ARI 93/2018
24 de julio de 2018

# Inteligencia artificial y poder

**José María Blanco** | Director de Ciberinteligencia Estratégica, Prosegur | @BlancoJoseMaria

**Jessica Cohen** | Coordinadora de la Unidad de Análisis Seguridad Internacional, Prosegur | @JessicaCohenV

## Tema

La Inteligencia Artificial aparece como uno de los avances más disruptivos de los próximos años, configurando el poder geoestratégico del futuro, al igual que la evolución social.

## Resumen

La implementación de aplicaciones de Inteligencia Artificial (IA) en sociedades e industrias puede suponer un cambio de carácter disruptivo, que configure una nueva distribución de poder geoestratégico. Entramos en una era donde la denominada IA "fuerte" trata de emular las habilidades cognitivas humanas creando oportunidades y riesgos para la seguridad política, económica, física y del ciberespacio. En consecuencia, las mayores potencias mundiales han iniciado una carrera con el objetivo de liderar las capacidades generadas por el uso de la IA, que se presenta como un indicador del presente y futuro liderazgo internacional, tal y como se describe en este ARI.

## Análisis

En septiembre de 2017 el presidente ruso, Vladimir Putin, advirtió que la Inteligencia Artificial (IA) "es el futuro, no sólo para Rusia, sino para la humanidad", añadiendo que ofrece "oportunidades colosales, pero también amenazas difíciles de predecir" y que "quien sea capaz de liderar esta esfera liderará el mundo". Destacó los riesgos de que alguna nación adquiera una posición monopolística, ofreciendo que "si nosotros nos convertimos en líderes en esta área, compartiremos el conocimiento con todo el mundo, al igual que lo hacemos con las tecnologías nucleares actualmente". No es el primer aviso sobre una evolución que se presenta como disruptiva. Stephen Hawking llegó a señalar que "podría ser el mayor suceso de la historia de nuestra civilización. O el peor. No lo sabemos aún". En términos prospectivos, estaríamos ante un claro "game changer", un factor de cambio de elevado impacto, tanto positivo como potencialmente negativo.

La mayor ventaja de la IA estaría en su capacidad para resolver problemas complejos, para los cuales las capacidades humanas son limitadas. En el actual entorno de disponibilidad de datos masivos, influidos adicionalmente por procesos de desinformación y manipulación, el ser humano es incapaz de identificar relaciones, extraer patrones y realizar inferencias y predicciones, sin disponer de una ingente

capacidad computacional. Por ello se asocia la IA a la inteligencia desarrollada para las máquinas. La expresión fue acuñada por John McCarthy en 1956, referida a "la ciencia e ingenio de hacer máquinas inteligentes, especialmente programas de cómputo inteligentes", lo que equipararía la IA a una rama de las ciencias computacionales encargada de desarrollar modelos de cómputo capaces de realizar tareas de los seres humanos, simulando razonamiento y conducta. Otros autores como Nils J. Nilsson, creen que la IA se refiere a cualquier tecnología que puede actuar con capacidad predictiva sobre su entorno, apoyada en algoritmos, redes neuronales artificiales y razonamiento mediante lógica formal.

Arend Hintze señala dos tipologías de IA de naturaleza disruptiva ya existentes: máquinas reactivas, que predicen en escenarios planteados, como Deep Blue, el programa de IBM que venció al ajedrez a Garry Kasparov; o IA de memoria limitada, que utiliza experiencias pasadas para informar el futuro. También define dos categorías aún inexistentes: 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). La criticidad actual deriva del paso de una IA "débil" a una IA "fuerte". En la primera, los sistemas son entrenados para tareas muy concretas y se han incorporado a multitud de desarrollos tecnológicos como Siri en Apple o la proliferación de chatbox. La verdadera disrupción se producirá en la segunda por la disponibilidad de datos, el incremento de la capacidad de computación y la reducción de su coste, y la mejora de los algoritmos. Este avance acercará la IA a las habilidades cognitivas humanas de forma generalizada y el factor diferenciador será la capacidad de computación, algo que no está al alcance de todas las naciones según Helen Lavoux. Para ello, esta nueva ola de IA se apoya en el *deep learning*, el *machine learning*, el procesamiento de lenguaje natural, el análisis predictivo, el reconocimiento de imagen y texto, la computación gestual, la realidad aumentada, la robótica y el reconocimiento emocional y, todo ello con el apoyo de la ciencia de datos, como se indica en el White Paper de la consultora Evry.

