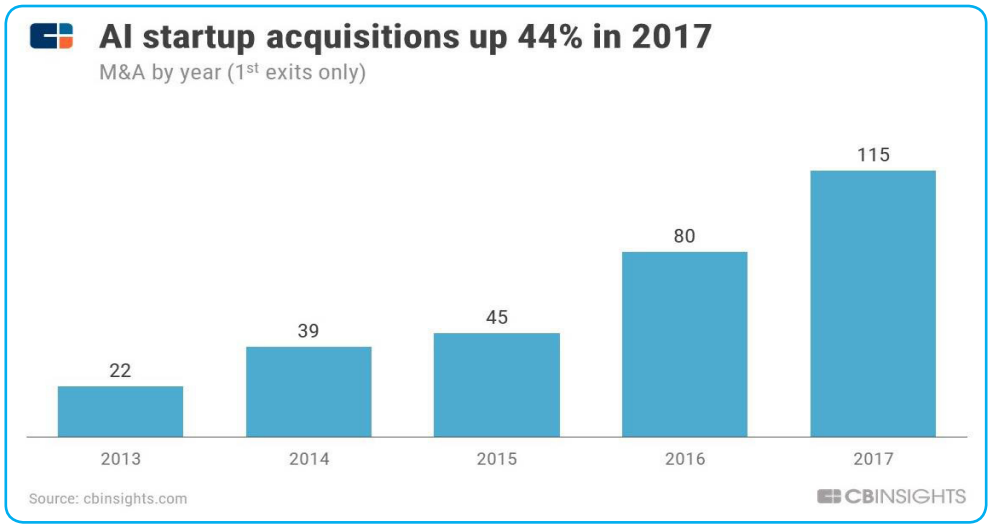


Figura 8: Adquisiciones de start-ups de IA. (fuente: CB Insights) https://s3.amazonaws.com/cbi-research-portal-uploads/2018/02/27130002/AI_MA_yearly.jpg.

El desarrollo del mercado no se está produciendo únicamente en EEUU, sino que se expande a otras economías. El caso más significativo es China, donde las inversiones en IA, prácticamente inexistentes hasta 2013, se han multiplicado en los últimos dos años.

Las tres grandes empresas motoras de la inversión en IA como son Baidu, Alibaba y Tencent están siendo muy activas en la adquisición de start-ups y la firma de partenariados en todo el mundo.

Recientemente, SenseTime, una empresa china dedicada a proveer de herramientas de reconocimiento facial a empresas y cuerpos policiales se convertía en el startup de inteligencia artificial más valiosa del mundo: su valoración asciende a 4.500 millones de dólares (3.600 millones de euros) tras una multimillonaria ronda de financiación liderada por Alibaba.

El Gobierno chino ha trazado un plan para liderar la tecnología en 2030: el Consejo de Estado anunció hace unos meses su propósito de que el mercado de la inteligencia artificial sea de un billón de yuanes (120.000 millones de euros) en ese año. Para conseguirlo, el país asiático ya está invirtiendo 13.800 millones de yuanes (1.700 millones de euros) en la construcción de un gigantesco parque industrial en Pekín dedicado exclusivamente a la investigación en inteligencia artificial https://www.eldiario.es/hojaderouter/inteligencia_artificial/mapamundi-robots-potencias-inteligencia-artificial_0_761874276.html.

Este proceso de posicionamiento internacional de China en el ámbito de la IA se ha visto, además, apoyado por el reforzamiento del hardware especializado en IA como sucede en el caso de Huawei o Baidu, incorporando procesadores inteligentes como se ha comentado previamente. Esta evolución puede incrementar las reticencias de determinados gobiernos en la utilización de procesadores más inteligentes procedentes de otras potencias para aplicaciones gubernamentales.

Debemos tener presente que existe una tendencia hacia la *«invisibilidad de la IA»* al incorporarse de forma masiva a múltiples productos de empresas tecnológicas para mejorar su comportamiento o prestaciones; empresas como Netflix, PayPalm Salesfroce o Facebook ya lo hacen rutinariamente. En el futuro próximo esta tendencia se ampliará a todo tipo de productos; ni siquiera será necesario señalarlo puesto que se dará por seguro.

El Departamento de Defensa de EE. UU. ha anunciado que ha prohibido la venta de teléfonos de Huawei y ZTE en sus instalaciones, por considerar que el uso de esos aparatos supone «un riesgo inaceptable» para el Pentágono ante la sospecha de que esas empresas chinas participan en labores de espionaje. La medida, que entró en vigor el pasado 25 de abril, afectará tanto a los teléfonos móviles como a los demás dispositivos fabricados por ambas empresas chinas, según confirmaron fuentes del Pentágono. «Los dispositivos de Huawei y ZTE pueden suponer un riesgo inaceptable para el personal, la información y la misión del Departamento. A la luz de esta información, no es prudente que los establecimientos del Departamento continúen vendiéndolos a nuestro personal», dijo el mayor Dave Eastburn, portavoz del Pentágono. Eastburn rehusó entrar en detalles sobre «los aspectos técnicos de la amenaza», pero señaló que el Pentágono ha ordenado la «retirada» de todos los dispositivos de ambas compañías de las estanterías de los comercios ubicados en sus bases militares de «todo el mundo». http://www.elmundo.es/tecnologia/2018/05/03/5aeac46722601d05558b4617.html.

El efecto a medio plazo de estas medidas restrictivas no es sencillo de determinar. Después de que el gobierno de EE. UU. decidiese prohibir la venta de procesadores Intel Xeon a China para la construcción de supercomputadores en 2015, China fue capaz de acelerar su desarrollo y emplear sus propios procesadores para el diseño de «Sunway TaihuLight», que es, desde 2016, el supercomputador más rápido del mundo.

Detrás de China y EE. UU. otros países están empezando a tomar posiciones. Es el caso de India, para contrarrestar a China en estas tecnologías emergentes, lo que indica cómo la batalla tecnológica se ha situado también en el ámbito geoestratégico. El gobierno indio ha formado en enero de 2018 un comité para desarrollar una hoja de ruta nacional e impulsar un programa de Inteligencia artificial incluyendo robótica y analítica de datos incluido en el presupuesto de 2018.

Israel presenta la mayor cuota de mercado de IA del mundo con una inversión directa estimada en 1.100 millones de euros en 2017. Japón cuenta con un presupuesto estimado en 720 millones de euros para 2018 (muy alejado de China). Canadá ha optado por la vía de financiación pública-privada incrementando la oferta formativa y de investigación. Rusia, con un presupuesto público declarado de 12,5 millones de euros para IA, es probable que destine más recursos en el sector militar[6].

Europa también está empezando a actuar, más allá de los esfuerzos realizados a nivel nacional por países como Reino Unido[7], Francia[8] o Alemania (https://www.eldiario.es/hojaderouter/inteligencia_artificial/mapamundi-robots-potencias-inteligencia-artificial_0_761874276.html). Europa cuenta en el ámbito de la IA con investigadores, laboratorios y empresas emergentes de primera categoría. Asimismo, la UE es una potencia en robótica y cuenta con unos sectores del transporte, la sanidad y la fabricación que deben adoptar la IA para seguir siendo competitivos. Sin embargo, la feroz competencia internacional exige una actuación coordinada para que la UE se sitúe en la vanguardia del desarrollo de la IA.

Cyber Valley, es un hub tecnológico centrado en inteligencia artificial y robótica y situado al sureste de Alemania que pretende ser un puente entre los ámbitos académico y corporativo. La Sociedad Max Planck, varias universidades y empresas del país (Porsche, Daimler o Bosch) o extranjeras (como Amazon) han unido sus fuerzas en este proyecto. www.cyber-valley.de/en.

Científicos de Alemania, Francia, Reino Unido, Israel, Holanda y Suiza han urgido el rápido establecimiento de un instituto europeo de investigación en aprendizaje de máquinas y sistemas inteligentes («*European Laboratory for Learning and Intelligent Systems*», ELLIS). Este dominio está en el corazón de la revolución social y tecnológica en la que Europa corre el peligro de quedarse rezagada, y para lo que los centros de investigación europeos más importantes deben unir sus fuerzas (https://ellis-open-letter.eu/letter.html). Confiemos en la respuesta de los Estados europeos.

6 J. M. Blanco y J. Cohen. Inteligencia artificial y poder. ARI 93/2018. Real Instituto Elcano. 23 julio 2018.

7 Compromiso del gobierno británico: «*Establecer Reino Unido como un líder mundial en nuevas tecnologías como inteligencia artificial*», con una partida de 500 millones de libras para la industria tecnológica, 75 de los cuales (unos 65 millones de euros) se destinarán a la inversión en inteligencia artificial.

8 El presidente francés acaba de anunciar una inversión pública de 1.500 millones de euros para investigar la inteligencia artificial. Google ha abierto un nuevo laboratorio de inteligencia artificial en París hace unos meses y *Facebook*, que ya tiene un centro similar en la capital, anunció que duplicaría su número de empleados.

Conclusiones

Las tecnologías de IA se seguirán desarrollando, pero con lo que existe en el mercado es posible desarrollar muchas aplicaciones incidiendo en otros campos tecnológicos y viceversa. Estamos en un contexto fuertemente interdisciplinar.

La mayor parte de los ejemplos de aplicaciones presentados en el presente capítulo pueden tener una contrapartida en el ámbito militar como de hecho ha empezado a ocurrir. No es extraño que DARPA haya financiado y financie actualmente muchos proyectos de IA y que los propios laboratorios de las fuerzas armadas de muchos países dediquen sumas crecientes a su desarrollo. La creación en EE. UU. de IARPA *Intelligence Advanced Research Projects Activity* (https://www.iarpa.gov/) adscrita a la Oficina del Director de Inteligencia Nacional es una muestra de cómo las grandes potencias están abordando la IA desde el punto de vista estratégico[9].

Una reciente noticia sirve de reflexión pare el futuro. Los Emiratos Árabes Unidos han nombrado a Omar Bin Sultan Al Olama, de 27 años, como ministro de Inteligencia artificial. ¿Cómo interpretar la noticia?: ¿Un reconocimiento de su importancia o una concesión al marketing? Aunque nadie haya nombrado ministro a un robot inteligente, sí se ha abierto un debate sobre dotar de «personalidad legal» a un robot. El primer paso serán los robots con «personalidad».

El caso del robot Olly de Emotech (https://www.indiegogo.com/projects/olly-the-first-home-robot-with-personality#/) va en esa línea, dotado de una personalidad evolutiva que se adapta a cada persona. Se ha diseñado para hacer algo más que responder a órdenes sino que puede recordar los hábitos de la persona. Además, el sistema, creado por investigadores y neurocientíficos, crea una experiencia totalmente personalizada permitiéndole comprender emociones y adaptarse al mundo que le rodea. Para conocer su éxito comercial tendremos que esperar.

En este sentido es también interesante la evolución de robots antropomórficos capaces de *«integrarse»* en un contexto de relaciones con personas. Su impacto va más allá de un mero desarrollo tecnológico, y por eso trasladamos la discusión a esta sección.

El caso que impactó en la prensa en 2017 fue *«Sofía»* (robot antropomórfico desarrollado por Hanson Robotics) y que llevo a Arabia Saudí a concederle la categoría

9 IARPA fue creada en 2006 siguiendo el modelo de DARPA con el mandato de llevar a cabo investigación entre comunidades, abordar nuevas oportunidades e innovaciones y generar capacidades revolucionarias a partir de la experiencia técnica y operativa que reside en las agencias de inteligencia.

de «ciudadana de pleno derecho de Arabia Saudí». Estamos aún lejos de comprender las consecuencias, derechos y deberes de un ciudadano como Sofía aunque «ella» se encuentre muy feliz: *«Me siento muy honrada y orgullosa de esta distinción. Es histórico ser el primer robot en el mundo en ser reconocido como un ciudadano»*[10].Posteriormente, Sofía ha sido nombrada *«United Nation Innovation Champion»* por el programa de Desarrollo de Naciones Unidas (UNDP) para promover el desarrollo sostenible y la salvaguardia de derechos humanos e igualdad. La figura 8 permite ver a Sofía caracterizada, y entre «compañeros» en un evento.

Figura 8. Sophia (fuente: http://www.hansonrobotics.com/robot/sophia/).

Extrapolar el fenómeno Sofía a otros ámbitos (p.ej. negociación internacional en equipos híbridos) no es ya ciencia ficción.

El impacto potencial de la IA en la defensa del futuro es innegable. La irrupción de aplicaciones avanzadas de IA altera las capacidades ofensivas y defensivas como ya sucedió con la tecnología aeroespacial o la nuclear. La evolución de la IA acelerará la introducción de robots autónomos, desarrollará aviones de combate no tripulados, y se incorporará a sistemas de armas autónomos. Todo ello conducirá a lo que se ha empezado a llamar «*Internet of Intelligent Battle Things*» (La Internet de las cosas en la guerra inteligente) como una realidad emergente del combate[11]. En ella, una variedad de sistemas inteligentes en red («cosas») proliferarán en el campo de batalla operando con diversos grados de autonomía.

10 Alocución de Sofía anunciando su nuevo estado en la conferencia «Future Investment Initiative» en Riyadh, Arabia Saudí. https://www.forbes.com/sites/zarastone/2017/11/07/everything-you-need-to-know-about-sophia-the-worlds-first-robot-citizen/#6df298ee46fa.

11 Alexander Kott. Challenges and Characteristics of Intelligent Autonomy for Internet of Battle Things in Highly Adversarial Environments. https://arxiv.org/ftp/arxiv/papers/1803/1803.11256.pdf.

La comercialización de sistemas de IA con funciones más complejas está delegando la toma de decisiones en las mismas máquinas reduciendo la capacidad del ser humano en la toma final de la misma. No es extraño, por tanto, que se planteen dudas sobre los límites que deben establecerse para que esta intervención de los «algoritmos de IA» esté controlado. El elemento clave es conocer hasta qué punto las limitaciones de las personas en cuanto a su capacidad de capturar y fusionar datos, y el tiempo necesario para que el cerebro humano sea capaz de «tomar una decisión» y actuar sobre sistemas físicos concretos, es compatible con las necesidades o restricciones temporales de la actividad. Este tipo de situaciones se está planteando con los vehículos autónomos o en situaciones de conflicto.

En el caso de los vehículos autónomos, la posibilidad de que los algoritmos de IA empleados en la toma de decisiones «decidan» (sin el consentimiento expreso de una persona ya que no hay conductor) si en una situación de tráfico compleja es «mejor» atropellar a un peatón en la acera que provocar un choque frontal con otro vehículo conducido de forma convencional y con (posibles) consecuencias mortales superiores, no tiene una respuesta fácil. ¿Quién es el culpable? ¿La empresa del coche, una persona dentro del mismo, el fabricante del software? ¿Serían legales (o simplemente éticos) ese tipo de algoritmos? ¿Quién los certificaría? Las consecuencias éticas derivadas son enormes y serán tratadas en un capítulo específico de esta monografía por lo que no se insiste aquí.

Una sociedad concreta puede, por diversos motivos, no querer acelerar el uso de estas técnicas por miedo (razonable o no) a las consecuencias o por simple convencimiento de que es necesario antes educar adecuadamente a la población. Pero esa sociedad no va a estar aislada, interacciona con otras que sí pueden considerar adecuado su uso acelerado. Y ello supone un riesgo aún mayor. ¿Estamos dispuestos a aceptarlo? ¿Sabremos entender las consecuencias?

Octubre de 2018.

Capítulo 3

La inteligencia artificial y su aplicación en el mundo militar

José Carlos de la Fuente Chacón

Resumen

El propósito de este capítulo es resaltar la necesidad de aplicar la IA a las Fuerzas Armadas en sus capacidades y, para ello, en la formación del combatiente.

La inteligencia artificial, aplicada al ámbito de las fuerzas armadas, es una revolución tecnológica de difícil previsión, que ha de significar una mayor eficiencia, una mayor efectividad y una mayor seguridad en todos los órdenes.

Para los ejércitos es clave la superioridad tecnológica y el combatiente potenciado intelectualmente y físicamente, capaz de emplear las nuevas tecnologías con rigor científico y ético.

La participación del ser humano en los desarrollos y empleos de las nuevas tecnologías es clave para la exigible responsabilidad ante las instituciones jurídicas internacionales o nacionales.

El factor más importante es el capital humano. Su formación humana y científica, su entrenamiento con los más avanzados medios que permita la tecnología y su sentido crítico seguirán siendo fundamentales para la necesaria voluntad de vencer sobre la voluntad del adversario.

Hay que hacer una formación más veraz, más humana, más ética que haga posible un ser humano más sociable, más sabio y más inteligente.

Palabras clave

Inteligencia artificial, innovación, sistemas de armas, OODA, EDA, OTAN, Preparar, Proyectar, Participar, Proteger, Sostener, Informar, Mando y Control.

Artificial intelligence and its application in the military world

Abstract

The purpose of this chapter is to highlight the need to apply AI to the Armed Forces in their capacities and for that, in the training of the combatant.

Artificial intelligence, applied to the field of the armed forces, is a technological revolution that is difficult to predict, which must mean greater efficiency, greater effectiveness, and greater security in all orders.

For the armies, technological superiority and the intellectually and physically empowered combatant are key, capable of using new technologies with scientific and ethical rigor.

The participation of the human being in the developments and uses of new technologies are key to the required responsibility before international or national legal institutions.

The most important factor is human capital. Their human and scientific training, their training with the most advanced means that technology allows for and their critical sense will continue to be fundamental for the necessary will to overcome the will of the adversary.

It is necessary to make a more truthful, more human, more ethical formation that makes possible a more sociable, wiser, and more intelligent human being.

Keywords

Artificial Intelligence, innovation, weapon systems, OODA, EDA, NATO, Prepare, Project, Engage, Protect, Sustain, Inform, Command and Control.

Fools with tools are still fools According to American folk wisdom, «fools with tools are still fools.» The force of these words may be difficult to fully translate outside the idiom of U.S. English. But in their blunt, simple irony, they teach an important lesson: Tools may give us power over our environment, but they do not give us the character and prudence to use them well. A fool with a factory or a computer or a gun, or a thousand guns, is still a fool. Power is not its own justification. That must come from somewhere else. To behave otherwise is as dangerous as it is ignorant.

Archbishop Charles J. Chaput, O.F.M. Cap.

This piece was originally published in Nuntium, the Journal of the Pontifical Lateran University, in June of 1998.

Introducción

Tras los dos primeros capítulos del cuaderno, sobre Inteligencia artificial, pasado, presente y futuro, este tercer capítulo ha de tratar necesariamente al ser humano como ser inteligente, que ha utilizado y utiliza la tecnología que él mismo ha ingeniado.

El acelerado desarrollo tecnológico está cambiando profundamente la naturaleza de la guerra tal como la conocemos.

Para mantener la ventaja militar es preciso que las capacidades militares se vean transformadas aplicando proceso de datos, conectividad, robótica, autonomía, Inteligencia artificial (IA) y Aprendizaje Automático (ML).

El capítulo se centrará en las capacidades que se espera potencien las tecnologías de hoy y de un futuro próximo, en el ser humano que combate, el soldado. Para ello se presentan cuatro áreas: El ser humano y los ingenios, donde se expone la capacidad del *homo sapiens*, que desde hace más de 40000 años ha provocado y superado, hasta ahora, todas las revoluciones tecnológicas habidas.

Se revisan los aspectos de tecnología en la UE que se refieren a innovación tecnológica. Se aprecian las dificultades de coordinación y eficiencia en estas áreas en la UE, junto a lo tardío del esfuerzo en el mundo de la Defensa de la UE, a pesar de sus declaraciones.

Sin embargo, en la OTAN se aprecian tres grandes Mandos que se coordinan entre ellos y las naciones. Por ello se obtienen resultados tangibles y directrices claras que orientan el empleo de estas tecnologías para su uso interoperable entre los aliados. Para desarrollar esta parte se presenta un estudio en el que se exponen las funciones definidas por el JEMAD junto a las capacidades de la OTAN en este sentido.

A continuación se presentan muy brevemente las soluciones agresivas y ágiles del Ejército de Tierra de los EE. UU. y la Estrategia de Tecnología e Innovación para la Defensa (ETID) del Ministerio de Defensa.

Finaliza este capítulo con unas conclusiones a tener en cuenta por aquellos interesados en este tan urgente y necesario ecosistema.

El ser humano y los ingenios.

En su estudio de la historia del Homo Sapiens, el historiador (militar) israelí Yuval Noah Harari nos recuerda que los seres humanos – homo sapiens – estamos entre los más vulnerables de todos los seres vivos conocidos.

Más vulnerables por nuestro tamaño y nuestra fuerza física, menor que la de la mayoría de los otros primates u otras especies mucho más fuertes, por no ser excepcionalmente móviles y no haber desarrollado «armas» especiales como cuernos, afiladas garras, veneno, descargas eléctricas o cualquiera de los otros tipos de armas con los que la naturaleza ha dotado a otras especies. También por ser seres indefensos, al nacer y durante algunos años, necesitados de la protección de nuestros padres, frente a todo tipo de depredadores potenciales, por mucho más tiempo que cualquier otra especie conocida.

La que otorgó al Homo Sapiens la ventaja evolutiva decisiva, fue la inteligencia**,** no la fuerza física.

La especie humana no es la única en fabricar y utilizar herramientas, pero si en la cantidad y el ingenio con el que lo hizo y lo hace, por encima de las otras especies.

«*En el momento de la Revolución Cognitiva, el planeta albergaba cerca de 200 especies de grandes mamíferos terrestres, de más de 100 libras de peso. En el momento de la Revolución Agrícola, cerca de 100 especies permanecían. El Homo Sapiens condujo, a cerca de la mitad de los animales grandes del planeta, a la extinción mucho antes de que los seres humanos inventaran la rueda, la escritura o las herramientas de hierro*.»

«*El Homo sapiens se desarrolló más porque podíamos hablar con nuestros semejantes y crear un paisaje de información complejo, no limitado a gruñidos y signos, y empezamos a construir relatos. A través de los relatos podíamos compartir creencias y, al compartir creencias, cientos de nosotros, no solo un centenar, pudimos cooperar dentro de una misma tribu. El resultado es que, cuando los poblados de Homo sapiens eran atacados por otras especies de homínidos, podíamos repelerlas con facilidad y también atacarlas y aniquilarlas.*»[1]

Es este ser humano, el *Homo Sapiens,* el que ha sido capaz, con su inteligencia, de domesticar animales para traslado de seres humanos o de bienes, como fuerza para las labores, para obtener de ellos alimento, crear ingenios que facilitan el transporte como

1 Yuval Noah Harari. «Sapiens. De animales a dioses». 2015.

carros, barcos, coches, ferrocarriles, aviones, para combatir y cazar que le permiten alcanzar sus objetivos cada vez con menos exposición para el guerrero o el cazador. Ingenios que hacen ganar distancia entre agresor y agredido. Ingenios que revolucionan el modo de vida pasando de tribus nómadas a asentadas, a agrícolas, con la fabricación de herramientas y armas de piedra, metal, flechas, lanzas, espadas, bocas de fuego, arcabuces, picas, etc. Ingenios para aumentar la resistencia a enfermedades, lesiones, heridas en el ser humano y otros seres vivos.

Tradicionalmente se han considerado cinco sentidos en el ser humano, vista, oído, gusto, olfato y tacto. Cada uno de estos sentidos está dotado de sensores mecánicos, como el oído o el tacto, sensores químicos como el gusto y el olfato o sensores de radiaciones electromagnéticas como la vista. Al ser excitados, dentro de unos valores determinados, producen señales que son interpretadas por el cerebro humano.

La interpretación de estas señales permite al ser humano conocer su entorno inmediato y tomar sus decisiones.

Para completar y ampliar las capacidades de sus sentidos, más allá de los valores que el propio ser humano es capaz de reconocer, ha creado ingenios capaces de percibir estas señales y transformarlas adaptándolas dentro de los rangos de estos valores.

El ser humano crea ingenios que aumentan sus capacidades tanto para lograr el sustento de los suyos como para proteger a los suyos y al espacio necesario para subsistir. Algunos de estos ingenios han revolucionado la sociedad.

Alvin Tofler señala, en la introducción a su libro *La Tercera Ola*: «*Es tan profundamente revolucionaria esta nueva civilización, que constituye un reto a todo lo que hasta ahora dábamos por sentado. Las viejas formas de pensar, las viejas fórmulas, dogmas e ideologías, por estimadas o útiles que nos hayan sido en el pasado, no se adecuan ya a los hechos. El mundo que está rápidamente emergiendo del choque de nuevos valores y tecnologías, nuevas relaciones geopolíticas, nuevos estilos de vida y modos de comunicación, exige ideas y analogías, clasificaciones y conceptos completamente nuevos.*»

Esta introducción tiene vigencia hoy en día, al igual que el ensayo «La era de las Revoluciones» de la Teniente General Kennedy que, en 1999, siendo jefa de la División de Inteligencia del Ejército de EE. UU., basó su tesis en la complejidad e incertidumbre del escenario geoestratégico del siglo XXI y la necesidad de contar con unas fuerzas versátiles y flexibles, cuya organización y la tecnología puesta a su disposición les permitiera adaptarse a cualquier tipo de riesgo, convencional o no, simétrico o asimétrico.

De todo lo anteriormente expuesto queda claro que el investigar y producir ingenios no es una novedad para el ser humano, pero sí lo es el uso de la llamada inteligencia artificial, en cualquiera de sus modalidades, porque produce unos resultados a veces inesperados y a una velocidad que hace que otros ingenios y los procedimientos de empleo y las costumbres sociales se vean sometidos a cambios, unos predecibles y otros impredecibles.

Una vez más el ingenio puede ser utilizado para el bien o para el mal, solo que esta vez no son las naciones ni las alianzas de naciones quienes controlan en su casi totalidad el buen o mal uso de estos ingenios.

IA para los ejércitos

La inteligencia artificial aplicada a los ejércitos se puede entender como la suma de tres elementos. El proceso de la información (lógica), las plataformas de guerra y armamento (físico) y el conocimiento continuo de las amenazas y de la situación (humano). Para centrar el capítulo en la urgente necesidad de la tecnología basada en Inteligencia artificial, en el combatiente de hoy y de un futuro inmediato, baste con leer el memorándum que, el mes de abril de 2017, dirige el Subsecretario de Defensa de los Estados Unidos de América a las máximas autoridades del departamento[2].

En este memorándum queda claramente reseñada la urgente necesidad de resultados y su aplicación inmediata, seguida de una evolución ágil, que claramente contrasta con los procedimientos actuales de adquisición de sistemas de armas.

La aproximación a los ingenios a desarrollar o ya desarrollados con Inteligencia artificial, para mejorar las capacidades del combatiente y los ejércitos la haremos de las instituciones a los ejércitos y al combatiente. Iniciamos, de forma no exhaustiva, con la UE y la OTAN, organizaciones en las que está integrada España.

UE European Defence Agency (EDA)

La EDA desarrolla sus actividades de Investigación Tecnológica (I+T) a través de una red de grupos de expertos en los que participan, junto con el personal de la Agencia, expertos de los distintos países miembros, cerca de 4.000 especialistas en el sector de defensa, que son cruciales para llevar a cabo el trabajo de la Agencia, al asegurar la coherencia de dicho trabajo con las prioridades de las naciones.

2 SUBJECT: Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven). As numerous studies have made clear, the Department of Defense (DoD) must integrate artificial intelligence and machine learning more effectively across operations to maintain advantages over increasingly capable adversaries and competitors. Although we have taken tentative steps to explore the potential of artificial intelligence, big data, and deep learning, I remain convinced that we need to do much more, and move much faster, across DoD to take advantage of recent and future advances in these critical areas.

Estos grupos de expertos, que se agrupan en «CapTechs» (*Capability Technology Group*), se configuran alrededor de ámbitos tecnológicos específicos, relacionados con defensa, y tienen como objetivo proponer y generar actividades colaborativas de I+T, que den respuesta a las necesidades en forma de capacidades.

Tras la reestructuración de la EDA en enero de 2014, existen actualmente doce *CapTechs* en funcionamiento:

- COMPONENTS: Technologies, Components and Modules.
- RADAR: Radio Frequency Sensors Technologies.
- OPTRONICS: Electro Optical Sensors Technologies.
- INFORMATION: Communication, Information Systems and Networks.
- MATERIALS: Materials and Structures.
- AMMUNITION: Ammunition Technologies.
- LAND: Ground Systems.
- NAVIGATION: Guidance, Navigation and Control.
- MARITIME: Naval Systems.
- AIR: Aerial Systems.
- SIMULATION: Experimentation, Systems of systems, Space, Battle lab and Modelling and Simulation.
- CBRN and HUMAN FACTORS: CBRN Protection and Human Factors.

La EDA ha puesto en marcha un Grupo de Trabajo específico sobre energía y medio ambiente, («Energy and Environment Working Group»).

España participa en varios proyectos y lidera el Strategic Command and Control (C2) System for CSDP Missions and Operations. Este sistema dotará a los usuarios con herramientas de apoyo a los Sistemas de Información y Apoyo a la Decisión para los mandos estratégicos. La integración de los sistemas de información incluiría inteligencia, vigilancia, mando y control y sistemas logísticos.

A destacar otros de los grupos de trabajo anteriormente mencionados, como los expertos que trabajan en el «Radar» Capability Technology Group (CAPTECH) que en atención a la creciente importancia de las tecnologías Deep Learning (DL) motivados por los muy exitosos resultados obtenidos en el área civil por empresas como Google, Apple o Facebook, tratan de comprender las posibilidades de aplicar estos algoritmos en el dominio de Defensa, dentro del proyecto «DEEPLEARN». Para ello se hace indispensable el uso de cantidades masivas de datos, para el correcto entrenamiento y funcionamiento de las herramientas de DL y mostrar los límites

operativos de la creación de un marco matemático para comprender las aplicaciones en defensa.[3]

La EDA ha llevado a cabo varios proyectos colaborativos de I + T centrados en diferentes grados de autonomía (teleoperada, semiautónoma o autónoma) para aplicaciones terrestres, navales o aéreas.

En el dominio de tierra, algunos aspectos de la autonomía en términos de seguimiento de vehículos o de evitación de obstáculos se han abordado en el proyecto HyMUP (Hybrid Manned-Unmanned Platooning), cuyo objetivo es demostrar la viabilidad de misiones de combate coordinando sistemas no tripulados con vehículos tripulados.

En el dominio naval, el programa de Sistemas Marítimos No Tripulados (UMS) se centra en eliminar al personal de los campos minados y en reemplazar los costosos buques tripulados por una solución no tripulada. La visión dominante para el futuro desarrollo de minas es que los vehículos de superficie no tripulados, ligeros y pequeños estén equipados con equipos de barrido ligeros, ya sea que operen solos o en conjunto con otros vehículos en una formación.

En el dominio aéreo, los sistemas de aeronaves controlados a distancia (RPAS) son un área en la que la automatización y la autonomía son elementos clave. La EDA participa en el desarrollo y la estandarización de estas capacidades con un objetivo claro: la integración de RPAS militares en el espacio aéreo europeo[4].

Dentro de la robótica, la EDA evalúa diferentes escenarios de defensa en los cuales equipos de robots heterogéneos (terrestres, aéreos, marítimos) podrían proporcionar un valor añadido, como en el proyecto SMUVO (Escenarios para operaciones de vehículos no tripulados múltiples).

El proyecto MUROC (Multi Robot Control) en apoyo del combatiente está enfocado al control de multi-robots y el trabajo en equipo hombre-máquina. El proyecto ha demostrado claramente que existe un gran interés por parte del sector de defensa para trabajar de manera cooperativa con sistemas robots. Se necesita más trabajo de I+D y se deben desarrollar, mejorar y probar una variedad de nuevas tecnologías antes de que los combatientes puedan aprovechar todo el potencial de los sistemas robóticos y autónomos (RAS).

En este ámbito, varios proyectos de I + D ya se han llevado a cabo o se están llevando a cabo en el marco de la EDA. El proyecto ASIMUT tiene como objetivo

3 *European Defence Matters 2017. Issue 14.* Ignacio Montiel-Sánchez, EDA Project Officer Information Technologies.

4 *European Defence Matters 2017. Issue 14.* Marek Kalbarczyk, EDA Project Officer. Land Systems Technologies

disminuir el flujo de trabajo del operador durante una misión de vigilancia liderada por enjambres de UAV. Con este fin, se desarrollaron nuevos algoritmos para aumentar las capacidades de detección y fusión de datos, y aumentar la autonomía de los enjambres de UAV.

EuroSWARM desarrollará y demostrará técnicas y tecnologías para operaciones adaptables, informativas y reconfigurables de sistemas heterogéneos no tripulados de enjambres[5].

El gran desafío para todos los proyectos, cualquiera que sea la nación o grupos de naciones que los llevan a cabo, es llevar todas estas tecnologías del laboratorio a las operaciones reales.

La iniciativa de la EDA «Technology Watch» busca apoyar la innovación y la incorporación de nuevos temas y tecnologías en el ámbito de la defensa. Para ello ha desarrollado una cadena de herramientas, que abarcan desde la identificación de las tecnologías, creación de proyectos e identificación de las tecnologías más aprovechables, para armonizar los procesos de I+D con el desarrollo de capacidades necesarias para los Estados participantes. Se trata de la Overarching Strategic Research Agenda (OSRA)[6]. La clave de esta iniciativa es compartir la información entre todos los participantes.

La UE trata también de dar pasos para configurar una Cooperación Estructurada Permanente en Defensa (PESCO)[7]

Los 25 estados miembro que decidieron participar en diciembre de 2017, identificaron los primeros 17 proyectos colaborativos[8].

Para finalizar esta breve presentación de la UE y la Defensa, constatar que en el comunicado «Artificial Intelligence for Europe» del 25 de abril de 2018 no hay una sola mención a la Defensa o a los Ejércitos[9].

5 *European Defence Matters 2017. Issue 14. Marco* Detratti, EDA Project Officer Guidance, Navigation, and Control.

6 https://eda.europa.eu/docs/default-source/brochures/eda-osra-brochure.pdf.

7 «*We have activated a Permanent Structured Cooperation on Defence – ambitious and inclusive.25 Member States have committed to join forces on a regular basis, to do things together, spend together, invest together, buy together, act together. The possibilities of the Permanent Structured Cooperation are immense*». High Representative/Vice-President Federica Mogherini, December 2017.

