Cuadernos de Estrategia 226

La inteligencia artificial en la geopolítica y los conflictos

Instituto Español de Estudios Estratégicos

ieee.es
Instituto Español de Estudios Estratégicos

MINISTERIO DE DEFENSA

Cuadernos de Estrategia 226

La inteligencia artificial en la geopolítica y los conflictos

Instituto Español de Estudios Estratégicos

ieee.es
Instituto Español de Estudios Estratégicos

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de Defensa
https://publicaciones.defensa.gob.es

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

publicaciones.defensa.gob.es

cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA

SUBSECRETARÍA DE DEFENSA

SECRETARÍA GENERAL TÉCNICA

Paseo de la Castellana 109, 28046 Madrid

NIPO 083-24-201-3 (edición impresa)
ISBN 978-84-9091-933-0 (edición impresa)

NIPO 083-24-202-9 (edición en línea)

Cuadernos de Estrategia, ISSN 1697-6924 (edición impresa)
Cuadernos de Estrategia, ISSN 2952-3443 (edición en línea)

Depósito legal M 14839-2024
Fecha de edición: junio de 2024
Maqueta e imprime: Imprenta Ministerio de Defensa

ÍNDICE

Página

Capítulo primero

Panorama internacional de la inteligencia artifical en las actividades de defensa y seguridad

Eduardo Olier Arenas

Resumen

La inteligencia artificial (IA) se ha convertido en los últimos años en un elemento esencial en muchas actividades económicas y sociales. La aparición de nuevos sistemas de IA con sus múltiples aplicaciones ha puesto a este conjunto de tecnologías en el centro de muchas discusiones respecto a sus efectos positivos o negativos. Independientemente de esta discusión, hay un aspecto de la inteligencia artificial que afecta a los sistemas de defensa y seguridad. Un hecho que tiene ya un relevante papel en muchos países, que ven estas tecnologías como uno de los ejes de predominio geopolítico. Con esta perspectiva se ha establecido el presente Cuaderno de Estrategia del Instituto Español de Estudios Estratégicos (IEEE) que trata de un inicio que esperamos que se vaya complementando con otros análisis más específicos en el futuro.

Palabras clave

Inteligencia artificial, defensa, seguridad, geopolítica.

International panorama of artificial intelligence in defence and security activities

Abstract

Artificial intelligence (AI) has become in recent years an essential element in many economic and social activities. The emergence of new AI systems with their multiple applications has put this set of technologies at the centre of many discussions regarding their positive or negative effects. Regardless of this discussion, there is one aspect of Artificial Intelligence that affects defence and security systems. A fact that already plays a relevant role in many countries, which see these technologies as one of the axes of geopolitical predominance. It is from this perspective that this Strategy Notebook of the Spanish Institute for Strategic Studies (IEEE) has been established, which is intended as a beginning that we hope will be complemented by other more specific analyses in the future.

Keywords

Artificial intelligence, defence, security, geopolitics.

1. Introducción

Dada la popularidad que ha alcanzado la inteligencia artificial, conviene, aunque sea un dominio muy conocido por los especialistas, hacer una somera síntesis de lo que encierra este, supuestamente, «nuevo» campo tecnológico.

Hay que remontarse al pasado siglo y considerar a John McCarthy, profesor del Massachusetts Institute of Technology (MIT), como el primero en usar el término de inteligencia artificial, en 1956, durante una conferencia en el Dartmouth College. Allí estuvo también otro profesor, Marvin Minsky de la Carnegie-Mellon University, que utilizó el mismo término para definirlo como «la ciencia de conseguir que las máquinas hagan tareas que requerirían inteligencia en caso de que fueran hechas por el ser humano». Dicho de otra manera, la inteligencia artificial era, para estos científicos pioneros, «la ciencia que construye programas informáticos que permiten a las máquinas llevar a cabo ciertas tareas más satisfactoriamente que los seres humanos». En definitiva: programas informáticos que utilizan técnicas como, por ejemplo: el aprendizaje perceptivo de las máquinas, la organización de la memoria electrónica o el razonamiento crítico de los sistemas informáticos. Una disciplina que, hoy, se conoce bajo el acrónimo de IA.

Ya se entiende, por tanto, que se trata de un conjunto de técnicas que incluyen diversas especialidades. Nada que ver con lo que se entiende hoy en día como una sola actividad tecnológica que hubiera surgido «de golpe».

Ciertamente, años antes, en 1950, Alan Turing, publicó un artículo en la revista *Mind* que puede ser considerado como el inicio de lo que entonces no se sospechaba que pudiera tener tanta trascendencia. Lo tituló: *Computing Machinery and Intelligence* (Turing, 1950; Hofstadter, 1987). Una indudable premonición de lo que ha venido después.

En dicho artículo Turing se planteaba la siguiente cuestión: «¿Pueden pensar las máquinas?» Una pregunta que, para aquel autor, le conducía a otras dos: definir, primero, que se entiende por «máquina»; y, segundo, qué significa «pensar».

Ante la aparente dificultad que tenía para Turing entrar en estos dos conceptos, decidía en su artículo dirigirse hacia otro problema que el describe como una suerte de juego que denomina «juego de imitación», que se daba en un escenario con tres personas, dos

de las cuales, hombre y mujer, estaban en una sala y una tercera en otra habitación, desde dónde les hacía preguntas a las otras dos para identificar el sexo de cada una de ellas. Para Turing, la pregunta de «si pueden pensar las máquinas» sería similar a cambiar una de las personas de la habitación —el hombre o la mujer— por una máquina y seguir el proceso de identificación. Entonces, el interrogador continuaría con las preguntas sin llegar nunca a la conclusión de que el hombre o la mujer fueran en realidad un computador digital. Es decir, la máquina en cuestión debería reaccionar como un ser humano persona ante las preguntas de la persona que se encuentra sóla en la otra habitación.

En definitiva, la máquina de Turing debería ser capaz, al menos, de resolver cuatro problemas de manera automática:

- Ser capaz de comunicarse en el idioma en que se la hicieran las preguntas (para lo cual debería ser capaz de procesar el lenguaje natural y proceder a responder en el idioma en que se hicieran las preguntas).
- Tener la posibilidad de representar el conocimiento a partir de lo que escuchara.
- Almacenar la información a fin de contestar razonablemente a las preguntas que se la hagan, sacando sus propias conclusiones de forma automática.
- Contar con la capacidad de adaptarse a nuevas situaciones con comportamientos coherentes; es decir, entre otras cosas, aprender.

Para lograr parecerse al comportamiento humano, tal máquina debería contar con la capacidad adicional de percibir visualmente objetos y, a la vez, poder moverse para manipular dichos objetos, lo que se entiende hoy como robótica. Una serie de atributos que, en el extremo, llevaría a tal computadora[1] a tomar decisiones y procesar la información recibida de manera similar a cómo funciona el cerebro y el sistema neuronal humano.

Actualmente, las aplicaciones de la inteligencia artificial (IA) son múltiples. Un conocido ejemplo serían los vehículos autónomos, que combinan decenas de sensores con cámaras, radares, y telémetros, para detectar el entorno; a lo que se añaden los necesarios desarrollos de *software* que permiten, con base en la información recibida, controlar la dirección del vehículo,

[1] Utilizaremos de manera indistinta los términos computadora, computador u ordenador, para referirnos a máquinas programables, tal como se usa en idioma español en diferentes geografías.

frenándolo o acelerándolo de manera correcta. Otra muestra, también conocida, sería el reconocimiento de voz, muy usado en ciertos servicios de atención de clientes mediante los cuales es posible tener una conversación guiada por un sistema automatizado de reconocimiento de voz y gestión del diálogo.

De la misma manera que existen sistemas de planificación y programación automáticos, usados, por ejemplo, en ingenios espaciales en los que «agentes remotos» pueden tomar decisiones a partir de objetivos preprogramados, teniendo la capacidad adicional de detectar y diagnosticar situaciones específicas sin el concurso humano.

En el contexto de este *Cuaderno de Estrategia* dedicado a la IA y sus aplicaciones a la defensa y la seguridad, es conveniente hablar de los sistemas de planificación logística y de operaciones, como el utilizado durante la crisis del Golfo allá por 1991. En aquel caso, el sistema DART fue capaz de realizar, de manera automátical la planificación logística de 50 000 vehículos, con sus cargas y transporte de personas, teniendo en cuenta puntos de partida, destinos, rutas y la resolución de conflictos entre todos los parámetros con que contaba el proceso. O, de manera similar, el sistema PackBot, desarrollado por la empresa iRobot Corporation, bien conocida por su aspirador doméstico Roomba, que puso en práctica un sistema robotizado para el ejército americano, que fue utilizado en Irak y Afganistán para manipular de manera automática materiales peligrosos, y retirar explosivos e, incluso, identificar la ubicación de francotiradores.

Lo anterior, aún sin mencionarlo, tiene su correspondencia con lo que en el contexto de la IA se denominan «agentes»: esos elementos que, a través de sensores, son capaces de actuar en un entorno determinado. Una circunstancia similar a un agente humano que utiliza como «sensores» los ojos, los oídos, y otros órganos del cuerpo, ejecutando sus acciones mediante las manos, las piernas, la voz, etc. Las órdenes del cerebro en este caso serían los programas de *software* que dictan las acciones que debe acometer el robot en cuestión.

En el caso de una máquina, el *software* deberá estar diseñado para que el agente se comporte «racionalmente»; es decir:

- Que tenga una medida de su capacidad de éxito.
- Que tenga suficiente «conocimiento» del entorno.
- Que sea capaz de realizar las acciones que se le soliciten.
- Que tenga un control de la secuencia de percepciones y acciones a llevar a cabo.

Lo que lleva a la necesidad de dotar a esa máquina de otras funcionalidades como son la autonomía y la capacidad de aprender. Aspectos que pueden ser implementados en la actualidad, pero que quedan aún lejos de las capacidades humanas como sería el caso de lo que se conoce como omnisciencia, que no es sino evaluar el resultado real de las acciones llevadas a cabo y actuar en consecuencia.

De manera general, lo anterior conduce a tener en cuenta que la IA es un conjunto de disciplinas que tienen cada una de ellas desarrollos independientes, aunque pueda darse el caso de complementariedades, en tanto que, de manera sintética, la IA se asienta en tres elementos fundamentales:

- Complejos sistemas de procesamiento electrónico, basados en avanzadas tecnologías digitales.
- Pueden procesar complejos algoritmos.
- Gestionan enormes volúmenes de datos (estructurados y no estructurados) a una enorme velocidad (Olier y Corchado, 2022).

Es decir: computadoras muy eficientes, algoritmos altamente complejos, y gran cantidad de datos, que se abren en una ramificación de tecnologías como muestra, a modo de ejemplo, la figura 1 (Russell y Norvig, 2004).

Aunque se comentará más adelante, el presente *Cuaderno de Estrategia* del Instituto Español de Estudios Estratégicos (IEEE),

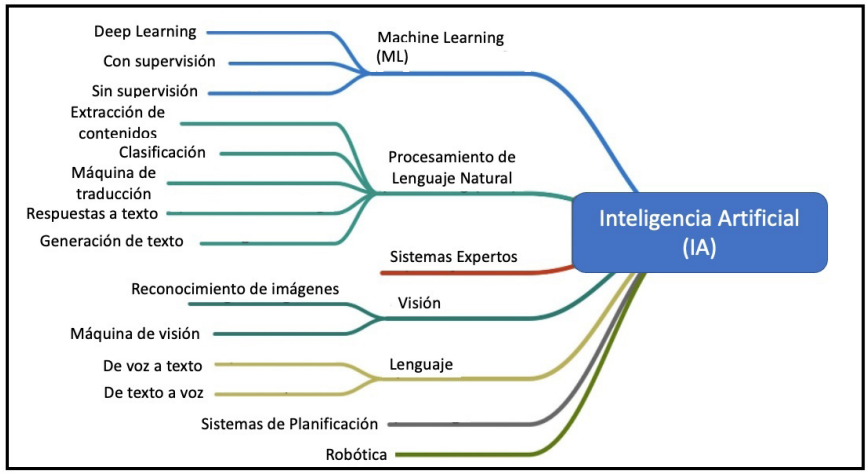


Figura 1. Algunas tecnologías utilizadas en sistemas de IA (Olier y Corchado, 2022)

es un primer análisis sobre las aplicaciones de la IA para la defensa y seguridad. En su ejecución se ha contado con reconocidos expertos, nacionales e internacionales, cuya visión ofrece un panorama general que deberá servir, si así se considera, para otros trabajos futuros más específicos.

