Documento de Investigación 01/2022

Inteligencia Artificial: aplicaciones a la Defensa

-

Artificial Intelligence: applications to Defence

Trabajo incluido en el Plan Anual de Investigación del Centro Superior de Estudios de la Defensa Nacional (CESEDEN) para el año 2022 como Documento de Investigacion "Inteligencia artificial", asignado al Instituto Español de Estudios Estratégicos (IEEE)

*

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

Centro Superior de Estudios de la Defensa Nacional (CESEDEN)

Trabajo maquetado, en abril de 2022, por el Instituto Español de Estudios Estratégicos (IEEE).

Índice

Inteligencia artificial: aplicaciones a la Defensa

Eduardo Olier y Juan Manuel Corchado

Inteligencia artificial: aplicaciones a la Defensa

Eduardo Olier
Profesor honorario del CESEDEN
Presidente del Instituto Choiseul España

Juan Manuel Corchado
Catedrático de la Universidad de Salamanca
Presidente del AIR Institute

Resumen

La inteligencia artificial (IA) es un campo tecnológico esencial en las estrategias de defensa del siglo XXI. Los países que sean capaces de dominar estas nuevas tecnologías marcarán el devenir de la geopolítica de este siglo, lo cual abrirá una brecha entre aquellos países que tengan estas capacidades y aquellos que no dispongan de las mismas. Una circunstancia que se complementará con una nueva forma de colonización tecnológica que aumentará las dependencias de unos con otros. Sin embargo, los riesgos que surgen de estas nuevas tecnologías van más allá de la ética en su utilización, y entran en el dominio de que los países más avanzados podrán controlar las propias tecnologías de los países menos avanzados. Una circunstancia que aumenta las fragilidades de Europa, que se encuentra en este campo muy por detrás de Estados Unidos y de China. España necesita urgentemente un programa integrado de IA para soportar sus estrategias de defensa en el marco geopolítico en el que está encuadrada.

Palabras clave:

Inteligencia artificial, ciberseguridad, militar, defensa, guerra, geopolítica, Rusia, Estados Unidos, China, Europa, España.

Artificial Intelligence: applications to Defence

Abstract:

Artificial Intelligence (AI) is an essential technological field in the defense strategies of the 21st century. Those countries that are capable of mastering these new technologies will mark the future of geopolitics in this century, which will open a gap between those countries that can benefit from these capabilities and those that do not. This will be complemented by a new form of technological colonization that will increase dependence on one another. However, the risks arising from these new technologies go beyond the ethics of their use and enter the domain of the more advanced countries being able to control the technologies developed by the less advanced countries. This circumstance increases the fragilities of Europe, which is lagging far behind the United States and China in this field. Spain urgently needs an integrated AI program to support its defense strategies in the geopolitical framework in which it is placed.

Key words:

Artificial Intelligence, Cybersecurity, Military, Defense, Warfare, Geopolitics, Russia, United States, China, Europe, Spain.

Introducción

La inteligencia artificial (IA) es una disciplina tecnológica que, gracias a las capacidades tecnológicas actuales, tiene un enorme impacto en las aplicaciones civiles y militares de muchos países, singularmente en aquellos más avanzados en este sentido. En síntesis, se puede decir que este desarrollo se debe a cuatro elementos fundamentales: (1) el enorme volumen de datos disponibles; (2) su posibilidad de manipulación con las tecnologías de *Big Data*; (3) el desarrollo de algoritmos cada vez más potentes, capaces de generar ellos mismos nuevos algoritmos en una especie de reproducción celular; y (4) la enorme capacidad de procesamiento de la información que ofrecen los actuales sistemas de computación, que pueden gestionar con enorme rapidez decenas de miles de millones de datos en tamaños que alcanzan los *zetabytes*[1], que sería algo así como llenar el océano Pacífico de granos de arroz; y que en poco tiempo serán capaces de manejar *yotabytes* que, siguiendo con el mismo símil, sería la manipulación de los granos de arroz que llenaran el volumen del globo terráqueo.

Actualmente, aparte de los sistemas ya en operación, están en marcha nuevos desarrollos basados en el potencial que ofrece la IA en la recopilación y análisis de la información logística, de actividades cibernéticas, de vehículos semiautónomos y autónomos, etc.; y en el campo de la defensa, igualmente, de muchas aplicaciones, donde la guerra, tal como se conoce, sería conducida prácticamente sin el elemento humano en los campos de batalla.

La IA, como es sabido, ya ha sido utilizada en actividades militares de Estados Unidos en Irak, en Siria y en otros lugares, y es aplicada casi a diario en misiones de información, muchas de las cuales son desconocidas, ya que tanto los que las ejercen a modo de ataque, como aquellos que las reciben y se prestan a su defensa, prefieren mantenerlas en la más absoluta reserva. A lo que se añade la aplicación de la IA en el dominio del espacio exterior, donde no hace mucho Rusia destruyó uno de sus satélites mediante otro ingenio espacial[2].

En este contexto, es preciso resaltar que las tecnologías de IA aplicadas al campo militar son un desafío enorme para aquellos países que no dispongan de estas nuevas tecnologías, ya que, en poco tiempo, se abrirá entre los diferentes sistemas militares una enorme brecha, separando aquellos países que dispongan de nuevos sistemas basados en IA de aquellos que no los tengan. Con la circunstancia de que hoy en día los desarrollos más avanzados en IA se dan en el mundo empresarial y el universitario, de manera que las Fuerzas Armadas (FAS) deberán apoyarse en el sector privado y

1 Un *zetabyte* consiste en 1021 *bytes* (un uno seguido de 21 ceros), siendo un *byte* la unidad de computación más pequeña, que se compone a su vez de 8 *bits*. Cada *bit* representa un 1 o un 0, ya que los circuitos electrónicos funcionan según el *álgebra de Boole* que manipula códigos binarios (unos y ceros), representando el 1 un circuito abierto y el 0 uno cerrado. Los *yotabytes* cuentan con 1024 *bytes*.

2 Ver por ejemplo: https://www.bbc.com/news/science-environment-59299101 (consultado el 14 de febrero de 2022)

universitario; con la circunstancia de que, si estos no están muy avanzados, las FAS podrían encontrarse con la imposibilidad de tener las capacidades necesarias por la imposibilidad de adquirir tales tecnologías en los mercados internacionales debido al cierre de los mercados por tratarse de productos de alto valor estratégico para la seguridad.

Así, la dificultad en el proceso de adquisición de sistemas de defensa basados en IA, o en el desarrollo de los mismos, determinará la capacidad de responder a los nuevos desafíos de seguridad que se darán en el siglo XXI; todo ello sin contar con la imperiosa necesidad de dotar con mandos y estructuras humanas en las propias FAS que sean capaces de comprender, analizar y manipular estas nuevas tecnologías, que podrían no estar disponibles para su utilización en el tiempo y la forma requeridos por la marcha de los acontecimientos en un contexto geopolítico mundial altamente cambiante.

Todo este panorama es nuevo en los sistemas de defensa en España, que necesitan desarrollar, a nuestro modo de ver, una estrategia global e integrada para poner en marcha nuevos sistemas basados en IA, con la necesidad de estructurar un programa consistente en el que participe la industria privada, la universidad y las propias FAS. Un programa que, dada la singularidad de estas nuevas tecnologías, deberá dotarse de los necesarios mecanismos de confidencialidad y de protección de la información, con las ayudas que la propia inteligencia militar pueda aportar en este sentido.