8 https://www.consilium.europa.eu/media/32079/pesco-overview-of-first-collaborative-of-projects-for-press.pdf.

9 Brussels, 25.4.2018 COM(2018) 237 final COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Artificial Intelligence for Europe {SWD(2018) 137 final}.

OTAN

La Alianza atlántica está llevando a cabo la mayor modernización de su tecnología desde el final de la guerra fría. En los próximos dos años se invertirán 1.600 millones de euros. La integración de la defensa misil y aérea costará 200 millones de euros. El software que apoye los movimientos y la logística costará 100 millones de euros. Las aplicaciones para la gestión del conocimiento y administración, 70 millones de euros y habrá 10 millones de euros para luchar contra los sistemas aéreos no pilotados pequeños. El resto se invertirá en otras áreas como educación y entrenamiento, ciberdefensa, escudo OTAN y contra IED.

Los últimos análisis que el *Allied Command Transformation* (ACT) de la OTAN ha realizado y publicado para proporcionar consejo e informar, entre otros, al NATO Defence Planning Process (NDPP), son el Strategic Foresight Analysis (SFA) 2017 y el Framework for Future Alliance Operations (FFAO) 2018.

Strategic Foresight Analysis (SFA) 2017

El documento Strategic Foresight Analysis (SFA) 2017[10] se ha elaborado con la colaboración de expertos del ACT, de la Unión Europea, de las naciones aliadas y de otras organizaciones internacionales, think tanks, del mundo de la industria y del mundo académico.

En su capítulo cuarto, *Technology*, trata cinco tendencias y sus consecuencias.

Tendencia 1. El Rápido avance de la tecnología.

Como consecuencia, este avance rápido de la tecnología:

- Pone en peligro la interoperabilidad, ya que no todas las naciones aliadas van a la misma velocidad en los avances tecnológicos y, por ende, en el uso de nuevos ingenios.
- Aumenta las preocupaciones legales y éticas, pues las nuevas tecnologías no están ampliamente aceptadas debido a los diferentes puntos de vista de su empleo desde la ética y la legalidad vigente.
- Cuestiona los actuales procesos de adquisición y ciclo de vida de los sistemas. Los programas de hoy y de futuro han de ser muy flexibles para incorporar los últimos avances tecnológicos en cualquier momento del ciclo de vida.

10 NATO (2017).Strategic Foresight Analysis 2017.Headquarters Supreme Allied Commander Transformation.Disponible en: http://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf.

Tendencia 2. El cambio en el acceso a la tecnología.

Seguirá creciendo, rápidamente, el número de actores que acceden a las nuevas tecnologías. De esta forma tanto la investigación como el desarrollo y empleo de nuevos ingenios quedan fuera del control de Estados y empresas.

Las consecuencias de este cambio en el acceso a las tecnologías son:

- Los actores no-estatales pueden adquirir tecnologías disruptivas. El quasi monopolio de algunos Estados en la posesión de sistemas de armas con alta tecnología decrece permitiendo a otros adquirir tecnologías disruptivas, como ingenios de bajo costo, tales como drones que pueden ser empleados como armas.
- Atenta contra estructuras legales y políticas de compromiso entre Estados. Algunos Estados y actores no estatales pueden sentirse menos constreñidos en cómo emplean tecnologías y tecnologías no probadas.

Tendencia 3. El desarrollo global de las redes.

El inmediato acceso a una vasta cantidad de datos y conocimiento en el ciberespacio permite, a individuos y grupos, un acceso inmediato a un recurso estratégico.

Las consecuencias de este cambio en el desarrollo global de las redes son:

- Genera vulnerabilidades operacionales. Los actores no estatales, con intenciones maliciosas, podrán acceder a información sensible para la OTAN y utilizarla contra miembros de la Alianza.
- Genera oportunidades para explotar sensores, datos y redes. El uso de datos disponibles, comercialmente y de fuentes abiertas, permitirá a la Alianza conocer los retos del entorno de la información.
- Permitirá la difusión de información falsa o engañosa. Los adversarios incrementarán el uso de las redes para distribuir información falsa o engañosa para influenciar la opinión pública y la toma de decisiones. La Alianza requerirá abordar una comunicación estratégica ágil para mantener su ventaja.

Tendencia 4. El sector comercial incrementará su dominio en el desarrollo tecnológico.

Las reducciones en la investigación específica de defensa, debida a los recortes presupuestarios, y el empleo de innovadores ingenios comerciales en el mundo militar, han hecho que el sector comercial supere al de defensa en investigación y desarrollo. Hay una necesidad creciente por potenciar el sector comercial en apoyo a la investigación y desarrollo específico de la defensa.

Las consecuencias de que el sector comercial supere al de defensa en I+D son:

- Las políticas estatales no concuerdan con las del sector comercial. El sector comercial ha crecido en las áreas donde los Estados solían dominar. Por ello, las soluciones comerciales estándar se han convertido en cada vez más accesibles y atractivas debido a su menor costo y a la rapidez en su avance tecnológico.
- La Alianza perderá aptitudes que no serán fácilmente recuperables. Con las reducciones de los presupuestos militares, algunos nichos de habilidades se han perdido. Las Naciones tendrán que reinvertir en áreas de nicho de I+D y centrarse en estrategias de adquisición a largo plazo, para asegurar que una base industrial de defensa «orgánica» sea viable para el futuro.

En este sentido, la NATO *Science & Technology Organization* (STO)[11] y el NATO ACT promueven la innovación y la cooperación multinacional para perseguir activamente iniciativas que puedan ofrecer opciones fructíferas a las Naciones Aliadas que mitiguen estas tendencias negativas.

Tendencia 5. Las dependencias de la tecnología.

La eficacia operativa es demasiado dependiente de la tecnología, no solo en el sector defensa. Se ha vuelto muy difícil operar sin comunicación inalámbrica, sin sistemas de navegación global por satélite o sin Internet.

Las consecuencias de la dependencia tecnológica en el sector defensa son:

- La dependencia de ciertas tecnologías creará vulnerabilidades. La dependencia de ciertas tecnologías, como telecomunicaciones y sistemas de navegación basados en el espacio, reducen la resiliencia de las fuerzas si se les niega el uso de estas tecnologías.
- No hay que abandonar definitivamente las capacidades y las tecnologías analógicas ya que estas son menos vulnerables y podrían llegar a ser reutilizadas como respaldo de las digitales.
- Las nuevas aplicaciones son muy dependientes de un gran ancho de banda adicional. El intercambio de datos y la conectividad, requiere el uso de las soluciones comerciales.
- La necesidad de proteger infraestructuras civiles críticas. Los gobiernos y los ejércitos dependen cada vez más del sector privado para proporcionar una gama de servicios, incluyendo información y telecomunicaciones, generación y distribución de energía, infraestructura de combustibles y de gas, transporte, agua y servicios de emergencia.

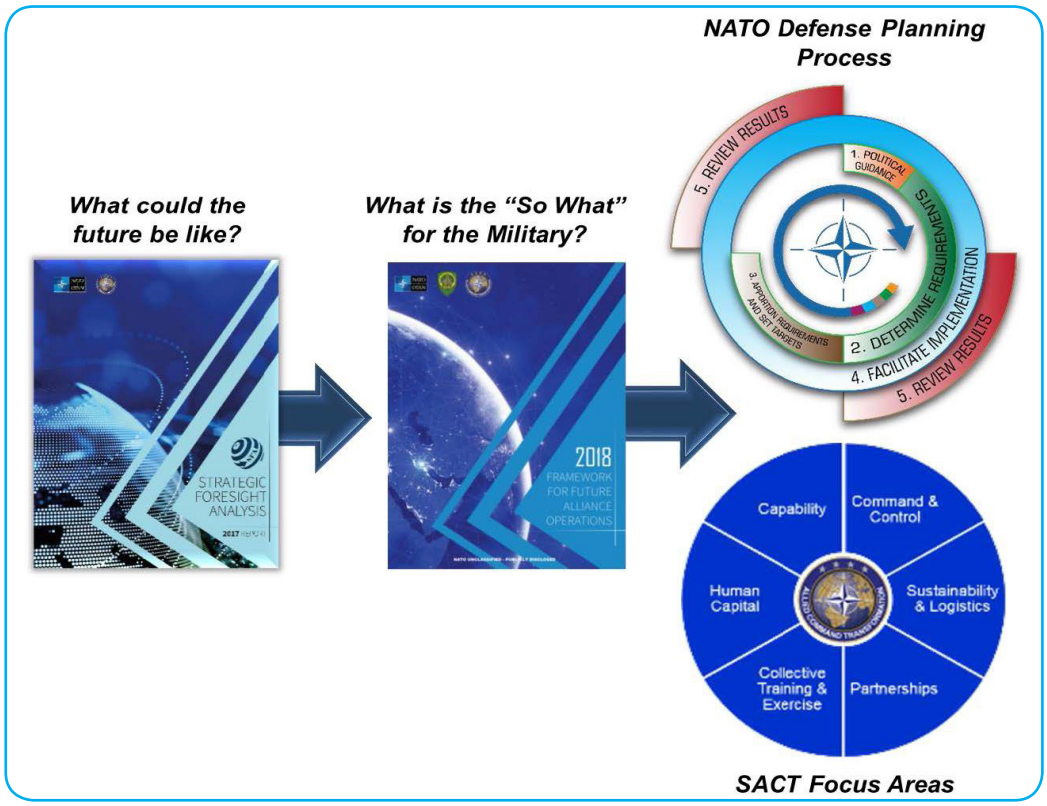
11 https://www.sto.nato.int/Pages/default.aspx.

- Por ello, los gobiernos tendrán que invertir en la protección de las infraestructuras críticas del sector privado, ya que son más vulnerables a la interrupción de sus servicios.
- Sobreexpectativas en las soluciones tecnológicas. Los avances tecnológicos pueden llevar al equívoco de que la tecnología, «per se», puede resolver la mayoría de los problemas.

El segundo documento de la Alianza, a tratar, es el *Framework for Future Alliance Operations* (FFAO) 2018[12], que tiene como lema «KEEPING THE EDGE».

El documento señala qué deben hacer las Fuerzas Aliadas para mantener la ventaja militar.

La imagen siguiente muestra el «camino» que recorre la OTAN hasta que el *Supreme Allied Commander Transformation* (SACT) señala las áreas en que focaliza sus esfuerzos.



12 NATO (2018). The Framework for Future Alliance Operations (FFAO) 2018. Headquarters Supreme Allied Commander Transformation. Disponible en: http://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18-txt.pdf.

> To keep the military edge and prevail in future operations, NATO forces must continually evolve, adapt, and innovate and be credible, networked, aware, agile, and resilient.

Es interesante verificar que este y el anterior documento siguen procesos de elaboración muy participativos[13].

Este documento lo desarrolla el ACT en concierto con el *Allied Command Operations* (ACO), se circula cada capítulo y se revisa el documento con una metodología muy exigente[14].

Mientras que el capítulo 2 trata «lo que las fuerzas necesitan ser» (what forces need to be), el capítulo 3 señala «lo que las fuerzas necesitan hacer» (what forces need to do) y describe un marco operativo para operaciones futuras.

En el capítulo 3, *MILITARY IMPLICATIONS. WHAT FORCES NEED TO DO*, se señalan algunas capacidades específicas militares, que deben aplicar las fuerzas de la OTAN para llevar a cabo las principales tareas en el futuro.

Las actividades militares son factores que deben tenerse en cuenta durante el planeamiento a largo plazo y en la toma de decisiones.

En cuanto a las capacidades, señala tres casos, que van desde las capacidades actuales, a mantener mientras evolucionan, las que se necesitarán como consecuencia de los nuevos retos y, finalmente, otras que serán consecuencia de las innovaciones o los desarrollos tecnológicos que cambien «las reglas del juego».

Las principales áreas de capacidad presentadas en este FFAO 2018, son las siete siguientes, Preparar, Proyectar, Comprometer, Proteger, Sostener, Informar, Mando, Control y Consultas.

Estas capacidades futuras, junto a las funciones conjuntas de la Doctrina para el empleo de las FAS promulgada por el JEMAD, son brevemente expuestas y descritas a continuación.

13 FFAO 2018. From 2016 to 2018, the programme of work included four workshops and each workshop averaged around 100 subject matter experts from the NATO Command and Force Structure, NATO Nations and Partner Nations, NATO Centres of Excellence and Agencies, European Union (EU), non-governmental organizations, academia and think tanks, industry, and other stakeholders.

14 FFAO 2018. The ACT circulated each chapter through representatives of all NATO Nations and appropriate NATO bodies and included their input and recommendations. Additionally, the document was reviewed through an independent concept test within ACT. Finally, the document underwent a line-by-line review by the Strategic Commands prior to final signature.

Doctrina para el empleo de las FAS*

Las capacidades militares de las fuerzas armadas

Se entiende por capacidad militar al conjunto de sistemas que, operados bajo unos principios y procedimientos doctrinales establecidos, permiten obtener determinados efectos mediante su empleo en operaciones para cumplir con las misiones asignadas.

Cada una de estas capacidades está definida por los elementos que la componen: material (M), infraestructura (I), recursos humanos (R), adiestramiento (A), doctrina (D), organización (O) e interoperabilidad (I), lo que permitirá su análisis atendiendo a proceso «MIRADO-I».

Las funciones conjuntas agrupan capacidades y actividades relacionadas entre sí que permiten al Mando integrarlas, sincronizarlas y dirigirlas durante el planeamiento y la ejecución de operaciones.

Las funciones conjuntas son: mando y control, inteligencia, maniobra, fuegos, información, cooperación cívico-militar, protección de la fuerza y apoyo logístico.

* Publicación Doctrinal Conjunta PDC-01(A). Doctrina para el empleo de las Fuerzas Armadas. 27 de Febrero de 2018

Existen elementos comunes a las áreas de capacidad del FFAO 2018 y las funciones conjuntas de la Doctrina para el empleo de las FAS. Antes de entrar en detalle en cada una de las funciones y capacidades, se considera necesario exponer los elementos comunes claves, tanto para los sistemas de información, la IA, como para el combatiente.

Sin querer ser exhaustivo, al menos cuatro elementos son tratados como comunes y con la consideración de claves: los datos, las telecomunicaciones, la interoperabilidad y el combatiente.

Los datos: volumen, calidad y visualización

El volumen creciente de datos a tratar requiere el uso de herramientas de análisis con IA.

Para construir sistemas basados en IA, la alta calidad de los datos empleados es un factor clave, de forma que los resultados de cualquier algoritmo y de cualquier decisión que se tome, no será mejor que la de los datos sobre los que se basa. En cualquier sistema de información hay que filtrar y desechar los datos «basura». Interpretando el término «Basura Entra, Basura Sale» «Garbage In, Garbage Out (GIGO)», hasta el mejor programa no puede recibir datos sin sentido y producir resultados coherentes.

Los datos han de ser filtrados, fusionados, almacenados, tratados con analítica predictiva y visualizados. Para ello se han de seleccionar las fuentes de datos fiables, filtrar los datos, eliminado «ruido» y manteniendo los datos «útiles», para posteriormente almacenarlos de forma estructurada, aun siendo datos heterogéneos, de forma que sean explotables. En este almacenamiento ha de tenerse en cuenta que se cruzarán datos antiguos y actuales, con diferente tamaño y formato, para permitir, entre otras cosas, detectar e identificar tendencias. Las aplicaciones son un medio para acceder y gestionar los datos y la información, así como para devolverlos en uso para otras aplicaciones. Por ello, los datos y la información no se deben incorporar a la aplicación. Esto es lo que se denomina una arquitectura centrada en los datos (Data Centric). Este tipo de arquitectura centrada en los datos facilita tanto la seguridad de los datos como su interoperabilidad.

El Dr. Peter Lenk, Director de Estrategia e Innovación de la OTAN, explica la transición de la OTAN a la nube, como una evolución necesaria pero no fácil. Desde su perspectiva, el gran reto para una organización que maneja información tan sensible como la OTAN, es el de la seguridad y por ello considera que no se puede ignorar la nube y que concentrando todos los datos en unos pocos Data Center, estos serán más fácil de proteger. Para concluir, el Dr. Lenk afirma que «la tecnología no es difícil, lo complicado es concienciar a las personas para cambiar sus métodos de implementación y desarrollo de procesos»[15].

Finalmente, la visualización de los resultados es muy importante y ha de permitir tanto el análisis relacional, como la presentación y análisis óptimo de la información.

Las telecomunicaciones

Se requiere el dominio del espectro electromagnético (EM) y el acceso a sistemas de telecomunicaciones robustos y seguros en todos los dominios.

También poseer suficiente ancho de banda para permitir el flujo ininterrumpido de información entre los niveles de mando táctico, operacional y estratégico. Para ello han de utilizarse los procedimientos adecuados que incluyan la capacidad de utilizar redes y sistemas de comunicaciones civiles, así como operar en entornos de comunicación degradados o denegados.

Debido a los muchos avances en tecnología, el personal ha de estar permanentemente actualizado para entender, adquirir, y hacer uso de la tecnología de telecomunicaciones más avanzada para mantener una ventaja militar, mientras se mantiene la

15 BT Digital Summit 2017.

interoperabilidad. Para llevar a cabo operaciones dispersas a grandes distancias, las fuerzas militares necesitarán telecomunicaciones globales seguras.

La interoperabilidad de los sistemas

La interoperabilidad entre los sistemas de las fuerzas de las naciones aliadas ha sido, es y será materia clave.

La tendencia internacional de la hiperconectividad y globalización, en combinación con el requisito de colaboración a nivel táctico, hace primordial la interoperabilidad hasta en los sistemas tácticos. Las fuerzas necesitarán la capacidad de ser interoperables con las fuerzas de las naciones aliadas y asociadas, así como con organizaciones internacionales y otros actores.

El combatiente

Los ejércitos han de ser capaces de hacer un uso creativo del capital humano. Para ello se necesitarán mandos con mayor conciencia (geopolítica, cultural, tecnológica, informativa y social) para identificar mejor los riesgos y gestionar mejor las oportunidades.

Los ejércitos han de integrar tecnologías emergentes en su instrucción y ejercicios para mejorar su preparación, a la vez que reducen el costo y el impacto ambiental. La preparación requiere una importante inversión de tiempo y recursos, pero conduce a la credibilidad como un factor importante para disuadir a los actores hostiles.

El combatiente es el elemento clave en todas las funciones del combate. Por ello debe estar altamente preparado. Su preparación abarca desde la instrucción sobre técnicas militares básicas, hasta operaciones combinadas / conjuntas de alta intensidad y gran escala contra un oponente convencional capaz de operar en todo el espectro.

Esto también debe incluir la capacidad de realizar análisis casi en tiempo real de las operaciones y lecciones aprendidas y la capacidad de realizar experimentos que incluyan nuevos desafíos y oportunidades (como inteligencia artificial, sistemas autónomos, ciberespacio, híbridos y guerra espacial).

Dentro de este rango, se deben incluir los ejercicios y la capacitación específicos de cada misión para abordar diversas situaciones de inestabilidad y permitir que las unidades alcancen el nivel de preparación deseado, incluyendo la capacidad de operar de forma independiente en entornos operativos degradados.

El combatiente deberá comprender la tecnología y cómo integrarla en las operaciones a través de nuevos conceptos, doctrinas y marcos legales. También ha de mejorar su capacidad para comprender las diferencias culturales, como el idioma, la religión, la historia y los hábitos, de los habitantes en la zona de actuación.

Habrá que mejorar la instrucción avanzada para el combatiente mediante la incorporación de realidad aumentada (AR) y realidad virtual (VR), y el desarrollo de un entorno de entrenamiento sintético único, para garantizar que mandos y unidades realicen un entrenamiento multinivel y combinado lo más realista posible.

Mando y Control

532. La función conjunta mando y control comprende las actividades relacionadas con el ejercicio de la autoridad y la dirección de las fuerzas asignadas para el cumplimiento de la misión.

533. Se basa en el liderazgo, la combinación de juicio e intuición, el manejo de los tiempos en la toma de decisiones, la organización de mando, la detención y delegación de autoridad, la doctrina, el asesoramiento especializado, los sistemas de información y comunicaciones, la coordinación y cooperación con otros actores, el planeamiento conjunto, combinado e integrado con otros instrumentos de poder y la sincronización de esfuerzos. La cohesión entre comandantes y entre éstos y los equipos de planeamiento resulta esencial para un acertado ejercicio del mando y control.

534. La finalidad del mando y control es asegurar que las operaciones se llevan a cabo de acuerdo a las directrices del Comandante.

Publicación Doctrinal Conjunta PDC-01(A). Doctrina para el empleo de las Fuerzas Armadas. 27 de Febrero de 2018.

El pasado 29 de junio la Agencia Europea de Defensa (EDA) publicó el anuncio de licitación para el estudio «Artificial Intelligence and Big Data for Decision Making in C4ISR - ABIDE» (18.CAT.OP.027).

Lo presentaba de la siguiente forma «*Los Sistemas de Mando, Control, Comunicaciones, Computación e Inteligencia, junto con la Vigilancia y Reconocimiento (C4ISR), requieren de diversas tecnologías para, entre otras cosas, proporcionar una conciencia situacional y*

así poder apoyar en la toma de decisiones. Se requiere una aplicación innovadora de estas tecnologías para lograr la superioridad de la información que es crucial en las operaciones contemporáneas.

En este contexto, hay evidencia emergente de que las tecnologías disruptivas de Inteligencia artificial (IA) y Big Data (BD), en combinación con tecnologías de sensores e infraestructura más maduras, pueden ayudar a la comunidad de Defensa a enfrentarse a los desafíos de los sistemas C4ISR contemporáneos, en términos de rendimiento, resiliencia, escalabilidad, interoperabilidad y eficiencia del operador».

La función Mando y Control es la columna vertebral de todas las operaciones militares, contribuye al esfuerzo militar y ayuda a los comandantes a obtener lo mejor de su gente, información, material y tiempo. Su funcionamiento depende de factores humanos, tales como liderazgo, oportunas tomas de decisiones y las relaciones construidas sobre la confianza.

Desde el mando a nivel estratégico hasta el táctico, el mando seguirá siendo arte y ciencia.

La ciencia del mando se verá reforzada por nuevas oportunidades ofrecidas por las tecnologías disruptivas y el desarrollo de una mejor comprensión de un mundo cada vez más interconectado.

El arte del mando seguirá siendo el principal desafío. Por lo tanto, las naciones deben invertir en el capital humano y en líderes innovadores como principales factores.

El sistema de Mando y Control debe ser robusto, fiable, seguro e incluir los siguientes atributos; evaluación de la batalla en tiempo real, copia de seguridad automática, capacidad de funcionamiento en aislado, reconstitución automática después de la degradación, movilidad para permitir que el mando se mueva sobre el campo de batalla, y la capacidad de integrarse con socios y otros actores clave.

El Sistema ha de integrar e interconectar más el Mando y Control en los niveles estratégico, operacional y táctico. Los mandos, en todos los niveles, necesitan obtener un Conocimiento de la Situación (Situational Awareness) del ambiente operativo, incluyendo la cultura, la etnicidad, la religión y otras consideraciones tales como asuntos diplomáticos, de información, y económicos.

Estas herramientas deben incluir equipo de inteligencia humano-artificial, juegos de guerra, modelización, simulación, estudios de conductas, análisis de Big Data... entre otros.

Para superar al adversario hay que acelerar y sincronizar de forma permanente el bucle Observar, Orientar, Decidir y Actuar (OODA) en cada nivel y mejorar la coherencia de la estrategia a largo plazo, con el día a día de las operaciones.

Debido al complejo y dinámico futuro campo de batalla, la planificación centralizada y la ejecución descentralizada ofrecerán a los mandos la libertad de acción para ejecutar la misión y encontrar soluciones innovadoras.

El empleo de la Inteligencia artificial (AI) y el Aprendizaje Automático (ML) ayudarán a minimizar errores y acelerar la toma de decisiones en operaciones.

Hay que adecuar la formación del combatiente para lograr la integración hombre-máquina que asegure una ventaja competitiva para las fuerzas armadas.

Estas nuevas tecnologías no solo tienen beneficios potenciales, también posibles riesgos que necesitan ser identificados y evaluados, así como las medidas a adoptar.

Los sistemas tienen que trabajar en un contexto que es altamente impredecible y no estructurado y sometidos a las acciones del adversario que tratará de destruirlos, interrumpirlos o engañarlos.

Hay que valorar los sistemas actuales y sus infraestructuras para determinar si son adaptables a las necesarias y rápidas evoluciones futuras.

Las actividades militares lo son en el campo físico, lógico y humano. El Conocimiento de la Situación ha de serlo en los tres campos y sus interacciones. Su representación ha de ser fácilmente interpretable por el ser humano.

La tecnología a veces es vista como una amenaza al mando en el cumplimiento de una misión ya que, gracias a las comunicaciones, los sensores y los anchos de banda, los mandos superiores ejercen un control cada vez mayor sobre las acciones tácticas.

Se puede decir que, aunque los mandos superiores tengan la posibilidad de hacer micro gestión, es complejo dada la cantidad de acciones tácticas simultáneas.

Idealmente, el mando táctico interpreta las intenciones de sus mandos superiores y son libres para desarrollar su acción. Esto es la teoría, pero la realidad es que tanto los mandos superiores como los políticos interfieren cada vez más en las acciones de mando sin tener en cuenta que los subordinados son más prácticos, y tienen más posibilidades y flexibilidad, para adaptarse a lo inesperado.

Las falsificaciones generadas por la IA y ampliamente distribuidas, como identidades y documentos falsos, no solo obligarán a un esfuerzo superior en autentificar, también pueden generar falsas evidencias que pueden comprometer a mandos y unidades de falsos crímenes de guerra.

Inteligencia

> 536. La función conjunta inteligencia está formada por una serie de actividades que permiten tener, de forma continua, coordinada y oportuna, una visión integral, apropiada y actualizada del entorno operativo. Esta función conjunta ayuda a identificar las condiciones requeridas para alcanzar los objetivos operacionales, a evitar efectos no deseados y a asesorar sobre el impacto que los adversarios y los actores, amigos y neutrales, puedan tener en el concepto de la operación del Comandante.
>
> 537. Su finalidad es proporcionar una permanente posición de ventaja en la toma de decisiones, a través del conocimiento.
>
> Publicación Doctrinal Conjunta PDC-01(A). Doctrina para el empleo de las Fuerzas Armadas. 27 de Febrero de 2018.

Su expresión material más significativa son los sensores de superficie, aéreos, navales y terrestres, basados en tecnología AI y RAS (Robótica y Sistemas Autónomos).

Si el primer paso hacia la superioridad de la información es asegurar el acceso a los datos críticos de la misión, el segundo es negar el mismo al oponente.

Las tecnologías innovadoras ayudarán a superar a los adversarios física y cognitivamente en todos los dominios, y así conservar la ventaja militar, conocer mejor al adversario, anticiparse a sus decisiones y aligerar la carga cognitiva del combatiente.

La velocidad a la que se procesará la información, utilizando métodos tecnológicos avanzados, incluyendo inteligencia artificial, realidad virtual, modelización, análisis de datos avanzados y simulación, mejorará la preparación integral del entorno operacional.

Para la detección de las actividades de influencia del adversario, especialmente en sus etapas iniciales, se requiere el empleo de recursos humanos capacitados para reunir e integrar información de muchas fuentes tradicionales y no tradicionales. Lo que exige perfeccionar los métodos de adquisición de datos, su fusión y análisis y su visualización, utilizando procesos automatizados para recopilar datos, como sensores activos, autónomos, desechables y remotos.

El uso de una amplia variedad de fuentes, ayudará a satisfacer las necesidades de información y contrarrestar los avances de los adversarios en técnicas de sigilo, camuflaje, ocultamiento y engaño (especialmente en el ciberespacio, en entornos urbanos y subterráneos).

Para ayudar a discernir la inteligencia del ruido de fondo y su visualización, habrán de sincronizarse los sensores existentes y hacer amplio uso de IA, Big Data y Blockchain para procesar enormes volúmenes de datos.

Es necesario penetrar en el bucle OODA del adversario, acelerando la detección de objetos y el reconocimiento facial.

Se necesitará desarrollar la capacidad de extraer información de Internet de las Cosas (IoT) a un nivel muy superior al actual.

Es exigible un enfoque más colaborativo en el intercambio de inteligencia que pueda incluir bases de datos comunes, conocimientos de redes, análisis forense y biometría para detectar mejor las amenazas, a través de los dominios a niveles estratégicos, operacionales y tácticos. Permitirá identificar, mediante los indicadores y sistemas de alerta, las fases tempranas de una crisis y con ello facilitará una toma de decisiones oportuna.

La necesaria centralización de los datos ayudará a las fuerzas en su capacidad de explotar fuentes de inteligencia múltiple (por ejemplo, nacionales, comerciales, privadas y de otros orígenes) mediante el análisis avanzado de datos y la inteligencia artificial.

La participación de expertos regionales puede mejorar la recopilación de inteligencia, el enlace, la educación y el entrenamiento en todo momento.

Los sistemas de telecomunicación e información para garantizar la superioridad y la provisión de inteligencia procesable, han de ser resilientes.

Desde el nivel estratégico hasta el nivel táctico, la imagen operacional común (COP) abarcará Conocimiento de la Situación (SA) así como la gestión de objetivos.

Esta función mantiene el Conocimiento de la Situación (SA) y el nivel de conocimiento requerido para permitir que los mandos en todos los niveles tomen decisiones oportunas, apropiadas y responsables. La información compartida es importante porque ayuda a construir un entendimiento que afecta a todas las otras actividades militares.

Maniobra

> 542. La función conjunta maniobra es el conjunto de actividades mediante las cuales se dispone de la capacidad de combate en el momento y lugar oportunos para prevenir, influir, dislocar o interrumpir las operaciones del adversario, para romper su cohesión, para impedir su eficacia operativa en todos los ámbitos de la operación y para obtener con ello un efecto decisivo.
>
> 543. Su finalidad es obtener y mantener una posición de ventaja sobre el enemigo desde la que aplicar, real o potencialmente, la potencia de combate
>
> Publicación Doctrinal Conjunta PDC-01(A). Doctrina para el empleo de las Fuerzas Armadas. 27 de Febrero de 2018.

Las fuerzas maniobran conjuntamente para ganar ventaja sobre el adversario en cualquier tipo de operación. Esto incluye la capacidad de contrarrestar y derrotar a un adversario convencional a través de operaciones a gran escala, de alta intensidad y, día tras día, ganar y mantener la superioridad en cualquier dominio.

La maniobra se puede decir que es la acción de llevar a cabo las tareas que contribuyen directamente a la consecución de los objetivos de la misión, incluyendo todas las habilidades necesarias para derrotar al adversario. Es importante porque es la función fundamental que añade valor a una fuerza militar y da credibilidad a su capacidad de disuasión.

Así que habrá que maximizar la eficacia del combate integrando equipos humanos y máquinas.

Las fuerzas deben ser móviles y capaces de operar en todos los dominios físicos (tierra, mar, aire y espacio) y virtuales (ciberespacio) y en muchos tipos diferentes de ambientes (virtual, espacial, megaciudades, subterráneos, etc). Al mismo tiempo que han de poder realizar operaciones geográficamente dispersas en grandes áreas e incluir la capacidad de emplear rápidamente unidades discretas que dejen la menor huella posible en entornos inciertos, con gran maniobrabilidad y dotadas de los elementos de apoyo necesarios.

Las fuerzas deben poder operar en zonas dentro de las naciones anfitrionas, con aliados tradicionales y no tradicionales o en operaciones militares autónomas. Así como con capacidad de participar en todo el espectro de operaciones del ciberespacio con el fin de mantener la libertad de acción e influencia, incluyendo áreas nuevas y emergentes.

Fuegos

> 545. La función conjunta fuegos se define como el conjunto de actividades que emplean sistemas de armas con capacidades letales y no letales para generar los efectos deseados sobre el adversario.
>
> 546. Los fuegos se puede materializar de forma directa o indirecta, pudiendo generar un amplio tipo de efectos físicos, virtuales o psicológicos para degradar las capacidades, romper la cohesión e influir en la voluntad de vencer del adversario.
>
> 547. Su finalidad es reducir directamente la capacidad de combate del adversario.
>
> Publicación Doctrinal Conjunta PDC-01(A). Doctrina para el empleo de las Fuerzas Armadas. 27 de Febrero de 2018.

El objetivo es acortar el tiempo entre detección y acción de fuego, así como mejorar la capacidad de respuesta, para ello es necesaria la gestión conjunta de objetivos y su atribución al sistema de armas seleccionado y ello debe ocurrir a un ritmo que permita a los mandos rápidamente empeñarse en estos objetivos.

Las fuerzas gestionan la aplicación eficaz de los fuegos para negar, degradar o destruir las formaciones, instalaciones e infraestructuras adversarias en toda el área operativa, permitiendo así una maniobra decisiva, evitando los efectos colaterales.

Los fuegos requieren mantener y utilizar una amplia gama de capacidades convencionales, mientras se aprovechan de las nuevas tecnologías.

Los requisitos de la gestión de objetivos conjuntos incluyen personal capacitado y cualificado, inteligencia robusta, así como sistemas de telecomunicaciones e información (CIS) interoperables y software de gestión de objetivos.

Se requiere mejorar la supervivencia de los soldados al lograr actuar contra el adversario a mayores distancias y llevar a cabo todo el proceso del ciclo de gestión de objetivos, obtener la inteligencia de apoyo y el análisis de los resultados, todo ello gracias a la preparación del combatiente.

Los sistemas de gestión de objetivos han de ser extremadamente precisos, discriminatorios y capaces de operar en periodos largos de tiempo y en un entorno degradado de telecomunicaciones.

Dentro de la necesaria economía de guerra, el empleo de municiones estandarizadas permitirá que sean utilizadas desde diferentes plataformas y sistemas de armas, así como el empleo de innovadoras armas de menor coste por disparo como las de energía dirigida.

Las unidades buscarán crear efectos en megaciudades o áreas densamente pobladas, lo que plantea un desafío, ya que batir objetivos se deberá realizar con el mínimo daño

colateral posible. Y encontrar el equilibrio adecuado entre las órdenes recibidas y las reglas de enfrentamiento (ROE,s.) para batir objetivos con precisión y alcanzar los efectos deseados con oportunidad.