En otro orden, cabe decir que las grandes potencias han apostado por la IA como un nuevo mecanismo de supremacía geopolítica y geoeconómica del que ningún país avanzado, como es el caso de España, debería quedarse atrás, ya que los nuevos ingenios de defensa y seguridad estarán, en el futuro, fundamentados en estas nuevas disciplinas que, como se ha apuntado más arriba, ofrecen diversas ramificaciones, todas ellas pilares esenciales en las nuevas estrategias de defensa y seguridad, en las cuales el elemento humano deberá estar altamente entrenado para ser capaz de gestionar de forma adecuada los nuevos tipos de conflictos, que serán más tecnológicos y más autónomos que en el pasado.

2. Breve comentario sobre las estrategias de IA

2.1. Plan estratégico de Estados Unidos

En mayo de 2023, bajo la dirección de Arati Prabhakar, director de la Oficina de Política de Ciencia y Tecnología del Gobierno de Estados Unidos (*Office of Science and Technology Policy,* OSTP), que asiste al presidente de Estados Unidos en los asuntos relacionados con ciencia y tecnología, se publicó el *Plan Estratégico Nacional de Investigación y Desarrollo de IA*[2], que cuenta con nueve elementos estratégicos que tratan, en concreto, de: inversiones (estrategia 1); colaboración entre seres humanos y la IA (estrategia 2); aspectos éticos, legales y sociales (estrategia 3); asuntos que aseguren la seguridad y protección de los sistemas de IA (estrategia 4); desarrollar entornos públicos y datos compartidos para entrenar la IA (estrategia 5); estándares y criterios de referencia (estrategia 6); evaluación de las necesidades de investigadores en el campo de la IA (estrategia 7); alianzas público-privadas para potenciar los desarrollos en IA (estrategia 8); y de desarrollo de programas de cooperación internacional (estrategia 9).

[2] Véase: https://www.whitehouse.gov/wp-content/uploads/2023/05/National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf. [Consulta: 11 de diciembre de 2023].

La estrategia 1 incorpora un interesante programa enfocado a la fabricación de semiconductores, que menciona la Ley aprobada en 2022 por el Congreso de Estados Unidos bajo la denominación: *Chips and Science Act*[3], que muestra de manera determinante la necesidad que tiene Estados Unidos, al igual que otros países, de mantener una independencia en este tipo de tecnologías, en tanto que la IA precisa de ordenadores digitales cada vez más potentes. Computadoras, en definitiva, que precisan de una enorme potencia de cálculo para gestionar los programas de IA, los algoritmos que los sostienen y la gran cantidad de datos que se han de manipular con técnicas de *big data*. Un aspecto que tiene unas consecuencias geoeconómicas para tener en cuenta.

La ley de ciencia y semiconductores estadounidense establece, entre otros aspectos, un importante programa de inversiones en cuatro apartados:

- Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America Fund.
- Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America Defense Fund.
- Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America International Technology Security and Innovation Fund.
- Creating Helpful Incentives to Produce Semiconductors (CHIPS) for America Workforce and Education Fund.

Que totalizan, entre todos ellos, incluidos fondos y préstamos aportados por el Gobierno americano, unos 60 000 millones de dólares para el período 2023-2027. Una estrategia que, como puede verse, se dirige de manera inequívoca a dotar a Estados Unidos de mayores capacidades en defensa y seguridad alrededor de estas nuevas tecnologías y, fundamentalmente, de incorporar nuevas capacidades en IA. Toda una serie de iniciativas en las que no es ajeno el Departamento de Defensa americano que, en septiembre de 2023, llevó a cabo la creación de una nueva entidad[4] (*AI Security Center*) para supervisar el desarrollo e integración de las capacidades de inteligencia artificial de los sistemas de seguridad nacional del país. Un centro esencial para la seguridad de Estados Unidos que será el punto focal para el desarrollo de

[3] Disponible en: https://www.congress.gov/117/plaws/publ167/PLAW-117publ167.pdf. [Consulta: 11 de diciembre de 2023].

[4] Véase: https://www.defense.gov/News/News-Stories/Article/Article/3541838/ai-security-center-to-open-at-national-security-agency/. [Consulta: 13 de diciembre de 2023].

mejores prácticas, metodologías de evaluación y estrategias de riesgo, con el objetivo de promover la adopción segura de nuevas capacidades de IA en todo el contexto de seguridad nacional y, adicionalmente, constituir la base industrial de la defensa. Un centro que coordinará todas las actividades relacionadas con la inteligencia artificial y la seguridad. Unas iniciativas que, unidas a otras, dotarán a Estados Unidos de una potente estructura de IA para los complejos tiempos del siglo XXI.

2.2. Estrategias de China

Analizar las estrategias de China respecto de la IA puede hacerse de dos maneras distintas. La primera, sería ver lo que opinan los diversos organismos occidentales al respecto. Y, una segunda, ver lo que el propio Gobierno chino pretende, contando siempre con la dificultad de desentrañar lo que se encuentra detrás de estos planteamientos.

Yendo al segundo caso —la estrategia de IA de China desde China—, se puede encontrar que, al menos desde 2017, el Gobierno chino tiene en marcha un decidido plan de desarrollo de la IA. Aquel año, fue el Consejo de Estado de China quien publicó una circular denominada: *Plan de Desarrollo de la Nueva Generación de Inteligencia Artificial*[5]. En su preámbulo, este documento indica que:

> «El rápido desarrollo de la inteligencia artificial cambiará profundamente la vida de la sociedad humana y cambiará el mundo. Con el fin de aprovechar las grandes oportunidades estratégicas para el desarrollo de la inteligencia artificial, siguiendo los requisitos del Comité Central del PCCh[6] y del Consejo de Estado, se llevará a cabo la formulación de este plan para construir las ventajas de China como pionera en el desarrollo de la inteligencia artificial, acelerando la construcción de un país innovador y una potencia mundial en ciencia y tecnología».

Un planteamiento inicial que continúa diciendo:

> «La inteligencia artificial aporta nuevas oportunidades para la construcción social. China se encuentra en una fase deci-

[5] Disponible en: https://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm. [Consulta: 19 de diciembre de 2023].

[6] Partido Comunista de China.

> siva en la construcción de una sociedad moderadamente próspera en todos los aspectos, aunque los retos del envejecimiento de la población y las limitaciones de recursos, así como las medioambientales siguen siendo graves. La amplia aplicación de la IA en los campos de la educación, la atención médica, las pensiones, la protección medioambiental, el funcionamiento urbano y los servicios judiciales, mejorará enormemente el nivel de precisión de los servicios públicos y mejorará de forma integral la calidad de vida de las personas. Las tecnologías de inteligencia artificial pueden percibir, predecir y advertir con precisión, los principales acontecimientos en las operaciones de infraestructura y seguridad social, captar a tiempo los cambios cognitivos y psicológicos del grupo y tomar la iniciativa en la toma de decisiones y la respuesta, lo que mejorará significativamente la capacidad y el nivel de gobernanza social y desempeñará un papel insustituible en el mantenimiento eficaz de la estabilidad social».

El plan del Gobierno chino de IA continúa con una serie de propuestas que se mueven en todos los aspectos que rigen el desarrollo de potentes sistemas de inteligencia artificial, incluyendo nuevas tecnologías de *big data*, computación perceptiva, inteligencia híbrida aumentada, mecanismos de inteligencia en grupo, aprendizaje automático, investigaciones sobre el comportamiento del cerebro humano y los mecanismos complejos que gestiona, así como los nuevos ordenadores basados en la computación cuántica que, como es conocido, pueden manipular múltiples estados entre los típicos «1» o «0» (circuito abierto o cerrado) de la *computación booleana* que tienen los sistemas tradicionales.

En lo referente a la defensa y seguridad, China, de nuevo, al igual que Estados Unidos mantiene una estrategia definida. El propio Gobierno chino tiene publicada *su Estrategia de inteligencia artificial para defensa y seguridad*[7], en cuyo texto se hacen afirmaciones como estas:

> «En el contexto de los desafíos multifacéticos a la paz y al desarrollo mundiales, todos los países deberían defender una visión común, integral, cooperativa y sostenible respecto de la seguridad global, buscando el consenso sobre cómo regular la aplicación militar de la IA mediante el diálogo y la coo-

[7] Disponible en: https://www.mfa.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/zclc_674645/rgzn/202206/t20220614_10702838.shtml. [Consulta: 20 de diciembre de 2023].

peración, construyendo un mecanismo de gobernanza eficaz y evitando que la aplicación militar de la IA provoque daños significativos o incluso desastres a la humanidad».

Para continuar, en el mismo texto, con una serie de indicaciones[8]:

«Para ello, pedimos:

1. En términos de seguridad estratégica, todos los países, especialmente las grandes potencias, deberían investigar, desarrollar y utilizar la tecnología de IA en el ámbito militar de forma prudente y responsable, sin buscar la superioridad militar absoluta, para evitar exacerbar los errores de cálculo estratégico, socavar la confianza mutua estratégica, desencadenar la escalada de conflictos y debilitar el equilibrio estratégico y la estabilidad mundiales.
2. En cuanto a la política militar, al desarrollar armas y equipos avanzados para mejorar las capacidades legítimas de defensa nacional, los países deben tener en cuenta que la aplicación militar de la IA no debe convertirse en una herramienta para hacer la guerra y perseguir la hegemonía, oponiéndose al uso de la superioridad tecnológica de la IA que pueda poner en peligro la soberanía y la seguridad territorial de otros países.
3. En términos de ética legal, la investigación y el desarrollo, el despliegue y el uso de los sistemas de armamento pertinentes por parte de todos los países deberían guiarse por los valores comunes de la humanidad, adherirse al principio centrado en las personas de "inteligencia para el bien" y cumplir las normas éticas y morales nacionales o regionales.
4. Se debería garantizar que las nuevas armas y sus medios de combate sean conformes con el derecho internacional humanitario y demás elementos del derecho internacional aplicable, esforzándose por reducir las víctimas colaterales y los daños a la propiedad de las personas, y evitar el uso indebido de los sistemas de armas con los consiguientes daños indiscriminados.
5. Seguridad tecnológica. Los Estados deben mejorar continuamente la seguridad, fiabilidad y controlabilidad de la tecnología de IA, mejorando su capacidad para evaluar y controlar la seguridad de la tecnología de IA, garan-

[8] *Ibid.*

tizando que los sistemas de armas estén siempre bajo control humano, y garantizando que los seres humanos puedan detener su funcionamiento en cualquier momento. Debe garantizarse la seguridad de los datos de IA y restringirse su uso militarizado.