Dada la novedad y la relevancia de la IA en los nuevos sistemas militares, este artículo ofrece un panorama inicial que ayude a reflexionar sobre la necesidad de proporcionar a los sistemas de defensa españoles sistemas de IA, tanto para soportar las necesidades actuales como las futuras. Sin olvidar que, aunque la IA puede aportar ventajas en el contexto de la defensa, puede también introducir importantes retos; pues a la vez de dotar a las misiones la posibilidad de operaciones autónomas, podría igualmente ser imprevisible en sus resultados. De ahí la necesidad de desarrollar toda una nueva capacidad estratégica que permita una manipulación segura de estas nuevas tecnologías en los planes militares, incluyendo en su caso las necesidades consideraciones éticas y legislativas, así como la formación de mandos y de equipos especializados.

Componentes de la inteligencia artificial (IA)

Decir qué es o qué no es la IA es objeto de muchas discusiones incluso entre los especialistas de esta disciplina, ya que son innumerables sus definiciones.

Muchos son los científicos que se han dedicado a este complejo asunto. Alan Turing (1912-1954), por ejemplo, uno de los padres de la computación, decía que «una máquina sería inteligente en el momento en que fuera imposible para un observador asegurar si sus acciones eran o no llevadas a cabo por un ser humano». Una definición excesivamente simple en la que muchos investigadores no estarían hoy de acuerdo con ella.

David Pool y Alan Mackworth ofrecen también una definición igualmente sintética, que abre a su vez el problema de entender lo que significa el concepto de inteligencia. Para estos autores: «la inteligencia artificial es el campo científico que estudia la síntesis y el análisis de los agentes computacionales que actúan inteligentemente[3]. Siendo un «agente computacional» un *instrumento informático* que interactúa en el ambiente, que puede incluir, según estos autores: gusanos, perros, termostatos, aviones, robots, seres humanos, empresas o países. De manera que un *agente computacional* actuará inteligentemente siempre que[4]: (1) lo que haga sea consistente con sus circunstancias y objetivos; (2) sea flexible a la hora de cambios en el entorno o en sus propios objetivos; (3) aprenda en base a su experiencia; y (4) lleve a cabo elecciones apropiadas de acuerdo con sus percepciones y limitaciones de cálculo. Lo cual lleva a entender mejor el concepto de inteligencia o, más propiamente dicho, la diferencia que existe entre una conducta no inteligente y otra inteligente. Un aspecto que el científico Douglas Hofstadter, al tratar la inteligencia artificial, la definió en los años 1970 como la capacidad para[5]: (1) responder flexiblemente a las más diversas situaciones; (2) sacar provecho de circunstancias fortuitas; (3) encontrar el sentido a mensajes ambiguos o contradictorios; (4) reconocer la importancia relativa de los diferentes elementos que se dan en una situación concreta; (5) encontrar similitudes entre distintas situaciones, pese a las diferencias que puedan existir; (6) descubrir las diferencias entre situaciones diversas a pesar de las semejanzas que las puedan vincular; (7) sintetizar nuevos conceptos en base a conceptos antiguos que pueden modificarse en nuevas maneras; y (8) proponer ideas nuevas.

Siguiendo este esquema de Douglas Hofstadter se podría decir que son tres los mecanismos que se encierran detrás de la IA: razonar, decidir, y planificar las acciones provenientes de la toma de decisiones, considerando siempre las incertidumbres sobre el resultado que existe en todo proceso de decisión. Pues todo proceso de decisión es habitualmente complejo, tan complejo como sea el entorno en que haya que tomar esas decisiones, siempre inmersas en gran incertidumbre. Siendo mucho más compleja esa toma de decisiones cuando se consideran situaciones militares, donde la imprevisibilidad es parte habitual del escenario.

Razonar en situaciones complejas tiene mucho que ver con la probabilidad de acertar. De donde nace la necesidad de representar el conocimiento en dominios inciertos, especialmente cuando el número de variables a considerar sea elevado. Con la circunstancia añadida de que tales variables pueden ser aleatorias, que, a su vez, pueden entrelazarse formando una red de múltiples probabilidades de ocurrencia. Una

3 POOLE, D. L. y MACKWORTH, A. K. *Artificial Intelligence*. Foundation of Computational Agents. Cambridge University Press, 2010, p. 3.

4 Ibíd, p. 4.

5 HOFSTADER, D. R. *Gödel, Escher, Bach: An Eternal Golden Braid*. Basic Books, 1979. Existe edición española en Tusquets Editores con el título*: Gödel, Escher, Bach: un eterno y grácil bucle*, publicada en 1987. Pp. 29-30.

circunstancia que conduce a lo que se define como *redes bayesianas*[6]: una estructura que permite predecir la probabilidad de que una de las posibles causas de un resultado provenga de uno de los factores que haya desencadenado dicho resultado, como sería, por ejemplo, en un caso simple, la relación entre la probabilidad de que suceda una enfermedad y los síntomas que la producen.

Y es aquí donde nace la necesidad de elaborar algoritmos que relacionen las causas con sus probabilidades de ocurrencia; lo que lleva a considerar la importancia de los algoritmos en la construcción de sistemas de IA, que, en síntesis, no son sino la combinación de reglas para incorporar datos o información en los sucesos a considerar, así como los sistemas computacionales (*hardware* y *software*) que procesen tales algoritmos con dichos datos.

Un algoritmo se puede entender como «una secuencia de instrucciones elementales explícitas, precisas, inequívocas y ejecutables mecánicamente, generalmente destinadas a lograr un propósito específico»[7]. Con esta definición pudiera pensarse que los algoritmos, en principio, no necesitan sistemas de computación electrónica —es decir, ordenadores— para su ejecución, como no sería preciso un ordenador para llevar a cabo una receta de cocina, que no es sino un algoritmo que entrelaza un proceso (la elaboración de la receta) con sus datos (las cantidades de los productos a incorporar) para conducir a un resultado, es decir, el guiso o plato finalmente elaborado.

Sin embargo, los algoritmos gestionados informáticamente vinieron a cambiar las reglas del juego; ya que los ordenadores modernos son capaces de resolver problemas altamente complejos, permitiendo analizar sucesos aleatorios capaces de modificar el orden de los *pasos* de cálculo que son necesarios para llegar al resultado deseado[8]. Con la circunstancia de que los algoritmos que tienen carácter aleatorio pueden utilizar variables desconocidas al principio del proceso, que se irán conociendo a medida que el proceso avance, o que se incorporen nuevas variables ya conocidas previamente (o no) durante el proceso, para modificar posteriormente el tratamiento de dichas variables de forma dinámica a fin de obtener nuevos resultados. Una circunstancia que, en el caso militar, es en extremo fundamental dada la complejidad e incertidumbre de los procesos en los que se basan los conflictos bélicos.

De esta manera, los algoritmos procesados informáticamente, de forma similar a como los humanos abordan la resolución de problemas, pueden buscar una solución óptima calculando el camino más corto, como hacen los actuales navegadores que se utilizan en cualquier vehículo; o bien, pueden dar una solución aproximada intentando minimizar los riesgos; o son capaces, finalmente, de utilizar un enfoque heurístico buscando la solución óptima en tiempos mucho más cortos que los mecanismos

6 RUSSEL, S. y NORVIG, P. *Inteligencia artificial. Un enfoque moderno*. Pearson, Prentice Hall, 2.ª Ed., 2004, pp. 561 y ss.