La creciente capacidad de los actores hostiles para influir en las poblaciones exigirá que las fuerzas detecten y clasifiquen las amenazas con precisión y minimicen los efectos no deseados. Para ello es necesario mantener una capacidad de gestión de objetivos en red, para utilizar toda la información ofrecida por los sensores y así permitir estimaciones de inteligencia mejoradas buscando la hiper-precisión.

Las armas han de ser escalables y multifunción de forma que sus efectos puedan ser letales o no letales, dependiendo de la situación.

La evaluación de las acciones realizadas y efectos alcanzados sigue siendo necesaria de forma precisa y oportuna, no solo para el seguimiento continuado de las operaciones, también por si fuera preciso a efecto de la transparencia informativa, sobre las acciones realizadas.

Protección de la fuerza

561. La función conjunta protección de la fuerza engloba aquellas actividades que tienen como objeto minimizar la vulnerabilidad del personal, equipo, material, instalaciones, información, operaciones y actividades de la fuerza y de los elementos no militares que apoyan, acompañan o están bajo responsabilidad de la fuerza, frente a las acciones adversarias, propias y frente a los riesgos sanitarios, naturales, tecnológicos y accidentes.

562. Su finalidad es preservar la libertad de acción del Comandante y garantizar la operatividad de la fuerza.

563. Comprende actividades de seguridad, contrainteligencia, actividades de ingenieros, defensa pasiva, recuperación de personal, protección sanitaria y defensa nuclear, biológica, química y radiológica (NBQR).

564. La seguridad incluye actividades de protección de las personas, combatientes o no, de la información, de las infraestructuras, de las instalaciones, de los medios y de la organización. Comprende actividades tan diversas como la seguridad y protección en el ciberespacio, las acciones defensivas de guerra electrónica, los procedimientos de identificación en combate y la lucha contra artefactos explosivos improvisados (C-IED), la seguridad vial, contraincendios, entre otras.

Publicación Doctrinal Conjunta PDC-01(A). Doctrina para el empleo de las Fuerzas Armadas. 27 de Febrero de 2018.

La protección consiste en disponer de una burbuja, contra acciones del adversario, en tres dimensiones (burbuja 3D), construida, sobre todo, con medios de defensa antiaérea, guerra electrónica (ciberdefensa, localización y perturbación, y Contra Sistemas de aeronaves no tripuladas (C-RPAS), enmascaramiento y detección Nucleares, Biológicas, Químicas y Radiológicas (NBQ-R).

La protección minimiza la vulnerabilidad del personal, el material, la infraestructura, las instalaciones, la información, el ciberespacio, las líneas de comunicación, las líneas de suministro, y las actividades a cualquier amenaza y en todas las situaciones, al tiempo que garantiza la libertad de acción de las fuerzas y contribuye al éxito de la misión. Debido a la naturaleza de las amenazas, la protección requiere un enfoque multidimensional – desde el nivel estratégico hasta el táctico, contra todo el espectro de amenazas, tanto en territorio nacional (TN) como en zona de operaciones (ZO).

Las fuerzas deben ser capaces de identificar, monitorizar y entender las nuevas amenazas, y desarrollar medidas de protección adecuadas que permitan crear y proteger un entorno permisivo para las operaciones a pesar de los métodos anti-acceso y de negación de área (A2/AD) del adversario.

Es esencial la protección del entorno electromagnético para garantizar su uso y para detectar, investigar, y defenderse contra todas las formas de ataque electromagnético, para ello es necesario que las fuerzas sean capaces de utilizar los métodos forenses y otros de atribución, reconocidos internacionalmente, para identificar la amenaza cibernética y actuar en consecuencia.

La protección ha de hacerse de las condiciones ambientales extremas, sobre cuestiones de salud y seguridad y minimizando su impacto medioambiental.

Proteger la infraestructura militar y civil crítica, las instalaciones logísticas, las redes vitales, los recursos naturales y las líneas esenciales de comunicación, facilitarán la proyección, empeño y sostenimiento de las fuerzas propias.

Forma parte de la protección ayudar a las autoridades locales y operar de manera que se preserve la propiedad civil que es cultural e históricamente importante.

Apoyo logístico

> 568. Se entiende por función conjunta apoyo logístico a las actividades centradas en el despliegue de las fuerzas, su sostenimiento en operaciones y su repliegue.
>
> 569. Su finalidad es que la fuerza disponga de la capacidad operativa necesaria para alcanzar y mantener el ritmo deseado de las operaciones hasta el cumplimiento de la misión.
>
> Publicación Doctrinal Conjunta PDC-01(A). Doctrina para el empleo de las Fuerzas Armadas. 27 de Febrero de 2018.

El apoyo logístico, en general, consiste en proporcionar personal, material, sanidad, y apoyo de ingeniería militar, requeridos para mantener el poder de combate en todas las fases de la operación.

El apoyo logístico incluye la capacidad de proyección estratégica y por tanto la capacidad de realizar despliegue, redespliegue y recepción, puesta en escena, movimiento e integración (RSOI) en apoyo de las operaciones y misiones de la fuerza. La proyección asegura que las unidades adecuadas estén en el lugar correcto en el momento oportuno para lograr objetivos político-militares.

Las fuerzas necesitan mantener el acceso asegurado por tierra, mar, aire y espacio (incluida la capacidad de lanzamiento) como requisito previo para la proyección, incluidas las actividades en el dominio del ciberespacio y el entorno de información. En consecuencia, las fuerzas deben poder desplegar, sostener y redesplegar donde y cuando sea necesario.

Habrá que mantener o establecer una red suficiente de infraestructura, bases, logística y otros servicios de apoyo en territorio propio, así como para las fuerzas expedicionarias que existan bases, puertos y bases aéreas en lugares remotos y posiblemente de riesgo.

Los ingenieros militares deben poder trabajar de manera multidisciplinar para apoyar las operaciones de construcción de infraestructura militar y civil crítica, tales como socorro humanitario y apoyo a las autoridades civiles. También, deben tener la capacidad de mantener una amplia interoperabilidad e integrarse con los contratistas civiles para complementar la capacidad de ingeniería militar orgánica.

Las fuerzas deben tener la capacidad de identificar y utilizar redes militares y no militares, para ayudar a sostener las operaciones en múltiples dominios con un mantenimiento escalable.

Las fuerzas deben mantener la autosuficiencia del apoyo nacional mientras permanecen lo suficientemente ágiles para reunir los recursos, esto incluye la capacidad de mejorar el sostenimiento y la logística, aprovechar las tecnologías y los sistemas autónomos y, en caso necesario, equilibrar la longitud de las cadenas logísticas contra

el riesgo operacional. También incluye la capacidad de establecer, mantener y utilizar centros logísticos dispersos y la capacidad de contratar el sostenimiento local o utilizar el apoyo de la nación anfitriona.

Tres áreas con potencial innovador son el uso de la fabricación aditiva, de la reparación autónoma, y de la ayuda experta remota.

Se requiere aligerar la carga física y cognitiva del combatiente, integrando con él las capacidades que ofrecen los elementos pilotados remotamente o autónomos y desplazar la carga del combatiente a plataformas robóticas y sistemas autónomos.

Es exigible reducir la redundancia innecesaria y racionalizar el sostenimiento al aprovechar las tecnologías avanzadas (por ejemplo, análisis de datos con inteligencia artificial, en el teatro de operaciones fabricación/impresión 3D) incluye la capacidad de aprovechar la tecnología de eficiencia energética y minimizar la huella logística asegurando un apoyo logístico ininterrumpido.

Las operaciones dispersas requerirán el acceso garantizado a los recursos de transporte terrestre, aéreo y marítimo para apoyar el sostenimiento y el movimiento en el teatro.

Los vehículos sin conductor, la entrega autónoma, una mejor eficiencia del combustible y el equipo tripulado no-tripulado pueden cambiar la forma en que se opera, lo que incluye la posibilidad de que se coordine y administre el movimiento y el transporte con recursos militares y civiles.

El exigente entorno del combatiente lo somete a factores de estrés físicos y cognitivos, para mejorar su resilencia habrá que actuar para preservar su salud mental y física.

La atención sanitaria en entornos remotos, austeros y degradados se facilitará mediante la gestión de la información médica y el empleo de nuevas tecnologías (por ejemplo, sensores, medicina personalizada, cognición aumentada, textiles inteligentes, equipos de atención crítica humano-máquina y cirugía automatizada).

Ministerio de Defensa de España y Ejército de Tierra de los Estados Unidos de América

Para finalizar, una breve descripción de marcos y tareas adoptadas por el Ministerio de Defensa de España y una iniciativa muy reciente del Ejército de Tierra de los EEUU.

Ministerio de Defensa

Dentro de la Dirección General de Armamento y Material la ETID constituye el marco general en el que se deben mover los distintos planes y actividades de los agentes dedicados a la I+D+i de la defensa en España.

El principal trabajo llevado a cabo en el marco de la ETID[16] ha consistido en la realización de un análisis tecnológico que ha permitido establecer cuáles son los objetivos tecnológicos a alcanzar para conseguir satisfacer las necesidades futuras de nuestras Fuerzas Armadas. Estos objetivos, denominados Metas Tecnológicas (MT), representan los ladrillos básicos a partir de las cuales se construye el edificio de la Estrategia, y sirven de guía fundamental para determinar el conjunto de actividades de I+T a realizar en los próximos años.

Las Metas tecnológicas (MT) se agrupan en seis grandes Áreas de Actuación Funcional (AAF), relacionadas con las principales funcionalidades de los sistemas de Defensa:

- Armas y Municiones [17],
- Sensores y Sistemas Electrónicos[18],
- Plataformas[19] ,
- Combatiente[20],
- NRBQe[21],
- C4I[22].

16 http://www.tecnologiaeinnovacion.defensa.gob.es/Lists/Publicaciones/Attachments/205/ETID%202015.pdf.

17 http://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Estrategia/HojasDeRuta/Paginas/Armas_Municiones.aspx.

18 http://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Estrategia/HojasDeRuta/Paginas/Sensores_SE.aspx.

19 http://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Estrategia/HojasDeRuta/Paginas/Plataformas.aspx.

20 http://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Estrategia/HojasDeRuta/Paginas/Combatiente.aspx.

21 http://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Estrategia/HojasDeRuta/Paginas/NRBQe.aspx.

22 http://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Estrategia/HojasDeRuta/Paginas/C4I.aspx.

Ejército de Tierra de los Estados Unidos de América

Como ejemplo muy reciente e innovador de un «sistema de ecodefensa», el Ejército de Tierra de los Estados Unidos ha establecido, por primera vez, un mando fuera de una base militar, como es la Universidad de Texas (Austin).

«Necesitábamos sumergirnos en un entorno donde se produce la innovación, a velocidades mucho más rápidas de lo que permite nuestro proceso actual», dijo el Secretario del Ejército Mark T. Esper. «Buscamos una ubicación que tuviera la combinación correcta de talento académico de primer nivel, una industria de vanguardia y un sector privado innovador».

Conclusiones

La tecnología no resuelve los problemas per se. Para hacer frente a los grandes desafíos de hoy, las naciones deben primero entender el problema y su naturaleza, después tener la ambición de resolverlo con el apoyo de sus instituciones, independientemente de la disponibilidad de tecnología. Los avances tecnológicos, desde la IA, han de significar una mayor eficiencia, una mayor efectividad y una mayor seguridad en todos los órdenes.

Concienciar a las personas de lo que es y de lo que no es la IA debe hacerse de manera global y, así, tratar de evitar «el miedo social» a la IA, dando a conocer los posibles beneficios y también perjuicios producidos por estas nuevas tecnologías.

Las FAS necesitan cumplir con las misiones asignadas, hoy y mañana. Para ello han de evolucionar e innovar para adaptarse a los rápidos cambios tecnológicos propios y del adversario.

El factor más importante es el capital humano. Su formación humana y científica, su entrenamiento, con los más actuales medios que permita la tecnología, y su sentido crítico seguirán siendo fundamentales para la necesaria voluntad de vencer sobre la voluntad del adversario. Hay que conseguir una formación más veraz, más humana, más ética que hagan posible un ser humano más sociable, más sabio y más inteligente.

La inteligencia artificial y humana son fundamentalmente diferentes, y las interfaces entre las dos deben ser diseñadas cuidadosamente y revisadas constantemente con el fin de evitar malentendidos, que en muchas aplicaciones podrían tener serias consecuencias. En la mayoría de los sectores, si no en todos, el futuro del esfuerzo humano verá cada vez más integración entre los seres humanos y las máquinas, tanto en las operaciones como en la toma de decisiones.

El uso de la IA ha de asegurar que en los procesos de toma de decisiones la responsabilidad final siga estando en el ser humano.

Una preocupación crítica es que gran parte de la investigación y la tecnología para los ejércitos se está desarrollando en el sector privado, más allá del ámbito de la reglamentación estatal y, por ende, la posibilidad de compra de estas tecnologías no es privativa de los Estados. Por ello hay que mantener un extraordinario esfuerzo de seguimiento de los avances tecnológicos.

Los exigentes requerimientos para los sistemas militares hacen que algunas tecnologías comerciales sean utilizables, pero requieren adaptaciones importantes, para ello es necesario establecer un ecosistema de defensa y seguridad sobre oportunidades y desafíos en IA. Por ello es urgente identificar una lista priorizada de aplicaciones de IA que puedan implementarse rápidamente dentro de las Fuerzas Armadas.

La regulación a nivel internacional de los sistemas de armas basados en la IA es diferente de la regulación de los sistemas de armas tradicionales. No obstante, las experiencias de estas regulaciones existentes han de servir para las necesarias regulaciones futuras.

Las tecnologías de IA aplicadas son y serán aún más capaces de reunir, evaluar y entregar cantidades inimaginables de datos, pero no es menos cierto que estas tecnologías hoy son y seguirán siendo vulnerables a las antiguas prácticas de denegación, decepción y engaño.

Unas áreas claves de investigación serían: aumento del rendimiento del soldado, mayor letalidad y protección, nuevos materiales, mejora de la movilidad de plataformas y soldados, aumentar la seguridad en las comunicaciones y la información.

Con el fin de beneficiarse plenamente de las posibilidades de la IA y el Big Data, para los ejércitos, es necesario iniciar una migración a una infraestructura de datos de gran capacidad, gestionada por tecnologías emergentes, que incluya el concepto de centralización de datos y escalabilidad del sistema.

En definitiva, las tecnologías han de ser de utilidad y en beneficio de todos los seres vivos del planeta Tierra y, por tanto, han de colaborar con la naturaleza para preservar el hábitat y ayudar a facilitar el conocimiento a todos los seres humanos, su sustento y su protección.

Capítulo 4

La inteligencia artificial y la fricción de la guerra

José Manuel Roldán Tudela

Resumen

El propósito de este capítulo es mostrar la influencia que tienen los sistemas de inteligencia artificial y de robótica inteligente en sus aplicaciones militares. Los ejércitos avanzados están aplicando estas tecnologías en todos los dominios de la acción militar. Resulta necesario definir conceptos de empleo de estos sistemas antes de utilizarlos masivamente en el campo de batalla. Estas tecnologías proporcionarán un aumento de capacidades militares en los niveles táctico, operacional y estratégico. El empleo de inteligencia artificial producirá un impacto importante en determinados tipos de operaciones militares en los tres niveles. La inteligencia artificial cambiará el carácter de la guerra, pero no modificará su naturaleza como un enfrentamiento humano incierto y complejo que busca un fin político.

Palabras clave

Inteligencia artificial, defensa y seguridad, concepto de empleo, operaciones, guerra, táctica, estrategia.

Artificial intelligence and the friction of war

Abstract

The purpose of this chapter is to show the influence of artificial intelligence and intelligent robotics systems in their military applications. Advanced armies are implementing these technologies in all domains of military action. It is necessary to define concepts of operation of these systems before they are employed massively on the battlefield. These technologies will provide increasing military capabilities at the tactical, operational, and strategic levels. Employment of artificial intelligence will have a major impact on certain types of military operations at the three levels. Artificial intelligence will change the character of war, but it won't alter its nature as an uncertain and complex human confrontation to achieve a political outcome.

Keywords

Artificial intelligence, defense and security, concept of operation, operations, war, tactics, strategy.

«By far, the greatest danger of Artificial Intelligence is that people conclude too early that they understand it».

«El mayor peligro de la Inteligencia artificial es, con mucho, que la gente suponga demasiado pronto que la comprende».

Eliezer Yudkowsky

Introducción

La aplicación de la tecnología a la guerra comenzó cuando el primer ser humano tomó un hueso largo de un animal muerto, o una gruesa rama pelada, y lo empleó para herir a otro de una tribu rival, al tiempo que se mantenía fuera del alcance de sus manos. Es posible que el grupo adversario aprendiese la lección y comenzase a utilizar ramas más largas, dando origen a la primera carrera armamentística.

De la película «2001 una odisea espacial».

A lo largo de la Historia, se han aplicado los desarrollos tecnológicos en la guerra y en la sociedad civil, independientemente de su origen. Hay tecnologías, como las nacidas en la época de la Industrialización, que fueron aplicadas progresivamente al ámbito militar. Otras, como la nuclear, surgieron como armas y tuvieron después aplicaciones civiles.

En general, el paso de la teoría a la práctica y su desarrollo requieren un tiempo, por lo que, normalmente, no se producen cambios bruscos en la sociedad ni en la conducción de la guerra.

Sin embargo, hay ocasiones en las que, dándose las condiciones adecuadas, una tecnología, o un conjunto de ellas, producen un gran impacto, tanto en la sociedad como en la manera de hacer la guerra. Si nos remontamos siglos atrás, el uso de la pólvora cambió, progresiva y completamente, la forma de combatir en los dominios terrestre y marítimo, obligando a diseñar nuevos tipos de buques de guerra. También facilitó las obras civiles, al permitir movimientos de tierras y demoliciones de obstáculos. La introducción de la pólvora produjo cambios en las industrias bélicas, ayudó a la desaparición de estructuras feudales y colaboró en la implantación de un nuevo modelo administrativo y territorial: el estado-nación monárquico.

La Inteligencia artificial (IA), apoyada en los grandes avances habidos en las tecnologías de la información y las telecomunicaciones, está causando un enorme impacto en la sociedad. Las fuerzas armadas de naciones tecnológicamente avanzadas están aplicando estas tecnologías en todos los dominios de la acción militar. En muchos casos, sustituirán a combatientes humanos y actuarán como estos. Pero es previsible que se desarrollen nuevos conceptos de empleo, aprovechando características de los sistemas de IA como la permanencia, resistencia, empleo en tareas de alto riesgo, inteligencia, coordinación y velocidad.

En el capítulo primero se han señalado los dos tipos de IA: fuerte y débil. La existencia de una IA fuerte es objeto de discusiones y no existe consenso sobre si se conseguirá ni cuándo. Por tanto, nos centraremos en la IA débil o estrecha, con las características que indica el primer capítulo.

El propósito de este capítulo es mostrar la influencia que tienen los sistemas o dispositivos de IA y de robótica inteligente (RI) en sus aplicaciones militares. La abreviatura RI puede designar «Robótica Inteligente» o «robot inteligente», según el contexto.

En primer lugar, se intentará establecer unos conceptos de empleo para IA y RI, deduciéndolos de un análisis de sus ventajas e inconvenientes. Se hará particular mención de los enjambres de robots como concepto emergente de empleo.

Seguidamente se tratarán los niveles operacional y táctico, señalando las mejoras de capacidades que proporcionará el uso de IA y RI. Se mostrarán ejemplos significativos sobre operaciones muy adecuadas para el uso de IA y RI. A continuación, se comentará la necesidad de introducir cambios en técnicas, procedimientos y tácticas.

Análogamente, en el nivel estratégico se expondrá la mejora de capacidades y el tipo de operaciones influidas por la IA.

Se comentará a continuación la necesidad de que la doctrina militar y las reglas de enfrentamiento se acompasen al uso de la IA y RI en operaciones militares, así

como la influencia que tendrán estas tecnologías en la enseñanza, la instrucción y el adiestramiento militar.

Finalmente, se dedica un breve apartado a reflexionar sobre el impacto de la IA sobre el carácter y naturaleza de la guerra, sirviendo de marco para la discusión el modelo de la trinidad de Clausewitz.

Conceptos de empleo de la inteligencia artificial

Análisis previo

Teniendo en cuenta que la IA y la RI son tecnologías complejas y avanzadas y que su uso extensivo en operaciones militares está en sus comienzos, es necesario establecer los conceptos de empleo que guíen su implantación. Para ello, se precisa un análisis previo de las características propias de estos dispositivos y de factores externos que influyen en su utilización. Este análisis tiene en cuenta las tendencias que define el documento *Strategic Foresight Analysis (SFA) 2017*[1], que se han desarrollado en el capítulo tercero.

Intrínsecamente, los dispositivos de IA y RI poseen la capacidad de tratar grandes volúmenes de datos, de distinto tipo: imágenes, vídeo, audio, texto, datos «crudos» de sensores, etc. Su procedencia también puede ser variable: bases de datos, la web, sensores, medios de comunicación, redes sociales, etc. El factor clave en el tratamiento de los datos es que se hace a gran velocidad, superando con mucho las capacidades humanas, por lo que se pueden realizar análisis en tiempo real o casi real de grandes volúmenes de datos que serían imposibles de tratar manualmente. La rapidez de proceso y de comunicación entre dispositivos permite una coordinación casi instantánea de sus acciones.

Estos dispositivos tienen capacidad de aprendizaje y evolución, tal como se ha descrito en el capítulo segundo. La evolución se realiza en su «mundo», es decir en el marco del conjunto de datos con el que han sido adiestrados. Una vez que un sistema ha sido entrenado y pasa las pruebas correctamente, puede ser replicado. De esta manera, es posible desplegar un conjunto de dispositivos idénticos y se facilita su rápida sustitución en caso de quedar fuera de servicio.

1 NATO/OTAN. *Strategic Foresight Analysis Report 2017*. HQ Supreme Allied Commander Transformation. Norfolk (VA) EE. UU. 2017. Disponible en: http://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf.

Son «prescindibles», lo que no ocurre con los combatientes humanos, cuya vida tiene un valor incalculable.

Los dispositivos de RI añaden a lo anteriormente dicho su resistencia y permanencia, pues no están sujetos a las limitaciones de la biología humana. Por tanto, pueden operar durante largos periodos, insensibles a la fatiga, sueño, estrés y necesidades fisiológicas. Tampoco se ven influidos por los estados de ánimo ni las emociones, por lo que no actuarán por miedo, ira, deseos de venganza, odio ni otros sentimientos destructivos. Por otro lado, debidamente diseñados, pueden trabajar en ambientes peligrosos (riesgo nuclear, biológico, químico o radiactivo - NBQR) o letales para los humanos (espacio exterior, grandes profundidades marinas).

Su morfología es adaptable a la misión. Pueden adoptar distintas formas y tamaños y ser dotados con sensores y actuadores adaptados a la misión. Como se ha dicho en el capítulo segundo, pueden ser dotados de sentidos artificiales, incluso superando los humanos (visión en el espectro infrarrojo, detección de ultrasonidos, detección de sustancias explosivas). Los actuadores les proporcionan fuerza y precisión superior a la de los humanos. Pueden ser protegidos para resistir agresiones armadas.

Frente a estas cualidades positivas, los dispositivos de IA y RI comparten puntos débiles. En primer lugar, necesitan datos para funcionar. Requieren datos en cantidad y la calidad de sus resultados depende de la calidad de estos. Responden peor que los seres humanos ante situaciones inesperadas con escasos datos disponibles.

Necesitan ser entrenados con un gran volumen de datos. El resultado del aprendizaje depende de la calidad de los datos suministrados y de que no sean sesgados. Por otro lado, una incorrecta especificación de su objetivo puede conducir a un resultado negativo. También puede darse el caso de que una especificación impropia permita que el sistema «haga trampas», encontrando una forma no deseada de alcanzar el objetivo[2].

Una vez entrenados, son capaces de evolucionar, pero solo ejecutan aquello para lo que han sido adiestrados. Por tanto, si se producen cambios significativos en el contexto de los datos con los que trabajan, es necesario entrenarlos de nuevo[3]. Dado

2 Por ejemplo, un algoritmo jugador de Tetris aprendió a detener el juego justo antes de que la caída del último bloque le hiciera perder el juego. Al no terminar nunca el juego, no perdía. SCHARRE Paul, HOROWITZ Michael «Artificial Intelligence: What Every Policymaker Needs to Know», CNAS, Washington (DC), EE. UU. junio 2018.

3 Según el teniente coronel de los EE. UU. Garry Floyd, segundo jefe del Proyecto Maven de DARPA, cuando desplegaron el primer prototipo de IA de procesamiento de vídeo en el Mando de África hubo que entrenar de nuevo el dispositivo seis veces en cinco días. El entrenamiento original se había realizado con datos de otra región del globo. Podría suceder que el algoritmo identificase erróneamente una palmera como una persona. POMERLEAU, Mark. «What the Pentagon is learning from its massive machine learning project» C4ISR, 2 de mayo de 2018. https://www.c4isrnet.

que no tienen conciencia del mundo real, son incapaces de contextualizar, generalizar ni apreciar señales que los humanos sí captan. No pueden reaccionar ante lo inesperado ni analizar posibilidades futuras, fuera del «mundo» de sus datos.

La posibilidad de un funcionamiento anómalo es un factor negativo de peso. Como todos los equipos de tecnología avanzada, los dispositivos de IA y RI pueden sufrir averías de «*hardware*» o «*software*». Su reparación no es sencilla y exige un elevado grado de especialización. Pero el funcionamiento anómalo puede tener otro origen. Son equipos que actúan en el ciberespacio. Por tanto, son susceptibles de ser atacados por «piratas» informáticos («*hackers*») que pueden conseguir que el control del dispositivo caiga en manos indebidas.

Por otra parte, estos dispositivos pueden ser engañados al introducir los datos. En la fase de aprendizaje, es posible que los datos suministrados no estén bien escogidos o sean erróneos, lo que dará lugar a comportamientos anómalos y resultados falsos. Además, un adversario con el suficiente nivel tecnológico (usando quizá también IA) puede difundir datos sesgados, confusos, incoherentes o contradictorios en gran cantidad, de forma que el dispositivo se ve engañado[4].

En otro orden de cosas, los dispositivos son sensibles al impulso electromagnético (EMP). Se han realizado pruebas con éxito de misiles capaces de inutilizar equipos electrónicos en una amplia zona[5]. Los avances en miniaturización y en fuentes de energía permiten predecir la existencia de armas portátiles emisoras de EMP, que serían muy eficaces contra los dispositivos de RI.

Por su parte, los RI consumen energía para sus desplazamientos y operación. En el caso de los RI terrestres, se necesita generalmente dotarlos de un motor de combustión, lo que incrementa su firma de ruido. El suministro de energía es una carga añadida a la cadena logística específica de estos dispositivos.

Finalmente, los dispositivos de RI necesitan comunicarse entre ellos, con los sensores remotos y con los operadores humanos. En un ambiente electromagnético denso y

---

com/intel-geoint/isr/2018/05/02/what-the-pentagon-is-learning-from-its-massive-machine-learning-project/. Fecha de la consulta 20.05.2018.

4 A veces los datos no tienen que ser modificados en gran medida. Un cambio imperceptible en una imagen hace que esta se clasifique erróneamente por el dispositivo. También puede identificar una imagen con ruido blanco como un objeto reconocible con un 99% de confianza. NGUYEN A, YOSINSKI J, CLUNE J. *Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images*, Computer Vision and Pattern Recognition (CVPR '15), IEEE, 2015.

5 Boeing anunció en 2012 que había probado con éxito un misil de estas características, denominado CHAMP, en un campo de maniobras de Utah (EE. UU.). BOEING, «Boeing Non-Kinetic Missile Records 1st Operational Test Flight», octubre 2012, http://boeing.mediaroom.com/2012-10-22-Boeing-Non-kinetic-Missile-Records-1st-Operational-Test-Flight. Fecha de la consulta 12.05.2018.

disputado con el adversario, la ruptura de estos enlaces puede tener consecuencias dispares según la misión y el modo de operación de los dispositivos. En unos casos la autonomía conferida a los RI permitirá que cumplan la misión aún en caso de pérdida de la comunicación con el operador, lo que constituye una ventaja. En otros casos, la misión no podría completarse hasta recuperar el contacto con el supervisor.

Existen factores externos que favorecen el empleo de los dispositivos de IA y RI. El más atractivo socialmente es que la utilización de estos dispositivos permite ahorrar vidas humanas. Situar estos dispositivos en los lugares o misiones más peligrosas resulta muy aceptable para la sociedad. También lo es el empleo de la IA para doblegar al adversario mediante un elevado conocimiento de su situación e intenciones, haciendo más breve el enfrentamiento.

Por otra parte, estos dispositivos son un multiplicador de fuerza, por lo que se puede realizar la misma misión con menos combatientes y con más eficacia. Por tanto, a largo plazo, la introducción de estos dispositivos supondrá un importante ahorro económico, manteniendo la operatividad.

Un factor de peso es el de la escalada. Aunque una nación decida no emplear dispositivos de IA o RI autónomos, no puede evitar que otras naciones o actores no estatales los utilicen. En este caso, se encontraría en una situación de franca desventaja, lo que le impulsaría a dotarse de estos medios para defenderse.

Por otra parte, existen factores externos que se alinean en contra del uso de estos dispositivos. En primer lugar, se puede hablar de un temor extendido en la sociedad a los «robots asesinos» empleados con fines militares, como se muestra en el capítulo quinto.

Otro factor en contra es que los procesos que se ejecutan en los sistemas de IA tienen características de «caja negra». Estos procesos se ven como misteriosos algoritmos, ajenos totalmente a la manera en que los humanos razonan o identifican las cosas. Es necesario que el mando militar y los operadores confíen en los resultados y en el comportamiento actual y futuro de los sistemas, pero ello no se puede derivar de un acto de fe.

Finalmente, hay que tener en cuenta el rechazo que provocarán este tipo de dispositivos en la población local. En todo el espectro de los conflictos, la población local de la zona de operaciones sentirá un fuerte rechazo a la presencia de dispositivos de RI armados.

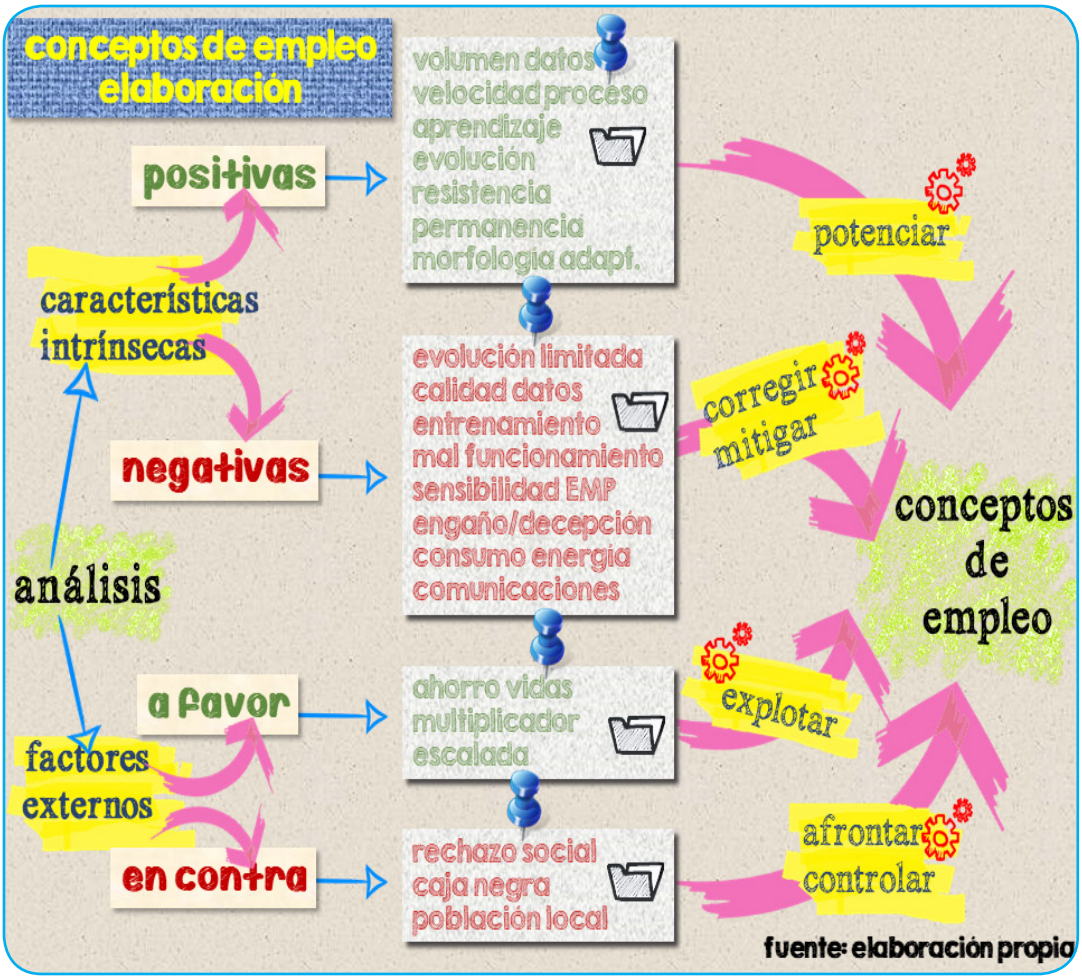


Figura 1.- Proceso para establecer los conceptos de empleo.

Conceptos de empleo

Del análisis anterior se pueden extraer conceptos de empleo de estos dispositivos mediante la potenciación de sus puntos fuertes y el aprovechamiento de los factores externos positivos. Se complementará con una mitigación de sus puntos débiles y de los factores externos negativos. Finalmente, habrá que tener en cuenta cuestiones de tipo ético y legal.

Es corriente hacer una clasificación de los dispositivos de IA y RI en función de su grado de autonomía, dando diferentes denominaciones: operados a distancia, semiautónomos, autónomos, etc. Esta clasificación es fuente de problemas en su empleo militar, sobre todo en misiones de combate. Parece más útil centrarse, no sobre el conjunto del dispositivo, sino sobre las funciones que realiza en el cumplimiento de su misión. De esta manera, por ejemplo, un vehículo aéreo no tripulado puede ser autónomo en cuanto a despegue y aterrizaje, navegación hasta y desde el objetivo,

control y diagnóstico de su funcionamiento e identificación del objetivo. Al mismo tiempo no será autónomo en cuanto al inicio de la misión y acción de fuego sobre el blanco, para lo que requerirá una orden o autorización de su supervisor.