La interconexión de sistemas basados en IA puede generar fallos o ciberataques, con elevado impacto económico en sectores como el de las infraestructuras críticas. Según el Barómetro de Riesgo de Allianz 2018 el impacto de la IA y otras tecnologías es el séptimo riesgo empresarial, por encima del riesgo político o el cambio climático. La IA aumenta el riesgo de que las máquinas y los algoritmos acaben adoptando las decisiones, el de que algunos Estados la utilicen para el control social de los ciudadanos o para reforzar su competencia geopolítica a nivel internacional, incluidas las guerras de información y desinformación. Según el mismo Barómetro, los ciudadanos se arriesgan a perder su privacidad, a que sus propios dirigentes configuren sus opiniones o a que se acentúe su exclusión según estén preparados o no para este nuevo entorno industrial y laboral. En el plano seguritario, existe el riesgo de que aparezcan fallos en los sistemas de IA, que se utilicen robots autónomos en los conflictos o en que se materialice la distópica "singularidad", un escenario en el que la inteligencia artificial, superior a la humana, tomaría el poder. Lo anterior explica que algunos expertos, entre quienes el filósofo Nick Bostrom destaca a Bill Gates o Elon Musk, o instituciones como el Parlamento Europeo, hayan comenzado a evaluar y advertir sobre los riesgos de la IA.

El sector de la ciberseguridad es uno de los que, en mayor medida, están siendo afectados por la IA. En el aspecto positivo, está contrastada su capacidad para reducir las ciberamenazas, mejorando la detección de ataques. Pero en la carrera por su utilización también están involucrados grupos de crimen organizado y hackers, que recurren crecientemente a la IA para perfilar los ataques, seleccionar un mayor número de objetivos de forma más dirigida y menos indiscriminada y mejorar su eficiencia pudiendo ser replicados en numerosos equipos. Para este fin, la IA se combinará con la tradicional ingeniería social. Se ha llegado a estimar que un ciberataque global pudiera llegar a generar pérdidas de 50 billones de dólares. Adicionalmente, la IA podría ser una vía para hackear dispositivos conectados a internet, vehículos o drones, tomando el control de los mismos con intenciones delictivas o criminales.

Para contrarrestar los riesgos se está trabajando sobre la gobernanza nacional e internacional de la IA. La Administración Obama elaboró en 2015 el Informe "Preparing for the future of IA", en línea con los publicados sobre "Big Data: Seizing Opportunities, Preserving Values" y "Big Data and Privacy: A Technological Perspective" en 2014, para valorar los impactos de la IA sobre individuos y sociedad, una línea emulada por algunas estrategias posteriores de seguridad nacional. En el mismo sentido, otros estados y organizaciones internacionales comienzan a tomar conciencia de los riesgos del ciberespacio. Por ejemplo, la nueva Estrategia de Seguridad Nacional española dedica varias reflexiones acerca de las denominadas amenazas híbridas, aquellas que combinan diferentes formas de ataque, tradicionales y no tradicionales, como los ciberataques o la manipulación de la información. Recoge, de esta manera, uno de los mayores riesgos a los que se están enfrentando las democracias en todo el mundo, procesos de desestabilización promovidos desde el exterior por actores tanto estatales como no estatales, y que tratan de polarizar y fragmentar nuestras sociedades. La salud de los sistemas democráticos depende de la existencia de un entorno informativo que garantice la pluralidad y la diversidad y un desarrollo malicioso de la IA puede ponerle en peligro automatizando "paquetes" de desinformación y viralizarlos a través de la multiplicidad de canales informativos existentes, de forma escalable y efectiva. Para ello, la IA utilizará los metadatos para perfilar objetivos, extraer patrones y definir vectores de ataque.

En el plano internacional, los expertos vienen solicitando la creación de una Agencia Internacional de Inteligencia Artificial, dependiente de Naciones Unidas, para alertar ante nuevos riesgos, debatir los aspectos éticos, prevenir una nueva fractura digital entre diferentes naciones y ciudadanos y asegurar transparencia en la investigación de la IA. A la construcción de esa gobernanza de la IA, todavía por elaborar, podría ser de utilidad la experiencia recorrida por la ciberseguridad en materia de gobernanza, lo que lleva a algunos expertos a proponer a este campo como el modelo a seguir a la hora de extender el uso de esta innovación a otras áreas. En este sentido, la clave radica en el aprovechamiento de las lecciones aprendidas y la selección de buenas prácticas en ciberseguridad, para utilizar la IA en aras de la seguridad y contrarrestar su uso malicioso, y su exportación a otros sectores, según un reciente estudio conjunto de varios think-tanks especializados sobre "The Mallicious Use of AI: Forecasting, Prevention and Mitigation". Con dicho fin, sería de interés la implementación de equipos de hackeo ético (*red teams*), sistemas de verificación formal e implementación de controles de seguridad en todo dispositivo conectado, teniendo en cuenta la ausencia

de principios de “security by design” en muchos de los productos que se ofrecen en el mercado y los que se ofrecerán dentro del denominado “Internet de las Cosas” (IoT en sus siglas inglesas).