7 ERICKSON, J. *Algorithms*. University of Illinois, pp. 1-3.

8 CORMEN, T. H. *et al. Introduction to algorithms*. MIT Press, 2009, p. 52.

conocidos de prueba y error[9] y, por supuesto, que en muchas de las soluciones que se aportan utilizando únicamente medios humanos.

Los algoritmos son también el motor interno de los *bots* que pueblan el espacio de Internet. Un término —*bot*— que define un robot informático capaz de recopilar, por ejemplo, información de los sistemas de búsqueda en internet (como es el caso de Google), o bien enviar miles de correos electrónicos en lo que se conoce como *spam*; o también generar miles de *post* en las redes sociales para influir en una determinada dirección a los usuarios, dando a conocer una marca o producto (los conocidos *like* o *don't like* en Facebook, por ejemplo).

En el caso de Twitter muchos de los *retweets* que se envían o, incluso, muchas de las supuestas personas que envían mensajes de manera casi constante no son realmente personas, sino robots informáticos, estimándose que más del 15 % de las cuentas de Twitter son *bots* y no personas. A esto se unen los llamados asistentes personales automáticos, como ocurre con *Siri* de Apple, el *Asistente* de Google o *Alexa* de Amazon, que no son sino otro tipo de robots. Todo un entramado de sistemas basados en complejos algoritmos que, en múltiples casos están diseñados para construir otros algoritmos en una forma de reproducción similar —con la gran distancia que los separa— de la reproducción celular. Un hecho que hoy es factible gracias a la capacidad de computación de miles de millones de elementos electrónicos (transistores) que se encuentran embebidos en millones de ordenadores que facilitan su proceso miles de millones de veces, haciendo que los algoritmos constituyan hoy en día una suerte de ecosistema creciente comparable a la complejidad de la propia vida[10].

Y es en este campo de los algoritmos donde la inteligencia artificial se complementa con potentes procesadores, capaces de realizar el tratamiento de complejos algoritmos «a la velocidad de la luz». Máquinas que proporcionan otra sorprendente capacidad como es la de *aprender*. De manera que si un algoritmo está diseñado para proporcionar un resultado a partir de un estado inicial —lo que técnicamente se conoce como *inputs* que dan como resultado *outputs*—, las máquinas que aprenden —*machine learning*— cambian totalmente el esquema, siendo capaces de construir el algoritmo que permite alcanzar el resultado a partir de los datos iniciales. Se trata entonces de algoritmos que *fabrican* otros algoritmos. Así, cuantos más datos se proporcionan, más capacidad de aprendizaje tienen este tipo de máquinas informáticas[11]. Aunque conviene indicar que estas tecnologías no son una novedad científica en tanto que se trata de una evolución en la que el análisis de *perceptrones*, por ejemplo, se daba ya a finales de los años 1940[12].

9 OLIER, E. y VALDERREY, F. *Algorithms Shaping the Future*. En: PARK S. Ho, et *al. The Palgrave Handbook of Corporate Sustainability in the Digital Era*. Palgrave Mcmillan, 2020, p. 40.

10 DOMINGOS, P. *The Master Algorithm*. Penguin Books, 2015, p. 5.

11 Ibíd, pp. 6 y ss.

12 Un perceptrón es una «red neuronal artificial» formada por múltiples capas, con capacidad para resolver problemas no lineales. En 1957 el científico Frank Rosenblatt desarrolló el *Mark I Perceptron*, considerado el primer ordenador capaz de crear redes neuronales. ROSENBLATT, F. *Principles of*

El tercer elemento esencial en el desarrollo de la inteligencia artificial, aparte de los algoritmos y los procesadores electrónicos, son los datos; lo que hoy en día, dada la masiva cantidad de datos disponibles, se hace posible con las nuevas tecnologías de *Big Data*. Los datos son en este contexto la materia prima de la IA, lo que algunos entienden como el nuevo *petróleo* del siglo XXI.

Big Data es un término que indica la capacidad de manipular gran volumen de cierto tipo de datos que tienen la característica de cambiar a gran velocidad (en tiempo-real), y de tener enorme variedad, pudiendo ser datos estructurados numéricos o alfanuméricos, vídeos o imágenes, así como datos no estructurados provenientes de fuentes de audio o de vídeo, textos de redes sociales, *blogs* o redes profesionales, mensajes electrónicos de sensores de todo tipo, imágenes de satélites, etc. De manera que, en síntesis, tal como muestra la figura 1, la inteligencia artificial se podría definir esquemáticamente como una estructura de sistemas complejos que usan avanzadas tecnologías digitales de procesamiento electrónico, manipulan complejos algoritmos y, a su vez, gestionan enormes volúmenes de datos estructurados y no estructurados, todo ello realizado a gran velocidad.

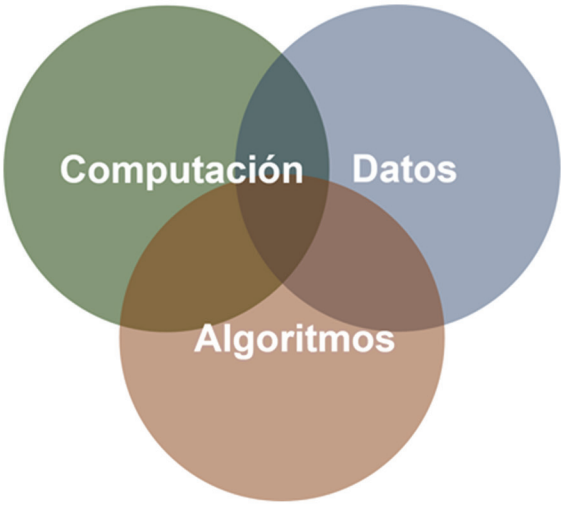

Figura 1. Elementos de la inteligencia artificial

Tecnologías alrededor de la IA

Se suele decir que lo importante no es lo que se conoce, sino lo que se hace con lo que se conoce. Una consideración muy apropiada cuando se considera la estrategia militar. De donde se deduce que las tecnologías que facilitan la implantación de sistemas basados en IA deben facilitar como primera función el análisis de complejas

Neurodynamics and the Theory of Brain Mechanisms. Spartan Books, 1962.

situaciones para facilitar la toma de decisiones, lo que conduce a la capacidad para construir escenarios futuros.

Más arriba hemos hablado de las máquinas que aprenden (*machine learning*). Una serie de técnicas informáticas que permiten a las computadoras *aprender* sin necesidad de ser explícitamente programadas para ello. Se trata, como se dijo, de algoritmos tratados informáticamente que muestran diversas denominaciones, como son, por ejemplo, los utilizados en teoría de juegos (aprendizaje por refuerzo o *reinforcement learning* en inglés), los algoritmos genéticos, las máquinas de vectores de soporte (*suport-vector machines*) o las *redes neuronales* ya mencionadas, en las cuales al modo de las redes de neuronas biológicas, las informaciones que entran en ellas son capaces de producir resultados después de un proceso de aprendizaje interno que se realiza de manera automática. Y dentro de este conjunto tecnológico de redes neuronales, sobresalen actualmente las máquinas que gestionan los algoritmos denominados *Deep Learning*, que utilizan diferentes estructuras de redes neuronales que, en capas sucesivas, aumentan su capacidad de aprendizaje a medida que son *alimentadas* con mayores cantidades de datos. Lo que ha llevado en la actualidad a que este tipo de máquinas tengan una capacidad similar al conocimiento humano para la comprensión del lenguaje hablado, para reconocer la escritura, o también aquellas usadas en sistemas de traducción automática, en el manejo de vehículos autónomos, en los ya referidos asistentes digitales (Siri, etc.), en la manipulación de juegos complicados como podría ser el ajedrez o el mucho más complejo juego chino *Go*, donde la máquina AlphaGo derrotó en 2016 a Lee Sedol, mejor jugador del mundo de este antiquísimo juego de fichas chino, cuyo tablero puede contener 10170 combinaciones diferentes[13].