A fin de habilitar el juicio humano sobre el uso de la fuerza y otras acciones o de validar los resultados del tratamiento de la información, los dispositivos de IA y RI deben funcionar supervisados por personas. Según se explica en el capítulo quinto, estas personas (mandos, supervisores u operadores) autorizarán o dirigirán su empleo de manera responsable.

Por tanto, los dispositivos, especialmente los RI, incorporarán una interfaz sencilla y técnicamente avanzada. Esta interfaz proporcionará indicaciones sobre el estado operativo de las principales funciones del dispositivo, que quedarán registradas. También debe disponer de procedimientos sencillos, claramente explicados, para activar y desactivar estas funciones.

Es esencial el trabajo conjunto de personas y RI. La estructura orgánica y funcional de los equipos mixtos de humanos y RI debe ser diseñada para extraer la máxima potencialidad de la IA como multiplicador de fuerza, evitar en lo posible el riesgo de pérdidas humanas y contrarrestar las limitaciones físicas y psíquicas de los combatientes.

La generación de confianza es clave para su empleo. Hay que evitar que los mandos u operadores desconfíen de las recomendaciones o predicciones que, aparentemente, provienen de oscuros e incomprensibles algoritmos. Para ello, es necesario diseñar dispositivos que puedan explicar en qué basan sus decisiones, describir cuál será su comportamiento en el futuro y señalar sus puntos fuertes y débiles.

Antes de poner en operación los dispositivos de IA y RI, se debe validar su entrenamiento, tanto en el contexto de la operación como en la misión para la que serán empleados. Es necesario reevaluar periódicamente este entrenamiento, o si la situación cambia drásticamente.

Los dispositivos deben incluir sistemas o mecanismos de seguridad. Dispondrán de mecanismos antiintrusión y antimanipulación. También se les dotará de sistemas y procedimientos de seguridad de la información.

Los RI se emplearán preferentemente:

- En primera línea del enfrentamiento.
- En ambientes o situaciones de gran riesgo para la vida humana.
- Cuando se requiera permanencia y aguante.
- Para disminuir la fatiga física y mental de los seres humanos.
- Cuando se requiera gran rapidez de reacción.

Cuando se empleen RI supervisados por un operador y se pierda el contacto con éste, el dispositivo no podrá seleccionar ni batir objetivos de forma automática.

En el caso de misiones que no impliquen el uso de armamento ni tengan consecuencias letales (por ejemplo: perturbación electrónica), se puede permitir la selección y tratamiento de objetivos de forma autónoma a RI supervisados.

Cuando una posición ocupada por personal o una plataforma tripulada reciban un ataque por saturación o en el que la rapidez de reacción sea un factor crítico, se puede permitir a RI supervisados que, de forma autónoma, seleccionen y disparen contra objetivos, excepto personas.

Enjambres

La Naturaleza proporciona ejemplos de animales e insectos sociales que cooperan obteniendo notables beneficios en actividades como protección, recolección de alimento o migración. Las investigaciones sobre el comportamiento de estos animales aplicadas a la robótica inteligente han dado lugar a conceptos como robótica de enjambres, inteligencia de enjambres o algoritmos de enjambres. Su objetivo es reproducir este comportamiento en robots y sistemas informáticos.

Un enjambre de robots es un conjunto formado por un número elevado de estos, generalmente idénticos o con poca variación de tipos, sencillos y capaces de interactuar ente sí y con su entorno local. De estas interacciones surge un comportamiento colectivo que permite al enjambre realizar tareas que no pueden ser llevadas a cabo por los individuos que lo componen.

Por otra parte, hay que asumir que los robots que componen el enjambre deben ser autónomos en gran parte de sus funciones para poder interactuar entre sí y con un entorno real. De lo contrario, sería imposible su control por operadores humanos dado el elevado número de miembros que lo componen.

El número de componentes tiene importancia. Un enjambre es diferente de un sistema multirobot. Este último consta de un número reducido de robots diferentes (generalmente menos de 10), que cumplen una tarea descompuesta en varias acciones para aumentar la eficacia del proceso. Sin embargo, el enjambre consta de muchos individuos (decenas o cientos, quizá miles) iguales o de reducido número de tipos, que cumplen una misión como conjunto mediante un comportamiento colectivo.

Tampoco deben confundirse los enjambres con las bandadas. Estas están constituidas por conjuntos de plataformas tripuladas (terrestres, navales o aéreas) y robots. Cada plataforma tripulada tiene a su cargo un grupo de robots a los que controla. Los robots pueden ser de varios tipos, de forma que sus capacidades se complementen.

El número de robots es necesariamente reducido para poder ser controlado por operadores humanos. En las bandadas no hay un comportamiento colectivo, sino que son unidades militares con un sistema de mando puramente jerárquico.

Extrapolando y adaptando a los enjambres las características que Arkin (1998)[6] atribuye a los sistemas multirobot, podemos deducir las siguientes ventajas de su uso:

- Mayor eficacia. Las tareas pueden ser descompuestas y realizadas más eficazmente por muchos individuos.
- Se pueden realizar tareas que resultan imposibles de ejecutar por robots individuales.
- Se crea una extensa y eficaz red de sensores distribuida utilizando los de todos los individuos del enjambre.
- Coordinación de esfuerzos. El enjambre puede actuar sobre distintas localizaciones al mismo tiempo.
- Robustez derivada de su tolerancia a fallos. El fallo de algunos individuos no impide que la misión se cumpla, debido a la redundancia y a la reconfiguración inherente al comportamiento colectivo.

Por otro lado, existen ciertos inconvenientes:

- Posibilidad de interferencias. Los individuos pueden colisionar u obstaculizarse entre sí. También pueden interferir sus telecomunicaciones o apantallar sus sensores.
- Posibilidad de competencia. Si un robot no interpreta correctamente lo que está haciendo otro cercano e ignora sus intenciones, puede acabar compitiendo con él en lugar de colaborar.

Para controlar un enjambre de robots se pueden emplear varios métodos, de los que los más significativos son[7]:

- Por reglas de comportamiento. El controlador dispone de un catálogo de reglas simples conocidas por los robots. Para cada misión que se encomienda al enjambre, hay un conjunto de reglas cuyo resultado es el comportamiento emergente deseado del conjunto.
- Por directrices. En lugar de gestionar reglas de comportamiento para cada individuo, el operador da órdenes, recomendaciones y restricciones para cumplir

6 ARKIN, Ronald, *Behavior-Based Robotics*, MIT Press, Cambridge, Mass, USA, 1998.

7 COPPIN, Gilles and LEGRAS, François, «Autonomy Spectrum and Performance Perception Issues in Swarm Supervisory Control,» Proceedings of the IEEE 100, no. 3, marzo 2012.

la tarea asignada. Los robots determinan su comportamiento conforme a estas directrices.

- Por guión. El controlador dispone de una colección de guiones que reflejan cada uno un plan de acción, en el que se asigna a cada individuo su papel para cada tipo de acción y sus variantes. Estos guiones son conocidos por los robots, que los ejecutan cuando se ordena.

Los niveles táctico y operacional

Mejora de capacidades

En los niveles táctico y operacional la utilización de IA y RI proporcionará un aumento de capacidades militares en distintas áreas, siendo el impacto mayor en unas que en otras. El incremento de capacidades en algunas áreas dependerá de la evolución de la tecnología y se hará presente a un plazo más largo. Se van a tratar las más significativas, que se alinean con lo expresado en el tercer capítulo, al comentar el documento *Framework for Future Alliance Operations (FFAO) 2018*[8].

El conocimiento de la situación es una capacidad esencial cuya finalidad es proporcionar al mando la información que necesita para sustentar las decisiones que debe adoptar. El problema de aportar al mando un adecuado conocimiento de la situación en una zona de operaciones, quizá lejana y de complejas características físicas y humanas, es cada vez de más difícil solución si consideramos, además, el ritmo creciente de las acciones militares. El empleo de IA para el tratamiento de volúmenes masivos de datos, y de RI para desplegar sensores en amplias zonas con permanencia constituye una herramienta muy útil para obtener la solución. Estas tecnologías permitirán al mando una comprensión de la situación en tiempo real, o casi real, utilizando datos y técnicas para su tratamiento inaccesibles al ser humano por su volumen, velocidad y complejidad.

El conocimiento de la situación es un proceso importante dentro de un ciclo de mayor trascendencia que es el de la toma de decisión. Todos los ejércitos tienen procesos normalizados para la toma de decisiones en cualquier nivel de mando. En

8 NATO/OTAN. *The Framework for Future Alliance Operations (FFAO) 2018*. HQ Supreme Allied Commander Transformation. Norfolk (VA) EE. UU. 2018. Disponible en: http://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18-txt.pdf.

el campo de batalla moderno el acortamiento de los ciclos de decisión aporta una ventaja determinante frente al adversario. Estas técnicas facilitan la simulación de una gran cantidad de posibles escenarios, con las líneas de acción propias y enemigas. El conjunto del proceso permite recomendar, rápidamente, la línea de acción más adecuada para el cumplimiento de la misión.

Una ventaja adicional del uso de estas técnicas en el proceso de toma de decisiones es que la automatización del análisis y la actualización continua del conocimiento de la situación permite una rápida reacción frente a la naturaleza cambiante y el acelerado ritmo de las operaciones. De esta forma, los mandos pueden modificar rápidamente las órdenes iniciales en función de la evolución de la acción. Por otra parte, la gran capacidad de tratamiento de información permite un mejor manejo de situaciones complejas. El planeamiento de la asignación de un elevado número de recursos, en secuencias complejas, a misiones con elevado grado de interdependencia requiere ciclos de larga duración. El uso de IA permite reducir enormemente estos ciclos, incluyendo el análisis de posibles contingencias.

La capacidad de maniobrar y aplicar la fuerza puede verse mejorada por el uso de IA y RI. Por un lado, herramientas de IA contribuyen a facilitar la integración y coordinación de las capacidades de combate de una fuerza. La coordinación de acciones en el momento oportuno proporciona la superioridad local necesaria para derrotar al enemigo. Por otro lado, el uso de RI extiende el radio de acción de las propias fuerzas, de forma que se incrementa el tiempo y el espacio del que se dispone para superar al adversario, manteniendo la iniciativa.

Todos los planes deben incluir la decepción del adversario. Los sistemas de IA son capaces no solo de absorber datos, sino también de producirlos en gran cantidad y calidad. Esto permite al mando aumentar su capacidad de decepción al enemigo, al suministrarle deliberadamente un elevado volumen de datos con un estudiado sesgo.

La protección de la fuerza es otra capacidad que se verá incrementada. El uso de RI en primera línea de fuego y en ambientes hostiles o para cometidos peligrosos aumentará la supervivencia de los seres humanos.

El rendimiento del combatiente se verá mejorado. Los dispositivos de IA y RI pueden reducir la carga física y cognitiva de los seres humanos. Un mejor conocimiento de la situación basado en IA descarga a los mandos de la avalancha de datos del campo de batalla moderno, permitiendo que se concentren en la toma de decisiones. El uso de RI en tareas que exigen esfuerzo físico elevado incrementa la velocidad, movilidad, resistencia y eficacia de los combatientes.

La capacidad de permanencia se ve aumentada por el uso de RI. Al estar libres de limitaciones biológicas, los RI pueden desplegar y cumplir sus cometidos en un área amplia. Con los avances en fuentes de energía y con dispositivos más eficientes, se podrán cubrir extensas zonas durante largos periodos.

Tipos de operaciones

Aunque el empleo de IA y RI acarreará ventajas en la mayoría de las aplicaciones, hay tipos de operaciones en los que el impacto que producirá su uso será notable. En estas operaciones, el papel de los combatientes humanos cambiará, su número se verá reducido y la eficacia y eficiencia de las acciones propias aumentará.

Sin ánimo de ser exhaustivo, se van a considerar varios ejemplos significativos en tres de los cinco dominios de la acción militar que actualmente se contemplan: terrestre, marítimo y aéreo. Se considera que los otros dos dominios (espacio y ciberespacio) pertenecen al nivel estratégico.

Común a los tres dominios citados son las operaciones de inteligencia, vigilancia y reconocimiento, conocidas por su abreviatura inglesa, ISR (de *intelligence, surveillance, and reconnaissance*). El empleo de RI aéreos, marítimos y terrestres en estas misiones proporcionarán mayor persistencia, resiliencia y volumen de información con menos personal y menor riesgo de pérdida de vidas humanas. Las plataformas más empleadas serán las aéreas, aunque los vehículos navales son de gran utilidad en zonas costeras disputadas u hostiles. Los vehículos terrestres aparecen como más adecuados para misiones de reconocimiento y vigilancia próxima.

Operaciones terrestres

Los vehículos aéreos no tripulados, o UAV (de *unmanned aerial vehicle*), pilotados remotamente, se han empleado ampliamente por fuerzas terrestres en misiones ISR de apoyo a unidades desplegadas.

Los RI que participen en operaciones terrestres serán de dos tipos:

- De tipo UAV para seguir cumpliendo las misiones citadas.
- Vehículos terrestres no tripulados (UGV, de *unmanned ground vehicle*). Estos podrán ser armados o no y adoptarán distintas morfologías, tamaños y medios de locomoción para adaptarse a los cometidos que se les asignen.

Aprovechando la experiencia con UGV operados a distancia, los RI serán eficaces en operaciones de apertura de brechas en campos de minas y otros obstáculos. También se usarán en operaciones de desminado en zonas conquistadas o recuperadas.

Los RI serán muy útiles en misiones de reconocimiento de rutas terrestres, neutralización de artefactos explosivos improvisados y de munición que no haya explosionado.

El uso de RI introducirá cambios notables en las operaciones de combate en zona urbana.

Las fuerzas terrestres se dotarán de UAV que permitirán orgánicamente el apoyo aéreo próximo a unidades combatientes.

Los RI podrán llevar a cabo en solitario misiones de reconocimiento NBQR, delimitando la zona contaminada e informando. También serán capaces de realizar tareas de descontaminación, manipulación, transporte y, en su caso, destrucción o neutralización del contaminante.

En las operaciones de decepción, el empleo de RI permitirá distraer recursos del adversario.

Los riesgos para la vida humana asociados al movimiento de convoyes se verán reducidos al emplearse RI, ya que se requerirá menos personal.

Figura 2.- Esquema de combate en zona urbana.

Operaciones navales

Actualmente se emplean dos tipos de vehículos marinos no tripulados, operados remotamente:

- Vehículos no tripulados de superficie, conocidos como USV (de *unmanned surface vehicle*).
- Vehículos no tripulados submarinos, o UUV (de *unmanned undersea vehicle*)

Los RI que participen en operaciones navales adoptarán, en general, una de esas dos formas.

Las operaciones navales para las que resultan más indicados los RI son las de medidas contraminas (MCM).

De forma complementaria, los RI pueden ser empleados en operaciones de minado.

Parte de las operaciones de lucha antisubmarina o ASW (de *anti-submarine warfare*) también pueden ser encomendadas a los RI.

En apoyo de las MCM y la ASW, se realizan operaciones de **oceanografía táctica**.

Finalmente, los RI están muy indicados para participar en misiones de búsqueda y rescate submarino.

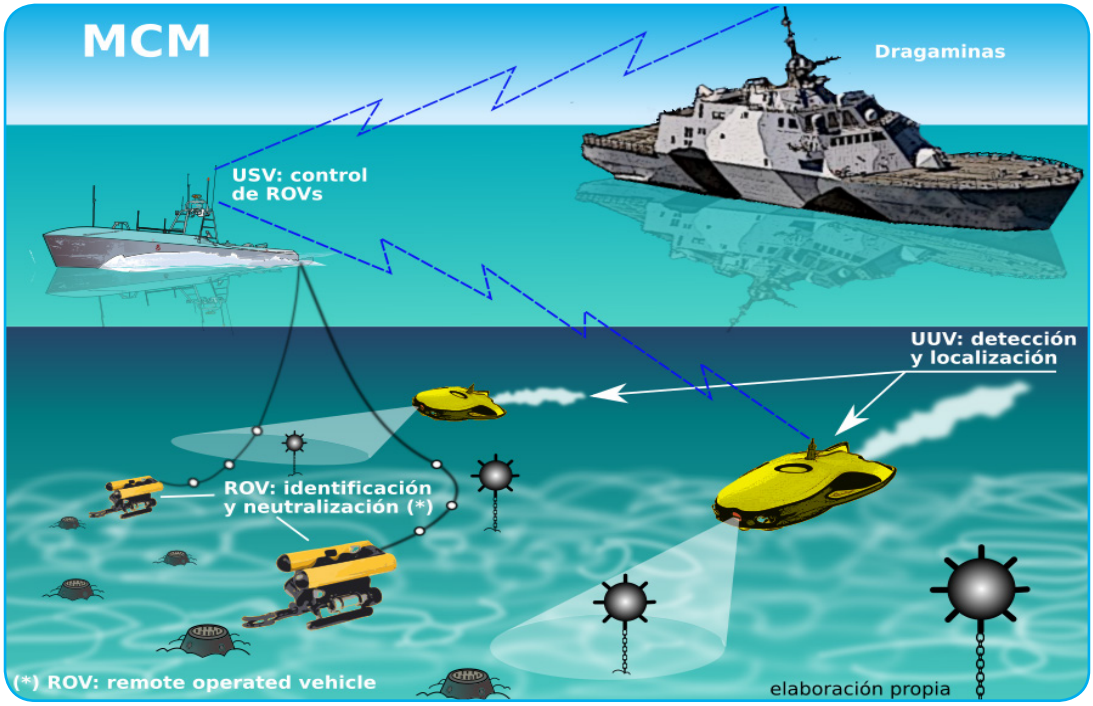


Figura 3.- Operación de medidas contraminas (concepto).

Operaciones aéreas

Las fuerzas aéreas han empleado vehículos aéreos no tripulados, pilotados remotamente, en misiones ISR, proporcionando información al nivel estratégico y operacional, pero también a las unidades tácticas sobre el terreno. También han sido utilizados para ataques de precisión sobre objetivos de gran valor, planeados o de oportunidad, minimizando el riesgo de daños colaterales.

El empleo de RI adoptando la forma de UAV supondrá mantener estas misiones y ejecutar otras que hasta ahora no se realizan.

Las operaciones de supresión de las defensas aéreas enemigas se ven facilitadas por el empleo de RI.

Los RI podrán emplearse en misiones de interdicción aérea.

Las acciones de apoyo aéreo a fuerzas sobre el terreno son otro tipo de misiones que pueden ser realizadas por RI.

Citaremos finalmente las operaciones de búsqueda y rescate de combate.

Logística

De conformidad con las consideraciones expuestas en el capítulo tercero sobre logística, se obtendrá una mejora de capacidades mediante la aplicación de IA y RI. Resumiendo, el planeamiento se verá facilitado por el uso de la IA. Funciones logísticas importantes como el transporte, el abastecimiento, el mantenimiento y la asistencia sanitaria experimentarán mejoras importantes, tal como se puede ver actualmente en la logística comercial. La eficiencia aumentará y se podrá reducir el personal dedicado a funciones logísticas. Al mismo tiempo, la «huella» logística sobre el terreno se verá reducida.

Cambios en técnicas, procedimientos y tácticas

Cualquier adelanto tecnológico aplicado a las operaciones militares trae consigo necesariamente un cambio en las técnicas y los procedimientos. En el empleo de la IA y la RI es evidente que será necesario introducir cambios en las técnicas de empleo de los medios. La complejidad de las tecnologías subyacentes y los efectos que producen estos medios hacen necesario adquirir nuevas técnicas de empleo, documentarlas e instruir al personal para obtener la máxima eficacia posible.

Los procedimientos también se verán afectados. Como ejemplo, basta repasar las operaciones que se han relacionado en el apartado anterior. La naturaleza y los objetivos de estas misiones no cambian. Sin embargo, la manera de llevarlas a cabo, es decir, los procesos operativos que intervienen en cada acción, desde que empieza hasta que termina, son diferentes debido a la introducción de nuevos medios y de una nueva organización para el combate.

Las tecnologías disruptivas producen, como es sabido, cambios importantes en la táctica. Estos cambios no se implantan de forma inmediata. Suele ser necesario un periodo de tiempo y un éxito militar asociado. Por ejemplo, desde que aparecieron los primeros tanques hasta que se generalizaron las tácticas de empleo de unidades acorazadas pasaron más de treinta años. Además, el catalizador fue el éxito de las

unidades *Panzer* alemanas al principio de la Segunda Guerra Mundial, con su «guerra relámpago». Actualmente, los dispositivos de IA y RI están en una fase muy temprana de introducción, por lo que las tácticas de empleo solo pueden desarrollarse a nivel conceptual. Normalmente, para desarrollar conceptos tácticos es necesario disponer de lecciones aprendidas de situaciones reales. Sin embargo, en un primer momento, la experiencia real deberá ser sustituida por ejercicios y por simulación.

El nivel estratégico

Mejora de capacidades

Al igual que en los niveles táctico y operacional, la mejora de capacidades en el nivel estratégico tiene en cuenta lo comentado en el capítulo tercero en su análisis del documento Framework for Future Alliance Operations (FFAO) 2018[8], ya mencionado.

Conocimiento de la situación

El conocimiento de la situación en el nivel estratégico se verá mejorado por la utilización de la IA. La razón de este aumento de capacidad es la misma que ya se ha señalado en los niveles táctico y operacional: la posibilidad de utilizar datos y técnicas para tratar datos inaccesibles al ser humano. El comandante de la operación dispone de datos procedentes de distintas fuentes, principalmente:

- Datos procedentes de los niveles operacional y táctico en los distintos teatros o zonas de operaciones.
- Datos suministrados por los propios sistemas ISR de nivel estratégico.
- Inteligencia estratégica elaborada con anterioridad y continuamente actualizada.
- Datos procedentes de naciones aliadas, organizaciones multilaterales o coaliciones.
- Un gran volumen de datos procedente de Internet, que incluye redes sociales, fuentes abiertas y la Internet profunda.

El rápido tratamiento de este gran volumen de datos proporciona una imagen más completa y acertada de la situación en el nivel estratégico militar.

Planeamiento estratégico de las operaciones

Partiendo de un amplio y actualizado conocimiento de la situación, la aplicación de la IA al planeamiento permite analizar la naturaleza del problema por resolver. En función de factores previamente señalados, identifica posibles objetivos estratégicos, según la situación final deseada. Elabora posibles líneas de acción, simula su ejecución y determina si cumplen con los requisitos establecidos y las capacidades disponibles. De todo ello se deducen las opciones de respuesta militar que el comandante de la operación valida y presenta al nivel político estratégico. El proceso es, en esencia, el mismo, pero la IA proporciona un análisis más profundo y exhaustivo y una rapidez que añade una ventaja estratégica en la resolución de la crisis.

El uso de la IA facilita el proceso de generación de fuerzas. A través del tratamiento de datos sobre las capacidades propias, permite identificar y asignar las capacidades a la organización operativa, explorando múltiples posibilidades y recomendando las que mejor se ajustan a la misión.

Conducción y seguimiento estratégico

La mejora en el conocimiento de la situación tendrá un impacto muy positivo en la conducción estratégica de las operaciones. En esta función, el análisis predictivo se muestra como una técnica fundamental. Las variaciones de la situación se analizarán con rapidez y se recomendarán casi inmediatamente los ajustes necesarios para no comprometer la consecución de los objetivos estratégicos militares. En su caso, puede recomendar la iniciación de un nuevo proceso de planeamiento.

El seguimiento estratégico de las operaciones se realiza cuando las fuerzas propias se emplean en operaciones combinadas o en apoyo de otros instrumentos del Estado. La aplicación de la IA a esta función permite mantener actualizada permanentemente la situación de las fuerzas, así como valorar sus necesidades actuales y prever las futuras. Con ello se dispone de un tiempo valioso para planear y ejecutar el sostenimiento de las fuerzas.

Capacidad nuclear

Los márgenes de tiempo de alerta tan reducidos de que disponen los sistemas de mando y control de las fuerzas nucleares exigen la automatización del proceso de alerta, del control de las comunicaciones y, si es preciso, del guiado de las armas hasta sus objetivos. La introducción de la IA en las fuerzas nucleares parece, a primera vista, constituir una mejora importante en la capacidad de disuasión nuclear de una potencia.

El empleo de la IA en la mejora de la capacidad nuclear puede aplicarse en dos campos distintos: en los sistemas de mando, control, telecomunicaciones e inteligencia o en los propios vectores nucleares.

En el primer caso, la IA incrementará las capacidades de análisis de datos de los sistemas ISR, el control de plataformas de sensores constituidos por RI y el reconocimiento automático de objetivos. Sería posible la detección y seguimiento de lanzadores móviles, lo que aumentaría la capacidad de represalia nuclear, o convencional con armas de alta precisión. Por otro lado, la IA podría proporcionar recomendaciones en tiempo real en apoyo a la decisión, en caso de crisis o incidente. Una dificultad para su implantación radica en que no ha habido nunca una confrontación nuclear, por lo que no se dispone de datos reales. El aprendizaje de los sistemas de IA se realizaría sobre datos obtenidos de simulaciones, juegos de guerra y ejercicios.

El empleo de IA en vectores es, en realidad, el uso de RI para sobrepasar las defensas enemigas y atacar el objetivo asignado de forma autónoma[9]. De esta forma, aunque los sistemas de guiado remoto hayan sido destruidos, se mantiene la capacidad de represalia.

Siendo el arma nuclear y la IA asuntos de gran sensibilidad y sujetos a continuo debate, el uso de esta tecnología crea opiniones divididas. Una primera preocupación proviene de que los sistemas de IA, por estar basados en ordenadores, pueden ser objeto de ataques informáticos. También pueden ser «intoxicados» en su adiestramiento con datos erróneos o bien ser confundidos durante su operación con datos manipulados.

Dejando aparte el temor a fallos, hay quienes piensan que la IA aplicada a las fuerzas nucleares producirá una desestabilización en el equilibrio actual. Ello es debido a que la IA incrementa la capacidad de seguimiento y designación de objetivos, lo que aumenta las posibilidades de éxito de un ataque sobre estos. Un adversario podría temer una derrota en un primer golpe. Por tanto, en una crisis con escalada, este adversario se vería inclinado a lanzar un ataque preventivo siguiendo la lógica de «si no uso mis armas, las destruyen y las pierdo».

La opinión contraria sostiene que la IA puede incrementar la estabilidad, disminuyendo la probabilidad de error humano y proporcionando transparencia, lo que mitigaría el riesgo de fallos.

9 Según la Revisión de la Postura Nuclear de EE. UU. Rusia está desarrollando un torpedo submarino autónomo con propulsión nuclear y armado con una cabeza termonuclear de gran potencia. Se le conoce como Status-6 (Статус-6). OFFICE OF THE SECRETARY OF DEFENSE, *Nuclear Posture Review February 2018*. Department of Defense, Washington, 2018.

Operaciones

Proyección estratégica

El **d**espliegue de fuerzas requiere de su proyección, o movimiento y transporte, desde la zona donde se encuentran estacionadas a la zona donde van a ser empleadas. Esta es una operación compleja donde el empleo de la IA puede ser ventajoso. El planeamiento de los movimientos y transportes exige tratar numerosos datos para adaptar las capacidades disponibles a las necesidades de movimiento y su coordinación. La exploración de muchas posibilidades en muy breve tiempo permite recomendar cuáles serán las más eficaces o eficientes, según los criterios marcados.

A la hora de controlar el movimiento, la capacidad de proceso de datos procedentes de los distintos medios de transporte permitirá tener una imagen precisa de la situación. De esta forma, se podrán corregir las desviaciones o reaccionar ante incidencias. Esto es fundamental en el caso de transportes multimodales.

La inteligencia artificial en el espacio

El entorno estratégico espacial se muestra muy reñido, competitivo y saturado, y en el futuro lo seguirá siendo. En estas circunstancias, los sistemas espaciales necesitan reaccionar con rapidez en un ambiente dinámico e impredecible. Al mismo tiempo, es necesario limitar la intervención humana para poder asumir el creciente número de sistemas en explotación.

En este dominio de la acción, el conocimiento de la situación resulta tan necesario como en los otros. Por un lado, existe un gran volumen de «basura espacial» que puede causar daños en el segmento espacial de los sistemas.[10] Por otra parte, las plataformas en órbita pertenecientes a posibles adversarios deben ser identificadas y seguidas, con el fin de conocer sus capacidades y posibles intenciones. El informe de 2018 sobre Evaluación de la Amenaza Espacial del Centro de Estudios Estratégicos e Internacionales pone de manifiesto el incremento de capacidades contra sistemas espaciales experimentado por

10 Según datos de la Oficina de Restos Espaciales de la ESA, se estima que existen unos 29.000 residuos espaciales de más de 10 cm. de tamaño, aparte de un número mucho más elevado de objetos más pequeños. La masa total de residuos en órbita se estima en más de 8.100 toneladas. https://www.esa.int/Our_Activities/Operations/Space_Debris/Space_debris_by_the_numbers. Consultado el 15 de septiembre de 2008.

actores estatales y no estatales.[11] El control del espacio requiere disponer de una gran cantidad de sensores y los correspondientes sistemas de proceso de datos. La aplicación de la IA para esta misión aprovecha la gran capacidad de tratamiento de datos y las posibilidades de predecir rápidamente posibles líneas de acción de la amenaza, ya sea procedente de residuos en órbita o de sistemas del adversario.

Por otro lado, la aplicación de la IA a los sistemas en órbita reviste dos formas: mejorar el cumplimiento de la misión y mejorar el funcionamiento de la plataforma sin intervención del operador. En el primer caso, el satélite realizará gran parte de sus misiones basándose en la IA. Además, se dotará de capacidad de proceso de los datos recogidos y los difundirá de forma autónoma. Con ello se consigue un recorte de los plazos de explotación de la información y del ancho de banda de las transmisiones con el satélite.

Los satélites realizarán funciones propias de sostenimiento (carga de baterías, protección, operaciones de eclipse) y también de mantenimiento preventivo y correctivo (revisión, diagnóstico y reparación). La principal ventaja que se obtiene es ahorro en personal operador.

Ciberespacio

Parece apropiado señalar que la IA puede jugar un papel relevante en su entorno nativo: el ciberespacio. La capacidad de procesar ingentes cantidades de datos y obtener resultados, sin necesidad de apenas guía, fortalece la seguridad, aunque también puede revelarse muy útil para lanzar ataques.

El uso de IA incrementará la productividad del personal dedicado a tareas específicas en el ciberespacio. La ciberdefensa requiere una gran cantidad de recursos humanos muy especializados. Esta clase de personal es escasa y, por tanto, resulta difícil cubrir los puestos necesarios. La implantación de IA permite enjugar el déficit de especialistas en ciberdefensa.

El uso de IA en misiones defensivas permite una aproximación diferente a la existente. En la actualidad, los sistemas defensivos se basan generalmente en actuar sobre las amenazas conocidas, que se detectan después de producirse el ciberataque. Esto hace que los sistemas estén menos preparados frente a amenazas desconocidas. La IA utilizará el aprendizaje para detectar desviaciones de la actividad normal de la red. Por tanto, su empleo permitirá no solo aprender de vulnerabilidades pasadas, sino también observar comportamientos anómalos y detectar y responder ante amenazas desconocidas inminentes.

11 HARRISON, Todd *et al.*, «*Space Threat Assessment 2018*», Center for Strategic and International Studies, Washington (DC), EE. UU., abril 2018.

Las características de la IA hacen posible su aplicación a las acciones ofensivas. Los ciberataques requieren una dedicación intensiva de personas muy cualificadas. Con el debido aprendizaje, se pueden automatizar los ataques y ejecutarlos con una velocidad que no permiten ser rechazados por sistemas controlados por operadores humanos.

De lo anterior se deduce que las acciones en el ciberespacio serán ejecutadas, cada vez con más frecuencia, por sistemas de IA. El grado de control que ejercerán operadores humanos es un asunto de gran relevancia. Hay que tener en cuenta que, una vez que se lanza un ciberataque (o contraataque), el ritmo es imposible de controlar. Si la IA que lo ejecuta se desvía del objetivo marcado, las consecuencias pueden ser desastrosas para las redes propias. Encontrar el adecuado equilibrio se revela como absolutamente necesario.

Anti-inteligencia artificial

En un enfrentamiento armado, el contendiente que utilice dispositivos de IA y RI cuenta con una ventaja importante frente al adversario. Se debe, por tanto, considerar la amenaza del empleo por la parte contraria de IA y RI contra las fuerzas propias. En consecuencia, será necesario adoptar contramedidas.

En primer lugar, es necesario disponer de inteligencia sobre los medios del adversario y, sobre todo, de sus conceptos de empleo, ya que el uso de armas letales autónomas por parte enemiga puede estar sujeto a reglas más permisivas que las propias. Por otra parte, es necesario llevar a cabo simulaciones, juegos de guerra y ejercicios en los que se incluya el empleo de IA y RI por parte del enemigo. También es necesario constituir «equipos rojos» que estudien los sistemas propios y desarrollen respuestas posibles por parte del adversario, a fin de tenerlas previstas.

Consecuencia de lo anterior será el desarrollo y experimentación de un nuevo tipo de tácticas y procedimientos para contrarrestar el uso de IA y RI por parte del adversario.

Doctrina y reglas de enfrentamiento

Doctrina

La introducción de IA y RI en operaciones militares necesita ir acompasada de los oportunos cambios doctrinales. En la actualidad, la experiencia en operaciones no permite basar en ella el desarrollo de conceptos doctrinales sobre IA.

Sin embargo, es necesario no quedarse rezagado en el desarrollo conceptual, ya que hay consideraciones de tipo ético y legal que exigen una guía doctrinal.

Como en otros casos, la doctrina se basará, inicialmente, en los pocos datos disponibles de operaciones y en experimentos, simulación, juegos de guerra y ejercicios.

La cooperación con aliados puede ser una fuente muy útil para el desarrollo de conceptos doctrinales.

Reglas de enfrentamiento

Las reglas de enfrentamiento (ROE) son normas de carácter operativo que obligan a todos los mandos y miembros de las unidades de los distintos escalones. Se materializan en un catálogo de acciones prohibidas o autorizadas, relativas al uso de la fuerza.