6. Operaciones de investigación y desarrollo. Los Estados deben reforzar la autocontención en las actividades de investigación y desarrollo de sistemas de IA, e implementar la necesaria interacción humano-ordenador a lo largo de todo el ciclo de vida del arma sobre la base de una consideración exhaustiva del entorno operativo y las características del arma.
7. Los Estados deben insistir siempre en que el ser humano es el sujeto responsable en última instancia, estableciendo un mecanismo de rendición de cuentas en materia de IA y proporcionando la formación necesaria a los operadores.
8. Gestión y control de riesgos. Los Estados deberían reforzar la regulación de las aplicaciones militares de la IA, especialmente la implantación de una gestión graduada y categorizada, evitando el uso de tecnologías inmaduras que puedan traer graves consecuencias negativas.
9. Los Estados deben reforzar la investigación y el juicio de los riesgos potenciales de la IA, incluida la adopción de las medidas necesarias para reducir el riesgo de proliferación de las aplicaciones militares de la IA.
10. Los países deben adherirse a los principios de multilateralismo, apertura e inclusión, con el fin de seguir la tendencia de desarrollo de la tecnología y prevenir posibles riesgos para la seguridad.
11. Los países deberían llevar a cabo diálogos políticos, reforzando los intercambios con organizaciones internacionales, empresas de ciencia y tecnología, comunidades tecnológicas, instituciones civiles y otros organismos principales, mejorando el entendimiento y la colaboración, y comprometiéndose a regular conjuntamente la aplicación militar de la IA, estableciendo un mecanismo internacional universal participativo con el fin de promover la formación de un marco ampliamente consensuado de gobernanza de la IA, y sus estándares y normas.
12. En cuanto a la cooperación internacional, los países desarrollados deberían ayudar a los países en desarrollo a mejorar su nivel de gobernanza, teniendo en cuenta la

> naturaleza de doble uso de las tecnologías de IA y, al tiempo que refuerzan la regulación y la gobernanza, evitando adoptar la práctica de trazar líneas basadas en la ideología y generalizar el concepto de seguridad nacional, eliminando las barreras científicas y tecnológicas creadas artificialmente para garantizar que todos los países disfruten plenamente del derecho al desarrollo tecnológico y a su uso pacífico. Todos los países deberían disfrutar plenamente del derecho a los usos pacíficos de la tecnología».

Unos principios que, dadas las diferencias geopolíticas, serán de muy difícil aplicación, al menos, si no se establecen unos mecanismos de entendimiento globales en el uso y desarrollo de sistemas de IA.

En definitiva, en el caso chino, la estrategia de IA se dirige a tres capítulos como muestra la figura 2: geopolíticos, económicos y éticos, este último conectado de alguna manera con los dos anteriores, ya que en su interior se dirige al control económico, social y político, no solo a nivel nacional, sino a nivel global.

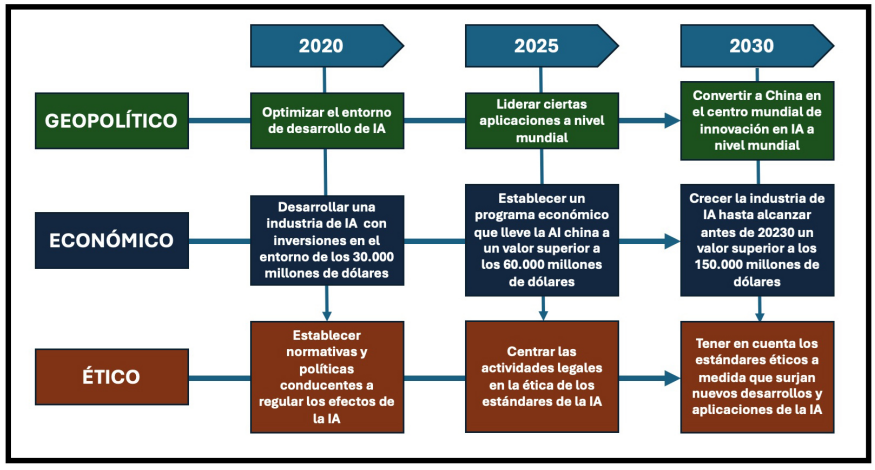


Figura 2. Esquema de la estrategia de China en IA (Roberts et al., 2021)

2.3. Japón y la IA

Conocido es que Japón es un indiscutible aliado de Estados Unidos. Japón, ante el creciente uso de la inteligencia artificial en los sistemas de defensa, se ha unido, con otros 44 países, a la iniciativa liderada por Estados Unidos para limitar el uso militar de este tipo de tecnologías. En este sentido, el Ministerio

de Asuntos Exteriores de Tokio declaró, en noviembre de 2023, que comparte el objetivo americano de reducir los riesgos y las incertidumbres que plantea la introducción de la IA en el ámbito militar[9]. A esto se han unido, por ejemplo: Alemania, Francia, Gran Bretaña, Canadá, Singapur y Corea del Sur. China y otras potencias «no alineadas», como la Federación de Rusia, quedan excluidas de estos acuerdos.

En paralelo, el Ministerio de Defensa japonés confirmó, en 2020, una inversión de unos 240 millones de dólares en un esquema público-privado (con empresas como Mitsubishi, NEC, Pasco Corporation o Kobe Steel) para el desarrollo de herramientas de seguridad basadas en IA para contrarrestar ciberataques. Paralelo a esta cifra, dicho ministerio había puesto en marcha otro programa de inversiones para construir un sistema de recopilación de información cibernética, con el objetivo de recoger información sobre tácticas, técnicas y procedimientos de potenciales ciberataques a entidades gubernamentales y privadas del país, ampliando los efectivos humanos del grupo de ciberdefensa[10]. Unas actividades que se han ido ampliando a los espacios marítimos y aeroespaciales[11].

Adicionalmente, Japón mantiene un programa de colaboración en el contexto de la IA que se puso de manifiesto en la última cumbre del G7 mantenida en Hiroshima en mayo de 2023. Allí se instó a la creación del llamado *Proceso de IA de Hiroshima del G7* (*G7 Hiroshima AI Process*) para armonizar los distintos marcos normativos y promover la coordinación de la gobernanza de la IA (Arisa *et al.,* 2023), en especial en lo que respecta a la IA generativa (United Nations Office of Information and Communications Technology, s.f.), capaz de crear nuevos datos similares a los originales que resultan difíciles de distinguir de los que hayan podido crear personas humanas. Una nueva disciplina, la IA generativa, que precisará, en nuestra opinión, un nuevo modelo de gobernanza global, más allá del que tratan de poner en práctica los países del G7. Unas estrategias que demuestran la política de Japón a la hora de buscar alianzas en sus entornos geopolíticos.

---

[9] Aunque hay muchas informaciones al respecto, damos esta simple nota de *The Japan Times*: Japan join U.S.-led effort to regulate military use of AI, puede servir de orientación. Disponible en: https://www.japantimes.co.jp/news/2023/11/14/japan/politics/japan-us-ai-military-declaration/. [Consulta: 23 de diciembre de 2023].

[10] Véase: https://cisomag.com/japan-embraces-ai-tools-to-fight-cyberattacks-with-us237-mn-investment/. [Consulta: 23 de diciembre de 2023].

[11] Disponible en: https://www.foxnews.com/world/japan-embraces-ai-boost-cyber-defense-fight-disinformation. [Consulta: 23 de diciembre de 2023].

2.4. La IA en Europa

En 2018, la Unión Europea (UE) creó un grupo de expertos para recabar su opinión y establecer las directrices éticas en el desarrollo e implementación de las diferentes estrategias y sistemas de IA en Europa. En principio, el grupo de expertos se apoyaba en la declaración del Grupo Europeo de Ética, de Ciencia, y de Nuevas Tecnologías de la Comisión Europea. Tres comisarios estaban involucrados: Andrus Ansip, vicepresidente de la comisión, responsable del Mercado Único Digital; Carlos Moedas, comisario responsable de Investigación, Ciencia e Innovación; y Mariya Gabriel, comisaria de Economía y Sociedad Digitales.

Después de este inicio, se pusieron en marcha una serie de iniciativas, manteniendo un diálogo en múltiples foros con diversos estamentos: sociedad civil, organizaciones empresariales y de consumidores, sindicatos, mundo académico, autoridades políticas, etc., a fin de abordar las posibilidades ofrecidas por la IA, así como los retos que se encuentran asociados a este tipo de nuevas tecnologías (European Commission, s.f.).

Todas esas acciones llevaron a establecer lo que se ha definido como la *Ley Europea de Inteligencia Artificial*, que se considera pionera en el mundo. Una ley que fue finalmente aprobada el 8 de diciembre de 2023, después de una maratoniana negociación que duró tres días —con la oposición inicial de los Gobiernos de Francia, Italia y Alemania—, en la que estuvieron involucrados el Consejo, la Comisión, y el Parlamento europeos. Una iniciativa legal que pretende regular todos los aspectos de la IA en los Estados de la Unión, yendo más allá del esquema de Directivas para establecer por vez primera una ley en el concierto europeo (European Parliament, 2023).

En principio, la ley se dirige a los aspectos de seguridad en las actividades económicas y sociales, sin entrar, dada la limitada capacidad de la Unión Europea, en los aspectos relacionados con la Defensa, ya que estos —salvo las limitadas acciones de la Agencia Europea de Defensa (AED), PESCO (*Permanent Structured Cooperation),* la European Defense Fund, unido al nuevo mecanismo determinado por la Brújula Estratégica de Defensa y Seguridad (Lozano Miralles, 2023)— quedan fuera de las competencias de la Unión Europea y son de responsabilidad de cada Estado miembro, así como su participación en otras organizaciones multilaterales como podría ser la OTAN.

De esta manera, la Ley Europea de Inteligencia Artificial se dirige en lo fundamental a regular los aspectos que puedan afectar negativamente a los derechos fundamentales de los europeos, ya sean aquellos sistemas de IA que se utilizan en productos que entran en el ámbito de la seguridad de la propia legislación comunitaria, o bien aquellos otros que atañen a sistemas tales como la gestión de infraestructuras críticas, educación, legislación europea, migración, asilo, etc.; con especial atención a los nuevos desarrollos de IA generativa (el ejemplo, clásico sería ChatGPT y otros sistemas similares[12]), que deberían cumplir unos requisitos específicos de transparencia: contenido generado por los sistemas de IA, protección de actividades ilegales, derechos de autor, aprendizaje de los sistemas, errores o incidencias, mal funcionamiento, etc.

2.5. La India y su capacidad tecnológica

China y la India son en la actualidad los dos países más poblados del mundo: China tiene hoy una población de algo más de 1400 millones de personas, al igual que la India; mientras que, en 2050, China habrá comenzado su descenso poblacional (tendrá un poco más de 1300 millones de habitantes). La India, sin embargo, continuará su ascenso, llegando cerca de los 1700 millones de almas en 2050, para acabar el siglo por encima de los 1500 millones, momento en el que China habrá consolidado su descenso poblacional y contará con unos 775 millones de habitantes[13].

Con este panorama, considerando que la IA tiene como fundamento la manipulación de grandes cantidades de datos, es previsible que estos dos países —India y China— tengan a su disposición un campo de experimentación inigualable respecto de los comportamientos y actitudes de su población, mediante el uso de sistemas avanzados de IA. Así lo asegura, en su extenso libro —al menos en el caso de China—, Kai-Fu Lee, antiguo presidente

[12] Hay que tener en cuenta que, aparte de ChatGPT o los sistemas desarrollados por Apple, Google o Microsoft, existen actualmente en el mercado decenas de sistemas similares. Véase, por ejemplo: https://writesonic.com/blog/chatgpt-alternatives. De la misma manera, empresas tecnológicas chinas como Baidu, están desarrollando sus propios sistemas. Aunque se puede encontrar mucha información al respecto en: https://www.technologyreview.com/2023/08/30/1078714/chinese-chatgpt-ernie-government-approval/. [Consulta: 3 de enero de 2024].

[13] Véase: https://www.populationpyramid.net. Esta información se mantiene accesible de manera permanente.

de Google China antes de fundar su propia empresa de inversiones tecnológicas Sinovation Ventures (Lee, 2018)[14].

En el caso de la India, conocida su capacidad en los servicios informáticos y tecnológicos como soporte de muchas multinacionales estadounidenses y europeas, es preciso tener en cuenta su actual posicionamiento como una de las grandes potencias económicas del siglo XXI, así como su independencia geopolítica entre Estados Unidos y China, lo que convierte al país en un actor fundamental en el enclave Indo-Pacífico, esencial en el desarrollo económico y geoestratégico en este siglo. Allí se dan ya cita todos los posicionamientos geopolíticos actuales, sin olvidar otros escenarios como son el, siempre conflictivo, Oriente Medio y sus permanentes complicaciones, así como la frontera este de Europa, con la Federación de Rusia y el «inacabable» conflicto de Ucrania.