## Inteligencia Artificial y poder

Mientras se construye la gobernanza internacional y se toma conciencia de los cambios asociados a la IA, las potencias internacionales tratan de provechar su poder disruptivo para cobrar ventaja sobre el resto de estados principalmente en tres dimensiones de poder: la económica, la militar y la informativa, según un estudio del 00 Center sobre “Artificial Intelligence and National Security”. La inversión internacional en IA ha venido creciendo desde 2010 en torno al 60% anual, lo que permite incrementar el cociente de inteligencia artificial de las empresas (Boost Your AIQ) de Accenture. Las estimaciones señalan que ya en 2018, el 20% del negocio global estará relacionado con la IA y, en 2020, realizarán el 85% de las interacciones entre empresas y clientes de servicios. La IA podría contribuir con 12,8 trillones de euros a la economía global en 2030 (7,4 debidos a venta de nuevos productos y 5,4 por mejora de la productividad), suponiendo un incremento del 14% del producto interior bruto global. De acuerdo con otro estudio del Mckinsey Global Institute sobre “AI, the Last Digital Frontier?”, los gigantes tecnológicos que lideran digitalización son quienes más están invirtiendo en IA (entre dos y tres cuartas partes de los 26-39 billones de dólares en 2016). A continuación, se situaría el sector de la automoción, el de los servicios financieros, energía y recursos, medios y entretenimiento, transporte y logística. Y aunque es difícil separar la inversión en las diferentes áreas que formarían parte de la IA, se estima que se dedicaron al *machine learning* entre 5 y 7 billones.

En la dimensión militar se está produciendo una carrera entre las principales potencias del mundo para optar al liderazgo geoestratégico, geopolítico y geoeconómico. La irrupción de la IA altera las capacidades ofensivas y defensivas, como ya sucedió con la tecnología aeroespacial, la nuclear, la cibernética y la biotécnica. La IA posibilitará introducir autonomía o semi-autonomía en robots, acelerará el uso de aviones de combate no tripulados, desarrollará artefactos explosivos improvisados móviles y robóticos y se incorporará a sistemas armamentísticos (lethal autonomous weapon systems).

El rango internacional en IA se puede medir por la cuota de mercado que representa cada país, lo que colocaría a Estados Unidos, seguido de China e Israel a la cabeza de la carrera global. También se puede medir por otros indicadores de posicionamiento internacional obtenidos del Times Higher Education, coincidentes con los que presenta Scopus, que tienen en consideración criterios académicos como el número o el de artículos de investigación realizados. Otros indicadores, como los aportados por Indeed, tienen que ver con la demanda de puestos de trabajo relacionados con IA que ha aumentado un 119% entre 2015 y 2018. Liderando Estados Unidos la demanda según el Informe de IA de 2017.

Varios son los países que se están posicionando en la carrera de la IA. Una revolución que “no sucederá en 50 o 60 años, está sucediendo ahora mismo”, como afirmaba el propio Emmanuel Macron esta primavera. Estados Unidos y China, son consideradas

en la actualidad las dos principales potencias en investigación y desarrollo de IA, aunque las autoridades de la segunda están mucho más concienciadas que las de la primera según medios de comunicación como el *New York Times*. Estados Unidos se ha centrado en los últimos años en disponer de una de las mayores fuerzas académicas en IA, un desarrollo controlado en su mayoría por manos privadas, seguido de inversiones militares o de servicios de inteligencia, como son los organismos de IARPA y DARPA. Evidencia no lejana de las pretensiones de Trump quien, desde su llegada al poder, ha manifestado su intención de poner el desarrollo de la IA al servicio de la mejora de la economía, pero, también de la seguridad nacional, pese a haber recortado la inversión prevista para 2018 en un 15%. China ha optado por mantener una agresiva inversión pública, en torno a 7.000 millones de dólares anuales, dentro de un ambicioso plan nacional de acción para generar una industria de 150.000 millones en 2030.