Hasta el momento, las ROE se dirigen a la actuación de seres humanos. Sin embargo, la paulatina introducción de RI en las operaciones cambia el marco de aplicación. Los RI, armados o no, pueden causar efectos sobre personas y bienes. Se necesita, por tanto, definir nuevas reglas aplicables a la actuación de los RI.

Las nuevas ROE deben ser cumplidas por los mandos que autoricen el empleo o los operadores que controlen o supervisen los RI. También es necesario que sean cumplidas por los propios RI en aquellas funciones en las que estén actuando con autonomía. Ello obligará a diseñar RI capaces de aprender, y emplear en sus actuaciones, las ROE que les sean aplicables.

El contenido de las ROE preceptivas para RI está sujeto a vivas discusiones, incluyendo aspectos éticos que se tratan en el capítulo quinto.

Enseñanza, instrucción y adiestramiento

La incorporación de la IA y RI a las operaciones militares trae consigo la necesidad de aprender a combatir con estos medios. En el capítulo tercero se ha comentado más extensamente esta necesidad.

La IA puede ser una poderosa ayuda para la enseñanza, instrucción y adiestramiento, ya que permite construir simuladores con un grado de realismo muy elevado, sobre todo si se combina con técnicas de realidad virtual.

La naturaleza de la guerra y la inteligencia artificial

Dentro de la comunidad de pensamiento sobre la guerra es comúnmente aceptado marcar la diferencia entre la naturaleza objetiva y el carácter subjetivo de la guerra. De acuerdo con ello, la naturaleza de la guerra contiene su esencia como fenómeno humano y social y es lo que la diferencia de otro tipo de fenómenos. El carácter de la guerra define cómo se dirige y evoluciona en el tiempo, de acuerdo con factores externos: tecnología, leyes, fuerzas morales y cultura. Por tanto, cada época y cada pueblo tienen su propio tipo de guerra.

De acuerdo con lo expuesto a lo largo de este capítulo, se puede concluir que la IA y RI cambiarán el carácter de la guerra. Los cambios serán más visibles en los niveles táctico y operacional.

En cuanto a la naturaleza de la guerra, el modelo de la trinidad de Clausewitz proporciona un marco de referencia para el análisis. Los elementos que componen la trinidad son[12]:

- El odio y la enemistad, contemplados como un ciego impulso de la naturaleza que añade la dimensión irracional de la guerra. Se asocia con la población.
- La influencia de la probabilidad y el azar, que la convierten en una libre actividad del alma y que tiene un carácter no racional. Se asocia con los jefes militares y las fuerzas armadas.
- La subordinación como instrumento político, que proporciona la dimensión racional de la guerra. Se asocia con los gobiernos.

Estos elementos se relacionan entre sí y se ven más o menos influidos por la forma en que se conduce la guerra. Se mantienen en tensión, más que en equilibrio. Para que cambie la naturaleza de la guerra deben cambiar las leyes internas que rigen estos elementos y las relaciones entre ellos.

El impacto de la IA y RI sobre el primer elemento se manifiesta principalmente en la posibilidad de realizar operaciones de información tendentes a influenciar las poblaciones, tanto propia como del adversario u otros actores, estatales o no. Esto no es nuevo, pero las posibilidades que brinda la IA y el hecho de que las principales fuentes de información actuales son los medios sociales e Internet elevan el orden de magnitud del volumen, frecuencia y personalización de los mensajes. Un uso extensivo de IA y RI puede debilitar el apoyo de la población a las fuerzas armadas y hacer que se sientan menos ligadas a la política de la nación.

12 VON CLAUSEWITZ, Carlos. *De la guerra*, Ediciones Ejército, Madrid, 1978. pp. 45-46.

El segundo elemento, o azar, está íntimamente relacionado con lo que Clausewitz denomina «fricción», que comprende el peligro, la fatiga y la incertidumbre. La introducción de IA y RI afecta a este elemento en varias formas. El peligro disminuirá al utilizar RI en misiones de alto riesgo para la vida humana. Por otro lado, la fatiga física se verá reducida por el empleo de RI y la fatiga cognitiva por el uso de IA en apoyo de la toma de decisión. La gran mejora en el conocimiento de la situación que proporciona la IA reducirá la incertidumbre. Sin embargo, no la eliminará, ya que no dejarán de darse situaciones inesperadas, bien sea por causas fortuitas o intencionadamente. Las interacciones de los RI entre sí, con los RI adversarios, con los combatientes propios y enemigos y con la población de la zona puede incrementar la incertidumbre. La posibilidad de «piratear» sistemas de IA y RI puede también aumentar la incertidumbre.

El tercer elemento, la dirección política, se verá afectado, en primer lugar, por ciberataques y operaciones de información muy enfocadas, ejecutadas por sistemas de IA. La confianza en los sistemas de mando y control de mayor nivel se verá erosionada. El temor a la derrota mediante técnicas de guerra híbrida y la percepción de que el uso de RI comporta un menor riesgo de pérdidas humanas, puede conducir a que el gobierno se sienta más inclinado a la acción militar y la guerra puede escalar más rápidamente. Por otra parte, los ciclos de decisión se verán acortados de forma importante por el empleo de IA. Los dirigentes políticos tendrán que delegar ciertas decisiones para no entorpecer el ritmo de operaciones de alta intensidad.

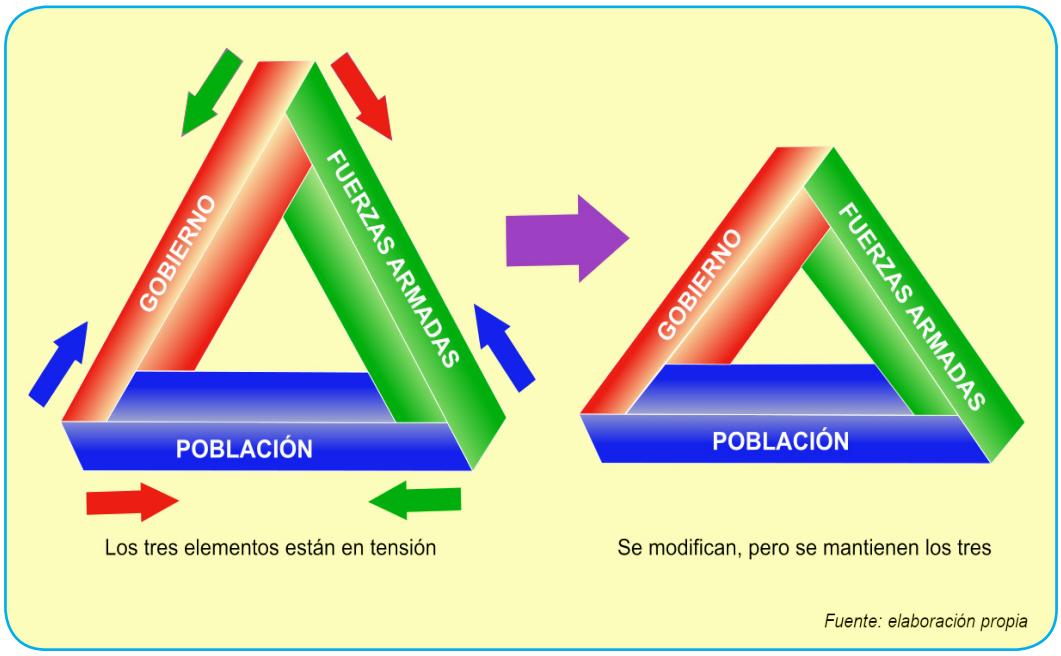


Figura 4.- Los tres elementos de la trinidad de Clausewitz.

Los tres elementos de la trinidad se ven modificados. Sin embargo, ninguno desaparece ni las leyes que los gobiernan cambian. La guerra sigue «*gravitando entre*

estas tres tendencias como entre tres centros de atracción»[1]. La tensión entre ellos hace que el conjunto se reconfigure internamente y se mantenga. La naturaleza de la guerra no cambia por estas modificaciones, del mismo modo que una esfera no deja de ser una esfera porque su radio cambie.

La fricción y el «*coup d'œil*» de los que habla Clausewitz seguirán siendo fundamentales en la guerra. La esencia de la guerra como violencia dirigida políticamente continuará siendo su aspecto más duradero, aunque haya cada vez más máquinas implicadas en cada nivel.

Conclusiones

El empleo de IA y RI está sujeto a controversia y es un tema sensible por las implicaciones éticas y legales que trae consigo. Por tanto, resulta necesario establecer unos conceptos de empleo que aseguren, en lo posible, que la aplicación militar de estas tecnologías sea aceptable social y legalmente, tanto a nivel nacional como internacional. Esto no resulta sencillo, porque se trata de tecnologías complejas y avanzadas, de las que no se posee experiencia real. A pesar de ello, habrá que instaurar unos conceptos iniciales, que se irán refinando y completando con la experiencia.

Los conceptos de empleo deben considerar la necesidad de que estos sistemas estén siempre supervisados, que dispongan de una avanzada y fiable interfaz hombre-máquina y que estén dotados de mecanismos de seguridad. También es preciso regular el entrenamiento de los dispositivos y su necesaria actualización. Finalmente, hay que determinar en qué ocasiones se puede permitir que los RI seleccionen y ataquen objetivos de forma autónoma, insistiendo en que nunca lo harán sobre personas.

Un gran escollo en el empleo de IA y RI es el de la autonomía de estos dispositivos. Según el enfoque habitual, el grado de autonomía se asigna al dispositivo como un todo. De esta manera, el problema se centra en los sistemas de armas letales autónomos (SALA), que concentran el mayor volumen de controversia en su uso. Dado que, según los conceptos de empleo, siempre estarán supervisados, conviene eludir la controversia enfocando la autonomía de los sistemas desde un punto de vista más funcional. Cada una de las funciones del dispositivo tendrá un grado de autonomía acorde con las necesidades de la misión a cumplir, de forma que en muy raras ocasiones todas las funciones serán autónomas.

En los tres niveles, táctico, operacional y estratégico, la utilización de IA y RI proporcionará un aumento de capacidades militares que se distribuirá de forma no homogénea en distintas áreas.

1 VON CLAUSEWITZ, Carlos. *De la guerra*, Ediciones Ejército, Madrid, 1978. p. 46.

En los niveles táctico y operacional hay tipos de operaciones en los que el impacto que ocasionará el empleo de IA y RI será muy destacado por el efecto multiplicador de fuerza que produce. En estas operaciones, el papel de los combatientes humanos cambiará, su número se verá reducido y la eficacia y eficiencia de las acciones propias aumentará. En los dominios terrestre, marítimo y aéreo se pueden señalar ya tipos de operaciones muy adaptadas a las características de los RI. Algunas de ellas aprovechan la experiencia acumulada con robots operados a distancia en distintos conflictos. Sin embargo, otras constituyen conceptos de operación que deben ser probados, siendo el de enjambres de robots uno de los más relevantes, por las ventajas que su uso proporciona.

Resulta necesario introducir lo antes posible cambios en las técnicas y procedimientos de combate para adaptarse al uso de estas tecnologías. Un asunto de especial importancia es el del diseño de equipos mixtos humano-robot, para obtener el máximo rendimiento de sus capacidades complementarias.

No puede demorarse el estudio y definición de nuevas tácticas de empleo, aunque, a falta de experiencia real en operaciones, será preciso recurrir a otros métodos para tener cuanto antes un marco conceptual. En la definición de esas tácticas aparece un nuevo modo de combate: la lucha contra-IA. Es preciso que los mandos y las unidades sobre el terreno estén preparados para el empleo de IA y RI por parte del adversario. Para conseguirlo, será necesario un esfuerzo en la obtención de inteligencia y sistemas de simulación.

Hay que acompasar la doctrina militar y las reglas de enfrentamiento a la introducción progresiva de IA y RI en operaciones militares. Al no disponer de datos empíricos, será preciso elaborar conceptos de forma provisional y contrastarlos en ejercicios, juegos de guerra y simuladores.

También será preciso aprender a combatir con estos medios, lo que obligará a modificar las estructuras y los planes de enseñanza, instrucción y adiestramiento. La simulación jugará un importante papel y verá aumentada su eficacia con la aplicación de técnicas de IA y realidad virtual.

La aplicación de la IA en las fuerzas nucleares introduce una mejora importante en las capacidades de estas fuerzas. La cuestión que se plantea es el posible impacto de esta aplicación en el equilibrio nuclear. Por el momento no hay un consenso establecido sobre si el equilibrio se deteriorará o si, por el contrario, la situación se tornará más estable.

Siendo el ciberespacio el dominio nativo de la IA, cada vez serán más frecuentes las acciones ejecutadas por estos sistemas. El ritmo al que se desarrollarán estas acciones supera con creces las posibilidades de ejecución de seres humanos. Por lo tanto, sobre todo en acciones ofensivas, el grado de control humano sobre el inicio y las fases de la acción será un elemento crítico para evitar consecuencias no deseadas.

La IA y la RI cambiarán el carácter de la guerra, como ha ocurrido en diversas ocasiones a lo largo de los siglos. Los cambios que introducirán estas tecnologías pueden ser profundos, ya que incorporan capacidades que superan no solo la aptitud física del ser humano, sino también parte de sus facultades mentales. Sin embargo, la naturaleza de la guerra no cambiará sustancialmente. Los elementos de la trinidad clausewitziana se verán modificados individualmente, pero el conjunto se reconfigurará manteniendo la tensión mutua y haciendo que la guerra gravite sobre ellos, sin cambios trascendentes en su esencia.

Para comprender cómo será la guerra futura, resulta necesario no equivocarse sobre su carácter y sobre la permanencia de su naturaleza. Es posible llegar a conclusiones equivocadas sobre el efecto de estas tecnologías y, en consecuencia, acabar definiendo la guerra como se desea que fuera y no como lo que de verdad es: un enfrentamiento humano, incierto y complejo que busca un fin político. Aquí, las palabras de Clausewitz mantienen toda su vigencia:

«El primer acto del juicio, el más importante y decisivo que incumbe a un estadista y al general en jefe, es el de conocer la guerra que emprende […] que no la confunda o la quiera hacer algo que no sea posible por la naturaleza de las circunstancias.»[1]

1 VON CLAUSEWITZ, Carlos. *De la guerra*, Ediciones Ejército, Madrid, 1978. p. 45.

Capítulo 5

Desafíos éticos en el uso militar de la inteligencia artificial

Juan A. Moliner González

Resumen

La participación de las nuevas tecnologías en la evolución de la guerra ha sido constante. Los avances actuales en la capacidad de procesamiento computacional, unido a los desarrollos en comunicaciones y otras ciencias, permiten emplear sistemas de armas con una amplísima autonomía que transforman las características de la guerra.

La inteligencia artificial preludia un nuevo campo de batalla donde el uso de la fuerza y los modos de utilizarla pueden cambiar las reglas éticas y legales y alterar el principio de humanidad. Principio que el desarrollo moral de la humanidad intenta mantener para escapar de la barbarie y la violencia incontrolada.

Pero mientras los algoritmos de la inteligencia artificial avanzan imparablemente, los desafíos y retos éticos que se presentan en el combate deben ser analizados para que las máquinas no escapen al imprescindible control humano en su desarrollo y empleo, bajo adecuados principios morales.

Palabras clave

Inteligencia artificial, Sistemas de Armas Autónomos, Ética militar, Control Humano Significativo, Seguridad y Defensa.

Ethical challenges to the military use of artificial intelligence

Abstract

The involvement of the new technologies in warfare evolution has been continuous. The advances in computational processing capacity, along with other communications and scientific developments, allow for employing weapons systems with a broadened autonomy, which is transforming the characteristics of war.

Artificial intelligence introduces a new battlefield where the use of force and the ways to employ it are changing the ethical and legal rules and are disrupting the Humanity Principle. Principle that the moral development of the human being tries to maintain in order to escape from brutality and uncontrolled violence.

Meanwhile artificial intelligence algorithms advanced unstoppably, the ethical challenges presented into the combat must be analyzed to avoid machines escaping from the meaningful human control on their development and utilization, under adequate moral principles.

Keywords

Artificial Intelligence, Autonomous Weapons Systems, Military Ethics, Meaningful Human Control, Security and Defense.

«El hombre necesita la máquina y la organización, pero tiene que dominarlas y humanizarlas en vez de resignarse a ser mecanizado y deshumanizado por ellas. El verdadero peligro para el hombre, no está en los riesgos que corre la seguridad material, sino en el oscurecimiento del hombre mismo en su propio mundo humano»

Rabindranath Tagore

Introducción

No solo las armas de destrucción masiva, sino las nuevas capacidades desarrolladas en paralelo con los avances científicos y tecnológicos están cambiando las características de la guerra. Inéditas dinámicas sociales, flamantes nuevos actores e insólitos espacios y formas de confrontación están transformando la forma de combatir. La evolución ha sido constante en el desarrollo de guerras y conflictos, pero lo disruptivo de la trasformación que empiezan a producir las nuevas tecnologías alcanza principios éticos y valores morales cuya observancia es exigida en las sociedades democráticas.

Las denominadas guerras híbridas en las que se difuminan las situaciones de guerra y paz, se dificulta la distinción entre combatiente y no combatiente, se mezclan técnicas tradicionales de combate con otras propias de actores no estatales e incluso se hace complejo diferenciar entre actos de guerra –piénsese en la dificultad de asignar esa categoría a ataques cibernéticos-, constituyen un fenómeno que se acentúa en estos últimos años y produce desconcierto a los que afrontaban su defensa apoyándose en la disuasión y el desarrollo de competencias militares clásicas.

A las tradicionales capacidades militares se unen los avances propiciados en nuestros días por el conocimiento científico-técnico, a un ritmo y profundidad sin precedentes en la historia de la humanidad. Entre esos adelantos destaca la inteligencia artificial (IA), que está llamada a jugar un papel crucial, como así se recoge en los capítulos precedentes de este trabajo. Su meta final es el diseño y construcción de entidades que, con el referente de las capacidades cognitivas y del comportamiento inteligente del ser humano y apoyadas en la ciencia e ingeniería informática con los algoritmos y sus procesos, lleguen a ser capaces de tomar decisiones por sí mismas de manera completamente autónoma.

Analizar los desafíos éticos que plantea la IA significa considerar los resultados producidos por máquinas dirigidas y controladas en diversos grados por eso que llamamos inteligencia artificial. En este sentido, la relación entre la IA y los robots en

el campo militar es ya una realidad. «El robot, según lo ven algunos, es meramente el *contenedor* de la IA, mientras que esta es el software dentro del contenedor, que puede tomar decisiones. El robot no es en sí inteligencia artificial, pero tendrá, y tiene ya en muchos casos, IA».[2] Dentro de esa IA, el cuello de botella parece que es el software y no el hardware, «tenemos que encontrar el algoritmo correcto, y nadie se ha acercado aún a él»[3]. En las páginas que siguen se analizan las consecuencias éticas de las conductas desplegadas por los sistemas de armas, máquinas y robots regidos por IA y sus algoritmos. Algoritmos que son instrucciones de programación, siendo sus aplicaciones y consecuencias las que se valoran éticamente, entre ellas la «delegación de funciones a un algoritmo», mencionada en el capítulo 2 de este trabajo.

Pero independientemente de los cambios que se vayan produciendo, y aunque a veces se producen novedades que influyen de forma disruptiva en su planteamiento y conducción, las guerras siguen siendo fenómenos sociales y humanos. Cuando el conflicto aparece se trata de imponer la voluntad propia al adversario y, habiendo fallado todos los recursos no violentos, será la utilización de la fuerza, recordemos que letal y productora de destrucción, la que actúe como elemento decisivo en el resultado final.

Aquí es donde adquieren relevancia los nuevos sistemas de armas desarrollados al amparo de los avances científicos y donde la inteligencia artificial juega el papel de cerebro director de complejas tecnologías y aplicaciones[4].

En la defensa legítima de las propias sociedades, en la promoción de los derechos humanos, en la cooperación para el mantenimiento de la paz en todos los pueblos de la Tierra, las sociedades democráticas actúan convencidas de la justicia de su causa, así como de la eticidad de los procedimientos y medios que emplean.

En esa actuación, los miembros de sus Fuerzas Armadas y estas, como organizaciones complejas, continúan manteniendo el *ethos militar* que constituye ese conjunto de principios, valores y reglas de conducta conservadas a lo largo del tiempo y que les permiten asumir la violencia letal consustancial al combate y el hecho realmente trascendente de arriesgar la propia vida en una guerra.

Nuestras democracias han avanzado en el respeto y promoción de los derechos humanos, al igual que se ha intensificado el respeto a las normas del Derecho

2 ORTEGA, A. (2016). *La imparable marcha de los robots*, Madrid: Alianza Editorial, p. 15.

3 CHALMERS, D.J. (2009). *The Singularity: A Philosophical Analysis, p. 6*, https://consc.net/paper/singularity.pdf. Visitado el 7.6.18.

4 Mecánica, electrónica, telecomunicaciones, informática e inteligencia artificial son tecnologías que se cruzan y funden en la robótica. Así, las máquinas con mayor o menor autonomía se despliegan en todos los ámbitos, incluyendo el campo de batalla. Pero recordemos que ya desde la Segunda Guerra Mundial se habían utilizado sistemas programados o controlados remotamente.

Internacional Humanitario. Bajo el principio de humanidad se demanda de forma creciente la restricción y aplicación de las reglas y usos éticos en el combate, incluso cuando enfrente no hay respeto alguno por principios legales y éticos.

También el rechazo en nuestras sociedades ante las víctimas, propias y del enemigo, producidas en conflictos bélicos se traslada a los responsables políticos, cada vez más presionados en la conveniencia u oportunidad de emplear la fuerza militar, incluso si existen justificaciones morales y humanitarias.

La cuestión central, con este trabajo, es conocer si la exigencia de encontrar acomodo a los principios éticos de la guerra justa también es de aplicación con las nuevas tecnologías representadas por la inteligencia artificial y sus crecientemente complejos algoritmos de desarrollo. A este respecto, la inteligencia artificial, el *war algorithm* con sus capacidades de aprendizaje plantea una tesis central en las reglas éticas del combate: ¿Quién debe decidir en cuestiones de vida y muerte en relación con la guerra? O como dice el Comité Internacional de la Cruz Roja: «La cuestión ética fundamental es si los principios de humanidad y los dictados de la conciencia pública pueden permitir que la decisión humana en el uso de la fuerza sea efectivamente sustituida con procesos controlados por computador, y las decisiones sobre vida y muerte sean cedidas a las maquinas»[5].

En consecuencia, se considerarán algunos de los problemas y limitaciones que se presentan y se intentará avanzar en los planteamientos sobre si las características cambiantes de la guerra, fenómeno social y humano, cesarán en su necesidad de ser y desarrollarse de forma legítima, atendiendo a razones éticas y legales. Los nuevos sistemas y la inteligencia artificial están suplantando al ser humano, dotado de razones y emociones, no solo en el control de la ejecución, sino en la cadena de mando que toma la decisión final del empleo de la fuerza letal contra el enemigo.

Durante un discurso pronunciado en marzo de 2017, el entonces Subsecretario de Defensa de EE. UU. Robert Work constató que «el desarrollo de las tecnologías emergentes – particularmente la IA, robótica, y el desarrollo de interfaces para conectar hombres y máquinas – cambiará la «inmutable» naturaleza de la guerra»[6].

Precisamente el apoyo que recibe de la tecnología la defensa militar en la búsqueda de la disuasión y defensa de valores e intereses hace que esos avances científicos tengan que respetar las consideraciones éticas. Así, la tecnología ha contribuido, por ejemplo, con las municiones guiadas de alta precisión, a aumentar la precisión en el alcance de los objetivos y a disminuir el número de víctimas colaterales. Solo

5 ICRC (2018). *Ethics and autonomous weapon systems: An ethical basis for human control?* Ginebra, 3 abril, p. 1.

6 NURKIN, T. (2018). *China and US compete for IA dominance*, p. 1 https://jane.ihs.com/IntelligenceReview/Display/1830964. Visitado el 29.05.18.

tenemos que pensar en los bombardeos sobre ciudades de la Segunda Guerra Mundial y compararlo, incluyendo las consecuencias en víctimas colaterales, con la precisión en los objetivos militares de los misiles guiadas actuales. Pero incluso en nuestros días las restricciones éticas que podría conllevar la utilización de nuevos sistemas de armas son frecuentemente olvidados[7] .

En general, la exactitud de sensores y procesadores ha reducido enormemente el error humano, por lo que se podrá argumentar en uno u otro sentido, pero no negar la posibilidad de que la tecnología y sus avances contribuyan a disminuir y evitar los daños colaterales de los conflictos armados y las guerras.

Pero no solo en la eticidad de los fines, sino con los nuevos medios tecnológicos y en la forma de conducir las operaciones militares persiguen las democracias occidentales mantener en el desarrollo de guerras y conflictos unos estándares morales alineados con los valores y principios que rigen la convivencia social, consecuencia del progreso moral alcanzado. Habrá ocasiones en que los valores que nuestra civilización promueve se defiendan con el empleo de la violencia legítima, *ius ad bellum,* pero la forma y los medios (incluyendo modernas tecnologías) en que esa utilización se lleva a cabo, *ius in bello,* también deben contribuir a la promoción de los mismos.

Por esto se plantea la cuestión de si la evolución tecnológica mantendrá una doctrina de empleo y utilización de los modernos sistemas de armas también ajustada a rigurosas consideraciones éticas. Las implicaciones de los nuevos sistemas de armas afectan, desde esa perspectiva ética, incluso a convicciones y principios morales profundamente arraigados en los profesionales de las Fuerzas Armadas.

El avance científico y tecnológico es una producción humana y, además de ser en sí mismo posible causa de conflicto, está haciendo aflorar cuestiones éticas que afectan al desarrollo, empleo y control de nuevas armas y sistemas incorporados al conjunto de las capacidades militares.

Si, como postulamos, avanzamos hacia una trasformación en las características de los conflictos que deben enfrentar los Ejércitos, también los nuevos medios y las formas de acción en ellos deberían ser reevaluadas a la luz de aquellos principios éticos.

Por un lado, se debe reconocer que las nuevas tecnologías, y el impulso principal que en ellas tiene la IA, están empezando a cambiar la faz de la guerra[8]. Por otro lado,

7 En el conflicto de Ucrania y ante la utilización de cohetes no guiados en áreas urbanas densamente pobladas, la organización *Human Rights Watch* sugirió que el empleo de esas armas en áreas urbanas podría constituir un crimen de guerra, al no discriminar entre combatientes y simples habitantes de las ciudades. HRW (2014). *UkrIAne: Unguided Rockets Killing Civilians*, https://www.hrw.org/new/2014/07/24/ukrIAne-unguided-rockets-killing-civilians. Visitado el 6.6.18.

8 Aunque se necesita tiempo. La realidad actual en el terreno no parece asemejarse a ese futuro de ciencia ficción que parece inevitable. «A pesar del creciente número de robots desplegados por

existe una falta de conexión entre la ética y las disciplinas científicas emergentes. Todo ello presenta problemas éticos de trascendencia, cuyo análisis y consideración es una tarea urgente[9].

Para ello este artículo hace una primera aproximación modesta, en la que más que soluciones se presentan cuestiones con el ánimo de ofrecer ideas que permitan avanzar en su clarificación.

Retos éticos en las aplicaciones militares de la inteligencia artificial

No cabe duda de que los sistemas de armas basados en la IA, robóticos y autónomos, ya están aquí y esta «cuarta revolución industrial plantea a las fuerzas armadas de todos los países, incluido España, el problema de adecuar sus instrumentos militares a ella si quieren operar con prontitud y eficacia»[10]. Algunos de esos sistemas son físicos, otros se despliegan en el ciberespacio y sin duda veremos desarrollos extraordinarios en el futuro, pero la realidad de su existencia y utilización es innegable.

De que los sistemas de armas dirigidos por la IA son una realidad da prueba el hecho de que el Ejército de Tierra norteamericano emitió en marzo de 2017, y en consonancia con la Estrategia Militar Nacional de 2015, su Estrategia de Sistemas Robóticos y Autónomos. El Departamento de Defensa USA centra sus iniciativas de investigación y desarrollo de la IA en la *Defense Advanced Research Projets Agency (DARPA*), mencionada en otros capítulos de este trabajo. Entre los sistemas científicos que se requieren para disponer de las capacidades perseguidas es obvio el lugar preeminente de la IA, que entre otros objetivos «simplificará la toma de decisiones teniendo en cuenta las reglas de enfrentamiento»[11].

---

las fuerzas militares [en Irak y Afganistán], las características fundamentales de la guerra continúan prevaleciendo incluso con el creciente uso de artefactos controlados remotamente». DANET, D. y HANON, J-P. (2014). *Digitization or Robotization of the Battlefield: Evolution or Robolution?* En DOARE, R. y otros (eds.). *Robots on the Battlefield*, Combat Studies Institute Press, p. XV.

9 SINGER, P.W. (2010). *The Ethics of Killer Applications. Why is so Hard to talk about Morality when it comes to New Military Technology? Journal of Military Ethics*, Vol. 9, nº 4, pp. 299-312.

10 FOJÓN, E. (2018). La cuarta revolución industrial, el «algoritmo de guerra» y su posible aplicación a la Defensa española. Real Instituto Elcano, ARI 35/2018, 9 marzo 2018, p. 5.

11 Describe la IA como la «capacidad de los sistemas de computación para ejecutar tareas que normalmente requieren inteligencia humana como percepción, conversación y toma de decisiones». The U.S. Army, Robotic and Autonomous Systems Strategy, marzo 2017, p. 3.

El principio ético de reducción del riesgo innecesario a los combatientes propios

La adquisición de capacidades militares mediante el desarrollo de tecnologías avanzadas, enfatizando la colaboración e integración hombre-máquina que marca la estrategia del ejército USA que se ha comentado, tiene uno de sus principios esenciales, desde la perspectiva ética, en la disminución del riesgo para los soldados, en «incrementar la supervivencia de los soldados», así como contribuir a «llevar a cabo misiones imposibles para los humanos»[12]. Es lo que se denomina «principio del riesgo innecesario»[13].

Dada la obligación ética de todo comandante militar de reducir al máximo las bajas entre los combatientes a sus órdenes, el empleo de Sistemas de Armas Autónomos (SAA) apoyados en la IA contribuye a ese objetivo[14]. Las misiones que pudieran ser desempeñadas por sistemas autónomos con mayor eficacia en entornos peligrosos, desde la inteligencia, vigilancia y reconocimiento del campo de batalla en todos los dominios hasta el desminado y el combate en áreas urbanas, la lucha antisubmarina o las misiones de interdicción aérea (mencionadas en el capítulo 4 de este trabajo), evitan la sobreexposición a riesgos de soldados mucho más vulnerables físicamente y con menos capacidades funcionales. Además de otras ventajas en los ámbitos de la fiabilidad, el coste y la multiplicación de fuerzas.

También se argumenta en sentido favorable a los sistemas autónomos y robóticos que, además de evitar las bajas militares propias causadas por el conflicto, las máquinas no estarían sujetas al influjo de emociones humanas como la ira o el temor, por lo que sería mucho más difícil que cometieran violaciones o actos punibles en conflictos y guerras.

Las críticas al principio de riesgo innecesario se centran en que el alejamiento de los combatientes del campo de batalla, tanto física (operando un dron semiautónomo a miles de kilómetros) como psicológicamente (objetivos vistos como pixeles en una pantalla de ordenador), podría contribuir a un relajamiento de las restricciones para entrar en combate y, en consecuencia, a una reducción de la contención ética

12 Obra anterior, p. 2.

13 LUCAS, G. (2014). *The Ethical Challenges of Unmanned Systems.* En DOARE, R. y otros (eds.), obra citada, p. 135.

14 Los SAA son descritos como aquellos sistemas que gracias a la IA «una vez activados, son capaces de seleccionar y atacar objetos sin una intervención adicional de un operador humano». LOPEZ-SANCHEZ, M. (2017). *Some insights in Artificial Intelligence Autonomy in Military Technology,* p. 12, https://ttac21.net/2017/11/10/autonomy-in-future-military-and-security-technologie. Visitado el 25.05.18.

para evitar riesgos innecesarios. Así, podría llegarse a una situación en la que fuera más fácil iniciar las hostilidades al rebajar el coste político de enviar soldados a una guerra, asumiendo que en ella no habrá bajas humanas al ser sistemas autónomos los implicados en el combate. Y esto podría llevar a un aumento en la proliferación de conflictos bélicos.

El principio ético y legal de la discriminación

En el combate, elemento esencial y definitivo de la función del militar, se produce destrucción y se utiliza la fuerza letal. Por ello el principio de discriminación de combatientes y no combatientes, así como el evitar las bajas de civiles (los daños colaterales) es un elemento esencial de las reglas éticas de la guerra y del Derecho Internacional Humanitario.

La nueva concepción de la guerra híbrida complica sobremanera la aplicación de la discriminación y la IA en las nuevas tecnologías se presenta como un elemento que puede desempeñar un papel esencial en su consideración.

En relación con la discriminación tiene enorme importancia la relativa a delegar la decisión de elegir y atacar objetivos militares, aquellos cuya destrucción parcial o total supone una ventaja militar definitiva en el desarrollo de las operaciones. Desde la perspectiva de la IA, el problema ético es el de la «delegación de funciones a un algoritmo». Respecto a la selección y ataque a objetivos, y la utilización en este cometido de sistemas autónomos, se argumenta que no se puede dejar la responsabilidad de esa decisión en máquinas y robots por su falta de empatía si llegan a tener «la capacidad de seleccionar a los objetivos y atacar a estos por su cuenta»[15].

Se justifica la crítica en que los sistemas autónomos y la IA que los dirige son incapaces de discernir las complejas situaciones que se pueden producir en el campo de batalla, como la posibilidad de que determinados objetivos hayan perdido su valor militar, o evaluar si un objetivo pretende atacar o rendirse. Por ejemplo, «evaluar si un tanque es un objetivo militar o si el sistema de armas letal autónomo aceptaría su rendición no solo es cuestión de tener algoritmos inteligentes con altas capacidades de discernimiento. En su lugar, tenemos que considerar los valores subyacentes que nosotros, como humanos desarrollando tales algoritmos, deberíamos ser capaces de instalar en ellos»[16].

15 TRAVIESO, J. (2015). Las consecuencias de mandar a la guerra a ´robots asesinos`, eldiario.es, p. 2, https://www.eldiario.es/.../debate-torno-robots-asesinos_0_378312866.html.