La India no tiene una estrategia nacional *per se* respecto de la IA. Existen, no obstante, algunas iniciativas como la establecida en 2018 por el NITI Aayog, un *think tank* vinculado con el Gobierno del país. Tales iniciativas incluyen, por ejemplo: una alianza con Microsoft; el establecimiento de un Centro Internacional de IA (*International Center for Transformative Artificial Intelligence*, ICTAI), en colaboración con Intel y la compañía india Tata; o un programa de «incubadoras tecnológicas» en colaboración con Google. Programas que se pretenden introducir horizontalmente en cualquier sector económico, incluyendo aspectos de ciberseguridad, seguridad, e impacto ético de la IA.

Igualmente, en febrero de 2021, NITI Aayog publicó el documento *Responsible AI: AI for all*[15], en el que se abordan una serie de cuestiones que centran la preocupación de las autoridades indias en el desarrollo e implementación de sistemas de IA, como son:

- Comprender el funcionamiento de los sistemas de IA para un despliegue seguro y fiable.
- Entender por qué, en un caso concreto, se tomó la decisión de lanzar un sistema de IA.
- Desarrollar los sistemas de IA, bajo principios de coherencia entre todos los implicados (stakeholders).
- Analizar errores de decisión para evitar la exclusión de personas o instituciones a servicios esenciales de IA.

[14] Existe versión en francés: *I.A. La plus grande mutation de l'Histoire.* (2019). Les Arènes. París.

[15] Véase: https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf. [Consulta: 7 de enero de 2024].

- Establecer las responsabilidades concretas en la toma de decisiones.
- Analizar y prever los riesgos a la intimidad de personas o instituciones.
- Considerar los riesgos a la seguridad, particularmente considerando que los sistemas de IA son igualmente susceptibles de ataques, como podrían ser la manipulación de los datos, o la manipulación del comportamiento de sistemas autónomos16.

El sector de la Defensa no es ajeno a la evolución de las tecnologías de IA y sus aplicaciones militares. Se trata de tecnologías que pueden aplicarse a la formación militar, a las actividades de logística y vigilancia, a la ciberseguridad, y a otras funciones como vehículos autónomos de combate, UAVs, o los denominados LAWS (*Lethal Autonomous Weapon Systems*), sistemas de armas capaces de identificar, atacar y neutralizar un objetivo sin intervención humana. Nuevas armas que, es preciso decirlo, podrían plantear, cuando estén totalmente operativas, multitud de problemas morales, jurídicos y, evidentemente, operativos[17].

Para finalizar, sin ser exhaustivos, en 2023, del 9 al 11 de agosto, se organizó un *Workshop*, sobre «Inteligencia Artificial para la Flota del Futuro», patrocinado por el Indian Naval Ship (INS). El objetivo del simposio fue identificar las aplicaciones y analizar la importancia de los sistemas basados en IA para la flota naval india. Como es habitual en este país, el esquema se llevó a cabo en colaboración con entidades privadas, como fueron, por ejemplo: Digital India, Menrva Technologies, Indrones, Google Research, IBM Research India, IIT, o Microsoft Research, todos en colaboración con el Centro de Incubación de Inteligencia Artificial de la Marina de la India (INICAI).

Otras iniciativas, siempre en colaboración con entidades privadas, es la aplicación general de la IA en las necesidades militares. De la mano de Delhi Policy Group[18], un importante *think tank* del país, se llevó a cabo, en febrero de 2023, un análisis para estudiar las aplicaciones militares de la IA en las Fuerzas Armadas de la India (Dheli Policy Group, 2023).

---

16 Disponible en: https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf. [Consulta: 7 de enero de 2024].

17 El Consejo de Europa ha mostrado su preocupación antes este tipo de sistemas. Ver, por ejemplo, el informe del Committee of Legal Affairs and Human Rights: https://assembly.coe.int/LifeRay/JUR/Pdf/TextesProvisoires/2022/20221116-LawsApprehension-EN.pdf.

18 Véase: https://www.delhipolicygroup.org.

Como se ha referido anteriormente, los datos son la clave en los sistemas de IA. En este sentido, este análisis soportado por Delhi Policy Group hizo énfasis en este importante tema, dado que los algoritmos, así como los computadores que los tratan, nada serían sin los datos. De manera que, cuando se estudian las potenciales aplicaciones militares de la IA, los datos, provenientes de diversas fuentes, necesitan ser «depurados, transformados, agregados, y aplicados al entorno operativo concreto», para constituir la base de los sistemas militares de IA.

De nuevo, para la India, en sus aplicaciones militares, la ética es un elemento esencial, como también la interoperabilidad, la seguridad, la potencia de computación, y la experiencia y conocimiento de los operadores de estos sistemas, lo que lleva a la necesidad de formar cuadros militares que conozcan y sean capaces de manejar los sistemas de IA con eficacia.

2.6. Desarrollos en IA de la Federación de Rusia

La Federación de Rusia es actualmente el sexto país del mundo en valor de Producto Interior Bruto (PIB) medido en Paridad de Poder Adquisitivo[19] (PPA o PPP, en inglés: *Purchasing Power Parity*).

En octubre de 2023, Rusia[20], de acuerdo con los datos del Fondo Monetario Internacional[21] (FMI), tenía un PIB (en términos de PPA) de 5,23 billones de dólares, similar al de Alemania (5,72 billones), aunque detrás de las grandes economías mundiales: China (35,04 billones), Estados Unidos (27,97 billones), India (14,26 billones), y de Japón (6,71 billones), aunque muy por delante de otras economías europeas, como Francia (4,01 billones), Reino Unido (3,98 billones), o Italia (3,29 billones), y por encima de Brasil (4,26 billones) o Turquía (3,81 billones).

[19] EL PIB medido en paridad de poder adquisitivo (PPA) determina el Producto Interior Bruto de los países, considerando el poder adquisitivo de sus distintas monedas, eliminando, en consecuencia, las diferencias de niveles de precios entre ellos. El indicador se mide en dólares estadounidenses. Es evidente que con un yuan en China se pueden adquirir más cosas que, con un dólar en Estados Unidos, de ahí la diferencia de PIB (PPA) entre los dos países.

[20] Al referirse a Rusia hay que entender que se refiere a la Federación de Rusia. En sus más de 17 000 km^2, la Federación de Rusia está formada por diferentes repúblicas, territorios, regiones, así como, ciudades de subordinación federal, todos ellos sujetos a la Constitución rusa.

[21] Véase: https://www.imf.org/external/datamapper/PPPGDP@WEO/WEOWORLD/DEU. Normalmente en línea. Los datos son de octubre de 2023.

Esta breve introducción muestra cómo Rusia puede invertir en rublos más cantidad que otros países en dólares o en euros, de ahí, por ejemplo, su volumen de inversión (en rublos) en sus sistemas de defensa.

Respecto de la estrategia de Rusia en IA, independientemente de otros análisis más generales (Bendett, 2019), el 10 de octubre de 2019 se aprobó, mediante el Decreto Presidencial número 490, la llamada *Estrategia Nacional de Desarrollo de la IA hasta 2030 (Национальная стратегия ИИ)*[22]. Dicha estrategia se dirige a cumplimentar unos objetivos que se deberían alcanzar en 2030, año en el que Rusia pretende convertirse en uno de los líderes mundiales en el desarrollo de la IA. En lo fundamental, la estrategia se enfoca en el desarrollo de proyectos relacionados con la visión por ordenador, la síntesis y procesamiento del lenguaje natural, y sistemas inteligentes de apoyo a la toma de decisiones.

Las inversiones en el período 2021-2024 se estimaban en 32 500 millones de rublos, a los que se añadían otros 25 300 millones adicionales incluidos en el presupuesto federal, y otros 6700 millones provenientes de otras fuentes. En total 62 500 millones de rublos. Unas cifras que, por otra parte, según el viceprimer ministro ruso, Dmitry Chernyshenko, alcanzarán un volumen económico superior a los 400 000 millones de rublos en 2023, para llegar, en 2025, al billón de rublos[23]. Cantidades exiguas según los parámetros occidentales, en tanto que un rublo se cotizaba el 12 de enero de 2024 a 0,011 dólares estadounidenses, de manera que las inversiones en IA no llegarían, en 2023, a los 5000 millones de dólares. Cifra muy inferior a las inversiones de Estados Unidos o China. Si bien hay que volver a la consideración de que estas inversiones se realizan en rublos íntegramente en Rusia, lo que vuelve de nuevo a la consideración que se hizo más arriba sobre el PIB (PPA) de Rusia comparado con otros países. En definitiva, una cantidad no menor.

Sin embargo, el ecosistema de IA ruso no es comparable al de China o Estados Unidos, que lideran este campo, tanto en industrias como en publicaciones científica (Petrella, 2024). De ahí que

[22] Véase: https://ai.gov.ru/strategy/n-strategiya-ii/. [Consulta: 8 de enero de 2024]. Ver, igualmente, *Указ Президента Российской Федерации от* (de 10 de octubre de 2019, n.º 490). Disponible en: http://www.kremlin.ru/acts/bank/44731. [Consulta: 8 de enero de 2024].

[23] Véase: http://government.ru/news/49296/. [Consulta: 8 de enero de 2024].

Rusia lanzara una nueva estrategia dentro del denominado proyecto nacional de «Economía de Datos» (*Экономика данных*), anunciado por el presidente Putin en julio de 2023, durante la sesión plenaria del foro de tecnologías del futuro denominado: *Computación y Comunicación. El mundo cuántico*[24], cuya versión final se prevé que esté terminada en el verano de 2024, cuando se determinará el alcance definitivo de los diez programas estratégicos federales establecidos por el Gobierno[25]:

- Infraestructura Digital.
- Inteligencia Artificial.
- Plataformas Digitales en la Administración Pública.
- Sistemas y Redes de Comunicación de Datos.
- Recursos Humanos.
- Infraestructura Informática y Servicios en la Nube.
- Soluciones Informáticas Domésticas.
- Desarrollo de Tecnologías Cuánticas.
- Ciberseguridad.
- Ciencia.

En el caso de la defensa y la seguridad, Rusia ha comenzado su andadura en la aplicación de la IA en los aspectos militares, lanzando, por primera vez, un programa estatal de armamento que incluye una sección independiente sobre IA (Tadviser, 2023; Zysk, 2023).

Dado que la IA se encuentra dentro de las tecnologías que están cambiando la faz de la guerra y, en este sentido será capaz de cambiar por completo el poder militar de los Estados más avanzados en este dominio, Rusia es consciente de su retraso, de ahí que trate de acelerar los procesos para lograr una posición igualitaria con otras potencias, especialmente, ante la evidente falta de un consenso mundial que regule los riesgos de que este tipo de tecnologías se conviertan en un elemento indudable de poder, aparte de la posibilidad de que grupos terroristas o grupos incontrolados accedan a estas tecnologías aumentando los riesgos. Lo cual, en el caso de Rusia, dado su indudable retraso y menor capacidad en desarrollos avanzados de IA, la obliga a buscar una alianza, quizás imposible, con China (Nocetti, 2020). Una circunstancia que, desde nuestro punto de vista, se demuestra difícil, en tanto que China pretender llegar a ser el país líder

[24] Véase: https://digital.gov.ru/ru/events/45686/?utm_referrer=https%3a%2f%2fwww.google.com%2f. [Consulta: 9 de enero de 2024].

[25] Disponible en: https://digital.gov.ru/ru/events/48369/

en este tipo de tecnologías compitiendo, principalmente, con Estados Unidos y solo accedería a sumar a Rusia en caso de ser imprescindiblemente necesario.

3. Geopolítica e inteligencia artificial

Se dice que la IA se ha convertido en un «arma de destrucción masiva». Se comenta igualmente, que la guerra en Ucrania ha aumentado este debate. Ahí está lo que hemos comentado anteriormente respecto de Rusia, la cual, aunque con retraso, necesita aumentar su capacidad armamentística con ingenios más eficaces e inteligentes. Aspectos que, sin perjuicio de sus consideraciones éticas y de la necesidad de que exista algún tipo de regulación internacional, no quita para que estos aspectos entren hoy de lleno en consideraciones geopolíticas, que no son sino cuestiones que afectan a los equilibrios de poder y al fragmentado orden mundial actual (Miller, 2022).