Toda una estructura tecnológica que se engloba en la nueva *ciencia de los datos*, que incluye métodos matemáticos, procesos y sistemas de computación que manipulan datos masivos para dirigir la toma de decisiones en situaciones complejas, con especial énfasis en el análisis predictivo y en la construcción de escenarios futuros, pues saber lo que puede ocurrir es uno de los elementos esenciales en cualquier proceso de toma de decisiones. Una circunstancia que es la base de la IA, es decir: convertir los datos en datos *inteligentes*, que no es sino ofrecerlos en información útil para la toma de decisiones, ya sea para las personas que han de tomar decisiones complejas en cualquier campo de actividad, o para *alimentar* máquinas inteligentes diseñadas para *decidir* por ellas mismas lo que se debería hacer en situaciones complejas (véase, por ejemplo, el caso de los vehículos autónomos).

La IA se construye en base a un conjunto de tecnologías en la que cada una de ellas interacciona con las demás para dar soluciones a problemas complejos. Por ejemplo, cuando se piensa en el vehículo autónomo, como primera medida se deberán incorporar múltiples sensores que, a su vez, serán gobernados por otros sistemas, como podrían ser máquinas con capacidad de aprender o máquinas que incorporan algoritmos

13 Ver por ejemplo: https://deepmind.com/research/case-studies/alphago-the-story-so-far (consultado el 15/3/2022).

que procesen el lenguaje natural, así como otras estructuras computacionales que construyan reglas para dar sentido a los posibles escenarios que puedan presentarse en la vida real. La figura 2 muestra un esquema simple con las diferentes tecnologías que pueden ser constitutivas de un sistema de IA.

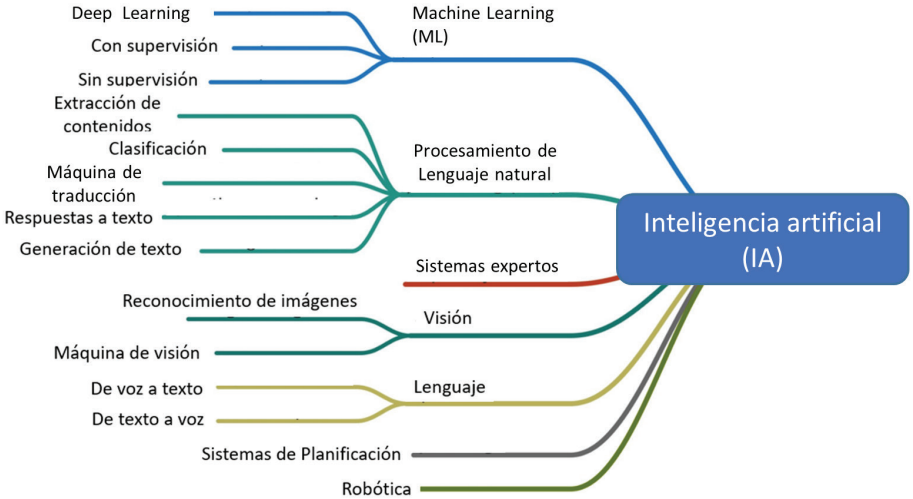

Figura 2. Algunas tecnologías usadas en sistemas de inteligencia artificial[14]

Dado que muchos algoritmos se construyen en base a reglas, a veces se han confundido los sistemas expertos como la base fundamental de la IA. Baste para ello un simple apunte sobre lo que es o no es un sistema experto.

Un sistema experto es un mecanismo lógico compuesto de tres elementos esenciales: (1) un conocimiento-base (*knowledge-base*); (2) un mecanismo de inferencia; y (3) un programa informático para facilitar la interacción de los usuarios, facilitar la construcción del conocimiento-base, y desarrollar un esquema de razonamiento posterior[15]. Siendo el conocimiento-base el archivo de sucesos y las asociaciones entre ellos que se conocen de un área concreta de análisis, donde el conocimiento viene representado por reglas según un esquema: «SI-ENTONCES». Es decir: «SI» hay la evidencia de que A y B son ciertos, «ENTONCES» se puede concluir que C será cierto. Y donde el mecanismo de inferencia, aunque puede tomar múltiples formas, es una estructura que controla la relación entre las reglas, de manera que los datos conocidos *infieren* las reglas para llegar a concluir el conocimiento de aquellos datos desconocidos.

14 MOHAMED, Ziyad. *Artificial Intelligence, Definition, Ethics, and Standards*. The British University in Egypt, 2018-2019, p. 6.

15 BUCHANNAN, B. C. y SHORTLIFFE, E. H. *Rule-Based Expert Systems*. Addison-Wesley, 1984, p. 4-19.

Se trata por tanto, cuando se considera la inteligencia artificial, de un conjunto de tecnologías informáticas basadas en procesos lógico-matemáticos que se encuentran en evolución permanente, donde las predicciones hacia el futuro en el desarrollo de sistemas basados en IA consideran que acabarán sustituyendo la acción y la capacidad humana en muchos supuestos (figura 3).

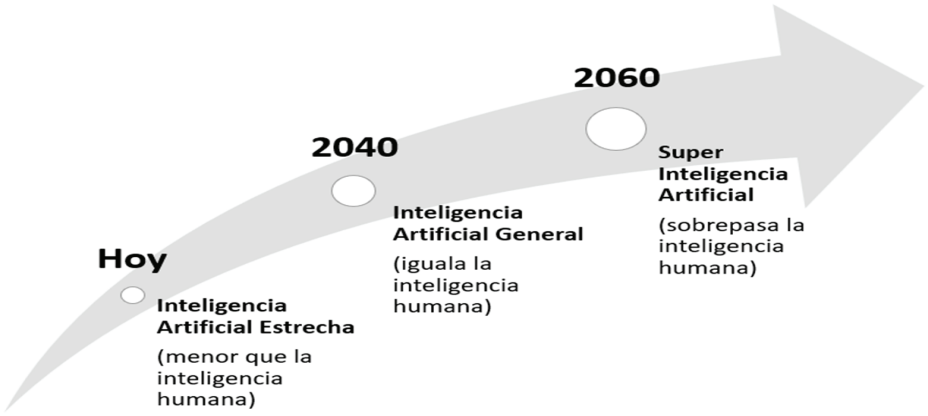

Figura 3. Futuro de la inteligencia artificial según algunos autores[16]

Aplicaciones a la defensa de la IA

Aparte de lo ya apuntado anteriormente, en el campo militar, incluyendo el entorno de la seguridad, las aplicaciones de la IA tienen un importante campo de aplicación, particularmente en asuntos relacionados con el análisis de inteligencia, la logística, la ciberseguridad y también en ciberoperaciones, sistemas de mando y control, y una enorme variedad de vehículos autónomos y semiautónomos de aplicaciones militares.