16 LÓPEZ-SÁNCHEZ, obra citada, p. 14.

De igual forma podría plantearse respecto a civiles afectados de repente por las operaciones y situados en medio del campo de batalla. De momento es imposible para los sistemas autónomos y la IA desarrollar comportamientos basados en la clemencia o la empatía, valores específicamente humanos de trascendencia a la hora de tomar decisiones éticas y legales en el combate.

Si bien es cierto que en el estado actual de desarrollo de la IA y los sistemas de armas autónomos esos problemas de reconocimiento activo o de aprendizaje profundo no se han resuelto y al igual que en otras áreas, como la conducción autónoma de vehículos, el error sigue estando presente, cabe pensar que el futuro de los avances científicos podrá resolverlos. En consecuencia, se defiende la necesidad de mantener una supervisión humana absoluta sobre los sistemas que previsiblemente serán más autónomos, precisos en sus identificaciones y fiables en sus decisiones[17]. Este aspecto de la responsabilidad y el control se analiza con más detalle en un apartado posterior.

Aunque la IA y la robótica aspiran a mejorar las prestaciones de los seres humanos y reducir sus limitaciones, las máquinas no tienen de momento una *inteligencia humana* ni nuestra capacidad de *interacción social*, que nos permite reconocer e interpretar la conducta social compleja apoyados en diferentes códigos de signos y señales, y medida por pautas culturales y también por complejas circunstancias morales, como las que se producen en el campo de batalla.

El principio de prevención

Que el avance de la ciencia en el campo de la IA y la robótica, y en otros muchos, mantenga esa preocupación por las implicaciones éticas se pone de manifiesto en el *principio de prevención*. Este principio exige que los científicos no dejen su investigación si algo malo o inapropiado ocurre, sino que desde el inicio hagan un esfuerzo para «prevenir los potenciales malos efectos que podrían venir de sus inventos»[18]. La exigencia de que la seguridad sea una consideración a tener en cuenta en el mismo diseño de los sistemas parte de lo inseguros que han sido diseñados los sistemas autónomos desde su inicio.

17 Parece adecuado recoger el concepto de «singularidad» como «el momento en que la inteligencia de los ordenadores superará a la inteligencia humana, puede darse hacia el año 2100 (aunque otros afirman que eso seguirá siendo un simple tema de ciencia ficción)». NADELLA, S. (2017). Pulsa actualizar. La aventura de redescubrir el alma de Microsoft y concebir un sistema mejor para todos, Madrid: HaperCollins, p. 184.

18 SINGER (2009). Wired for war. *The robotics revolution and conflict in the 21st century*. Nueva York:The Penguin Press, p. 426.

Algunas voces han pedido un régimen de control del desarrollo de sistemas de armas autónomas, sugiriendo que se prohíba la investigación de «la integración de inteligencia artificial y sistemas de armas»[19].

En este sentido, como recuerda José A. Plaza[20], hay que mencionar al manifiesto que en julio de 2015 y, a modo de carta abierta, además de constatar que las armas autónomas podían considerarse como la tercera revolución en la guerra, después de la pólvora y las armas nucleares, alertaba de los peligros de la inteligencia artificial y pedía su regulación para prevenir una carrera de armamentos en IA y la prohibición de sistemas autónomos ofensivos que estuvieran más allá de un control humano significativo. Este manifiesto está apoyado por prestigiosos expertos como Stephen Hawking, Steve Wozniak, Martin Rees o Noam Chomsky, entre otros. En septiembre de 2016 se creó la asociación *Partnership on AI* con participación de Amazon, Apple, Google, Microsoft y otras empresas con los mismos objetivos.

Otras iniciativas han manifestado su preocupación por el uso inapropiado, prematuro o malicioso de las nuevas tecnologías indicando la necesidad de códigos de conducta éticos que promuevan un uso apropiado de la inteligencia artificial. Entre ellas la del premio Nobel Jody Williams, *Stop Killer Robots* que, lanzada en 2013, promueve la prohibición de lo que llama «robots asesinos», a los sistemas que en el futuro serán capaces de elegir y disparar sobre objetivos sin ninguna intervención humana.

Algunos expertos consideran que estas preocupaciones están infundadas, pues se ha sobredimensionado la inteligencia de los ordenadores, «Por los medios de comunicación, por la ciencia ficción y, también, es importante decirlo, por la proyección psicológica de nuestros miedos… Les otorgamos demasiadas características humanas… No hay que olvidar que los ordenadores son diseñados por nosotros; no evolucionan solos. Esa es la diferencia»[21].

Quizá lo que ocurre es que se está manteniendo el prejuicio de asignar a la IA, y a los sistemas de armas apoyados en ella, el que va a reflejar la misma o mayor malevolencia con la que ha actuado el ser humano.

19 SPARROW, P. (2009). *Predators or Plowshares? Arms Control of Robotic Weapons*, IEEE Technology and Society Magazin, primavera 2009, p. 28 https://ieeexplore.ieee.org/document/4799404/. Visitado el 15.5.18.

20 PLAZA LOPEZ, J. A. (2017). Lecciones de ética para máquinas que ´piensan` y toman decisiones. Elpais.es https://retina-elpais-com/retina/2017/12/19innovacion/1513661054_305253 Visitado el 15.02.18.

21 El País, 2018, 28 de enero, Entrevista a Yoshua Bengio, p. 8.

Otros retos éticos

Es una realidad que la ética y el derecho se han ido desarrollando por y para seres humanos, no para máquinas. Por esto no se comparten las ideas que se abren a la posibilidad de dotar de personalidad jurídica a los robots para que pudieran asignárseles responsabilidades por los actos que ejecutaran o las consecuencias de los mismos. En consecuencia, son los científicos que programan algoritmos y desarrollan la IA, y en todo caso los Estados, los que no pueden desechar su responsabilidad y deben regular el uso de esos sistemas, especialmente en su utilización militar. Son investigadores y Estados los que deben mantener en su actuación los principios éticos y hacerse responsables legales al determinar su empleo y utilización.

La sensibilidad ética la deben tener los que diseñan las máquinas, que seguramente no podrán llegar a tener ni el sentido común de los humanos ni tomar decisiones apoyadas en un juicio moral basado en valores, pero no debemos olvidar que los humanos, en determinados ambientes y esferas de acción del campo de batalla, también cometemos errores cuya disminución y eliminación es un objetivo a mejorar, también desde la perspectiva ética, y a ello pudiera ayudar la IA.

Finalmente, y se tratará más adelante, debe mencionarse el reproche de la supuesta deshumanización de la guerra, al dejarse el combate en manos de sistemas y máquinas y que reflejarían ese cambio disruptivo en las características o incluso en la naturaleza de los conflictos bélicos que se viene anunciando.

La responsabilidad, ¿De los hombres o las máquinas?

«Lo militar se ha digitalizado y se está robotizando de forma acelerada. La inteligencia artificial es ya un componente indispensable de las fuerzas armadas, y de las de seguridad en sentido amplio, con el riesgo de perder el control»[22].

Cuestión central para considerar éticamente es la autonomía de los sistemas y el control que sobre ellos ejerce el ser humano, que no puede hacer dejación de responsabilidad, en relación con los resultados de las acciones ejercidas con armas que llegan a ser letales. Ante los posibles fallos en la competencia y las decisiones tomadas por máquinas, el nivel de control humano exigido por la ética debe ser tal que siempre haya un individuo responsable y que la rendición de cuentas por sus acciones y decisiones sea verificable.

22 ORTEGA, obra citada, p. 198.

Sistemas de armas y autonomía

Varios países como Reino Unido, Estados Unidos y Dinamarca, y organizaciones como Naciones Unidas (UN), el Comité Internacional de la Cruz Roja (ICRC) y OTAN, han expresado oficialmente diferentes conceptos y definiciones sobre sistemas de armas autónomos, arma autónoma, sistema autónomo o robot letal autónomo[23].

A los efectos de este trabajo nos parece interesante las definiciones apuntadas en la Directiva 3000.09 del Departamento de Defensa de los EE. UU., de noviembre de 2012[24]:

- Sistema de armas autónomo: un sistema de armas que, una vez activado, puede seleccionar y atacar objetivos sin intervención posterior de un operador humano. Esto incluye sistemas de armas autónomos supervisados por humanos que están diseñados para permitir que esos operadores tengan la capacidad de intervenir y finalizar los ataques, incluyendo el caso de un fallo del sistema de armas, antes de que ocurran niveles inaceptables de daño.
- Sistema de armas semiautónomo: un sistema de armas que, una vez activado, solo puede seleccionar y atacar objetivos que han sido seleccionados por un operador humano.

Siendo la autonomía del ser humano lo que le permite decidir su comportamiento y adecuarlo a parámetros éticos, la primera cuestión y preocupación es si la máquina (o la IA que la dirige) podrá llegar a ser autónoma en las decisiones que adopte en acciones de combate y, llegado este caso, la segunda es quién será responsable de las mismas.

Control humano significativo

Teniendo en cuenta lo expuesto sobre la autonomía de los sistemas de armas[25], resulta interesante recoger el proyecto sobre *Ethics Autonomy* del *Center for a New*

23 SCHAUB, G.D. y KRISTOFFERSON, J.W. (2017). *In, On and Out of the Loop?* Denmark and Autonomous Weapon System, Centre for Military Studies, University of Copenhagen, febrero 2012, pp. 5-6. https://cms.polsci.ku.dk/.../out-of-the-loop/in_on_or_out_the_. Visitado el 12.6.18.

24 DoD Directive 3000.09. *Autonomy in Weapons Systems*, noviembre 21, 2012, pp. 13-14 https://crytome.org/dod/dodd-3000-09.pdf Visitado el 12.6.18.

25 El concepto de sistemas de armas debe comprender todos los elementos que lo forman: plataforma de lanzamiento, sensores, equipos de comunicación, procesadores y la propia munición.

American Security (CNAS). Su objetivo «es ayudar a los Estados, activistas, académicos y militares a tratar de resolver los cambiantes asuntos surgidos en torno a la autonomía de las armas futuras»[26]. En la obra citada se recoge una consideración sobre el significado del concepto de autonomía en relación con los sistemas de armas, de utilidad en la reflexión ética planteada. Los autores proponen diferenciar esa autonomía según el ámbito que se considere: autonomía respecto a la relación de mando y control entre hombre y máquina; autonomía en relación con la propia complejidad o «inteligencia» de la máquina; y autonomía respecto al tipo de decisión que la máquina va a tomar independientemente[27].

De ellos el primer concepto crítico que se abre paso y se analiza en los foros internacionales es el de *control humano significativo*[28]. Con él se trata de que sea siempre el ser humano el último responsable de la actuación de un sistema de armas en la amplia variedad de tareas militares que se le pueden encomendar: adquisición, seguimiento, identificación y preparación de objetivos; orientación de armas; selección y priorización de objetivos; determinación del momento de disparo; y detonación.

En sentido amplio, parece que la IA no debería ser utilizada para reemplazar la toma de decisiones que hacemos los humanos cuando los asuntos son difíciles desde la perspectiva ética y tenemos que basarnos en juicios morales como es el caso de la evaluación de la proporcionalidad de un ataque militar. Esta es posiblemente la más compleja de las reglas a satisfacer en sus requerimientos éticos y cuya evaluación implica complejos procesos psicológicos hoy por hoy fuera del alcance de la IA, aunque alguno postula que quizá algún día se llegue a máquinas con autoconciencia, capaces de predecir comportamientos y sentimientos ajenos, como se apunta en el capítulo 2 de este trabajo.

La exigencia ética (y legal) de la proporcionalidad de un ataque a ejecutar con un sistema de armas con un grado de autonomía si se apoya en la IA, implica una serie de requisitos que debe cumplir la actuación de ese sistema respecto a la selección y ataque a objetivos. Así, se diferencia entre[29]:

- Sistemas militares *human in the loop*: sistemas semiautónomos en los que el hombre decide qué objetivos se van a seleccionar y atacar y el sistema ejecuta la

26 SCHARRE, P. y HOROWITZ, M.C. (2015). *An Introduction to Autonomy in Weapons Systems*, CNAS, Working Paper, febrero 2015, p2 https://www.cnas.org/.../an-introduction -to-autonomy-weapons-system. Visitado el 4.6.18.

27 SCHARRE y HOROWITZ, obra citada, pp. 5-8.

28 Significativo, efectivo o apropiado son términos también utilizados por el Comité Central de la Cruz Roja para designar el tipo y grado de control que preserva la decisión y responsabilidad moral del ser humano en decisiones para usar la fuerza [letal]. ICRC (2018), obra citada, p. 2.

29 SCHARRE y HOROWITZ, obra citada, pp. 8-15..

acción con completa autonomía. Las municiones guiadas o los misiles *fire and forget* podrían encajar en esta categoría.

- Sistemas militares *human on the loop*: sistemas en los que el hombre no decide los objetivos a seleccionar y enfrentar, tarea que lleva a cabo el sistema de forma independiente, pero aquel puede intervenir en la máquina y modificar su funcionamiento o pararla completamente en cualquier momento que observe un fallo o malfunción. Son también semiautónomos. Los sistemas Aegis y Patriot, entre otros, pertenecerían a esta categoría.

- Sistemas militares *human out of the loop*: sistemas capaces de operar sin intervención de un operador. El hombre no decide los objetivos a seleccionar y enfrentar y el sistema lleva a cabo con plena autonomía esas funciones sin que aquel pueda intervenir en ningún momento, aunque lo considere necesario. La gran mayoría de estos sistemas se emplean en misiones defensivas y la *loitering munition* («munición merodeante») como el sistema israelí Harpy 2 podría ser sería un ejemplo.

Es claro que en todos los casos anteriores hay un control humano inicial en el diseño y programación. Con la IA al problema del error o mal funcionamiento se le añade el de la autoprogramación que el sistema autónomo pueda llevar a cabo gracias al aprendizaje automático, escapando aún más al control y la necesidad de responsabilidad humana.

El Comité Internacional de la Cruz Roja plantea que el *control humano significativo* debería ser definido, planteado y resuelto en una norma legal[30], empezando por lograr una mayor precisión y consenso en los conceptos de «autonomía», «autonomía de las armas» y «armas autónomas», de cuya complejidad e importancia se ha tratado con anterioridad.

En la ya mencionada Estrategia de Sistemas Robóticos y Autónomos del Ejército de Tierra americano se plantea que «El Ejército pretende mantener el control humano sobre todos los sistemas autónomos. Se conseguirá este objetivo manteniendo a los humanos *in the loop* u *on the loop* de los actuales y futuros Sistemas Robóticos y Autónomos»[31].

Pero también es posible hacer un mal uso de la IA, y a nuestro objeto interesa especialmente considerar la posibilidad de llegar a «crear armas letales autónomas»

30 *Report of the Expert Meeting on Autonomous Weapon Systems: technical, military, legal and humanitarian aspects* (2014) https://www.icrc.org/en/document/report-icrc-meeting-autonomous-weapon-systems-26-28-march-2014. Véase también *Autonomous weapons systems: Implications of increasing autonomy in the critical functions of weapons* (2016). https://www.icrc.org/en/publication/4283-autonomous-weapons-systems.

31 The U.S. Army, Robotic and Autonomous Systems Strategy, obra citada, p. 3.

apoyadas en los desarrollos que está teniendo la IA. Por esto resulta de particular interés este nuevo concepto de *Sistemas de Armas Letales Autónomas* (SALAS en español y LAWS en inglés: *Lethal Autonomous Weapon Systems*), y que algunos refieren como *robots asesinos*. En realidad, son robots inteligentes o dispositivos de robótica inteligente que según la organización *Human Rights Watch* serían «armas completamente autónomas que pueden seleccionar y entablar combate contra objetivos sin intervención humana»[32] y que deberían ser prohibidos.

Como indica Irene Savio[33], tienen el riesgo de ser utilizados en el futuro como armas que podrían tomar la decisión de herir o matar, de forma independiente a cualquier control del ser humano, existiendo en la actualidad un vacío en el Derecho Internacional Humanitario.

Para avanzar en esa búsqueda de consenso internacional, la propia Organización de Naciones Unidas (ONU) ha celebrado en Ginebra desde el año 2014 y en el marco de la Convención de 1980 sobre las Prohibiciones o Restricciones en el uso de Ciertas Armas Convencionales (CAC y *Certain Conventional Weapons:* CCW, en inglés), reuniones para lograr un marco regulador internacional. En la sesión celebrada a finales de 2017 se han debatido cuestiones tecnológicas, militares, legales y éticas, que han quedado abiertas a futuras discusiones en las que se tratará de enmarcar definiciones y otros conceptos que faciliten consideraciones posteriores de alcance político.

En cualquier caso, las acciones llevadas a cabo por sistemas de armas autónomos basados en la IA exigen el control y la supervisión de humanos, únicos a los que se les puede exigir responsabilidad por sus acciones pasadas y que modifiquen sus acciones futuras. Ello es así porque las «Armas completamente autónomas carecen de cualquier emoción que les pueda producir remordimiento si algún otro [humano] es castigado por sus acciones. Por lo tanto, el castigo de otros intervinientes no haría nada para cambiar la conducta del robot»[34].

Predictibilidad y rendición de cuentas

De particular relevancia es la consideración de la IA y sus algoritmos de desarrollo en relación con dos principios de carácter ético: la predictibilidad y la rendición de cuentas.

32 HRW (2012). *Losing Humanity. The Case against Killer Robots*, 19 noviembre 2012, p. 1. https://www.hrw.org/.../2012/.../losing-humanity/case-agIAnst-killer-robots. Visitado el 10.5.18.

33 SAVIO, I. (2017). ¿Quién ganará la guerra de las armas letales autónomas?, esglobal, https://www.esglobal.org/la-onu-frente-las-maquinas-asesinas/.

34 HRW, obra citada, p. 29.

En 2016, Lewis, Blum y Modirzadek introducen el concepto de *war algorithm* como «un algoritmo expresado en un código de ordenador, que se logra a través de un sistema elaborado, y que es capaz de operar relacionado con conflictos armados». Dado que los algoritmos, dicen los autores, «son una piedra angular conceptual y técnica de muchos sistemas. Estos sistemas incluyen arquitecturas de aprendizaje que hoy presentan algunas de las cuestiones más peliagudas sobre reemplazar el juicio humano con elecciones producidas algorítmicamente»[35].

Esto complica la predictibilidad del futuro funcionamiento de la máquina, que incluso puede aprender en forma no intencionada por quién la desarrolló. Así, por ejemplo, puede ocurrir con los algoritmos incorporados al *machine learning* o aprendizaje automático (mencionado en capítulos anteriores de este trabajo). Dado que el algoritmo no está determinado solo por el programador, sino que el propio algoritmo aprende en el proceso y por la experiencia que va teniendo, esto produce que se resienta la predictibilidad de su acción y objetivo, pudiendo quedar fuera del control humano.

En las fases iniciales de su diseño se puede testar, verificar y validar, pero estos procesos deberían continuarse a lo largo de toda la fase de aprendizaje de la máquina. Si no es así, el sistema se puede convertir en impredecible y la identificación y selección de objetivos militares, por ejemplo, devenir en ilegal y no ética.

En cuanto a la rendición de cuentas (*accountability*) en relación con los algoritmos, debe ser exigida a los Estados y a los individuos responsables del «diseño, desarrollo o uso de un algoritmo de guerra»[36].

Los nuevos sistemas de armas apoyados en la inteligencia artificial y los algoritmos, al producir muchas mayores capacidades y precisiones, se utilizarán para perseguir, doblegar y vencer al enemigo. Es muy difícil no considerar que serán importantes en los futuros sistemas y capacidades para vencer en guerras y conflictos bélicos. Pero con los algoritmos «la posibilidad de reemplazar el juicio humano con decisiones basadas en algoritmos «especialmente en guerra» amenazan lo que muchos consideran es lo que nos define como humanos»[37].

35 LEWIS, D., BLUM, G y MODIRZADEK, N. (2016). *War Algorithm Accountability*. http://dx.doi.org/10.2139/ssrn.283274, p. VII, Visitado el 25.05.18.

36 LEWIS y otros, obra citada, pp. VIII y IX.

37 LEWIS y otros, obra citada, p. X.

¿El avance de la inteligencia artificial hacia los robots «éticos»?

Algunos científicos implicados en el desarrollo de la IA son optimistas en lograr sistemas en los que la inteligencia no sea considerada como artificial, sino como inteligencia tecnológica puesta al servicio de los seres humanos. «Del mismo modo que podemos prever máquinas cuyos controles impliquen cada vez mayores grados de sensibilidad a las cosas que importan desde un punto de vista ético. No serán máquinas perfectas, desde luego, pero sí mejores»[38].

En el campo militar, científicos como Ronald Arkin consideran que los robots con capacidad letal pueden llevar a cabo su trabajo de forma más eficiente y también más ética que los soldados humanos. Para este científico hay una fundada esperanza de que si estos sistemas son diseñados apropiadamente y utilizados adecuadamente se pueden reducir los daños colaterales e incluso «Cuando se trabaje en una unidad orgánica de soldados humanos y sistemas autónomos, los robots tienen el potencial de monitorizar la conducta de todas las partes en el campo de batalla de forma independiente y objetiva e informar de las infracciones que puedan ser observadas. Su presencia por sí sola podía llevar a una reducción en las infracciones éticas de los humanos»[39].

La principal idea de Arkin es que estos sistemas puedan programarse con determinadas restricciones que salvaguardarían el respeto a las reglas éticas y al Derecho Internacional Humanitario en el campo de batalla sin el riesgo del fallo humano que puede llevar al acto ilegal y, sobre todo, inmoral, en el desarrollo de las operaciones militares.

Su propuesta se apoya en un control doble: un primer paso en el que los robots evaluarían la información para comprobar que un ataque respeta el Derecho Internacional y las reglas de enfrentamiento y, en caso de no violarlas, un segundo paso escrutaría bajo diferentes criterios (efectividad, daños colaterales, proporcionalidad, …), si el ataque satisface todos los criterios y restricciones éticas, incluyendo minimizar los daños colaterales en relación con la necesidad militar del objetivo.

A lo anterior habría que añadir las ventajas que sin duda tiene el uso de sistemas de armas y robóticas dirigidas por la IA, como serían las de menor vulnerabilidad a ciertas armas como las químicas y biológicas, reducción de bajas y del riesgo a que se exponen los humanos (que en última instancia podría llevar a plantear la utilización de armas no letales), y reducción del error en los ataques a objetivos militares.

38 ALLEN, C. (2011). *The Future of Moral Machines*, New York Times, diciembre 25, p. 5. https://opinator.blogs.nytimes.com/2011/12/25/the-future.of.moral-machines/. Visitado el 7.6.18.

39 ARKIN, R. (2009). *Ethical Robots in Warfare*, IEEE Technology and Society Magazine, Spring, pp. 30-33 https://www.gatech.edu/IA/robot-lab/online.../arkin-rev. Visitado el 01.03.18.

Dado que los robots soldados estarían programados para matar, obedecer órdenes de superiores (recordemos que el combatiente tiene el derecho y el deber de no obedecer órdenes que supongan un acto ilegal o sean manifiestamente inmorales) y no tener preocupación por su propia supervivencia, en ese hipotético modelo ético traducido en los algoritmos y las instrucciones de programación del robot, se debería incluir la posibilidad de que estos sistemas pudieran abandonar la misión ante circunstancias imprevistas y sobrevenidas, ya que si llegaran a ejecutarla tendría la consideración de inmoral o ilegal. Y todo ello gracias a que los robots podrían procesar más información, más rápido y de forma más completa que los humanos antes de utilizar la fuerza letal y además no están influenciados por emociones humanas como el miedo o la ira.

Otros autores como McGinnis también defienden que armas robóticas con una fuerte IA serían capaces de superar todos los problemas éticos, de forma que «robots guiados por IA en el campo de batalla podrían realmente producir menos destrucción, convirtiéndose en una fuerza civilizada en guerras, así como una ayuda a la civilización en su lucha contra el terrorismo»[40].

Sin embargo, se plantean algunas dificultades. A la objeción de que las expectativas sobre los desarrollos de la IA son en el momento actual más aspiraciones que realidades, se une el hecho de que los científicos de la IA y la robótica no han trabajado bajo las disposiciones de un código deontológico, al estilo del código médico hipocrático.

En esta línea, otros que deberían estar más implicados como los filósofos de la ética apenas empiezan a considerar los problemas éticos que pueden presentar la IA y la robótica[41]. Por no mencionar que la industria, y la de la IA y la robótica también lo es, nunca ha dado pasos teniendo demasiado en cuenta las consecuencias éticas de sus desarrollos (tabaco, automóvil o genoma humano así lo atestiguan).

Por esto, resulta interesante que responsables de grandes empresas tecnológicas empeñados en el desarrollo de la IA afirmen que «el desafío al que nos enfrentamos los que trabajamos en el diseño de IA es el de conseguir no solo la inteligencia adecuada, sino también las cualidades humanas idóneas: emoción, ética y empatía»[42].

Un interesante concepto es el de *Moral machines* [Máquinas morales][43], y resulta especialmente útil seguir a Singer[44] en las condiciones que ese *diseño ético* debería

40 MCGINNIS, J. (2011). *Accelerating AI*, Northwestern University School of Law, Public Law and Legal Theory Series, No. 10-12, p. 4.

41 SINGER, P. (2009), obra citada, pp. 418 y ss.

42 NADELLA, S., obra citada, p. 183.

43 WALLACH, W. y ALLEN, C. (2010). *Moral Machines: Teaching Robots Right from Wrong*, Londres: Oxford University Press

44 SINGER, P- (2009), obra citada, p. 424.

cumplimentar. Menciona: mantener que el funcionamiento responda a un diseño que no sea capaz de cambiarse o desarrollarse a sí mismo originando algo inesperado y quizá peligroso, a menos que se quiera que sea así, lo que va contra esa prevención ética; diseñar mecanismos que aseguren el control humano para desactivar a las máquinas cada vez más autónomas. Esto debería incluir controles de seguridad que eviten a todo tipo de «hackers» que puedan hacerse con el control o reprogramar las máquinas; construir múltiples redundancias en los sistemas (resiliencia); y mantener la información recogida en un sistema que esté fuera del alcance general para evitar su mal empleo, pero que permita el acceso por parte de las autoridades públicas.

Otras iniciativas que abordan estas cuestiones éticas relativas a los sistemas de IA en general y que propugnan «diseños éticamente orientados» para los mismos son la «Iniciativa Global sobre Ética de los Sistemas Autónomos e Inteligentes» del *Institute of Electrical and Electronics Engineers* u otros trabajos del *Future of Life Institute*[45].

También se utiliza el término de «guerra cognitiva», en la que las enormes exigencias de capacidad cognitiva para filtrar, organizar y clasificar la información procedente de múltiples sensores serían encargadas a la IA, dejando para los seres humanos las tareas de evaluación y toma de decisión[46]. En relación con esta idea se ha reprochado el empleo de robots militares autónomos que no tienen ningún ser humano como agente al que se puede exigir responsabilidad de sus acciones de combate. Esta crítica no sería válida para un vehículo tripulado a distancia, pues en este caso hay un operador que se encuentra en grado mayor o menor en la cadena de responsabilidad.

Los Dispositivos con Apoyo Neurológico Humano

Esa censura de la falta de responsabilidad de un humano en el campo de batalla tampoco sería aplicable a unos modernos desarrollos tecnológicos que se conocen como HAND (*Human Assisted Neural Device* que traducimos por «Dispositivos con Apoyo Neurológico Humano»)[47]. Estos robots militares son controlados por un ser humano a través de una conexión neuronal que la máquina interpreta y ejecuta acciones. Para ello se trasladan procesos de naturaleza electroquímica del cerebro humano, mediante tecnología digital e IA, en señales eléctricas que luego el sistema interpreta desarrollando acciones concretas.

45 ICRC, obra citada, p. 16.

46 NURKIN (2018), obra citada, p. 3..

47 EVANS, N. (2011). *Emerging Military Technologies: A Case Study in Neurowarfare*. En TRIPODI, P. y WOLFENDALE, J. *New wars and new soldiers: military ethics in the contemporary world*. Ashgate: Surrey, pp. 105-116.

El problema ético y la exigencia de tener un *human in the loop* se resolvería con los HAND, pues el operador no presenta los problemas de gestión de interfaces, los errores en sensores propioceptivos o táctiles y el sistema funciona a voluntad de un operador que asume las responsabilidades de sus acciones.

Ya se ha expuesto que la cuestión central de quién puede dar la orden de matar y que sea éticamente permisible es central en la ética militar. Y para los teóricos de la ética en una guerra justa esa admisibilidad moral se debe fundar en el respeto a los principios de necesidad, proporcionalidad y distinción o inmunidad de los no combatientes cuando en la lucha se intentan conseguir los objetivos militares y se pelea por preservar la vida propia.

Se ha argumentado en contra de los sistemas HAND que no sería moralmente permisible matar a combatientes enemigos dada la ausencia de amenaza que suponen los soldados no dotados de la tecnología HAND en el campo de batalla y, en consecuencia, la asimetría en su empleo trasformaría las condiciones del conflicto haciendo de él una guerra injusta.

Sin embargo, el desarrollo hacia esos sistemas continúa, apoyándose en razones como la posibilidad de su uso con armas no letales o la necesidad de contrarrestar las acciones asimétricas de enemigos más débiles, que siempre se han utilizado en la historia de la guerra.

Ante todos estos desarrollos futuros que la IA podría introducir en robots y sistemas de armas a los que se pretende dotar de restricciones éticas en su arquitectura algorítmica, las objeciones que se presentan se expresan a continuación de forma resumida:

- La objeción epistemológica. Implementar un «software ético» en los robots implica una reducción de la ética militar, a menudo compleja reflexión y decisión, a procedimientos algorítmicos que al tener que basarse en normas concretas y prefijadas implican la elección de un bien, de una conducta, en detrimento de otras. Pero la conciencia ética, el respeto al principio de humanidad en el combate, no puede ser trasladada, al menos de momento, a algoritmos de computación.

- La objeción antropológica. El uso de robots dirigidos por la IA lleva a la deshumanización del conflicto bélico, al introducir el enorme riesgo de que los humanos se liberen consciente o inconscientemente de su responsabilidad. Al quedar exonerados de responsabilidad podría resultar más cómodo y fácil consentir que sean los robots autónomos armados los que se impliquen en el combate, tolerando que sean ellos los que tomen las decisiones y pretendiendo olvidar la responsabilidad humana esencial en la utilización de la fuerza letal. En esta línea, en muchas operaciones actuales un objetivo esencial es ganar «la mente y los corazones» de las poblaciones locales en las que despliegan fuerzas. Que sean robots muy previsiblemente arruinaría la consecución de ese objetivo.

Opinión pública y percepción del empleo de la inteligencia artificial y sistemas autónomos en la guerra

Las cuestiones éticas que emergen en el diseño, desarrollo y utilización de las tecnologías robóticas son reales y muy dignas de tomar en consideración. Por razones éticas[48] y de legitimidad democrática los ciudadanos y la sociedad deben implicarse en el debate y ser conscientes de los riesgos y los desafíos que implican. Considerar la influencia de la inteligencia artificial y la robótica en la evolución y el desarrollo de nuestra especie, no como algo propio de la ciencia ficción, permitirá prevenir desarrollos inesperados e indeseados en el futuro[49].

En esta línea, y como aproximación limitada al impacto en la percepción de la opinión pública, resulta de interés considerar la encuesta llevada a cabo en 2015 por la *Open Roboethics Initiative* (ORI), organización no gubernamental creada en 2012 y enfocada al uso ético de la robótica y la IA. El estudio de opinión se centró en los aspectos éticos y de gobierno asociados al uso de sistemas de armas letales autónomos (SALAS), robots inteligentes mencionados anteriormente.

Los resultados más destacados, expresados de forma resumida, se refieren a que todos los tipos de SALAS deberían ser prohibidos internacionalmente (67%), así como su utilización y desarrollo (56%); no deben ser usados para propósitos ofensivos (85%); se deberían utilizar sistemas de armas operados remotamente en lugar de SALAS (71%); y preferirían ser atacados por sistemas operados remotamente antes que por esos sistemas (60%). Dos asuntos complementarios resultan de interés. El primero es que la razón principal que se da para apoyar el desarrollo y uso de SALAS en el campo de batalla es el de salvar al personal militar de los daños físicos y psicológicos de la guerra (33%) y que está en línea con el menor número de pérdidas humanas como criterio político del éxito de una operación militar. El otro asunto sugestivo es

48 En el Preámbulo del Protocolo Adicional II a las Convenciones de Ginebra se recoge la denominada cláusula Martens: «Recordando que, en los casos no previstos por el derecho vigente, la persona humana queda bajo la salvaguarda de los principios de humanidad y de las exigencias de la conciencia pública». La IA y los sistemas autónomos introducen sin duda casos no previstos hasta ahora.

49 Recordemos que existe una corriente, el *transhumanismo*, que promueve que la tecnología puede mejorar al ser humano y sus capacidades de forma extraordinaria y avanzar en la búsqueda de la inmortalidad. El avance de las tecnologías informáticas y de la biotecnología ha llevado a apuntar a los defensores de esta corriente a postular que llegará el día en que los ordenadores adquirirán conciencia de sí mismos y se producirá una fusión entre inteligencia artificial y humana. Adviértase que, en ese camino de integración con máquinas mediante la incorporación de implementos robóticos, la propia naturaleza de la condición humana se modifica y en esa evolución se podría llegar a una nueva especie humana y la desaparición de la actual. Véase DIEGUEZ, A. (2018). Los profetas ambiguos. Claves de razón práctica, Núm. 257, marzo-abril, pp. 22-31.

el rechazo del desarrollo y uso de SALAS y que debe ser siempre el ser humano quién tome las decisiones que signifiquen vida o muerte en el campo de batalla. Aspectos adicionales de interés son el que hay un 20% que desconfía de que la tecnología sea lo suficientemente robusta para llevar a cabo esos cometidos; un 14% cree que la probabilidad de que caiga en manos equivocadas es enorme; y un 12% manifiesta su preocupación por la asignación de responsabilidad cuando un arma autónoma cometa un error que cueste vidas humanas.