Tanto es así, que la IA ha salido de los ambientes tecnológicos y políticos para adentrarse también en las finanzas. Un asunto que ha puesto a los bancos de inversión tras la pista de este nuevo fenómeno. Así, por ejemplo, Lazard (2023), aunque no sea la única institución financiera que estudia este fenómeno, publicó, en octubre de 2023, un interesante análisis sobre la geopolítica de la IA. Asunto igualmente del interés para la mayor institución mundial de gestión de activos (*Asset Management*), Black Rock[26].

Lazard, en su análisis —considerando que China y Estados Unidos son los países más avanzados en IA, tanto en inversiones como en tecnologías—, muestra once naciones que están en la carrera por entrar en la carrera del dominio de la IA. Ahí aparecen, sorprendentemente, los Emiratos Árabes Unidos, con una inversión de 10 000 millones de dólares (G42 Expansion Fund), al que siguen Rusia, con programas que totalizan 6100 millones de dólares (sin considerar lo anteriormente anotado respecto del PIB en términos de PPA), Alemania (3200 millones) y la República de Corea (1950 millones de dólares).

Y es que se da la circunstancia de que la inteligencia artificial, tal como indica la RAND Corporation (Pavel *et al.,* 2023), afectará

[26] Disponible en: https://www.blackrock.com/us/individual/insights/ai-investing. [Consulta: 10 de enero de 2024].

al desarrollo y, también, a la decadencia de las naciones en este siglo. De manera que, al decir de los analistas de la RAND Co., la IA más que ser un factor de desarrollo o económico, se convertirá en un actor principal en las confrontaciones geopolíticas, distinguiendo en este capítulo a aquellos que tengan este poder de los que sean meros seguidores tecnológicos. Independientemente de los peligros a los que se enfrenta el mundo, que, en palabras de Henry Kissinger en su artículo publicado en 2018 en *The Atlantic* decía que: «filosófica e intelectualmente, en todos los sentidos, la sociedad humana no está preparada para el auge de la inteligencia artificial» (Olier, 2023: 251 y ss.).

Cuando se analiza la situación actual, la carrera por dominar globalmente la IA se centra, en lo fundamental, entre Estados Unidos —con sus aliados—, y China con su propia estrategia. Ambos países pretenden dominar el siglo XXI, no solo con las tecnologías que hacen posible su uso, sino en los entornos donde se pueden llevar a cabo.

Dado que, como dijimos en la introducción, la IA se fundamenta en tres elementos (datos, algoritmos y computación), aparte de la construcción de algoritmos y el uso masivo de datos, el dominio sobre la fabricación de potentes semiconductores se presenta como uno de los elementos geopolíticos fundamentales. Los denominados chips se convierten de esta manera, en el contexto de la IA (aunque no solo), en un elemento esencial. Y ahí surge Taiwán como objetivo preeminente, dada su capacidad en la fabricación de estos elementos electrónicos[27]. Lo que lleva a entender, si bien someramente, las dificultades tecnológicas de la fabricación de chips.

Sin entrar en detalles, como decimos, el proceso de fabricación de un chip tiene una alta complejidad. La base de un semiconductor es el silicio, el segundo elemento más abundante de la Tierra (cerca del 30 % de la masa de la corteza terrestre es de silicio), aunque es muy apreciado por su capacidad de conducir la electricidad. Un elemento que es preciso purificar, dado que su extracción minera va acompañada de muchas impurezas. Una vez

[27] Aunque existen muchos informes sobre este asunto, sirva de manera sintética el siguiente: https://worldpopulationreview.com/country-rankings/semiconductor-manufacturing-by-country. Lo que demuestra igualmente las alianzas que existen, por ejemplo, entre Estados Unidos y la República de Corea (Véase: https://www.cnbc.com/2023/07/20/texas-becomes-chip-hub-with-47-billion-investment-from-samsung-and-ti.html).

alcanzado un silicio de extremada pureza, hay que convertirlo en cristales cilíndricos mediante una complicada técnica, y cortarse posteriormente en forma de pequeñas obleas planas (*wafers*, en inglés) de un grosor oscila entre 675 y 725 micrómetros, donde se podrá asentar luego la circuitería electrónica, y donde, previamente, también con complicadas tecnologías, se llevará a cabo un proceso de estratificación, depositando diferentes materiales (aislantes, semiconductores y conductores) sobre la oblea de silicio, cada uno con propiedades y funciones específicas, incorporando, a su vez, elementos dopantes para hacer que la oblea pueda conducir convenientemente la electricidad. Finalmente, se lleva a cabo el proceso de gravado que permite crear los patrones que constituyen la base de los circuitos miniaturizados que se introducen en el chip, a la vez que se eliminan selectivamente otros componentes, como el dióxido de silicio, capas metálicas o incluso el propio sustrato de silicio (Boston Consulting Group y Semiconductor Industry Association, 2021).

Este largo y complejo procedimiento, que no suele ser bien conocido, viene a demostrar que las tecnologías de fabricación de chips no están al alcance de la mayoría de los países, siendo, en este caso, Taiwán, sobre todo en las fases de gravado, una potencia mundial, de ahí el interés por controlar su industria de semiconductores.

El control de Taiwán por China se opone al mantenimiento, como país independiente, por parte de Estados Unidos, lo que incrementa las tensiones geopolíticas entre las dos superpotencias. De ahí que el nuevo presidente electo de Taiwán, Lai Ching-te, saliera el día de su elección, en julio de 2023, a declarar que: «No queremos convertirnos en enemigos de China. Podemos hacernos amigos». No hay duda de que Taiwán será un elemento de confrontación geopolítica de gran intensidad en la era de la IA que se vivirá en este siglo.

4. El cuaderno estratégico sobre inteligencia artificial

Este *Cuaderno de Estrategia* del Instituto Española de Estudios Estratégicos es un primer análisis que muestra la relevancia que tienen las nuevas tecnologías asociadas a la IA respecto de la defensa y la seguridad. Un asunto que se demostrará esencial en la defensa de las democracias actuales y las alianzas en las que se encuentra España al lado de los países occidentales de su entorno.

En su elaboración se ha tratado de incorporar a los expertos internacionales más adecuados para este propósito, así como aquellos reconocidos expertos en cada una de las áreas que este primer documento exige para dar una visión de conjunto del problema. Sus responsabilidades y experiencia no dejarán ninguna duda.

De esta manera, en este *Cuaderno de Estrategia* se incluyen varios importantes aspectos que ofrecen un panorama multidisciplinar en relación con la IA en la defensa y la seguridad, como son: una visión sobre operaciones especiales apoyadas por la IA; la importancia de la inteligencia económica, la necesidad de conocer cómo los países alineados de Asia (Corea y Japón) desarrollan sus estrategias en relación con la IA; el análisis geopolítico global mediante estas nuevas tecnologías; cómo se utilizan en el contexto de la desinformación en el actual conflicto en Ucrania; la gestión de crisis mediante la IA; el entorno aeroespacial como un nuevo elemento de potenciales riesgos geopolíticos y tecnológicos; y, finalmente, la problemática relacionada con la huella climática, aspecto relevante en el contexto mundial.

Estamos convencidos de que este primer documento, promovido por el Instituto Español de Estudios Estratégicos, servirá para canalizar en el futuro otros análisis de igual relevancia.

Bibliografía

Arisa, E. *et al.* (2023). International Collaboration in AI Governance. Key Considerations of the Council of Europe's AI Convention and Japan's Response. *IFI Policy Recommendation*. N.º 25. [Consulta: 23 de diciembre de 2023]. Disponible en: https://ifi.u-tokyo.ac.jp/en/wp-content/uploads/2023/10/policy_recommendation_tg_20231031e.pdf.

Boston Consulting Group y Semiconductor Industry Association. (2021). *Strengthening the Global Semiconductor Supply Chain in An Uncertain Era.* [Consulta: 2024]. Disponible en: https://www.semiconductors.org/wp-content/uploads/2021/05/BCG-x-SIA-Strengthening-the-Global-Semiconductor-Value-Chain-April-2021_1.pdf.

Dheli Policy Group. (2023). *Implementing Artificial Intelligence in the Indian Military.* [Consulta: 8 de enero de 2024]. Disponible en: https://www.delhipolicygroup.org/publication/policy-briefs/implementing-artificial-intelligence-in-the-indian-military.html.

European Commission. (s.f.). *A European Approach to Artificial Intelligence.* Shaping Europe's Digital Future. [Consulta: 2 de enero de 2024]. Disponible en: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.

European Parliament. (2023). *DPG Policy Brief*. *EU IA Act: First regulation on Artificial Intelligence*. [Consulta: 2 de enero de 2024]. Disponible en: https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

Hofstadter, D. R. (1987). *Gödel, Escher, Bach. Un eterno y grácil bucle*. Tusquets Editores.

Lazard. (2023). The geopolitics of Artificial Intelligence. Geopolitical Advisory. [Consulta: 10 de enero de 2024]. Disponible en: https://www.lazard.com/research-insights/the-geopolitics-of-artificial-intelligence/.

Lee, K. (2018). *AI Superpowers. China, Silicon Valley, and the New World Order*. New York, Houghton Mifflin Harcourt Publishing.

Lozano Miralles, J. (dir.). (2023). *Brújula Estratégica de la Unión Europea y terrorismo*. Editorial Aranzadi.

Miller, C. (2022). *Chip War: The Fight for the World's Most Critical Technology*. Simon & Shuster UK.

Nocetti, J. (2020). *Russia in the race for Artificial Intelligence*. Instituto Francés de Relaciones Internacionales. Russia/NIS Center.

Olier, E. (2023). *La debacle de Occidente. Las guerras del siglo XXI*. Sekotia.

Olier, E. y Corchado, J. M. (2022). Inteligencia Artificial: aplicaciones a la Defensa. *Documento de investigación 01/2022*. Instituto Español de Estudios Estratégicos. [Consulta: 2024]. Disponible en: https://www.ieee.es/Galerias/fichero/docs_investig/2022/DIEEEINV01_2022_EDUOLI_Inteligencia.pdf.

Pavel, B. *et al*. (2023). AI and Geopolitics. How Might AI Affect the Rise and Fall of Nations? *RAND Corporation.* [Consulta: 10 de enero de 2024]. Disponible en: https://www.rand.org/pubs/perspectives/PEA3034-1.html.

Petrella, S. *et al*. (2020). *Russia's Artificial Intelligence Strategy: The Role of State-Owned Firms*. [Consulta: 9 de enero de 2024]. Disponible en: https://sites.tufts.edu/hitachi/files/2021/02/1-s2.0-S0030438720300648-main.pdf.

Roberts, H. *et al*. (2021). *The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation*. AI & Society. N.º 36, pp. 59-77.

Russell, S. y Norvig, P. (2004). *Inteligencia Artificial. Un enfoque moderno.* Pearson Educación. 2.ª edición.

Tadviser. (2023). *Искусственный интеллект в ВПК* [en línea]. [Consulta: 9 de enero de 2024]. Disponible en: https://www.tadviser.ru/index.php/Статья:Искусственный_интеллект_в_ВПК#.

Turing, A. M. (1950). *Computing Machinery and Intelligence*. *Mind*. *New Series.* Vol. 59, n.º 236, pp. 433-460.

United Nations Office of Information and Communications Technology. (s.f.). *Generative AI Primer.* [Consulta: 26 de diciembre de 2023]. Disponible en: https://unite.un.org/sites/unite.un.org/files/generative_ai_primer.pdf.

Wright, N. D. (ed.) y Bendett, S. (2019). The Development of Artificial Intelligence in Russia. Artificial Intelligence. China, Russia, and the Global Order. *Fairchild Series.* Air University Press, pp. 168-177. [Consulta: 2024]. Disponible en: https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0161_WRIGHT_ARTIFICIAL_INTELLIGENCE_CHINA_RUSSIA_AND_THE_GLOBAL_ORDER.PDF.

Zysk, K. (2023). *Strugling, Not Crumbling: Russian Defence AI in a Time of War*. Rusi. [Consulta: 2024]. Disponible en: https://rusi.org/explore-our-research/publications/commentary/struggling-not-crumbling-russian-defence-ai-time-war.