Sin embargo, como dijimos en la Introducción de este artículo, dado que estas tecnologías se desarrollan principalmente en el mundo civil aparecen de manera persistente problemas de desconfianza cuando se trasladan al campo militar; siendo uno de los aspectos de dicha desconfianza las posibilidades de que un país no alineado, o incluso beligerante, realice inversiones en empresas que dispongan de avanzadas tecnologías de IA gracias a los movimientos de capitales que se dan en el contexto de la globalización económica, pudiendo incluso suceder que un país *amigo* sea el instrumento elegido por un país contrario para realizar dicha inversión y adquirir una capacidad tecnológica que no posee. Este sería el caso, por ejemplo, de complejos algoritmos de IA capaces de detectar de manera autónoma fallos en equipos militares

16 MOHAMED, Ziyad, *op. cit.*, p. 5.

de software, o sistemas de IA con el potencial de realizar intrusiones no deseadas en equipos militares en escenarios bélicos o de defensa.

Es interesante a este respecto, considerar lo que se piensa respecto de las nuevas tecnologías de IA aplicadas al campo militar en China, dada la tendencia occidental a considerar únicamente los desarrollos tecnológicos que, en materia militar, suceden en Occidente y, en particular, en Estados Unidos.

Un informe de *China Defense News* accesible desde internet[17], asegura que el mundo «está actualmente en vísperas de una revolución de la inteligencia, con la sociedad humana pasando de la era de internet a la era de la inteligencia». De manera, que en los últimos años, «impulsada por el *Big Data*, los nuevos algoritmos y la supercomputación, la inteligencia artificial está cambiando e incluso modificando todos los sectores que toca, donde la guerra no es una excepción». Asegurando que: «desde los submarinos hasta los *clusters* de drones, y desde el software de mantenimiento predictivo hasta los asistentes inteligentes para la toma de decisiones, la IA está cambiando los escenarios de la guerra con una amplitud y profundidad sin precedentes, impulsando una nueva ronda de cambios militares y modificando silenciosamente la forma y el rostro de la guerra». Un contexto en el que el tiempo es el elemento clave, siendo necesario calcular y predecir los posibles resultados de un conflicto armado, donde aparece la importancia de la IA que, con algoritmos avanzados y sistemas de supercomputación, pueden ayudar a predecir tales resultados con mayor precisión que la intuición o el conocimiento humano.

Es lo que refiere el autor de este análisis cuando dice que en la era de la información, la guerra sigue la regla de «lo rápido se come a lo lento» (快吃慢). De ahí la importancia de nuevas tecnologías, como pueden ser los sistemas de armas inteligentes, las contramedidas autónomas, las armas hipersónicas y la guerra de racimos, según los cuales, la guerra entrará en la era del «tiempo en segundos» y de los *enjambres*, con el uso de sistemas inteligentes para la confrontación autónoma, siendo casi los únicos elementos a tener en cuenta en los futuros escenarios bélicos; en los cuales, según el autor que comentamos, la denominada guerra de racimos (集群作战，), o guerra con «bombas de racimo», será la que vuelva a la actualidad conceptos más antiguos como el conocido como guerra de desgaste.

Otras potencias, como sería el caso de Rusia (sin entrar en los sistemas militares utilizados en el actual conflicto con Ucrania), desarrollan una especial estrategia en el contexto de la IA militar, dando prioridad a las tecnologías y capacidades que pueden utilizarse para debilitar los sistemas de mando y control, así como las comunicaciones del adversario. Una estrategia para ganar superioridad en relación con los sistemas de información. Conviene recordar, sin embargo, que Rusia se encuentra por detrás de China o de Estados Unidos en relación con las capacidades de IA. Tanto por

17 HANG HUI, Chen. *Inteligencia artificial: cómo alterar el futuro de la guerra*. 人工智能:如何颠覆未来战争. http://www.mod.gov.cn/jmsd/2018-01/02/content_4801253.htm (consultado el 24/3/2022).

las capacidades de sus empresas, como también por la carencia de una industria de semiconductores de altas capacidades de computación, imprescindible para el tratamiento de sistemas basados en IA. Aquí, Rusia aparece enormemente dependiente de Estados Unidos, de la República de Corea o de Taiwán. Con la consideración de que, mientras que la cultura de innovación occidental —especialmente la estadounidense— se caracteriza por una tendencia a utilizar tecnologías de vanguardia como solución a los problemas tácticos y estratégicos en el dominio militar, el enfoque ruso de las aplicaciones militares de la IA es más utilitario y pragmático[18]. Dicho esto, sin embargo, los estrategas rusos consideran que la guerra de la información es el elemento central de los conflictos contemporáneos, llegando a considerar la guerra de la información basada en la IA como una «baza estratégica para ganar la guerra en los conflictos entre Estados»[19]. Y será en este campo en el que la IA, según el pensar de los estrategas rusos, lo que permita a Rusia enfrentarse más eficazmente al entorno de la información y a las ciberguerras en los nuevos escenarios de guerras cibernéticas en el nuevo contexto de guerras electrónicas[20]. Sin olvidar, por supuesto, la capacidad actual de Rusia en la construcción de vehículos autónomos como es, por ejemplo, el URAN-9, un tanque de combate de gran capacidad operativa (sistemas que en el argot militar se definen como *Unmanned Ground Vehicles* o UGV)[21].

Sin embargo, aparte de las tecnologías basadas en IA que son dirigidas a sistemas de mando y control o servicios de información, incluidas todas aquellas que se encuentran en el contexto de la ciberguerra, un aspecto esencial de las aplicaciones militares de la IA, se dirigen, como en el caso indicado del URAN-9, a los vehículos autónomos no tripulados y, en especial, a los *drones* o vehículos aéreos no tripulados (*Unmanned Aerial Vehicles* o UAV). Unas tecnologías en las que conviene hacer la distinción entre vehículos autónomos y vehículos automatizados. En los primeros —vehículos autónomos—, a partir de la información recibida desde sus distintos sensores y de sus sistemas de IA, será el propio vehículo quien *razone* sobre el curso que ha de tomar para, de manera probabilística, alcanzar el objetivo marcado. Sin embargo, los segundos —vehículos automatizados—, actuarán según reglas determinadas a la manera «SI-ENTONCES», referidas para los sistemas expertos, dando como resultado un comportamiento constante en todos los casos; pues para un conjunto de entradas (*inputs*) se obtendrán un conjunto único de salidas (*outputs*)[22].

18 CHATHAM HOUSE. *Advanced Military Technology in Russia*. https://www.chathamhouse.org/2021/09/advanced-military-technology-russia (consultado el 25/3/2022).

19 Ibíd.

20 Ibíd.

21 https://www.janes.com/defence-news/news-detail/russia-to-conduct-mass-testing-of-uran-9-ugv-in-2022 (consultado el 17/03/2022).

22 Cummings, M. L. *Artificial Intelligence and the Future of Warfare*. Chatham House, enero 2017. https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf (consultado el 22 de marzo de 2022).

En general, las tecnologías de aplicación militar basadas en sistemas de IA pueden dividirse en cinco grandes grupos como muestra la figura 4: (1) inteligencia, vigilancia y reconocimiento; (2) logística; (3) ciberoperaciones; (4) desinformación (profunda); (5) mando y control; (6) vehículos autónomos y semiautónomos; y (7) sistemas de armas letales autónomas[23].