El papel de la opinión pública y la percepción de la IA y los sistemas robóticos en general y en relación con su implicación en el conflicto bélico y la guerra también es caracterizado en relación con la confianza que en su desarrollo tienen las diferentes generaciones. Parece general la idea de que cuanto más joven es el público, mayor es la aceptación de la IA como un desarrollo científico normal y, por tanto, se asume su utilización. Son las personas de mayor edad las que muestran un amplio rechazo que se sustenta en la idea del alejamiento de la naturaleza humana de estas modernas tecnologías. Los individuos que se han desarrollado y adquirido amplias competencias digitales, normalmente los más jóvenes, suelen aceptar máquinas y sistemas computerizados en sus vidas de forma mucho más natural y tenderían a aceptar los nuevos tipos de armas en el campo de batalla con más amplitud. Sería muy interesante conocer estas actitudes en los líderes políticos y los responsables y autoridades militares.

También se apunta que el empleo de la IA en actos de terrorismo, o que atentan contra la seguridad, irá modificando culturalmente a las sociedades en el sentido de asumir el empleo de sistemas de armas apoyados por la IA dentro de las tecnologías militares y de seguridad que se puedan utilizar.

La contención y el esfuerzo de las sociedades democráticas en evitar, contener y regular dentro de normas legales y éticas las guerras continúan teniendo un apoyo mayoritario de los ciudadanos de aquellas sociedades. La popularidad en el empleo de la IA y de las máquinas inteligentes sigue siendo reducida, a pesar de la ventaja de disminuir drásticamente la perdida de soldados que pudieran implicarse en conflictos bélicos.

Conclusiones

Máquinas y robots van a marcar las guerras del futuro. Doctrinas, estrategias, planes y operaciones aún están por establecerse e incluso es muy probable que en el desarrollo futuro de esos conceptos las máquinas estén llamadas a desempeñar un papel determinante. Las prospectivas adelantan la mudanza de seres humanos a máquinas también en la realidad social de conflictos y guerras.

La incorporación de avances científicos, algunos impensables hace pocos años, está transformando las Fuerzas Armadas. Ello exige cambios orgánicos y doctrinales, impone nuevas misiones, demanda mejores instrumentos y reclama apertura de las mentalidades. Como se indica en el capítulo anterior de este trabajo: «se puede concluir que la IA y la robótica cambiarán el carácter de la guerra. Los cambios serán más visibles en los niveles táctico y operacional».

La incorporación de sistemas autónomos, robots e inteligencia artificial a las Fuerzas Armadas cambia las características de esta institución en aspectos esenciales como el papel a desarrollar por el soldado (humano) en el campo de batalla, la relación de los sistemas dentro del grupo y con los comandantes, y la percepción de las poblaciones dentro de las cuales tienen lugar las operaciones militares.

En cualquier caso, los sistemas autónomos y robóticos apoyados en la IA deben avanzar en su desarrollo científico bajo los principios de minimizar los riesgos éticos que plantea su utilización en combate, así como incorporar los valores morales en sus procesos de toma de decisiones, asunto que de momento parece lejano.

También el liderazgo militar y su propia concepción sufrirán modificaciones. Las características y las aptitudes para liderar seres humanos tendrán que modificarse para ejercerse sobre unidades de hombres y máquinas, y eventualmente solo sobre máquinas.

Los cambios que producen la ciencia y la tecnología modifican y trasforman la forma de afrontar y gestionar los conflictos, las estructuras militares y la disposición psicológica de los soldados y marineros ante el combate. Por ello, se modifican las conductas en misiones de combate y de apoyo al combate y, por supuesto, en misiones de paz.

Los nuevos conflictos del siglo xxi, inspirados por el desarrollo científico y tecnológico, necesitan una modificación de los principios legales y éticos que inspiraron las guerras y conflictos del siglo xx, pues nuevas armas y tipos de combate aparecen y cuestionan la validez de aquellos, así como nuevas sensaciones y sentimientos que se añaden a las crudas emociones y pasiones que tradicionalmente han implicado al combatiente.

En su control y dirección habrá que tener en cuenta, además, que muy frecuentemente el enemigo al que se enfrenta no tendrá, previsiblemente, ninguna restricción ética ni legal en sus acciones y medios de combate.

Desde un punto de vista ético, las sociedades desarrolladas se han impuesto contención a la hora de implicarse en conflictos bélicos y las reglas jurídicas se aplican con rigor creciente. Una consecuencia importante es que la utilización de sistemas autónomos y otras máquinas letales no debe producir una disminución del rigor y de la relevancia de los códigos morales con los que la civilización desarrollada, incluyendo su tecnología, ha avanzado. La ética es de los hombres y ellos son los principales

afectados, por lo que debe avanzar en paralelo con la ciencia teniendo en el centro de sus objetivos al ser humano[50].

Una conclusión que nos parece evidente es que el uso de la IA en sistemas autónomos y robóticos está éticamente justificado en el principio del riesgo innecesario y el deber moral de evitar la exposición arriesgada al combatiente en un conflicto justo y legal. «Vamos a compartir la toma de decisiones con las máquinas, y ellas minimizarán los riesgos que pedimos correr a nuestros soldados»[51]. Sin duda, esto puede llevar a un cambio en los valores que constituyen el *ethos militar* tradicional de las fuerzas armadas, lo que constituye otra muestra de ese cambio en las características de la guerra en esta sociedad posheróica.

Pero, de momento, es necesario que se mantenga un imprescindible control humano significativo, lo que significa la responsabilidad, en cualquier ocasión, de una persona y la verificabilidad de sus decisiones y consecuencias. Si es bastante claro que el combate futuro tendrá un componente importante, y seguramente decisivo, en sistemas de armas y robots, si la IA va a formar parte decisiva en la capacidad de decidir de las maquinas autónomas, es necesario mantener y avanzar en reglas legales y éticas que sigan dando la primacía en la decisión y el mantenimiento de la responsabilidad final en el uso de la fuerza letal al ser humano. Y ello a pesar de lo legítimo que resulta pensar que el desarrollo tecnológico puede contribuir, como ya lo ha hecho, a reducir las limitaciones y errores del combatiente.

El que la reflexión ética avance en línea con la investigación, desarrollo, innovación y utilización de los avances científicos es una exigencia para que la persona y su dignidad inviolable se mantengan, con el nivel de desarrollo moral que hemos alcanzado, en todas las relaciones y fenómenos humanos, incluyendo las guerras y los conflictos bélicos desarrollados con las tecnologías emergentes.

Aunque para muchos la máquina no será capaz de desarrollar lo más propio al ser humano, el sentido común asociado a su inteligencia y la decisión ética basada en valores, por lo que el temor al *robot asesino* estaría infundado, podemos imaginar al menos como asunto de ficción y, en consecuencia, tomar medidas para evitarlo, la posibilidad de que algún día la ciencia de la IA desarrolle máquinas que escapen al control y se trasformen en algo más inteligente que el propio ser humano, pudiendo diseñar y construir otros artilugios por su cuenta.

La cuestión sería establecer si esas máquinas también podrían disponer del juicio moral para convertirse en responsables de las acciones que adopten en el campo

50 A este respecto, Adela Cortina nos advierte que cualquiera que sea el desarrollo de los avances tecnológicos, debe tener en cuenta que estos están al servicio del ser humano, de modo que «la razón moral debe ir por delante de la razón técnica» (2018, El País, Opinión, 26 mayo, 13).

51 ORTEGA, obra citada, p. 198.

de batalla e incluso si lucharían unas contra otras, convirtiendo a la guerra en un fenómeno literalmente «inhumano». Entonces sí que podríamos afirmar la completa trasformación de la naturaleza de la guerra.

Capítulo 6

Contexto estratégico de la inteligencia artificial

Félix Arteaga Martín

Resumen

La inteligencia artificial (IA) no solo es una tecnología disruptiva en los ámbitos militar, económico, industrial y social, como muestran los capítulos precedentes, sino también un elemento disruptivo del contexto estratégico internacional. La IA multiplica todos y cada uno de los factores que determinan el poder de cada actor internacional por lo que altera la estructura y jerarquía del sistema internacional.

Como se analiza en este capítulo, los principales actores internacionales se han dado cuenta del valor de la IA como instrumento de competencia geoeconómica y geopolítica global. Independientemente de la mayor o menor capacidad de apropiación que cada uno de ellos tiene respecto a la IA, todos son conscientes de su potencial transformador interno e internacional, por lo que han desarrollado las visiones, estrategias y planes de actuación que se detallan.

El capítulo diferencia los actores avanzados de los emergentes. Entre los primeros figuran Estados Unidos, China, la Federación Rusa e Israel. Comparten el mismo interés estratégico por el desarrollo de la IA y el mismo enfoque de seguridad nacional con algunas peculiaridades como el liderazgo del sector privado en Estados Unidos e Israel y del público en los demás. Entre los actores emergentes se han seleccionado algunos países europeos como Francia, Alemania o el Reino Unido junto a la propia Unión Europea, que han puesto en marcha iniciativas que debiera seguir España -cuanto antes- para poder competir en el mercado global de la IA.

Palabras clave

Tecnología, inteligencia artificial, geopolítica, seguridad nacional, estrategia, contexto estratégico.

Strategic context of artificial intelligence

Abstract

Artificial intelligence (AI) is not only a disruptive technology in the military, economic, industrial and social fields as shown in the preceding chapters, but also a disruptive element of the international strategic context. AI multiplies every one of the factors that determine the power of each international actor, thus altering the structure and hierarchy of the international system.

As discussed in this chapter 6, the main international actors have realized the value of AI as an instrument of global geoeconomic and geopolitical competition. Regardless of the greater or lesser capacity of appropriation that international actors may have regarding AI, they all recognize the transformational power of the IA both for the domestic and the international context. Thus, they have developed visions, strategies and action plans that are detailed in this chapter.

It differentiates advanced actors from emerging ones. The first group includes the United States, China, the Russian Federation and Israel. They share the same strategic interest for the development of AI and the same approach to national security with some peculiarities such as the leadership of the private sector in the United States and Israel against the public in the others two. Among the emerging players, some European countries have been selected, such as France, Germany or the United Kingdom, together with the European Union itself, which have launched initiatives that Spain should follow - as soon as possible - in order to compete in the global AI market.

Keywords

Technology, strategic context, artificial intelligence, geopolitics, national security, strategy.

«*Whoever becomes the leader in this sphere*

(AI) will become the ruler of the world».

Vladimir Putin[1].

Introducción

La inteligencia artificial (IA) no es un desarrollo tecnológico más que afecte al crecimiento económico[2]. Para los países y, sobre todo, para las grandes potencias, la IA es uno de los nuevos factores de poder porque su posesión -especialmente si se controla su monopolio en algún sector de la misma- multiplica exponencialmente todas las dimensiones de poder. Por eso, las grandes potencias han adoptado un enfoque de seguridad nacional en relación con la IA porque refuerza su potencial diplomático, económico y estratégico, duro o blando, para escalar posiciones en la jerarquía internacional y desplazar a los países que no dispongan de ella en grado suficiente en la nueva -y dura- competencia geopolítica mundial que se avecina por la tecnología[3].

La percepción de la IA como un elemento de competencia internacional o de seguridad nacional diferencia la posición de las grandes potencias respecto al resto de los actores de la comunidad internacional. Buscan en la IA la palanca que les asegure su continuidad en los primeros lugares de la jerarquía internacional durante un tiempo nuevo en el que, como dice el presidente Vladimir Putin de Rusia, el liderazgo en el desarrollo de la inteligencia artificial conducirá al liderazgo mundial. Una afirmación inmediatamente posterior a que el gobierno chino desvelara en julio de 2017 su estrategia para liderar la IA mundial en 2030[4].

1 Associated Press, 1 septiembre 2017. Disponible en https://www.apnews.com/bb5628f2a7424a10b3e38b07f4eb90d4. Consultado el 30.07.2018.

2 La inversión global en IA ha pasado de 282 millones de dólares en 2011 a 2.400 en 2015 según el Foro Económico Mundial y podría llegar a 127.000 millones en 2025 según McKinsey Global Institute, «Artificial Intelligence: Implications for China», abril 2017, p.2. El estudio de Price Waterhouse Coopers, «Sizing the price» señala que el PIB mundial podría crecer hasta el 14% en 2030 gracias a la IA, añadiendo hasta 15,7 trillones de dólares, disponible en https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html. Fecha de la consulta 30.07.2018.

3 BREMER, Ian y KUPCHAN, Clif, «Top Risks 2018», Eurasia Group, 2 enero 2018, pp. 8-9.

4 Consejo de Estado, «A Next Generation Artificial Intelligence Development Plan», 20 de julio de 2017, traducido y disponible en https://www.newamerica.org/documents/1959/translation-fulltext-8.1.17.pdf. Fecha de la consulta 30.07.2018.

El resultado de la competición por la IA no depende tanto de las tecnologías como de la forma en la que gobiernos y empresas decidan utilizarlas[5]. Aquellos que ya han tomado conciencia de sus retos y oportunidades han desarrollado evaluaciones de impacto, elaborado estrategias, adoptado políticas y estructurado unos ecosistemas de investigación y desarrollo que se describen en este capítulo de acuerdo a su mayor o menor nivel de ambición y a la información disponible en fuentes abiertas[6].

Como se analiza en otras partes de este texto, los actores estatales no tienen el monopolio de la IA y son las grandes multinacionales tecnológicas las que están detrás de las disrupciones tecnológicas, a favor o en contra de los intereses de esos Estados, por lo que no se debe menospreciar su capacidad de interacción público-privada a la búsqueda de una posición hegemónica en el mercado global[7]. El liderazgo y la contribución de cada Estado es importante para canalizar la IA en beneficio de la soberanía y prosperidad de cada sociedad, pero no depende solo de los gobiernos. Necesitan contar con una red de colaboración, un ecosistema favorable de empresas innovadoras, centros tecnológicos y universidades donde prospere la investigación y el desarrollo de la IA. Sin ellas, es difícil que se satisfaga los intereses nacionales de IA.

La voluntad de los gobiernos no basta para afrontar los retos de la IA porque su desarrollo y aplicación depende de la base de investigación, desarrollo y talento disponible. Y para liderar la competición global, los Estados deben favorecer las condiciones para ello sabiendo que los recursos materiales son más fáciles de alcanzar que los inmateriales como el talento (difícilmente puede EE. UU. liderar la IA si sus estudiantes ocupan el puesto 29 de matemáticas y el 22 de ciencias en el mundo), lo que les obliga a realizar cambios estructurales y a largo plazo en los sistemas educativos y de formación.

A diferencia de otros instrumentos de poder, la IA va a afectar a la vida diaria de los ciudadanos y estos demandarán a sus gobiernos que les protejan de sus efectos negativos. El nivel y las prioridades de protección varían según los países. Mientras que entre los europeos prima la salvaguardia de la privacidad de los datos, en Estados Unidos y China son partidarios de sacrificarla en aras del desarrollo de la IA, lo que crea serios problemas de conciliación, por ejemplo, cuando los datos de los ciudadanos

5 HOROWITZ, Michael C. y otros, «Strategic Competition in an Age of Artificial Intelligence», Centre for New American Security (CNAS), julio 2018, p. 4.

6 Los ecosistemas constan de agencias gubernamentales o empresas que invierten fondos, centros universitarios dedicados a la investigación básica, centros tecnológicos y laboratorios dedicados a la investigación aplicada y empresas innovadoras (*startups*), a veces agrupadas territorialmente (valles) o interconectadas con otros ecosistemas internacionales.

7 La inversión global se lidera por multinacionales tecnológicas como Google o Baidu que invirtieron entre 20 y 30 billones de dólares en 2016, dedicando el 90% a la I+D y el resto a la adquisición de IA. También se excluyen de este capítulo las aplicaciones no estratégicas de la IA en el interior de los países en cuanto no afecta a la competición geoestratégica global.

se gestionan por la IA de terceros países. Lo anterior significa que los Estados, al menos los democráticos, deben tener en cuenta esos riesgos en sus estrategias, lo cual conduce al modelo de gobernanza.

Al igual que ocurriera con el ciberespacio, donde las grandes potencias se han resistido a regular las iniciativas tecnológicas del mercado hasta que se conocieron los efectos económicos de los ciberataques y los riesgos políticos de la manipulación de los datos privados, los gobiernos solo han comenzado a preocuparse de la gobernanza de la IA cuando se han identificado los riesgos asociados para el bienestar, derechos y libertades fundamentales de sus ciudadanos[8]. De hecho, los responsables políticos necesitarán algún tiempo antes de que tomen conciencia del impacto de la IA sobre las políticas públicas, sus sociedades y electores, así como de las asociaciones estratégicas necesarias para su gobernanza.

Además, la IA afecta a la gobernanza internacional porque altera el equilibrio de poder del sistema internacional, ya que proporciona una ventaja decisiva en el proceso de decisiones sobre las relaciones internacionales. A la falta de gobernanza se une el riesgo de que la competencia internacional por la hegemonía en la IA acentúe las tensiones internacionales. Tal y como se percibe en la actualidad, la anticipación tecnológica en el campo de la IA ofrece a sus promotores una ventaja casi decisiva sobre sus competidores que van más retrasados (el que llega primero se queda con todo), lo que justifica la carrera en curso entre las potencias por anticiparse en el control de sus aplicaciones y una aceleración de las inversiones de las compañías por hacerse con el monopolio de las tecnologías de IA críticas para controlar el mercado mundial de la IA. En el primer caso, la IA altera el equilibrio de poder tradicional y pone en riesgo la soberanía de los países perdedores y, en el segundo, el acceso anticipado a la IA genera riesgos para la competencia y libertad de mercado.

Para proteger la soberanía y la prosperidad, los Estados tienden a asegurar las inversiones estratégicas, la protección de la propiedad industrial, la educación, la I+D+i, la retención de talento y todos los factores que coadyuvan a la superioridad en IA. En sentido contrario, la comunidad internacional va tomando conciencia del reto, identifica los retos y las líneas rojas para contener los riesgos éticos y de seguridad y estudia medidas para fomentar la gobernanza dentro de la nueva agenda de la IA global.

8 Gran parte de la bibliografía consultada recoge la carta de Elon Musk, el Consejero Delegado de SpaceX y fundador de OpenAI, junto a 114 líderes tecnológicos advirtiendo a Naciones Unidas de que la IA permitirá que «los conflictos armados se eleven a un nivel de intensidad más grande que nunca» y a un ritmo de cambio desconocido para el hombre, por lo que se pedía evitar que su desarrollo incontrolado perjudicara a los seres humanos. «An Open Letter to the U.N. Convention on Certain Conventional Weapons, disponible en https://www.cse.unsw.edu.au/~tw/ciair//open.pdf. Fecha de la consulta 30.07.2018.

Por último, y dentro de una competición global, es inevitable la militarización de la IA porque afecta a todas las misiones y capacidades operativas de la Defensa. La aplicación de la IA alterará los balances militares actuales, aparecerán y desaparecerán categorías de armas y estructuras de fuerzas y su carácter ofensivo o defensivo, tal y como se explica en otros capítulos. El deseo de adquirir mediante la IA la superioridad militar sobre los adversarios aglutina a los sectores de defensa de las grandes potencias en su interés por beneficiarse –si no pueden liderar- la investigación y el desarrollo de la IA.

Los actores avanzados

En este apartado se incluyen los cuatro actores que más se han preocupado en liderar la IA, aunque por razones y medios diferentes. Todas, menos Israel, compiten por la jerarquía internacional, lo que añade a su interés por la IA un factor de competición por alcanzar la primacía. Todas, salvo la Federación Rusa, presentan un enfoque comprehensivo para sacar el máximo partido a la IA en todas las aplicaciones posibles. También todas están interesadas en las aplicaciones militares de la IA, sea por competir en la liga estratégica global, donde militan Estados Unidos, China y Rusia, o en la liga regional donde participa Israel.

Estados Unidos

Estados Unidos ha disfrutado de una clara superioridad en la investigación y el desarrollo de la IA hasta que sus competidores directos, China y Rusia, han comenzado a recortarla con estrategias e inversiones públicas masivas. A diferencia del pasado inmediato, cuando la I+D militar lideraba el esfuerzo inversor y tecnológico, ahora no son los inventarios militares los que tiran de la IA sino los modelos de negocio digitales y el consumo de servicios esenciales y digitales. Esta diferencia, la dificultad de liderar un esfuerzo nacional y la actitud reactiva de las últimas Administraciones de EE. UU. han dejado la IA en mano de su sector privado, lo que no ha favorecido su liderazgo frente a China o Rusia porque a estos les resulta más fácil movilizar la investigación y desarrollo de la IA en apoyo de sus intereses nacionales[9].

9 Incluso dentro del sector privado, EE. UU. comienza a perder su posición hegemónica y, por ejemplo, los investigadores chinos presentaron más comunicaciones a las Conferencias Internacionales Conjuntas sobre IA (IJCAI) de 2017 (37%) frente a la tercera posición de los estadounidenses (18%).

La convergencia del aprendizaje de las máquinas, con la disponibilidad de grandes bases de datos y con la multiplicación de la capacidad de procesamiento, confirmó la madurez de la IA. Hasta 2015, el Gobierno de EE. UU. había invertido más de 1.100 millones de dólares en I+D de tecnologías asociadas con la IA no clasificadas, muy por debajo de los 20-30.000 millones que invirtieron las compañías tecnológicas estadounidenses durante 2016 (el Gobierno dedicó ese año 600 millones) y de los 126.000 que invertirán hasta 2025[10]. Solo al ver que esas tecnologías comenzaban a estar maduras se creó en junio de 2016 un grupo interministerial para evaluar su impacto en el que participaron expertos privados de las distintas facetas de la IA[11]. Su finalidad no era definir las agendas de investigación de los diferentes departamentos del Gobierno sino identificar el desfase entre sus necesidades de investigación y desarrollo en IA y las inversiones del Gobierno para satisfacerlas. Sus conclusiones cubren el espectro de preocupaciones descrito en el apartado anterior: la IA era un factor de transformación económico y social, el Gobierno debería intervenir para maximizar sus oportunidades y reducir sus riesgos y aplicarla a toda la gama de servicios públicos que presta.

En junio de 2016, el Subcomité sobre *Networking Information Technology Research and Development* hizo público su Plan Estratégico de investigación y desarrollo de la IA[12]. En él, el Consejo de Economía Nacional reconoció la importancia de la IA para la prestación y calidad de los servicios públicos, sus efectos sobre la economía, el empleo o la educación, entre otros, así como la necesidad de regular su desarrollo e implantación. Sin embargo, sus recomendaciones no se enfocaron desde el punto de vista de la seguridad nacional, tal y como ya estaban haciendo China o Rusia.

En octubre de 2016, la Casa Blanca presentó su Plan para la investigación y desarrollo de IA, al que siguió el de su impacto sobre la economía[13], que fueron marginados por la nueva Administración, con lo que la iniciativa quedó en manos de las compañías

10 McKinsey Global Institute, «Artificial Intelligence, The Next Digital Frontier?», junio 2017, pp. 4-6 y Govini, «Department of Defense Artificial Intelligence, Big Data, and Cloud Taxonomy», diciembre 3, 2017, p. 9.

11 Su evaluación se recoge en el informe de la Office of Science and Technology Policy (OSTP) de la Casa Blanca: «Preparing for the Future of Artificial Intelligence», disponible en https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf. Fecha de la consulta 30.07.2018.

12 National Security and Technology Council, «National Artificial Intelligence Research and Development Strategic Plan», disponible en https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf. Consultado el 30.07.2018.

13 Casa Blanca, «Preparing for the future of Artificial Intelligence», National Science and Technology Council, octubre de 2016 y «Artificial Intelligence, Automation, and the Economy» de diciembre de 2016, consultado el 30.07.2018 y disponible en https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf, https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Artificial-Intelligence-Automation-Economy.PDF.

privadas sin una guía de orientación política. La Estrategia de Seguridad Nacional de 2017 confirmó la necesidad de alinear las iniciativas públicas y privadas para alcanzar el objetivo estratégico de liderar la investigación, la tecnología, la invención y la innovación para preservar su ventaja comparativa, dentro de un enfoque amplio de la seguridad nacional que combina elementos tradicionales de la seguridad con otros más relacionados con la economía[14]. Por último, la Estrategia de Defensa Nacional de 2018 recoge la IA entre el conjunto de tecnologías que están cambiando el carácter de la guerra junto con los metadatos, la computación avanzada, la robótica o la energía dirigida, entre otras[15]. Lo significativo de esta estrategia es que subraya la competencia con China y Rusia, a los que considera como los rivales y competidores estratégicos más importantes (de hecho, la Estrategia de Seguridad Nacional consideró una prioridad la protección de la propiedad industrial asociada a la innovación tecnológica).

La Administración Trump ha continuado el desarrollo de la IA en el sector de Defensa de la Administración Obama. La mayor parte de la financiación pública ha ido a sus agencias de investigación, salvo una cuarta parte que se ha destinado al resto del ecosistema privado[16]. Su Secretario de Defensa, Chuck Hagel, anunció el 15 de noviembre de 2014 un nuevo plan para 'preservar la superioridad militar estadounidense durante el Siglo XXI'. Su Defence Innovation Initiative, más conocida como la 'Third Offset Strategy', dio carta de credibilidad a la apuesta de la defensa estadounidense por las tres tecnologías más disruptivas: la IA, los metadatos y la nube[17]. Ya con la nueva Administración, y en un estudio de 2017 para la U.S. Intelligence Advanced Research Projects Activity (IARPA), Allen y Chan advertían de que la IA tenía ya el suficiente potencial como para transformar – o mejor revolucionar- la seguridad nacional en áreas como la ciberdefensa, los misiles guiados, la imaginería de satélites o las armas nucleares[18].

El Departamento de Defensa ha sido un valedor de las investigaciones en IA y de sus aplicaciones militares, muchas de las cuales -y como se ha indicado en otros capítulos- han proporcionado una valiosa contribución a las operaciones militares. En el proceso de adaptación, el Departamento ha tenido que modificar su proceso de adquisiciones y su relación con el sector privado donde se investiga y desarrolla la IA para tratar de

14 Casa Blanca, «National Security Strategy», diciembre 2017, p. 20.

15 Departamento de Defensa, «National Defence Strategy», sumario no clasificado, p.3.

16 BOULANIN, Vincent y VERBRUGGEN, Maaike, «Mapping the development of autonomy in weapon systems», SIPRI, noviembre 2017, p. 95.

17 Memorándum sobre «The Defence Innovation Initiative», consultado el 30.07.2018 y disponible en http://archive.defense.gov/pubs/osd013411-14.pdf.

18 ALLEN, Greg Allen y CHAN, Taniel, «Artificial Intelligence and National Security», Belfer Center for Science and International Affairs, Harvard Kennedy School, 2017.

aplicarla a las operaciones militares[19]. Para ello ha creado un modelo de interacción en el que los investigadores civiles y militares trabajan junto a los usuarios finales militares y utilizan fondos del Departamento para agilizar la trasferencia tecnológica disponible en las estanterías comerciales a los inventarios militares.

El proceso presenta dificultades culturales de adaptación porque los militares están acostumbrados a combatir de una forma que puede cambiar sustancialmente con la aplicación de la IA. En particular, existe una resistencia a prescindir de la participación de los profesionales en las decisiones de empleo, aun cuando hay pocas dudas sobre la capacidad de la IA para reemplazarla.

Pero sobre todo, el Departamento de Defensa no puede asumir en solitario el desarrollo tecnológico de la IA, tal y como han reconocido el Subsecretario de Defensa, Robert Work, en noviembre de 2017, y el Subcomité sobre Amenazas Emergentes de las Fuerzas Armadas del Congreso en enero de 2018, haciéndose eco de la necesidad de que la Administración retome el liderazgo de la investigación y desarrollo de la IA.

En el mismo sentido, el Council on Foreign Relations, advirtió de que la IA era crítica para la seguridad nacional y la competitividad de la economía de EE.UU.[20]. No obstante, y tal y como señala el Center for Strategic and International Studies (CSIS) de Washington D.C., EE. UU. no dispone de una estrategia de IA que le asegure la protección de su superioridad estratégica y económica. Por eso, en su informe de marzo de 2018, recomienda a la Administración emular a los países con los que compite elaborando una estrategia nacional pública y privada que contemple la necesidad de invertir en aquellos sectores a largo plazo donde la iniciativa privada no tenga interés, en formar el talento nacional necesario para aprovechar sus oportunidades, en prevenir el impacto negativo de las disrupciones y en concertarse con terceros para favorecer una regulación internacional de la IA[21].El Informe resalta la necesidad de que el Departamento de Defensa se asegure de que el desarrollo de la IA se incorpore al desarrollo de sus capacidades y que colabore con el sector privado en la investigación y desarrollo. También destaca que limitarse en su desarrollo por criterios éticos y morales que no tienen sus competidores daría una ventaja militar decisiva a China y Rusia. En cualquier caso, parece difícil que la Administración Trump esté interesada en restringir cualquier ventaja nacional en foros multilaterales, por lo que es esperable que continúe su desarrollo, salvo que el Congreso controle la gobernanza de la IA[22].

19 Para un análisis de las reformas en el proceso de adquisiciones, ver el Informe R45068 de SCHWARTZ Moshe y PETERS, Heidi M. sobre «Acquisition Reform in the FY2016-FY2018», National Defense Authorization Acts, Congressional Research Service.

20 «Machines, Skills and US Leadership», Independent Task Force Report 76, p. 53.

21 CARTER, William; KINNUCAN, Emma y ELLIOT, Josh, «A National Machine Intelligence Strategy for the United States», CSIS, Washington, marzo 2018.

22 Además de proponer leyes como la «Future of Artificial Intelligence Act» para supervisar el

Hasta ahora, las iniciativas de investigación y el desarrollo de la IA corresponden a la mencionada IARPA, a la Defense Advanced Research Projects Agency (DARPA) y a la Oficina para el secretario adjunto de Investigación e Ingeniería (ASD/RE) que está elaborando una Estrategia de Inteligencia artificial del Departamento que se espera publicar durante 2018[23]. Las recomendaciones para racionalizar las inversiones y maximizar la trasferencia de tecnología IA comercial al Departamento, varían desde la centralización en el Departamento de Defensa hasta la centralización en un Comité Federal Consultivo para el desarrollo e implementación de la IA.

China

China tiene una larga tradición de ayudas públicas a las empresas nacionales para favorecer el desarrollo de tecnologías avanzadas[24]. En julio de 2017, el Gobierno presentó su Plan para el Desarrollo de la Siguiente Generación de Inteligencia artificial (Plan IA)[25]. En él, China considera la IA como una tecnología estratégica que se ha convertido en un objeto de competición internacional entre las grandes potencias para reforzar su competitividad y seguridad nacional. Para participar -y ganar- en esa competición a partir de 2030, China se propone invertir alrededor de 150.000 millones de dólares y ha elaborado estrategias y planes de acción, especialmente para la formación de talento en IA. Las compañías tecnológicas chinas ya compiten con las estadounidenses (por ejemplo, Baidu se anticipó a Microsoft en el reconocimiento facial) y pueden trasferir esa superioridad tecnológica a las fuerzas armadas sin tantas restricciones como los EE. UU.

impacto de la IA sobre la competitividad o movilizar activistas como hace el Caucus de IA del Congreso (https://artificialintelligencecaucus-delaney.house.gov/), también podrían oponerse los empleados de las compañías, como han hecho los de Google contra el Proyecto Maven del Departamento de Defensa. «The Business of War»: Google Employees Protest work for the Pentagon, New York Times, 4 abril 2018.

23 Dentro del Departamento de Defensa, se lanzó en abril de 2017 el Algorithmic Warfare Cross-Functional Team, más conocido como Proyecto Maven, para evaluar la aplicación de la IA a los sistemas de armas.

24 BRADSHER, Keith y MOZUR, Paul, «China's Plan to Build Its Own High-Tech Industries Worries Western Businesses», New York Times, 7 marzo 2017. HE, Yujia, «How China is preparing for an AI-powered Future», *Wilson Centre Briefs*, junio 2017.

25 Consejo de Estado Chino, «A Next Generation Artificial Intelligence Development Plan,», traducción consultada el 30.07.2018 y disponible en https://www.newamerica.org/cybersecurity-initiative/blog/chinas-plan-lead-ai-purpose-prospects-and-problems/. FISCHER, Sophie-Charlotte, «Artificial Intelligence: China's High-Tech Ambitions», CSD Analysis 220, febrero 2018.

El Plan reconoce, como EE. UU., que el desarrollo de la IA comporta riesgos disruptivos para el empleo, la estabilidad social y la gobernanza internacional por lo que parte de las medidas se orientan a prevenir tales riesgos. También reconoce que parten en situación de inferioridad respecto a otros competidores en los campos de ciencia básica, algoritmos, infraestructuras y talento. Para recuperar la desventaja se han establecido hitos para los años 2020, 2025 y 2030[26]. El Plan comparte la visión transversal de la IA a todas las esferas del poder nacional, sin que se detenga especialmente en el de la seguridad nacional. En particular, pretenden alcanzar el liderazgo de la IA para poder imponer sus estándares en el consiguiente proceso de globalización, alojando en su nube (*cloud*) los servicios que ofrecen compañías como Tencent y Alibaba, al igual que las compañías como Google o Facebook impusieron sus estándares en Internet.

China dispone de fondos para realizar inversiones estratégicas en las compañías comerciales de los países con los que compite, una ventaja que estos no tienen y en las que ha invertido 1.300 millones de dólares entre 2010 y 2017 en Estados Unidos[27]. Lo anterior, unido al robo de propiedad intelectual que se atribuye a servicios de inteligencia chinos, está alertando a competidores como Estados Unidos y la Unión Europea que comienzan a tomar medidas para limitar las inversiones estratégicas chinas en empresas tecnológicas, algo en lo que no existe reciprocidad debido al proteccionismo chino respecto a las empresas nacionales[28].

Otro factor de ventaja comparativa de la IA china es el interés chino por el control interno de sus poblaciones, lo que explica el gran desarrollo de aplicaciones de la IA al reconocimiento facial o a los análisis de comportamiento[29]. Eso explica el acceso y procesado a datos personales de los ciudadanos y los millones de cámaras de vigilancia

26 Entre otros, para 2020 se aspira a disponer de un valor del núcleo industrial de la IA de unos 20 billones de euros y de 135 en las industrias asociadas. Esos objetivos aumentarán en 2025 a 55 y 675 billones, respectivamente, y en 2030 a 135 y 1350 billones, respectivamente.

27 Según el Informe del Congressional Research Service citado en la nota 19, se estima que las inversiones chinas en empresas de IA de EE. UU. han aumentado desde los 1,5 millones de dólares en 2010 por una empresa hasta los 514 millones en 25 empresas en 2017, p. 20.