Capítulo segundo

IA en la defensa de la República de Corea y de Japón

Ángel Gómez de Ágreda

Resumen

La República de Corea y Japón son dos referentes tecnológicos en Asia y en el mundo. Apoyados en sus industrias de semiconductores, han desarrollado numerosas aplicaciones que emplean la inteligencia artificial en el ámbito militar. El dinámico entorno geopolítico en el que se encuentran ubicadas y las similitudes en la evolución de su pirámide poblacional guían, de alguna manera, los esfuerzos de ambos en su empleo de aquella. Este se centra especialmente en los vehículos y plataformas no tripulados que requieran menos personal y generen menos bajas, y en el apoyo a su entorno cibernético.

Palabras clave

Inteligencia artificial, Sistemas de armas autónomos, Ciberseguridad, Innovación militar, Corea, Japón.

AI in defense of the Republic of Korea and Japan

Abstract

The Republic of Korea and Japan are two technological references in Asia and the globe at large. Leveraging their semiconductor industries, they have developed numerous applications using artificial intelligence in the military field. The dynamic geopolitical environment in which they are located and the similarities in the evolution of their population pyramid guide, somehow, the efforts of the two countries in their use of artificial intelligence. This is especially focused on unmanned vehicles and platforms that will require fewer personnel and generate fewer own casualties, and on support for their cyber environment.

Keywords

Artificial intelligence, Autonomous weapons systems, Cybersecurity, Military innovation, Korea, Japan.

1. Introducción

Tanto la República de Corea como Japón son referentes en el ámbito de las tecnologías digitales. Ambas, cada una a su manera, están realizando grandes aportaciones en el campo de la inteligencia artificial (IA) y alrededor de él. Su posición geográfica y geoeconómica, su historia y las circunstancias sociales en que se encuentran también condicionan grandemente su aproximación a esta tecnología.

En ese marco, tanto Seúl como, sobre todo, Tokio, mantienen relaciones cooperativas con otros actores relevantes como su vecino Taiwán, India, los países de la Unión Europea y otros europeos ajenos a la misma, y con los Estados Unidos como principal referente mundial. Su relación con China, sin embargo, presenta ambivalencias derivadas de su posición en el mercado y en el tablero geopolítico mundial (Glosserman, 2023).

Asia en su conjunto constituye un escenario ineludible en lo que respecta a la IA. Por un lado, como fuente de buena parte de los recursos materiales y minerales que habilitan el ámbito digital. Por otro, como creciente fuerza motriz de una parte importante del talento que se despliega en la investigación, desarrollo y producción de los componentes básicos de la misma. También, como el principal mercado mundial de los sistemas y aplicaciones, consecuencia en parte del peso demográfico de la región. Finalmente, por el dinamismo social de muchas de sus comunidades, las regulaciones nacionales menos restrictivas y por el empleo que hacen de lo digital en general y de la IA en particular.

Encarrilados por todos estos condicionantes, positivos y negativos, los países asiáticos juegan un papel determinante en ambos lados del mercado. No es de extrañar, por lo tanto, que las grandes compañías multinacionales cortejen a las asiáticas, intenten atraer su talento e inversión, y busquen formas de infiltrar sus mercados (López, 2023).

En las siguientes páginas vamos a ver algunos de los desarrollos asiáticos más importantes en IA, pero también sus principales políticas al respecto y la estrategia de sus corporaciones. El hecho de centrarnos en Corea del Sur y en Japón es consecuencia de la experiencia directa del autor, pero otros países asiáticos están contribuyendo de forma sobresaliente a esta industria.

1.1. Un tema trasversal: el cambio necesario en el modelo de abastecimiento

Los procesos de adquisición de capacidades y, muy en especial, los de diseño y desarrollo de estas implican todavía plazos extraordinariamente largos que son, también, incompatibles con la obtención de sistemas de armas capaces de suponer una diferencia fundamental en el campo de batalla. A pesar de algunos progresos nacidos de la mano de la colaboración entre los ejércitos y el sector industrial privado, se requieren nuevas fórmulas y una mayor agilidad.

La República de Corea ha desarrollado el concepto de «adquisición rápida» como parte de la estrategia «Defense Innovation 4.0». Se trata de un mecanismo que simplifica los procesos que tienen lugar en la contratación de material. Al acortamiento de los plazos se añade la posibilidad de incorporar tecnologías de última generación antes de que se queden obsoletas en el cambiante mundo digital.

El modelo no es solo una mejora en la eficiencia, sino una necesidad operativa en el momento actual. El enquistamiento en formatos obsoletos no conducirá más que a la dotación a las Fuerzas Armadas con material igualmente caduco. Además, requiere venir acompañado de una flexibilidad equivalente en la adopción de doctrinas y formas de empleo que consigan extraer el mayor partido de estas tecnologías punteras.

La República de Corea ha establecido incluso un instituto que se encarga de gestionar este nuevo modelo de adquisición. DRATRI es el *Defense Rapid Adquisition Technology Research Institute*. De hecho, la medida parece muy adecuada, teniendo en cuenta la necesidad de establecer unos controles específicos para este tipo de procesos que garanticen la transparencia y eviten ineficiencias y corrupciones asociadas a la reducción de plazos.

La misma IA tiene un gran potencial para servir de apoyo en la planificación, identificación y gestión de estos casos, en muchos de los cuales se convertirá en objeto y sujeto de la contratación.

2. La península de Corea

Al hablar de la península de Corea, tenemos que considerar el uso que se hace de la IA a ambos lados de la Zona Desmilitarizada que separa a la República Popular Democrática de Corea (DPRK)

y a la República de Corea (ROK). La primera, un régimen de corte autocrático, sometido a numerosas sanciones internacionales; el segundo, que sigue un modelo democrático liberal y que ha venido escalando posiciones en el *ranking* de las economías más avanzadas en las últimas décadas.

A pesar de todo, cuando se trata de investigación tecnológica con aplicaciones militares, los logros de ambos países difieren menos de lo que su renta per cápita o su producto interior bruto podrían hacer sospechar. Las diferencias son, en muchos casos, relativas a los modos de empleo y a los procedimientos y doctrinas que se siguen en cada caso. Mientras que el Sur pretende, principalmente, preservar su nivel de vida privilegiado y proteger a su industria y a sus ciudadanos, el Norte emplea la tecnología militar digital con un carácter ofensivo. A menudo, estos ataques están más vinculados a intereses económicos o industriales que a los militares, pero siempre en el contexto del estado jurídico de guerra en el que se mantienen.

Ambas centran buena parte de los proyectos en el desarrollo de sistemas de armas autónomos y en el uso de la IA en apoyo de la ciberseguridad, bien sea de forma ofensiva o defensiva (Su, 2019).

Poco puede saberse, a ciencia cierta, sobre las actividades de Corea del Norte, más allá de algunas escasas publicaciones académicas y de lo que se deduce de los resultados obtenidos en sus desarrollos. No obstante, de estas dos observaciones se infiere que hay una intensa actividad investigadora en los campos de la autonomía de navegación de plataformas y en ciberseguridad.

Según los analistas, los esfuerzos en ciberseguridad se centran más en las labores ofensivas. Esto sería consistente con el uso tradicional que viene haciendo Pyongyang del ámbito digital, en el que muestra grandes capacidades para la disrupción de redes ajenas (como muestra el caso Sony), pero escasa resiliencia ante los ataques adversarios (como también se aprecia en la continuación de dicho caso ante la reacción estadounidense).

La incursión reciente de cinco UAV norcoreanos a través de la frontera en la región próxima a Seúl y la cuestionable respuesta surcoreana plantea escenarios en los que la aplicación de la IA al uso de enjambres de drones en un escenario tan condensado y complejo como el coreano pueda constituir una seria amenaza, no ya a las Fuerzas Armadas, sino a la población en general. Las inversiones en su constitución y en su acometimiento se han disparado, presumiblemente, en ambos bandos.

La reciente cooperación militar con Moscú puede proporcionar nuevos conocimientos y herramientas a Kim Jong-un relacionados con la aplicación de sistemas dotados de IA a la defensa.

Corea del Sur, por su parte, cuenta con numerosos centros universitarios (empezando por la universidad KAIST, nacida como un *spin off* del MIT de Boston) y de investigación. Al mismo tiempo, la industria surcoreana recibe un fuerte apoyo estatal y se beneficia de la existencia de un puñado de enormes conglomerados que dominan la producción a nivel nacional y son, en muchos casos, referentes internacionales. Varios de ellos están vinculados al sector digital (Samsung, LG, SK-Hynix), mientras que otros aportan, además, un carácter integrador en la fabricación de armamento (Hyundai, Hanwha).

El esfuerzo investigador en el Norte está mucho más centrado en la acción estatal. Ante la dificultad para aplicar las agresivas estrategias de mercado internacional de Seúl, Pyongyang recurre a la apropiación de tecnologías foráneas mediante ciberataques. Estos últimos también le sirven para la obtención de fondos para la financiación de sus proyectos y programas.

Las grandes masas de soldados del Norte siempre han condicionado las políticas del Sur, incluyendo el servicio militar obligatorio de hasta dos años de duración para todos los varones. A pesar de ello, sus números no alcanzan a la mitad de los efectivos que puede movilizar Pyongyang, mucho menos teniendo en consideración el menguado número de nacimientos que registra el país. De ahí que buena parte de sus esfuerzos se centren en el diseño de sistemas autónomos que no requieran tripulación y que reduzcan la probabilidad de bajas.

Ambos países han estudiado también sistemas submarinos no tripulados. La DPRK ha hecho gala en los últimos meses de un sistema de características supuestamente similares al Poseidón ruso y que sería capaz de portar y detonar un ingenio nuclear submarino en las inmediaciones de los puertos japoneses o surcoreanos con un alto grado de autonomía (Europa Press, 2024).

En lo que respecta al apoyo a la ciberseguridad, la Estrategia Nacional de Ciberseguridad de la República de Corea, recogía, ya en su primera edición de 2019, la necesidad de «ampliar el objetivo de detectar ciberataques para permitir su detección y bloqueo en tiempo real, y desarrollar tecnologías de respuesta basadas en IA», frase que se repite de forma literal cuatro años después

en la edición de 2023 (*Republic of Korea National Cybersecurity Strategy*, 2023).

Esta labor recae en KISA, la *Korean Internet & Security Agency*[1]. En la práctica, no consiste solo en aplicar la IA al día a día de las operaciones cibernéticas, sino también a ayudar a los analistas a comprender los mecanismos que constituyen o son susceptibles de constituir vulnerabilidades y a predecir ciberataques con base en comportamientos anómalos de la red.

También se ha venido poniendo sobre la mesa la necesidad de compilar ciberataques capaces de interrumpir la secuencia de lanzamiento de los misiles norcoreanos en lo que se llama un ataque *left of launch*, es decir, preliminar o previo al lanzamiento. Aunque el concepto lleva en discusión desde, al menos, 2015, los últimos documentos surcoreanos siguen mencionándolo como desiderátum. La aplicación de algoritmos puede resultar de gran ayuda dada la esperable gran cantidad de datos acumulados en los cientos de lanzamientos efectuados desde entonces.

2.1. Estrategia de Seguridad Nacional y *Libro Blanco de la Defensa*

Estos mismos conceptos se repiten, como no podía ser de otro modo, en la *Estrategia Nacional de Seguridad* del actual presidente Yoon Suk-yeol[2]. Publicada en junio de 2023, su capítulo número cinco se titula «Desarrollando unas Fuerzas Armadas poderosas y tecnológicamente avanzadas». Más allá de la retórica, el día a día muestra una obsesión a nivel nacional por la tecnología. Dentro de ella, la aplicación de IA a los sistemas militares es una constante que permea a la mayor parte del resto de la industria.

Los tres aspectos más mencionados son: la misma IA, los sistemas no tripulados y los robots. En todos ellos —y en su gestión— hay un importante componente algorítmico. La IA figura como primera prioridad entre las diez que se identifican, aunque es trasversal a todas ellas.