Inteligencia, Vigilancia, Reconocimiento	Logística	Ciberoperaciones	Desinformación profunda (Deep Fake)	Mando & Control	Vehículos autónomos y semiautónomos	Sistemas de armas letales autónomas
▪ Visión computarizada ▪ Algoritmos para adquisición de datos ▪ Vehículos autónomos para identificación de acciones hostiles ▪ Análisis automático de múltiples fuentes de información(satélites, drones, etc.) ▪ Apoyo a la Comunidad de Inteligencia (reconocimiento de imágenes, análisis predictivo, reconocimiento multi-lenguaje de voz en ambientes ruidosos, creación de imágenes 3D a partir de fotos 2D, análisis de comportamiento, etc.)	▪ Mantenimiento predictivo de sistemas de defensa ▪ Ejecución de mantenimiento a medida según necesidades (aviones, buques, etc.)	▪ Análisis "inteligente" en el comportamiento de redes y sistemas informáticos ante ataques del exterior	▪ Detección de noticias o información falsa de carácter sensible en contra de la sociedad o de objetivos militares	▪ Generación de fuentes unificadas para planificación centralizada de operaciones conjuntas (tierra, mar, aire, satélites, ciberespacio) ▪ Análisis en tiempo real de ataques contra sistemas informáticos o redes de comunicaciones	▪ Plataformas autónomas contra eventos no programados u obstáculos imprevistos ▪ Vehículos con incorporación de armas adicionales ▪ Contra interferencia de ataques electrónicos ▪ See Hunters y Submarine Hunters ▪ Sistemas de ataque electrónico o sistemas de apoyo a fuerzas terrestres	▪ Sistemas autónomos para identificar y destruir objetivos sin intervención humana

Figura 4. Algunas tecnologías militares basadas en sistemas de IA[24]

Sin embargo, la aplicación de los sistemas de IA en el campo militar no está exenta de riesgos. La figura 5 expone algunos de ellos. Unos riesgos que no excluyen otros muchos beneficios en los sistemas de defensa cuando se utilizan sistemas de IA, por ejemplo: la posibilidad de integrar datos masivos, mayor rapidez en la toma de decisiones, mejora en las capacidades de visión y comprensión de los escenarios bélicos, menor necesidad del elemento humano, disminución de bajas en el campo de batalla, posibilidad de evitar una toma de decisiones basada en emociones o situaciones de estrés, menores costes en la acción militar, y un largo etcétera de ventajas siempre que los sistemas de IA se consideren un complemento y no la anulación de otras funcionalidades de la acción militar.

Éticos	Operacionales	Estratégicos
• Leyes de la guerra • Responsabilidades morales • Derechos humanos	• Confianza y funcionamiento de los sistemas • Posibilidad de manipulación por el adversario • Accidentes y riesgos en emergencias	• Gestión de la proliferación de sistemas autónomos • Umbrales de uso • Estabilidad de la estrategia militar

Figura 5. Riesgos asociados al uso militar de la IA[25]

23 Congressional Research Service. *Artificial Intelligence and National Scurity.* 10 de noviembre de 2020.

https://sgp.fas.org/crs/natsec/R45178.pdf (consultado el 15 de marzo de 2022).

24 La figura ha sido realizada en base a la información obtenida del Congressional Research Service, *op. cit.*

25 MORGAN F. E. *et al. Military Applications of Artificial Intelligence. Ethical Concerns in an*

El caso de la ciberseguridad

Anualmente se producen miles de ciberataques contra instituciones privadas y públicas alrededor en todo el mundo, siendo unos países más atacados que otros, fundamentalmente aquellos que se encuentran en el capítulo de economías avanzadas. Los ataques de *hackers* (piratas informáticos) o la diseminación de *ransomware*[26] se cuentan por cientos de miles anualmente en contra de grandes compañías privadas o incluso contra potentes agencias de inteligencia, como fue el caso de los *Shadow Brokers* que, según se dijo, fueron capaces de acceder a los sistemas de la potente agencia de inteligencia americana NSA (National Security Agency) en el mes de agosto de 2016[27]. Como también fue el caso de *WannaCry* que fue capaz de *infectar* a todos los sistemas de la Sanidad del Reino Unido (el National Health Service); o el denominado *Petya* que alcanzó a manipular los ordenadores de medio mundo, incluido el conocido ciberataque a los sistemas de distribución de energía eléctrica de Ucrania[28]. Y, para terminar esta brevísima exposición, conviene igualmente recordar que más de 60.000 ficheros pertenecientes al Gobierno de Estados Unidos aparecieron accesibles públicamente en los servicios en la nube de Amazon (Amazon Web Services) por una supuesta mala operación de un técnico de esa empresa[29]. Errores que no evitan la realidad de ser conscientes de la multitud de ciberataques que ocurren diariamente contra empresas o instituciones en el mundo.

Como se ha indicado anteriormente las aplicaciones de la IA en el dominio militar son fundamentalmente operacionales y tácticas, muchas de ellas dirigidas a la toma de decisiones. Ya sean vehículos autónomos o semiautónomos, apoyo a la inteligencia militar, análisis de escenarios, mantenimiento predictivo, operaciones logísticas, etc., la inteligencia artificial es un componente que puede proporcionar ventajas defensivas y ofensivas. Sin embargo, como también se ha dicho, la IA proporciona riesgos inherentes a sus propias capacidades, de manera que, a la vez de presentar nuevas capacidades, abre la posibilidad de dar ventajas a un oponente tecnológicamente más avanzado. Una circunstancia que hace que, las grandes potencias apuesten definitivamente por dotarse de una superioridad en el ámbito de la guerra basada en

---

Uncertain World. RAND Corporation, 2020. https://www.rand.org/pubs/research_reports/RR3139-1.html (consultado el 6 de marzo de 2022).

26 Se trata de programas informáticos hostiles (virus, gusanos informáticos, programas espía, etc.), denominados *malware* en inglés, que se basan, en el caso del *ransomware*, en la extorsión, e impiden a los usuarios la posibilidad de acceder a sus propios archivos salvo que se pague la cantidad exigida.

27 https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/ (consultado el 25 de marzo de 2022).

28 Este vídeo muestra la situación de sorpresa que se produjo entre el personal técnico que se ocupaba del control de la red de distribución de electricidad ucraniana. https://www.wired.com/video/watch/watch-hackers-take-over-a-ukranian-power-station (consultado el 25 de marzo de 2022).

29 https://es.gizmodo.com/como-un-comando-mal-escrito-por-un-ingeniero-de-amazon-1792910295 (consultado el 25 de marzo de 2022).

inteligencia artificial. Un caso paradigmático de esta estrategia es el programa lanzado por el US Strategic Operations Control (SOCOM), que no es sino el Mando de Operaciones Estratégicas para la defensa de Estados Unidos, que tiene en marcha una «hoja de ruta» invirtiendo fuertemente en tecnologías apoyadas por la IA, donde el aprendizaje automático es uno de los puntales de tal estrategia, que mantiene en lo esencial tres objetivos principales: (1) personal operativo experto en técnicas de IA; (2) desarrollo de aplicaciones específicas de IA para las fuerzas armadas; y (3) análisis del alcance y potencial de las aplicaciones de IA en el campo militar[30].

Cuando se consideran los aspectos estratégicos de un conflicto armado, la inteligencia artificial viene a potenciar las capacidades C3I (*Command, Control, Communications, and Intelligence*), incluyendo los aspectos relacionados con el seguimiento y guiado de misiles de todo tipo, así como la intercepción de los misiles enemigos, incluidos los nuevos tipos de misiles hipersónicos. Y, en este sentido, surge como campo esencial de aplicación todos los aspectos relacionados con la ciberseguridad, lo cual presenta la otra cara de la moneda: la vulnerabilidad de los actuales métodos de defensa ante potentes ciberataques de potenciales adversarios, que pueden disponer de nuevas armas *inteligentes* contra las que no sea posible una respuesta eficaz. Haciendo que la separación entre los métodos de ciberdefensa y los de ciberataque ofrezcan una línea extremadamente delgada.