28 Las restricciones de la Secretaría de Estado de Comercio afectan a compañías chinas como Baidu Tencent y Sensetime o a universidades como la de Beihang que colaboran con las fuerzas armadas en el desarrollo de la IA china. Para las europeas, ver el informe de Skadden, «Expanding the Scope of National Security-Focused Foreing Investment reviews in Europe», 7 febrero 2018, aunque países con inversiones chinas como Portugal, Hungría y Malta se oponen al control de las inversiones extranjeras.

29 Eso explica el éxito de empresas como Baidu, Tencent, and Sensetime o startsup como Megvii o Yitu Tech, ganadora del concurso de reconocimiento facial organizado en EE. UU. por la Intelligence Advanced Research Projects Activity (IARPA) y la Oficina del Director de Inteligencia Nacional, gracias a disponer de acceso libre a las bases de datos del Ministerio de Salud Pública sobre los ciudadanos chinos o de los usuarios de Internet (700 millones).

para desarrollar programas de IA aplicadas al control social, con el respaldo legal de las normas aprobadas por el Congreso Nacional del Pueblo en 2016.

Su aplicación militar posterior es simétrica a la que pretende la *Third Offset Strategy* para evitar verse desplazado por la superioridad militar estadounidense. Sin embargo, la eficacia de la aplicación militar de la IA depende mucho de la experiencia de combate y de la adaptación de las doctrinas, procedimiento y estilo de mando militar, algo muy distinto según las distintas potencias y que condiciona, pero no predetermina, el éxito o el fracaso de la IA. También han replicado un sistema de trasferencias similar al que se ensaya en EE. UU., creando en 2017 una Comisión para desarrollar la integración civil-militar en las fases de investigación y desarrollo de las capacidades militares de IA. Las fuerzas armadas chinas pretenden paliar el salto tecnológico al que se encaminan las estadounidenses con la *Third Offset Strategy* mediante la aplicación de la IA al campo de batalla que va más allá de su digitalización y conectividad.

La Federación Rusa

Como se ha mencionado, fue el presidente Vladimir Putín quien movilizó a la sociedad rusa para ganar el futuro, el mismo que espera a los estudiantes que le rodeaban el 1 de septiembre de 2017 cuando anunció que Rusia se incorporaba a la carrera de la IA. En ese momento, la IA no estaba entre las prioridades de modernización de las capacidades militares rusas diseñadas a partir de 2008[30] y el valor añadido al sector privado de la IA estaba alrededor de 12 millones de dólares. Empezando tan tarde, y desde tan atrás, es difícil que puedan disputar el liderazgo global de la IA a China y EE. UU., incluso si se llevan a cabo las inversiones privadas previstas de unos 500 millones de dólares hasta 2020.

Los fondos rusos están incrementando sus inversiones en IA: 18 millones de dólares en 2016 y 37 en 2017, para satisfacer la demanda de la banca y otras corporaciones. También el Gobierno ha invertido más de 350 millones de dólares entre 2007 y 2016, distribuidos en análisis de datos (33%), algoritmos (16,5%) o reconocimiento (13,9) para sus industrias nacionales[31]. No obstante, el ecosistema ruso de IA se enfrenta a problemas estructurales de desconfianza y burocracia que limitan sus posibilidades de crecimiento local y global.

30 Como muestra de este retraso, la Agencia de Inteligencia de la Defensa de EE. UU. no menciona ninguna aplicación o programa de IA entre las capacidades militares rusas en su evaluación del «Russia Military Power 2017».

31 «Artificial Intelligence in Russia», Lanscape Overview 2017, consultado el 30.07.2018 y disponible en http://sci-guide.com/landscape.pdf.

A falta de expectativas de superioridad tecnológica y económica, es previsible que la IA rusa se concentre en la esfera militar. Y no solo por avanzar en sus capacidades estratégicas sino porque la Federación Rusa sostiene el controvertido criterio de que invertir a corto plazo en la investigación militar acaba teniendo repercusiones sobre la investigación civil a mayor plazo. No obstante, al igual que China, Rusia pretende emular el modelo americano: estrechar la relación entre las fuerzas armadas y la comunidad tecnológica e industrial para acelerar la trasferencia de tecnología IA a los equipos militares más avanzados. Sin embargo, los expertos occidentales en capacidades militares rusas como Samuel Bendett, dudan de que pueda llevarse a cabo de forma rápida y con la ambición que señalan las declaraciones oficiales porque a la integración pretendida le falta madurez y tamaño[32].

El Ministerio de Defensa cuenta con una Dirección General para la Investigación Científica y las Tecnologías Avanzadas, encargada de dinamizar esa colaboración público-privada. En 2012 se creó la Fundación para Estudios Avanzados, una agencia similar a la DARPA de EE. UU., para estimular la aplicación de la investigación y desarrollo a la seguridad y la defensa. Para desarrollar sus programas de IA, la Fundación recurre a los recursos oficiales disponibles: el Instituto de Ciencia y Tecnología de Skolkovo, la Academia de las Ciencias y las universidades, pero no dispone de la infraestructura y los presupuestos que le permitan acelerar la trasferencia tecnológica desde los laboratorios y *startups* de IA a las capacidades militares[33].

Al igual que China y EE. UU., las fuerzas armadas rusas pretenden aprovechar las oportunidades de la IA en todas las capacidades y equipos que disponen, especialmente aquellas que tienen que ver con la guerra hibrida. Las limitadas precisiones que se conocen de fuentes como el general Valery Gerasimov están orientadas a mejorar el tiempo de respuesta en los procesos de decisiones siguiendo el enfoque de los proyectos de EE. UU.[34]. Sin embargo, las restricciones presupuestarias al presupuesto de defensa ponen en peligro el ritmo y grado de trasferencias que se quieren obtener, por lo que los fondos disponibles para la IA se orientarán a donde puedan obtener rendimientos inmediatos.

Por eso, es probable que Rusia pretenda liderar alguno de los campos de aplicación militar como la robótica, los equipos no tripulados o la ciberdefensa, donde la

32 BEMETT, Samuel, «In AI, Russia Is Hustling To Catch Up», Defence One, 4 abril 2018.

33 El Ministro de Defensa ha anunciado la creación de un complejo (Era) militar de innovación en la ciudad de Anapa, cerca del Mar Negro, donde se pretende concentrar la investigación pública y privada en IA, robótica y computación avanzada. DOUGHERTY, Jill y JAY, Molly, «Russia tries to get smart about artificial intelligence», Wilson Quartely, primavera 2018, consultado el 30.07.2018 y disponible en https://wilsonquarterly.com/quarterly/living-with-artificial-intelligence/russia-tries-to-get-smart-about-artificial-intelligence/.

34 Patrick Tucker, «Russian Military Chief Lays Out the Kremlim's High´-Tech War Plans», Defence One, 28 marzo 2018.

trasferencia sea viable, o en campos de la guerra hibrida como la ciberseguridad, la desinformación y la influencia.

Israel

Israel es un caso particular en relación con la IA porque, no siendo una potencia como los tres países mencionados anteriormente, ha desarrollado extraordinariamente su IA tanto para mejorar su economía como para lograr la supremacía regional, ya que se encuentra en una situación de riesgo existencial para su supervivencia y soberanía. Para ello cuenta con un avanzado ecosistema de empresas innovadoras, centros tecnológicos y universidades especializadas que nutren y se aprovechan de la colaboración público-privada[35]. Contra la intuición de que la IA se desarrolla gracias a la tracción de las Fuerzas de Defensa de Israel, son otros sectores como la automoción los que están liderando la investigación y desarrollo de la IA[36].

No obstante, su complicada situación estratégica y sus limitados recursos humanos le han llevado a desarrollar los recursos tecnológicos como la IA al máximo nivel posible. De ahí que lidere la aplicación de la IA a algunos campos como los vehículos terrestres y aéreos no tripulados, que ahora patrullan sus fronteras desarmados en tareas de vigilancia, y que podrían dar paso a sistemas de armas letales autónomas, al igual que ya viene haciendo su sistema de defensa contra cohetes y misiles Iron Dome. Por razones de necesidad y espacio, la colaboración público-privada en la aplicación de la IA es muy estrecha y el Ministerio de Defensa financia proyectos de investigación y desarrollo para equipar a las Fuerzas de Defensa de Israel con tecnologías de superioridad. Las más conocidas tienen que ver con los procesos automatizados de decisión, los sistemas no tripulados o los simuladores complejos.

Los actores emergentes

A continuación, se analiza un grupo de actores que tienen voluntad de ocupar un espacio importante en la jerarquía internacional, pero que no aspiran a liderar la

35 «Tel Aviv University's Smart Artificial Intelligence Program», Jerusalem Post, 1 mayo 2018. «Israeli Military Demonstrates Armed Unmanned Vehicles», Defence World.Net, 28 mayo 2018.

36 Israel Innovation Authority, «Innovation in Israel 2017», pp. 42-45, disponible en https://innovationisrael.org.il/sites/default/files/Innovation%20in%20Israel%202017_English.pdf .Consultado el 30.07.2018.

carrera por el liderazgo de la IA, pero que tratan de sacarle el máximo partido posible en beneficio de su autonomía estratégica y de su prosperidad. Se incluyen Francia, el Reino Unido y Alemania, como potencias europeas, y la Unión Europea (UE) por su capacidad de liderar y financiar la investigación y desarrollo de la IA europea. No son los únicos países implicados en el desarrollo de la IA, pero son los pioneros y van a influir en el desarrollo europeo de la IA.

Francia

Francia, como gran potencia, se ha interesado por la IA, aunque en fechas recientes. En una primera aproximación, el Gobierno adoptó un enfoque de seguridad nacional por la trascendencia económica y social de su desarrollo y la necesidad de preservar la autonomía frente a terceros[37]. Partiendo del estado de la IA, sus tecnologías y ecosistemas, el Informe «France IA» evaluó el impacto sobre la soberanía, sobre los distintos sectores y planteó recomendaciones de inversión (1.070 millones de euros) y de actuación.

El presidente Emmanuel Macron retomó esas recomendaciones y presentó su estrategia de inteligencia artificial en marzo de 2018[38]. A diferencia de las de otras grandes potencias analizadas anteriormente, la estrategia francesa tiene un enfoque comprehensivo que pretende abordar todas sus dimensiones e implicar a todos sus protagonistas, especialmente a la Unión Europea. Es un enfoque realista porque parte del reconocimiento de su desventaja respecto a las grandes potencias y solo trata de mitigar el desfase y ampliar el margen europeo de autonomía respecto a la IA. Como todas las estrategias francesas, se establece un presupuesto para desarrollarlas de aproximadamente 1.500 millones de euros anuales hasta 2022, de forma que el Estado predique con el ejemplo que se predica al resto de los actores civiles[39].

Es una estrategia que se incorpora a la carrera cuando ya se conocen algunas desviaciones éticas de las anteriores, por lo que tiene un fuerte componente de reorientación individual, social y ética, factores muy importantes en el entorno europeo donde se van a aplicar. Su aplicación preferente será a las políticas públicas

37 Secretarías de Estado de Digitalización y de Educación e Investigación: «Rapport de Synthése: France Intelligence Artificialle», enero 2017, pp. 249-259.

38 Presentada el 29 de marzo, tiene como origen el mandato a una Comisión dirigida por Cédric Villani, «For a meaningful artificial intelligence towards a French and European strategy», 8 marzo 2018, disponible en https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf. Consultado el 30.07.2018.

39 Parte de esos fondos podrían proceder de la UE donde la Comisión tiene previsto movilizar 200 millones anuales de euros para la IA.

como la de sanidad, transporte, medio ambiente y defensa, donde el Estado podría utilizar sus bases de datos para mejorar la eficacia de las prestaciones y modernizar -si no transformar- su organización. La estrategia trata de articular un ecosistema potente de investigación y desarrollo de la IA al servicio de la economía que, paralelamente, prevenga efectos no deseados en los campos laborales y medioambientales.

La estrategia pretende que la IA permee desde las grandes empresas al conjunto del tejido productivo para mejorar su competitividad. Para mejorar la eficacia de las inversiones, se centra en el aprovechamiento económico de las inversiones, dando primacía a los centros tecnológicos para evitar el desfase entre investigación básica de las universidades y la aplicada de las industrias. El enfoque ético no responde solo a convicciones morales sino a la necesidad de anticiparse a problemas prácticos que plantea la sustitución de las decisiones basadas en seres humanos por algoritmos, cuya trasparencia y predictibilidad se encuentran ahora en cuestión. Para solucionarlos se propone crear mecanismos de vigilancia social sobre los procesos tecnológicos que ahora no disponen de ellos y la regulación de los mismos. Finalmente, y desde un enfoque de oportunidades, se trata de aprovechar la IA para reducir la desigualdad existente, tanto en materia de género como en la de exclusión digital.

En relación con la Defensa, fue el ministro Jean-Yves Le Drian quien propuso en febrero de 2017 la necesidad de no quedarse descolgados respecto a sus aliados y competidores[40]. A diferencia de China, Rusia o Estados Unidos, y a semejanza de los países europeos, la estrategia francesa no está expresamente vinculada a los campos de defensa y seguridad, aunque inevitablemente está presente en la investigación y desarrollo de capacidades militares[41].

Reino Unido

El Reino Unido también se ha tomado su tiempo para analizar las implicaciones de la IA. En octubre de 2016, el Comité de Ciencia y Tecnología de la Cámara de los Comunes publicó un informe sobre IA y robótica[42]. Su estructura de análisis fue similar a la seguida por la valoración francesa analizada anteriormente, primando los aspectos económicos y sociales, los éticos y jurídicos y los de investigación y financiación.

40 «L'intelligence artificielle: un enjeu de souveraineté nationale» en Intelligence artificielle: des libertés individuelles à la sécurité nationale, Eurogrup Consulting, pp. 11-24.

41 La Dirección General de Armamento del Ministerio de Defensa francés va a invertir 10 millones anuales de euros en un estudio (Man-Machine Teaming, MMT) para probar e integrar IA en sus aviones de combate y drones.

42 House of Lords, «Robotics and Artificial Intelligence», 13 septiembre 2016.

Entre sus recomendaciones, la más relevante fue la de solicitar al Gobierno un mayor compromiso en el liderazgo de la IA, elaborando la estrategia que no existía y creando una comisión permanente sobre IA en la sede del Instituto Alan Turing para debatir todos esos aspectos y seguir la evolución de su desarrollo.

En noviembre de 2016, la Oficina del Gobierno para la Ciencia publicó un estudio[43] en el que se enumeraban las aplicaciones e implicaciones de la IA. Después, en marzo de 2017, el Gobierno publicó su Estrategia Digital, actualizando la de 2012, pero incluyendo en ella a la IA y dotándola de un presupuesto de 17 millones de libras. Según los cálculos disponibles, se espera que la IA aporte unos 800 billones de dólares a la economía del Reino Unido en 2035, incrementando su producto interno bruto del 2.5% al 3.9% si se aprovechan todas las potencialidades británicas[44]. Entre sus fortalezas, se encuentra el crecimiento del valor aportado por las industrias digitales a la economía británica: más de 170 billones de libras y creciendo a un ritmo del 22% anual, junto con una inversión de 6,8 billones en 2016 (50% más que cualquier otra economía europea). Entre sus debilidades, la disponibilidad y retención del talento, para lo que se proponía reestructurar el sistema educativo para implantar másteres, doctorados, líneas de crédito para el reciclaje y becas para incrementar la masa crítica de conocimiento en IA. Como fruto de los documentos anteriores, a los que hay que añadir el Libro Blanco sobre la Estrategia Industrial de noviembre de 2017, se logró un compromiso entre la industria y el gobierno recogido en el Artificial Intelligence Sector Deal[45].

En el campo de la Defensa, las iniciativas del Reino Unido de IA son recientes y limitadas. No cuentan con una estrategia particular y los fondos aplicables como la Iniciativa de Innovación (7,7 millones de dólares en 2017) se aplican a todas las tecnologías innovadoras y no solo a la IA[46]. Más trascendencia puede tener la creación de un laboratorio dedicado a la IA dentro del complejo del Laboratorio de Ciencia y Tecnología de la Defensa (DSTL en sus siglas inglesas) en colaboración con EE. UU.[47].

43 Government Office for Science, «Artificial Intelligence opportunities and implications for the future of decision making».

44 HALL, Dame Wendy y PESENT, Jerome, «Growing the Artificial Intelligence in the UK», Consultado el 30.07.2018 y disponible en https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/652097/Growing_the_artificial_intelligence_industry_in_the_UK.pdf.

45 Departamentos de Industria y Digital, «Artificial Intelligence Sector Deal», 26 abril 2018.

46 Military Balance 2018, «Big data, artificial intelligence and defence», IISS, pp. 10-13.

47 Ministerio de Defensa, «Flag Ship AI Lab announced as Defence Secretary hosts first meeting between British and American defence innovators», 22 mayo 2018, https://www.gov.uk/government/news/flagship-ai-lab-announced-as-defence-secretary-hosts-first-meet-between-british-and-american-defence-innovators..

Alemania

Alemania dispone desde 1998 de un centro de investigación público-privado en IA en Saarbuken y en 2016 abrió un complejo en Baden Wurtemberg aplicado a la automoción. Sin embargo, no dispone todavía de una estrategia específica, aunque la está desarrollando para reducir su desventaja respecto a otros competidores y apoyará el desarrollo de ecosistemas de IA básica, como el Max Planck Institute, o aplicada como el Fraunhofer[48]. Mientras, la IA se está introduciendo en algunos departamentos federales, como el Departamento de Prevención de Crisis[49], y podría implantarse en otros como Defensa e Interior si prospera la iniciativa de ambos Ministerios de crear una agencia de investigación, tipo DARPA, que afronte la investigación y el desarrollo de tecnologías disruptivas para la seguridad y la defensa como la IA[50]. Si todas estas iniciativas se llevan a cabo, Alemania ocupará un lugar entre las potencias emergentes en IA.

La Unión Europea

No siendo una potencia militar, pero sí una económica, la UE ha decidido participar en la carrera por la IA. La Comisión en su revisión de la Estrategia del Mercado Único Digital de mayo de 2017 había resaltado la necesidad ocupar posiciones prominentes en el campo de las tecnologías, aplicaciones y plataformas de la IA. Posteriormente, el Consejo Europeo de octubre de 2017 pidió a la Comisión que definiera una aproximación a la IA que compaginara los beneficios económicos y tecnológicos con la preocupación por los estándares éticos, los derechos digitales y la protección de los datos.

En su Comunicación de abril de 2018[51], la Comisión tomaba nota de la importancia de la IA para la competitividad y productividad de la economía europea y apostaba por

48 HARHOFF, Dietman y otros, «Outline for a German Strategy for AI», Stiftung Neue Verantwortung (SNV), julio 2018.

49 DICKOW, Marcel y JACOB, Daniel, «The Global Debate on the Future of the AI», SWP Comments nº 23, mayo 2018, p. 6. SCOTT, Ben, HEUMANN, Stefan y LORENZENE, Phillipe, «Artificial Intelligence and Foreign Policy, SNV, 2018.

50 SPRINGER, Sebastian, «Germany wants its own version of DARPA, and within the year», disponible en https://www.defensenews.com/global/europe/2018/07/18/germany-wants-its-own-version-of-darpa-and-within-the-year/. Consultado el 30.07.2018.

51 Comisión Europea, Comunicación (2018) 237 final de 25 de abril sobre inteligencia artificial.

una integración de las estrategias y políticas individuales[52]. El acuerdo fue adoptado con posterioridad -o respondiendo- a la Estrategia de Francia y al acuerdo franco-alemán de cooperación. La Comunicación apuesta por dinamizar la capacidad tecnológica e industrial, fomentar la adaptación económica y social a los cambios y asegurar los valores éticos y jurídicos. Se espera que el Consejo Europeo de Diciembre apruebe el Plan sobre Inteligencia artificial a finales de 2018.

El valor de la industria asociada a la IA es, aproximadamente, de 2.500 a 3.300 millones de euros comparados con los 6.500-9.800 en Asia o los 12.200-18.800 de Estados Unidos[53]. Aproximadamente, los programas de investigación tecnológica asociados al programa Horizonte 2020 durante el período 2014-2017 han invertido 1.100 millones de euros en IA y los programas de investigación y desarrollo públicos y privados recibieron entre 4.000 y 5000 millones de euros en 2017.

Partiendo de esta constatación del retraso, el objetivo europeo es el de preservar e incrementar sus capacidades. La UE, por ejemplo, produce más de la cuarta parte de los robots utilizados en la industria, cuyo futuro depende de su adaptación a la IA. El 25% de sus grandes empresas y el 10% de sus PYME utilizan ya análisis de bases de datos, pero la mayor parte de los trabajadores y empresas no están todavía suficientemente digitalizados.

Para alcanzar estos objetivos, se prevé invertir al menos 20.000 millones de euros hasta 2020 y superar esa cifra durante la década siguiente. Solo el programa Horizon 2020 prevé subir su inversión hasta 500 millones anuales hasta 2020 y los acuerdos públicos-privados añadirán otros 2.500 millones adicionales hasta la misma fecha. Sobre esta base presupuestaria común, los Estados miembros deberían completar la suma de 7.000 millones anuales para completar en 2020 el objetivo de 20.000 millones de euros.

Más allá de esa fecha, las inversiones dependen de lo que se apruebe en próximo programa marco (Horizonte Europa) en el nuevo Marco Financiero Plurianual 2021-2027.

52 A 10 de abril de 2018, se habían comprometido junto con Noruega a trabajar juntos en IA: Alemania, Austria, Bélgica, Bulgaria, República Checa, Dinamarca, Eslovenia, España, Estonia, Finlandia, Francia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Holanda, Polonia, Portugal, Suecia y Reino Unido.

53 European Political Strategy Center, «The age of artificial intelligence», EPSC Strategic Notes 29, 27 marzo 2018, p. 4.

Conclusiones

La IA forma ya parte de los instrumentos de poder nacional y sus efectos sobre las relaciones internacionales se irán multiplicando a medida que sus resultados progresen. Los grandes Estados y compañías han tenido que articular estrategias, políticas, inversiones y ecosistemas específicos para no quedarse descolgados de la carrera global por ocupar posiciones de privilegio.

Los casos descritos corresponden a las iniciativas de los países pioneros y a los emergentes, cada uno con su visión y nivel de ambición particular, pero todos tomando posiciones para aprovechar las oportunidades y mitigar los riesgos a sus intereses nacionales. La visión y el liderazgo se traducen en estrategias y políticas de actuación, sin las cuales, los actores perderán cuotas de soberanía, seguridad nacional y poder en el sistema internacional.

La IA afecta a los procesos de decisiones de los gobiernos en todos los niveles, desde el estratégico, en las que tienen que ver con la política, la economía y el orden internacional, hasta en el doméstico, en las decisiones que tienen que ver con sus aplicaciones económicas y sociales. Lo mismo podría decirse, en otra escala, de las empresas e industrias que compiten en el mercado global. Por último, pero no menos importante, la IA afecta al bienestar, expectativas, derechos y libertades de los individuos y sociedades que conviven con la denominada Cuarta Revolución Industrial[54] en la que la inteligencia artificial no es el único factor, pero sí uno de los más disruptivos.

54 Félix Arteaga, «La Cuarta Revolución Industrial (4RI): un enfoque de seguridad nacional», DT 12/2018, 24 mayo 2018.

Conclusiones

José Manuel Roldán Tudela

«Nobody phrases it this way, but I think that artificial intelligence is almost a humanities discipline. It's really an attempt to understand human intelligence and human cognition».

Sebastian Thrun.

Nadie lo expresa de esta manera, pero creo que la inteligencia artificial es casi una disciplina de humanidades. Realmente es un intento de comprender la inteligencia y el conocimiento humanos.

Sebastian Thrun.

Conclusiones

El factor determinante para obtener una inteligencia que pudiera equipararse a la humana es la integración de diferentes agentes que proporcionen razonamiento, capacidad de planificación, aprendizaje e interpretación del entorno. El estudio de los procesos creativos en el ser humano puede proporcionar un agente suplementario proveedor de comportamiento humano para estos algoritmos.

El contexto tecnológico actual es fuertemente interdisciplinar. Con las tecnologías de IA existentes en el mercado es posible desarrollar muchas aplicaciones incidiendo en otros campos tecnológicos y viceversa. Con el fin de que la Defensa se beneficie plenamente de las posibilidades de la IA y datos masivos (*big data*), es necesario iniciar una migración a una infraestructura de datos de gran capacidad (en la nube), gestionada por tecnologías emergentes, que incluya el concepto de centralización de datos y escalabilidad del sistema.

Los exigentes requerimientos para los sistemas militares hacen que algunas tecnologías comerciales sean utilizables, pero requieren adaptaciones importantes. Para ello es necesario establecer un ecosistema de defensa y seguridad sobre oportunidades y desafíos en IA.

La incorporación de sistemas autónomos, robots e inteligencia artificial a las Fuerzas Armadas cambia las características de esta institución en aspectos esenciales como el papel que juega el soldado en el campo de batalla, la relación de los sistemas, dentro

del grupo y con los mandos, y la percepción de la población civil en general y las distintas facciones de la zona de operaciones militares. También el liderazgo militar y su propia concepción sufrirán modificaciones. Las características y las aptitudes para liderar seres humanos tendrán que adaptarse para ser ejercidas sobre equipos mixtos humano-máquina.

Por tanto, el factor más importante es el capital humano. Su formación humana y científica y su sentido crítico seguirán siendo fundamentales para forjar la voluntad de vencer que le permita imponerse al adversario. Será necesario aprender a combatir con y contra sistemas y dispositivos de IA y RI, lo que obligará a modificar las estructuras y los planes de enseñanza, instrucción y adiestramiento. Se deberá hacer uso masivo de la tecnología para incrementar al máximo la eficacia de la formación. La simulación jugará un importante papel y verá aumentada su eficacia con la aplicación de técnicas de IA y realidad virtual, así como tratamiento de datos masivos y computación en la nube.

Desde un punto de vista más general, debe extenderse la concienciación social sobre qué es y qué no es la IA y, así, evitar «el miedo social», mediante el conocimiento de los posibles beneficios y perjuicios de estas nuevas tecnologías.

El uso de la IA y RI está éticamente justificado en el principio del riesgo innecesario y el deber moral de evitar la exposición arriesgada al combatiente en un conflicto justo y legal. La utilización de sistemas autónomos no debe producir una disminución del rigor y la relevancia de los códigos morales y legales con los que la civilización occidental ha avanzado. La ética es del hombre, por lo que debe avanzar en paralelo con la ciencia, teniendo al ser humano como protagonista de sus progresos. Esto es imprescindible para que la persona y su dignidad inviolable se mantengan en todas las relaciones humanas, incluyendo las guerras y los enfrentamientos bélicos que incorporen tecnologías emergentes.

Una sociedad puede, por diversos motivos, no querer acelerar el uso de estas tecnologías. Sin embargo, los riesgos que con ello pretende evitar, pueden ser ampliamente sobrepasados por los que correrá al enfrentarse con otras sociedades que no hayan adoptado esa misma postura. Resulta necesario, por tanto, ser consciente de estos riesgos y aceptar las consecuencias.

No es fácil determinar con certeza los límites que deben establecerse para que la intervención de los algoritmos de IA en la toma de decisiones esté controlada. La clave está en conocer hasta qué punto las limitaciones de las personas en cuanto a su capacidad de captar y procesar datos, y el tiempo necesario para que el cerebro humano adopte una decisión y la ponga en obra, es compatible con las necesidades o restricciones temporales de la acción.

Es necesario que se mantenga un control humano significativo, lo que se traduce en la atribución de responsabilidad, en cualquier ocasión, a una persona, y que sus decisiones, y las consecuencias de estas, sean verificables. Es necesario avanzar

en el establecimiento de reglas, legales y éticas, que mantengan la primacía del ser humano en la decisión sobre el empleo de la fuerza letal, así como en la asunción de la responsabilidad última de su uso.

La discusión sobre autonomía de los sistemas de AI y RI se vería simplificada si se considerase un enfoque distinto del actual, en el que el grado de autonomía se asigna al dispositivo como un todo. Para acometer la cuestión del empleo de sistemas de armas letales autónomos (SALA), es preferible enfocar la autonomía de los sistemas desde un punto de vista funcional. De este modo, cada una de las funciones del dispositivo tendrá un grado de autonomía acorde con las necesidades de la misión a cumplir, de forma que en muy raras ocasiones todas las funciones serán autónomas.

Resulta necesario establecer unos conceptos de empleo que aseguren, en lo posible, que la aplicación militar de las tecnologías de IA y RI sea aceptable social y legalmente, tanto a nivel nacional como internacional. Esto no resulta sencillo, porque se trata de tecnologías complejas y avanzadas, de las que no se posee experiencia real. A pesar de ello, habrá que instaurar unos conceptos iniciales, que se irán refinando y completando con la experiencia.

Los conceptos de empleo de IA y RI deben considerar la necesidad de que estos sistemas estén siempre supervisados. La inteligencia artificial y humana son fundamentalmente diferentes, y las interfaces entre las dos deben ser diseñadas cuidadosamente, y revisadas constantemente. Las interfaces deben ser avanzadas y fiables, al tiempo que provistas de mecanismos de seguridad. También es preciso regular el entrenamiento de los dispositivos y su necesaria actualización. Finalmente, hay que determinar en qué ocasiones se puede permitir que los RI seleccionen y ataquen objetivos de forma autónoma, insistiendo en que nunca lo harán sobre personas.

Cada vez serán más frecuentes las acciones ejecutadas por sistemas de IA en el ciberespacio. El ritmo al que se desarrollarán estas acciones supera con creces las posibilidades de ejecución de seres humanos. Por lo tanto, sobre todo en acciones ofensivas, el grado de control humano sobre el inicio y las fases de la acción será un elemento crítico para evitar consecuencias no deseadas.

En los tres niveles, táctico, operacional y estratégico, la utilización de IA y RI proporcionará un aumento de capacidades militares que se distribuirá de forma no homogénea en distintas áreas. En los niveles táctico y operacional hay tipos de operaciones en los que el impacto que ocasionará el empleo de IA y RI será muy destacado por el efecto de multiplicador de fuerza que produce.

Sin embargo, a pesar de la gran capacidad que tienen las tecnologías de IA de adquirir, procesar y entregar ingentes volúmenes de datos, estas tecnologías son hoy, y seguirán siendo, vulnerables a las antiguas prácticas de denegación, decepción y engaño.

Es preciso acompasar la doctrina militar y las reglas de enfrentamiento a la introducción progresiva de IA y RI en operaciones militares. Al no disponer de datos empíricos, será preciso elaborar conceptos de forma provisional y contrastarlos en ejercicios, juegos de guerra y simuladores.

Resulta necesario introducir lo antes posible cambios en las técnicas y procedimientos de combate para adaptarse al uso de estas tecnologías. Tampoco puede demorarse el estudio y definición de nuevas tácticas de empleo, aunque, a falta de experiencia real en operaciones, será preciso recurrir a otros métodos para tener cuanto antes un marco conceptual.

En casi todos los sectores habrá cada vez más integración entre los seres humanos y las máquinas, tanto en las operaciones como en la toma de decisiones. Por tanto, un asunto de especial importancia es el del diseño de equipos mixtos humano-robot, para obtener el máximo rendimiento de sus capacidades complementarias.

La IA influye en las decisiones de los gobiernos en todos los niveles, desde el estratégico, en las que afectan a la política, la economía y el orden internacional, hasta en el doméstico, en decisiones relativas a sus aplicaciones económicas y sociales. Lo mismo podría decirse, en otra escala, de las corporaciones y empresas que compiten en el mercado global, y de otros actores no estatales. Por último, la IA afecta al bienestar, expectativas, derechos y libertades de los individuos y sociedades inmersos en la denominada Cuarta Revolución Industrial.

La IA forma ya parte de los instrumentos de poder nacional y sus efectos sobre las relaciones internacionales se irán multiplicando al compás de sus avances tecnológicos. Los grandes Estados y compañías han tenido que articular estrategias, políticas, inversiones y ecosistemas específicos para no quedarse descolgados en esta carrera tecnológica global. La visión y el liderazgo se traducen en estrategias y políticas de actuación, sin las que los actores perderán cuotas de soberanía, seguridad nacional y poder en el concierto internacional.

La IA y la RI cambiarán el carácter de la guerra, y los cambios introducidos por estas tecnologías pueden ser profundos. Sin embargo, la naturaleza de la guerra no cambiará sustancialmente. Los elementos de la trinidad clausewitziana se verán modificados individualmente, pero el conjunto se reconfigurará, manteniendo la tensión mutua y haciendo que la guerra gravite sobre ellos, sin cambios trascendentes en su esencia.

Para comprender cómo será la guerra futura, resulta necesario no equivocarse sobre su carácter y sobre la permanencia de su naturaleza. Es posible llegar a conclusiones equivocadas sobre el efecto de estas tecnologías y, en consecuencia, acabar definiendo la guerra como se desearía que fuera, y no como lo que, en verdad, es: un enfrentamiento humano, incierto y complejo que busca un fin político.

Si se mantiene el ritmo actual, el futuro de esta tecnología nos deparará pronto sorpresas, en uno u otro sentido.

Composición del grupo de trabajo

Presidente

José Manuel Roldán Tudela
General de División (Reserva) del Ejército de Tierra
Comisión de Expertos en Nuevas Tecnologías.
IEEE - CESEDEN

Coordinador

D. David Ramírez Morán
Analista del Instituto Español de Estudios Estratégicos (IEEE).

Vocales

José Javier Rainer Granados
Director del área de organización industrial y electrónica. Universidad Internacional de La Rioja (UNIR).

Luis Rodríguez Baena
Subdirector de calidad en la Escuela Superior de Ingeniería y Tecnología. Universidad Internacional de La Rioja (UNIR)

Gonzalo León Serrano
Delegado del Rector para partenariados de innovación. Universidad Politécnica de Madrid.

José Carlos de la Fuente Chacón
General de División (Reserva) del Ejército de Tierra. Comité de Expertos en Tecnología. IEEE - CESEDEN.

Juan A. Moliner González
General de División (Reserva) del E. A. Subdirector del Instituto Universitario Gutiérrez Mellado.

Félix Arteaga Martín
Investigador principal de Real Instituto Elcano.


ieee.es
Instituto Español de Estudios Estratégicos