El *Libro Blanco de la Defensa 2022* (Ministry of National Defense Republic of Korea, 2023) es anterior en unos meses a la Estrategia, ya que, a pesar de su nombre, se publicó en febrero

1 Véase: https://www.kisa.or.kr/EN

2 Véase: https://www.president.go.kr/download/648037c2bf5e7

de 2023. La tercera sección de su cuarto capítulo se dedica a tratar el uso de la IA en Defensa y la transformación digital. Significativamente, la República de Corea es uno de los países que hablan sin rodeos de una autonomía total de los sistemas de armas en un tercer escalón tras los tripulados de forma remota y los semiautónomos.

En un relato muy bien estructurado, el libro propone la creación de una «Iniciativa de introducción de la IA en Defensa» y de un «Centro de IA en Defensa». Para ello, propugna el establecimiento y gestión de una base de datos de Defensa de alta calidad sobre la que basar el entrenamiento de los algoritmos. El otro pilar fundamental es una infraestructura de altas prestaciones basada en redes de muy alta velocidad e hiperconectadas.

El talento digital en Corea está muy ampliamente distribuido entre la población. Para capturar nuevas ideas, se pretende establecer una plataforma digital de gobierno en Defensa Nacional que permita contribuciones de terceros actores. Eso no obsta para que también se contemple el fomento de la formación y entrenamiento de expertos militares y reservistas para generar innovación en el entorno militar.

La concienciación y la cooperación internacional son piedras angulares de la seguridad digital. Foros como el *14.º Simposio internacional en seguridad y Derecho Militar*, celebrado el pasado 15 de noviembre de 2023, en Seúl, están teniendo un carácter casi monográfico en el tratamiento del uso de tecnologías como la IA por parte de las Fuerzas Armadas de Corea.

2.2. Algunos casos de usos en Corea

Entre los desarrollos más recientes de sistemas robóticos y de IA en la República de Corea está el sistema antiminas navales que está diseñando y construyendo la empresa Hanwha, sobre la idea del desarrollo francés de Thales llamado MiMap. El diseño coreano utiliza sistemas submarinos no tripulados (UUS) y sónares remolcados para la obtención masiva de datos de los fondos marinos con los que alimentar un sistema de aprendizaje máquina profundo (Cha, 2023).

En este caso, la IA está presente tanto en la recopilación de datos por los sensores embarcados en los UUS como en su estudio y en la identificación de patrones. Cabe esperar una aplicación

simétrica a aplicar a las propias minas para mejorar la eficacia de estas en el futuro próximo.

La vigilancia de los 250 km de la zona desmilitarizada que separa las dos coreas absorbe una parte importante de los recursos militares de Seúl. La misma capital —y, en ella, la mitad de la población del país— se encuentra a menos de 30 km de la línea fronteriza, lo que reduce sustancialmente los márgenes temporales de reacción ante posibles amenazas. Estas, además, se materializan cada vez más en forma de drones no tripulados enviados por Corea del Norte, y ante los que las defensas tradicionales tienen una respuesta muy ineficiente.

El nuevo sistema que está implementando la Administración de Programas de Adquisiciones de Defensa (DAPA) —un equivalente a la Dirección General de Armamento y Material (DGAM) española— pretende recoger datos de imágenes en el espectro visible y en el infrarrojo para su análisis, mediante sistemas dotados de IA (Lee, 2024). También recopila sonidos que pudieran complementar la información y que, debidamente filtrados, pueden servir de alarma o para descartar una intrusión.

La compañía S-1 está desarrollando el sistema, que debería permitir mejorar la precisión de la identificación de posibles intrusiones y las condiciones de vida de los militares que patrullan la frontera. Hay que tener en cuenta que la meteorología coreana es muy hostil y que los 4 km de anchura de la franja vallada están densamente poblados por fauna salvaje que ha encontrado ahí un hábitat seguro, pero que genera numerosos ecos y falsas alarmas.

El incremento de la tensión geopolítica en la región hace más necesario este tipo de soluciones, perfectamente extrapolables a otras de las numerosas zonas fronterizas que existen en diferentes regiones.

En la línea de demarcación entre ambos países, la presencia de hasta cuatro túneles excavados desde Corea del Norte para permitir una infiltración rápida y segura de tropas en el Sur forzó, en su momento, la ejecución de trabajos de contra-túnel mediante la ejecución de las propias obras para interceptar los conductos adversarios. La vigilancia del subsuelo es, por lo tanto, otra de las preocupaciones constantes en Seúl.

Para apoyar esta labor —y perfectamente extrapolable a otras funciones civiles o militares— la Agencia para el Desarrollo de

la Defensa surcoreana ha encargado (también a la empresa Hanwha) un *Robot Autónomo de Exploración de Túneles*[3] capaz de operar en ese entorno.

El sistema se compone de varios robots autónomos u operados a distancia desde un teléfono móvil o una *tablet*. Es capaz de navegar en escenarios desconocidos y generar mapas en tres dimensiones, aunque no exista cobertura de posicionamiento satelital. Puede detectar objetos peligrosos o significativos e ir colocando repetidores radio para mantener el enlace con su operador o con otros robots del equipo.

De nuevo, el uso de la IA será dual. Por un lado, en la guía del robot y, por otro, en la identificación y clasificación de objetos (también en el aprendizaje en ambos aspectos).

También en este caso será crítica la dotación de los sensores adecuados para llevar a cabo la misión. En este caso, se tratará de LIDAR y sensores infrarrojos. La modularidad en el equipamiento es fundamental para adaptarse a los distintos ambientes y a las cambiantes misiones en las que puede participar. Tanto los programas como los equipos suponen una cantera inagotable de nichos tecnológicos en los que pueden implicarse otras compañías o divisiones. En este caso concreto, la investigación y desarrollo se llevó en paralelo con otro del *Ground Vehicle System Center* del *US Army.*

Esto muestra la posibilidad de utilizar también sistemas civiles para misiones militares. La clave está en la carga de pago y en la sensorización con que se dote a estos equipos. Por ejemplo, sobre el muy conocido modelo de robot cuadrúpedo de Boston Dynamics, el gigante empresarial Hyundai Rottem y la empresa Rainbow Robotics están construyendo un modelo armado pensado para operaciones contraterroristas. La menguante población surcoreana, que adolece de un decreciente índice de natalidad, está dando lugar a una crónica falta de personal susceptible de ser reclutado, va a requerir de sistemas autónomos como este para complementar la labor de los humanos en determinadas tareas particularmente peligrosas.

El mayor riesgo, sin embargo, —aunque no necesariamente el de mayor probabilidad de ocurrencia— sigue siendo el lanzamiento de misiles dotados de cabezas nucleares por parte de Corea del Norte. La amenaza es compartida con otros países y especialmente

[3] Véase: https://www.add.re.kr/board?menuId=MENU02924&siteId=SITE00003

sentida en Japón. No es de extrañar, por tanto, que una compañía surcoreana haya desarrollado un *software* que, partiendo de las imágenes de satélites comerciales de observación, es capaz de detectar alteraciones en las instalaciones norcoreanas de lanzamiento de misiles que puedan indicar la inminencia de uno. El programa está dotado de IA y lleva en desarrollo desde 2018 (Demarest, 2023).

También por iniciativa de la Agencia para el Desarrollo de la Defensa surcoreana, se están llevando a cabo estudios tendentes a la creación de un *software* de guiado de vehículos autónomos, específicamente diseñado para los medios militares. En este sentido, es preciso recordar que los ambientes militares son, normalmente, mucho menos estructurados que los civiles. No se puede dar por sentado que vayan a existir rutas fijas o reglas de tráfico, ni siquiera que el terreno vaya a ser regular (Kim, 2022).

Precisamente, la capacidad para operar fuera de los parámetros establecidos o estándar es una de las principales ventajas operativas en el entorno militar. Esta añade la posibilidad de mejorar las opciones de sorpresa y de minimizar los daños recibidos por las fuerzas propias. La complejidad del escenario es, no obstante, mucho mayor, igual que lo serán los requisitos necesarios —tanto de *hardware* como de *software*— para poder operar en él.

2.3. Army Tiger[4]

El Ejército de la República de Corea mantiene un programa que podría considerarse equivalente a la Brigada 2035. El *Army Tiger* es un programa de investigación y desarrollo tecnológico para las operaciones terrestres de las Fuerzas Armadas surcoreanas. Su estructura es la de una Brigada de Infantería reforzada con un batallón de carros de combate, uno de Artillería e Ingenieros y una compañía de mantenimiento. Tiene, por el momento, una capacidad limitada para la operación independiente.

Viene a constituirse en un prototipo experimental de nuevos equipamientos y conceptos doctrinales. Estos últimos se recogen en el documento *Defense Innovation 4.0* (2023), que tiene como objetivos:

[4] Extraído de la conferencia *Development of ROK Army AI based MUM-T (Manned-Unmanned-Teaming) Systems: Army Tiger.* Impartida por el general de brigada del Ejército de la República de Corea, Cha Won-ju, el 22 de septiembre de 2022 en el marco de la 8.ª Conferencia Internacional del ROK Army en Seúl.

- Rediseñar el sistema de planeamiento de la Fuerza y el I+D, mediante la integración de los ejércitos, la industria, la academia y los centros de investigación.
- Expandir la infraestructura de ciencia y tecnología de la Defensa aplicando la IA a todas las áreas de la Defensa para poner los cimientos de sistemas de combate autónomos o robóticos.
- Optimizar la gestión de la Defensa y la estructura militar.
- Desarrollar estrategias militares y conceptos operacionales.
- Cambiar de forma cualitativa la potencia de combate asegurando armamento de alta tecnología clave.

Aunque su contribución al conjunto del *Army Tiger* es modesta —y muy relacionada con la aplicación de sistemas dotados de IA—, la visión global del documento resalta la necesidad de acometer un planteamiento integral de la evolución para que no sea, simplemente, una incorporación de tecnologías novedosas capaces de llevar a cabo las mismas tareas que se venían haciendo con otros medios. La doctrina subyacente está basada, en gran medida, en los conceptos estadounidenses que permean de las fuerzas norteamericanas en la península.

Uno de los focos fundamentales del *Army Tiger* es el conocido concepto MUM (*Manned/Unmanned* o tripulado/no tripulado) que pretende combinar elementos autónomos con otros que portan humanos en su interior. Se basa en el uso de la IA, la hiperconectividad de los sistemas y la super inteligencia. Finalmente, pretende la integración de los sistemas autónomos en el conjunto de la operación, manteniendo el foco en el elemento humano.

La movilidad de los combatientes en vehículos blindados sobre ruedas y los elementos autónomos (vehículo multipropósito, vehículo de combate ligero, robot cuadrúpedo, dron armado y dron lanzagranadas) se combinarán a través de un equipo de monitorización integrado y dotado de IA y de un sistema inteligente de apoyo a la decisión mediante satélites de órbita baja y equipos de comunicaciones cuánticos individuales. El plazo temporal para conseguirlo es 2027, una fecha que aparece reiteradamente en los planes de Defensa en la región.

El objetivo es conseguir una fuerza «más rápida, más inteligente y más cercana», que aplique la IA en cada escalón y en cada función que lleva a cabo. La velocidad se deriva de una toma de decisiones más ágil, mediante el apoyo de los algoritmos; la inteligencia, de una gestión apoyada en sistemas de IA para las funciones de apoyo a la Fuerza; finalmente, la cercanía implica el

uso de sistemas hiperconectados que incrementan la supervivencia individual de los combatientes y su letalidad. La compartición de información resulta fundamental para las tres funciones.