En este sentido, el Departamento de Defensa de Estados Unidos considera que la IA es un instrumento esencial para predecir, identificar, y responder a ciberataques y otras amenazas físicas que provengan de fuentes diversas. Para lo cual se dirigen a la cooperación público-privada, seleccionando aliados comerciales y académicos para desarrollar estos nuevos sistemas con especial atención en áreas tales como tratamiento de datos, evaluación y pruebas de nuevos sistemas, basados en IA y, fundamentalmente, en todo el amplio espectro de la ciberseguridad[31].

Sin embargo, como se ha apuntado, más arriba los sistemas *inteligentes* basados en IA pueden aumentar las vulnerabilidades de cualquier defensa ante potenciales ciberataques, en los que contrariamente a lo que se establezca, un potencial enemigo podría utilizar *malware* para hacerse con el control, manipular o engañar al respecto del comportamiento de los sistemas de IA diseñados para el ataque o la defensa, sin olvidar la posibilidad de reconocer (*hackear*, diríamos utilizando un anglicismo) los patrones y la estructura de los sistemas autónomos. Este sería el caso del *Proyecto*

30 SOCOM. *Plans New Artificial Intelligence Strategy*. https://www.nationaldefensemagazine.org/articles/2019/8/9/socom-plans-new-artificial-intelligence-strategy (consultado el 26 de marzo de 2022).

31 US Department of Defense. *Summary of the 2018 Department of Defense Artificial Intelligence Strategy. Harnessing AI to Advance Our Security and Prosperity.* https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF?source=GovDelivery (consultado el 26 de marzo de 2022).

Maven de Estados Unidos[32] capaz de extraer de forma autónoma objetos de interés de imágenes en movimiento o fijas, que buscan lograr una gran capacidad de ciberataque a la hora de ser detectados. Pero es un hecho que los ciberataques existen porque los sistemas informáticos o computacionales son vulnerables. Siempre habrá quien encuentre la manera de desarticular un algoritmo o un programa informático por muy robustos que sean. Los ciberataques se dirigen habitualmente a interrumpir, alterar, confundir, degradar o destruir los sistemas y redes informáticas del adversario, como también hacer lo mismo con la información o con aquellos sistemas que residen en sus aliados como forma de debilitar al conjunto.

Al lado de los ciberataques, se encuentra también la ciberexplotación que se dirige a la adquisición de información sensible de manera clandestina sin perturbar el correcto funcionamiento de los sistemas. Un entorno complejo en el que no es ajeno el ciberespionaje, lo que algunos denominan «sombras en la nube»[33]. Nótese, sin embargo, que tanto los ciberataques como estos nuevos modelos de ciberexplotación fundamentados en sistemas de IA no se dirigen únicamente a los sistemas de computación o a los sistemas de armas fijos o móviles, sino que tienen también como objetivo primordial las redes de comunicaciones, de manera que, a mayor tecnificación de los sistemas militares, mayores son los peligros y los riesgos de ser interceptados.

Teniendo en cuenta que el ciberespacio puede ser considerado como un quinto espacio que se suma a las tres dimensiones de tierra, mar y aire, así como al espacio exterior donde se mueven los sistemas satelitales, todo este conjunto se hace cada vez más vulnerable en tanto que se encuentra integrado informática y tecnológicamente en el quinto espacio. Un quinto espacio que no debe olvidar otro espacio adicional pocas veces tenido en cuenta, como es el espacio radioeléctrico donde se transmiten las comunicaciones en sus diferentes tramos de frecuencias. De manera que el ciberespacio, de acuerdo con la RAND Corporation[34], se compone de tres capas que interactúan en los otros espacios indicados: la capa física, la capa sintáctica y la capa semántica tal como muestra la figura 6. Todo un conjunto susceptible de ser destruido en una u otra forma o de poder destruir a un posible oponente.

En definitiva, la IA es útil para ayudar en la toma de decisiones en el contexto del ciberespacio debido a que la rapidez es esencial y los sistemas basados en IA son capaces de gestionar enormes cantidades de datos a mucha mayor velocidad que el cerebro humano. Sin embargo, aunque sea posible desarrollar ingenios militares autónomos o semiautónomos que pueden dar mayor capacidad operativa, los sistemas militares

32 https://www.defense.gov/News/News-Stories/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/ (consultado el 26 de marzo de 2022).

33 DEIBERT, R. y ROHOZINSKI, R. *Shadows in the Cloud. Investigating Cyber Espionage 2.0.* https://www.nartv.org/mirror/shadows-in-the-cloud.pdf (consultado el 11 de marzo de 2022).

34 LIBICKI, M. C. *Cyberdeterrrence and Ciberwar*. RAND Corporation, 2009. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (consultado el 28 de marzo de 2022).

basados en IA son igualmente vulnerables a los ciberataques, lo cual abre importantes consideraciones respecto de su uso, e incluso induce a pensar sobre la posibilidad de adquirir armas o sistemas militares del exterior que pueden haber sido manipulados por los propios vendedores para debilitar las capacidades operativas del país o de las Fuerzas Armadas adquirientes en caso de conflicto. Una dependencia que, dada la presencia global del ciberespacio en las operaciones militares puede ser muy negativa si no se disponen de capacidades propias, tanto humanas como tecnológicas para desarrollar los propios sistemas basados en IA al margen de mercados internacionales, ya sean de aliados o, por supuesto, de otros países no alineados[35].

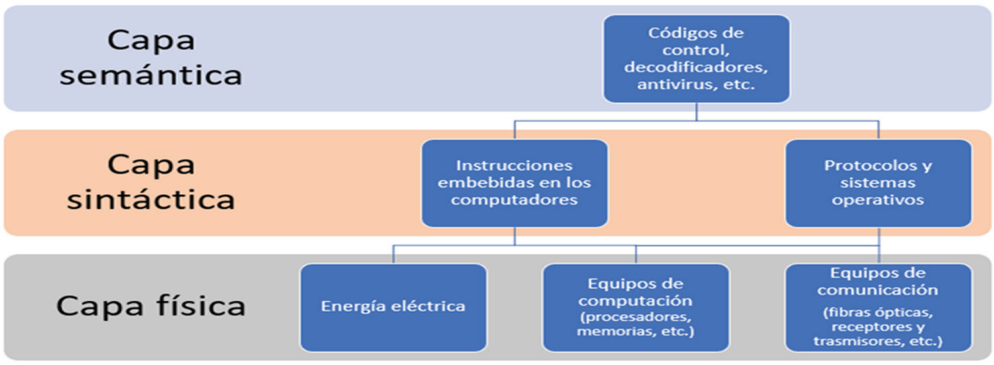

Figura 6. Estructura del ciberespacio

Geopolítica de la IA

Se dice que el presidente de la Federación Rusa, Vladimir Putin, comentando con un grupo de periodistas y estudiantes rusos en 2017 declaraba que: «Quien se convierta en el líder en esta esfera [la inteligencia artificial] se convertirá en el gobernante del mundo»[36]. Es de común entendimiento en el contexto de las relaciones internacionales que el orden internacional durante el siglo XXI vendrá determinado por el poder que otorgue la tecnología.