Israel presenta la tercera mayor cuota de mercado de IA del mundo con una inversión directa estimada en 1.100 millones durante 2017, año en el que siete compañías de titularidad israelí figuran entre las más avanzadas del mundo en materia de IA según clasificaciones privadas. La conexión que tradicionalmente ha existido entre el ejército israelí y la industria tecnológica del país, así como una fortificada estructura académica y una madura tradición emprendedora son variables que favorecen esta situación. Japón cuenta con un presupuesto estimado en 720 millones de euros para 2018, muy lejos del invertido por su vecina China. Canadá ha optado por la vía de la financiación público-privada para potenciar los proyectos de emprendimiento relacionados con la IA, elevando la oferta formativa y de investigación en este campo a cargo del Departamento de Finanzas. Rusia, a pesar de contar con un discreto presupuesto de 12.5 millones de euros para IA, parece dispuesta a invertir en sectores específicos como el militar.

En el contexto europeo, la Comisión Europea acaba de presentar su estrategia sobre IA que tiene como objetivos impulsar la capacidad industrial europea en IA bajo un enfoque ético y legal acorde a los cambios que este avance generará y preparase para los cambios socioeconómicos. Más allá de estas premisas, será una Alianza Europea de IA la encargada de redactar, antes de finalizar 2018, los borradores por los que se desarrollará el futuro de la IA en Europa. En tanto se produce este escenario, los principales avances europeos en esta tecnología se han dado bajo la envergadura de los proyectos Horizonte 2020, aunque aún con limitados resultados. El presidente Emmanuel Macron ha anunciado una inversión de 1.500 millones de euros hasta 2020, centrando su estrategia de crecimiento en el enfoque en la disponibilidad y uso de los datos de la IA. En abril de 2018, Angela Merkel confirmaba la intención de Alemania de competir en la carrera de la IA, nombrando incluso la intención de desafiar la hegemonía China, aunque sin mencionar acciones o inversiones concretas. Esta situación, que puede ser más próxima a la posición de Reino Unido dadas las limitaciones presupuestarias con las que cuenta, se ve sin embargo reforzada por la creación, bajo fondos de inversión extranjera liderados por Amazon, del cuarto mayor centro de investigación de IA del mundo, sito en Berlín. El Reino Unido mantiene una línea, tanto pública como privada, de respaldo a proyectos con una inversión prevista que ronda los 200 millones de dólares y enfocada a promocionar aquellas líneas de investigación que promuevan ventajas competitivas, dentro de una enfoque ético. Finalmente, España está lejos de rivalizar con estas iniciativas y aún no cuenta con estrategia y presupuesto, aunque trabaja desde 2017 en la redacción de un libro blanco sobre la materia.

## Conclusiones

En atención a las diferentes estrategias en materia de IA que mantienen las principales potencias mundiales, es posible observar, entre otros factores, un desarrollo orientado a favorecer los intereses geopolíticos y geoeconómicos nacionales. Este tipo de enfoque, si bien sigue la pauta histórica de cómo los estados-nación se han centrado en la defensa de sus propios intereses, contradice tanto el alcance como los efectos que una tecnología así es susceptible de tener, cuyo impacto solo se puede medir en términos globales.

Un desarrollo que, hasta la fecha, se ha centrado principalmente en fomentar la investigación, tanto pública como privada, postergando a un segundo plano el enfoque de uso de esta tecnología en la solución de problemas reales según el estudio sobre el "Global Artificial Intelligence Landscape". A medida que surgen alertas sobre los riesgos derivados de un uso pernicioso de la IA se incrementa la necesidad de introducir perspectivas integrales, basadas en análisis de riesgos y que traten de equilibrar los intereses públicos y privados, en beneficio de nuestras sociedades.
Pese a los efectos eminentemente tecnológicos, pero también económicos, sociales y éticos que la IA es susceptible de generar, pocos son los países que tiene en cuenta estas variables en la definición de sus estrategias. Reino Unido y Francia son algunos de los ejemplos, exponiendo de manera directa que su preocupación va más allá de la propia inversión, los avances y su posicionamiento internacional.

Finalmente, las experiencias que se vienen desarrollando en el ámbito de la ciberseguridad, donde la IA presenta un claro doble uso, puede ser un modelo, a través de la extracción de lecciones aprendidas y determinación de buenas prácticas, extrapolable a otros sectores en los que la IA podrá tener un papel determinante.