En este nuevo escenario, Estados Unidos y China surgen como las dos grandes potencias que, presumiblemente, dominarán el ciberespacio. Europa, por su parte, parece adolecer de estas capacidades tecnológicas y corre el riesgo de padecer una suerte de *cibervasallaje* o *cibercolonización*, con los peligros que esto entraña para la

35 Stanley Center for Peace and Security. *The Militarization of Artificial Intelligence*. 2009. https://front.un-arm.org/wp-content/uploads/2020/06/Stanley-Stimson-UNODA-2020-TheMilitarization-ArtificialIntelligence.pdf (consultado el 1 de marzo de 2022).

36 MIAILHE, N. *Géopolitiuqe de l'Intelligence artificielle : le retour des empires ?* Politique étrangère, Vol. 83, Issue 3, 2018.

independencia y la autonomía europea en el contexto global[37].

Si históricamente los imperios se han caracterizado por implantar su poder en un extenso territorio, ejercido desde un lugar central, a la vez que trasladaban sus modos de ejercer la política y sus normas sociales en dicho territorio, la IA viene a ser el instrumento clave en la constitución de imperios en el ciberespacio[38]. Y esto es así porque, como expresamos en la introducción de este artículo, una de las claves en el desarrollo de las capacidades de IA, aparte de las capacidades de computación y el desarrollo de potentes algoritmos, está en los datos. Siendo la manipulación de datos masivos lo que ha cambiado el contexto económico global y el desarrollo de las grandes empresas tecnológicas mundiales, como Google (Alphabet), Apple, Amazon, Facebook (hoy Meta) o Microsoft que, con las chinas Tencent y Alibaba, constituyen el poder tecnológico global. Solo la petrolera saudí Saudi Aramco es capaz de entrar en ese selecto grupo de empresas cuyo valor de capitalización bursátil supera en cada caso los 600.000 millones de dólares (en valores de 2020)[39]. Unas empresas que dominan el ciberespacio gracias a sus potentes instrumentos y sistemas basados en inteligencia artificial y la manipulación de miles de millones de datos de todo tipo de usuarios, ya sean personas, empresas o instituciones a nivel mundial. Un poder geopolítico poco considerado, que influye determinantemente en las inversiones de múltiples Gobiernos de todo el mundo, así como en muchos de los desarrollos tecnológicos de empresas y universidades[40] en todo el escenario público-privado que se pueda imaginar.

El World Economic Forum no es ajeno a esta realidad[41], haciendo énfasis en la necesidad de que los desarrollos de IA cumplan los necesarios estándares éticos, sacando a colación el despliegue de cámaras y otros dispositivos que Tencent o Alibaba han desplegado en China para controlar a los ciudadanos, o cómo Facebook ha sido el instrumento para atacar virulentamente a los musulmanes rohinyás en Birmania. Donde Estados Unidos tiene previsto invertir unos 50.000 millones de dólares en desarrollos de IA hasta 2025[42]; siendo el país que más esfuerzo inversor ha realizado en este dominio tecnológico entre 2021 y 2016, muy por delante de China: Estados

37 Ibíd.

38 Ibíd.

39 PAGANINI, P. *Data, the New Power in Geopolitics*. ISPI (Italian Institute for International Political Studies). 2021.
https://www.ispionline.it/en/pubblicazione/data-new-power-geopolitics-30657#:~:text=The%20governments%20that%20invested%20more,data%20is%20the%20new%20power
(consultado el 25 de marzo de 2022).

40 En este artículo de P. Paganini se muestras las 17 universidades más relevantes en el desarrollo de IA, siendo las más relevantes las que se encuentran en Estados Unidos.

41 PAUWELS, E. *The new geopolitics of artificial intelligence.* World Economic Forum.
https://www.weforum.org/agenda/2018/10/artificial-intelligence-ai-new-geopolitics-un/ (consultado el 25 de marzo de 2022).

42 Ibíd.

Unidos, 17.900 millones de dólares; China, 2.600 millones de dólares[43]. Toda una tendencia que pone a los desarrollos de IA al frente de la geopolítica del siglo XXI, con especial énfasis en nuevas armas basadas en estas tecnologías; con lo cual es esencial conocer quiénes son los que dominarán estas nuevas tecnologías de defensa y ataque, y cómo será el nuevo escenario de la guerra en el presente siglo. Sin olvidar los riesgos inherentes a estos desarrollos como ya han sido puestos en perspectiva.

La IA esta cambiando el equilibrio de poder en el mundo. Todo lo relativo a la IA es hoy un nuevo eje de cambio que cambiará no solo el ciberespacio, sino lo que algunos denominan como *geoespacio*[44], tanto uno como otro el espacio natural de la geopolítica.

Conclusiones

La inteligencia artificial, como hemos explicado, es el campo donde se determinará el nuevo orden mundial. Un nuevo orden que, como ha sido la tónica de la historia humana, vendrá determinado por las estructuras de poder político y, por ende, militar, donde China y Estados Unidos aparecen como las dos grandes potencias de este siglo, sin olvidar otros países que juegan igualmente a ocupar y defender aquellos espacios geopolíticos que consideran propios. Un nuevo contexto en el que la civilización occidental, dominada por Estados Unidos, se enfrenta de alguna manera con otras civilizaciones aún existentes: la civilización ortodoxa (dominada por Rusia), la civilización del Extremo Oriente (bajo la hegemonía de China), la civilización islámica (con Irán como país quizás predominante), y la civilización hindú (con India como país preponderante)[45].

Sin embargo, como se ha expresado en estas páginas, las aplicaciones de IA en el dominio militar aportan indudables ventajas pero, también, importantes riesgos. Riesgos que provienen esencialmente de los desarrollos tecnológicos que se dan en este nuevo campo de actuación. No solo las consideraciones éticas, sino la posibilidad de que países contrarios aprovechen sus mejores potencialidades para convertir la IA en un arma de doble filo, volviéndose en contra de aquellos que supuestamente tienen grandes capacidades en sus desarrollos de inteligencia artificial. A lo que se une lo que hemos dado en llamar *cibervasallaje* o *cibercolonización* que hará que muchos países pasen a ser dependientes de otros y, por tanto, ocupen un lugar secundario en su peso

43 Ibíd.

44 PANDYA, J. *The Geopolitics of Artificial Intelligence*. Forbes. https://www.forbes.com/sites/cognitiveworld/2019/01/28/the-geopolitics-of-artificial-intelligence/?sh=25d27d1a79e1 (consultado el 25 de marzo de 2022).

45 OLIER, E. *Les guerres puniques du XXIe siècle*. Éditions L'Harmattan, París, 2022 (de próxima aparición).

geopolítico y geoeconómico a nivel global. Una circunstancia que aparece con nitidez en Europa donde los desarrollos tecnológicos en el campo de la inteligencia artificial quedan muy detrás de Estados Unidos, de China e incluso de Rusia.

A esto añadiríamos, aunque no es el caso central del presente artículo, a España, que se encuentra lejos de tener un sistema público-privado organizado para no perder el paso en las aplicaciones autóctonas relacionadas con la inteligencia artificial. Una necesidad que en el campo de la defensa se muestra absolutamente crucial para poder participar con independencia en los retos geopolíticos que presenta el siglo XXI. Sirva, por tanto, el presente artículo como una llamada de atención para poner en marcha con urgencia un plan integrado de aplicaciones de IA en la defensa española, en el que las FAS deberán ser el motor de dicha integración, con mandos y personal especializado y con un programa específico que analice, desarrolle y englobe todas las capacidades disponibles. Más que un reto, se trata de una necesidad imperiosa.


ieee.es
Instituto Español de Estudios Estratégicos