3. Japón

La IA ofrece un gran potencial para mejorar sustancialmente la aplicación de otras tecnologías en el ámbito militar. Más que aplicaciones propias, estará presente en multitud de sistemas y en la configuración de formas de empleo. En el caso de Japón se identifican varias oportunidades (Hornung *et al*., 2021):

- Permitirá dificultar/facilitar la atribución de acciones, según el caso. Esto es, confirmar la autoría de una agresión o disimularla cuando esa acción ha sido propia. De esta manera, se contribuye a espesar la «niebla de la guerra» para el adversario y disiparla para el bando propio.
- Aumentará sustancialmente el tempo de las operaciones, limitando la participación humana en la toma de decisiones o en la elaboración de planes o, en su caso, programas de armamento. En el primer caso estamos hablando de planeamiento operativo, en el segundo de programas informáticos para la realización de ataques cibernéticos o acciones de guerra electrónica.
- El uso de vehículos y plataformas no tripulados va a ser (ya lo es) generalizado en la guerra. Casos como el de Japón, en el que la pirámide poblacional está descompensada hacia las capas superiores, tenderán a hacer un uso mayor de estos medios para compensar la falta de personal y para limitar las bajas, aspecto este que es particularmente crítico en estas comunidades.
- La precisión y rapidez en el ciclo de targeting que puede introducir el uso de la IA tiene la capacidad de reducir el gasto de munición. Este es otro tema que se ha demostrado crítico en conflictos como el de Ucrania y del que Tokio ha extraído lecciones significativas.
- El uso de la IA en campañas de desinformación y contrainteligencia requerirá de profesionales especializados en el relato y en la comunicación más allá de las técnicas tradicionales del periodismo. En ocasiones, estas serán más propias de actividades de marketing.
- Las labores de I+D en todos los campos tecnológicos se benefician también del uso del aprendizaje máquina. Aunque no

directamente vinculada a las operaciones, la capacidad para desarrollar sistemas de armas o componentes más avanzados en plazos útiles en el marco del conflicto puede resultar determinante en su resultado.
- Aunque muchas veces permanece ignorado o se deja, como aquí, para el final, el uso de los sistemas dotados de IA en labores logísticas y de apoyo incrementa sustancialmente la eficiencia de estas labores. No cabe minusvalorar las aportaciones que, en este campo, son susceptibles de aparecer de la mano de sistemas inteligentes de gestión.

La cooperación con el único aliado japonés, Estados Unidos, y con su más próximo país afín en la región, Australia, en materia de IA ha comenzado ya, pero promete proporcionar nuevos frutos próximamente con la creación de una agencia especializada basada en la americana DARPA (*Defense Advanced Research Projects Agency*). La JARPA sería el homólogo japonés que estaría destinada a cooperar también con ASRA, la agencia australiana afín (Warren *et al*., 2023).

Esta cooperación no se limita a los aspectos operativos de la IA. Tokio también se ha posicionado como un referente en lo que respecta a la regulación del uso de los algoritmos. Su presidencia del G7 durante 2023 se centró, en buena parte, en sentar unos principios con vocación universal para el empleo ético y lícito de la IA (Pérez, 2023; *The Mainichi*, 2023).

También en los usos militares de la IA Japón fue uno de los primeros países en sumarse a la iniciativa estadounidense para la regulación de su uso (Domínguez, 2023). La falta de acuerdo en las negociaciones en Naciones Unidas invita a abrir otras vías para generar un código de conducta universal y retener el control y la responsabilidad de los humanos sobre sus actuaciones. Tanto a nivel individual como insertos en una cadena de mando, estos dos aspectos deben permanecer, en todo momento, vinculados a una responsabilidad que es indisociable del carácter humano.

En claro contraste con el caso coreano, la excesiva dependencia en el juicio de las máquinas es un aspecto que preocupa particularmente al Gobierno de Kishida (Kyodo, 2023), habida cuenta del extenso uso que se hace de esta tecnología en el ámbito social japonés. De hecho, el japonés medio está muy en contacto con la IA en labores de apoyo sociológico y psicológico. Este aspecto vuelve a estar relacionado con la pirámide poblacional nipona, con una de las más altas esperanzas de vida del mundo

y el menor porcentaje de población por debajo de los veinte años (junto a Corea del Sur).

El empuje legislador japonés en esta área ha tenido repercusiones en la región completa. Filipinas ha sugerido a sus socios de la ASEAN una iniciativa similar, a la que Tokio no es completamente ajeno.

Hay que recordar que este impulso legislador tiene un firme apoyo en una industria digital puntera, tanto en lo que respecta al *hardware* como al *software.* En el primer caso, con empresas como Canon, que están a la vanguardia de la fabricación de microchips (Protector indefinido, 2023), o colaboraciones con grandes multinacionales como NVIDIA (López, 2023; *Libre mercado*, 2023) o la taiwanesa TSMC, que ha establecido factorías en territorio japonés. En el segundo, con innovaciones que tendrán indudables usos en el ámbito militar (Kyodo, 2023b).

El Libro Blanco de la Defensa de Japón (Ministerio de Defensa de Japón, 2023) hace pocas menciones explícitas de la IA. Normalmente, las que hay hacen referencia a tendencias y a su papel en la configuración de la política y el campo de batalla. Sin embargo, sí pone mucho énfasis en su aplicación en los vehículos autónomos. El presupuesto quinquenal (2023-27) para este apartado se ha decuplicado respecto del periodo anterior hasta el billón (*trillion*) de yenes. Además, estará presente en otras partidas de forma trasversal. En concreto, se destinan hasta 8 billones de yenes a capacidades para operaciones interdominio, que incluyen el ciberespacio y el espacio exterior.

Idéntica posición adoptan la Estrategia de Seguridad Nacional (ESN Japón, 2022) y la Estrategia de Defensa Nacional, publicadas ambas a finales de 2022. El sustantivo crecimiento del presupuesto de Defensa nipón, desde entonces, atestigua la importancia que Tokio concede a su seguridad y a la alianza estratégica con Estados Unidos. Dentro de ese marco, es muy probable que las oportunidades para colaborar en desarrollos tecnológicos con Japón sean inminentes.

3.1. Algunos casos de uso japoneses

El concepto de *loyal wingman* resulta extremadamente atractivo para la situación japonesa actual. Los enjambres de drones asociados a los cazas de la próxima generación figuran en la práctica

totalidad de los proyectos actuales. La participación de Japón en el desarrollo del Tempest (GCAP), junto con el Reino Unido e Italia, favorece su implicación directa en este tipo de proyectos (Kadial y Kumar, 2023).

Sin embargo, la línea de investigación que se abre desde el 22 de diciembre de 2023 no es con los países afines europeos, sino con el aliado estadounidense. Con un nombre tan significativo como *Overwhelming Response through Collaborative Autonomy*, ambos departamentos de Defensa pretenden hacer converger los estudios sobre aeronaves no tripuladas con los que analizan la IA y el aprendizaje máquina de última generación.

Los resultados se aplicarán en el futuro caza de combate japonés y en los desarrollos de la USAF (*Next Generation Air Dominance*) y la USN (F-A/XX) (Waldon, 2023).

Otra aplicación directa de la IA a la defensa del archipiélago japonés y sus ciudadanos se produce en el campo de la ciberseguridad. En un país con frecuentes y graves contenciosos con vecinos muy avezados en operaciones cibernéticas ofensivas como la República Popular de China, la Federación Rusa o Corea del Norte, la ciberseguridad es un elemento imprescindible. No lo es solamente en relación con la información, sino también en el funcionamiento de los propios sistemas de Defensa.

En el primer caso, el reciente descubrimiento por parte de la NSA estadounidense de una infiltración de un actor procedente de China que había estado operando dentro de las redes de Defensa niponas desde 2020 ha activado todas las alarmas. La prensa recogió incluso la preocupación estadounidense por la capacidad de su aliado para proteger la información compartida. Aunque no trascendió nada más, Tokio ha incluido entre las tecnologías críticas a la inteligencia artificial, mencionando su uso para contrarrestar ciberataques enemigos (Noyes, 2023).

Cabe recordar que Japón es también la víctima favorita de los criminales informáticos norcoreanos. Una parte muy sustancial de los fraudes —generalmente sobre operaciones con criptomonedas— cometidos desde Pyongyang tiene como objetivo a empresas y particulares japoneses. Si bien no hay una relación directa entre estos ataques y el Ministerio de Defensa nipón, sí es cierto que los fondos sustraídos alimentan la industria de Defensa norcoreana y son, por lo tanto, fuente de amenazas para el archipiélago.

4. Conclusiones

Tanto la República de Corea como Japón enfrentan retos similares en cuanto a la modernización de sus Fuerzas Armadas. La escasez de personal en edad militar, provocada por las bajadas de natalidad, condiciona su operatividad y fomenta la investigación en sistemas autónomos guiados por IA. Por otro lado, su ubicación en un escenario complejo en el que la República Popular China, la Federación Rusa y la República Popular Democrática de Corea —las tres potencias nucleares— se encuentran muy próximas, obliga a dotarse de una capacidad de reacción —o, mejor, de anticipación— que favorece el empleo de la IA en el proceso de toma de decisiones.

Finalmente, tanto en tiempo de paz como en periodos bélicos, las amenazas cibernéticas representan una constante espada de Damocles para su propiedad intelectual y para la preservación de la capacidad de ejercer mando y control sobre sus unidades. El uso de algoritmos para mejorar sus capacidades de ciberdefensa pretende, al menos, contrarrestar esfuerzos similares de potenciales adversarios en la región y fuera de ella.

Ambos países cuentan con la notable ventaja de poseer una excelente industria digital, notable talento y el apoyo de su aliado estadounidense y de los países afines. Al mismo tiempo, la proximidad física al peligro ahuyenta el riesgo de complacencia. A pesar del carácter pacifista nipón, la población se posiciona a favor del desarrollo de capacidades defensivas (aunque no necesariamente de su financiación).

Por su parte, Corea del Norte, privada no solo de apoyos occidentales, sino también castigada con numerosas y crecientes sanciones, recurre a la IA para crear un espejo de los usos de sus vecinos occidentalizados. Sus campañas cibernéticas se han venido centrando, hasta el momento, en la obtención de fondos con los que financiar los programas armamentísticos nucleares y de misiles. No obstante, sus *hackers* están mejorando también sus capacidades de la mano de los algoritmos. La necesidad de defender su cadena de mando estratégica de interferencias hostiles debe forzar también un mayor compromiso con la propia Defensa.

Bibliografía

Agency for Defense Development. (s.f.). Autonomus Tunnel Exploration Robot. [Consulta: 2024]. Disponible en: https://www.add.re.kr/board?menuId=MENU02924&siteId=SITE00003.

AI Summit Seoul. (2024). AI Summit Seoul 2024 [en línea]. [Consulta: 2024]. Disponible en: https://aisummitseoul.com/[5].

Cha, E. (2023). South Korea to develop AI system for mine warfare. *Naval News.* [Consulta: 2024]. Disponible en: https://www.navalnews.com/naval-news/2023/12/south-korea-to-develop-ai-system-for-mine-warfare/.

Crunch base [en línea]. (s.f.). [Consulta: 2024]. Disponible en: https://www.crunchbase.com/hub/south-korea-artificial-intelligence-companies[6].

Demarest, C. (2023). South Korea company fuses AI with imagery to detect ballistic missiles. *Defense News*. [Consulta: 2024]. Disponible en: https://reader.defensenews.com/2023/05/23/south-korea-company-fuses-ai-with-imagery-to-detect-ballistic-missiles/content.html.

Domínguez, G. (2023). Japan joins U.S.-led effort to regulate military use of AI. *The Japan Times*. [Consulta: 2024]. Disponible en: https://www.japantimes.co.jp/news/2023/11/14/japan/politics/japan-us-ai-military-declaration/.

Electronic and Telecommucations Research Institute. (s.f.). *Artificial Intelligence Computing Research Laboratory* [en línea]. [Consulta: 2024]. Disponible en: https://www.etri.re.kr/eng/sub6/sub6_0101.etri?departCode=10.

Europa Press. (2024). Corea del Norte afirma haber probado un "sistema de armas nucleares submarinas" ante las tensiones en la región. [Consulta: 2024]. Disponible en: https://www.europapress.es/internacional/noticia-corea-norte-afirma-haber-probado-sistema-armas-nucleares-submarinas-tensiones-region-20240119043034.html.

Expert Market Research. (2024). *South Korea Artificial Intelligence Market Outlook* [en línea]. [Consulta: 2024]. Disponible en: https://www.expertmarketresearch.com/reports/south-korea-artificial-intelligence-market[7].

Glosserman, B. (2023). The Washington-Beijing tech war is just getting started. *The Japan Times*. [Consulta: 2024]. Disponible en: https://www.japantimes.co.jp/commentary/2023/12/12/

[5] Convocatoria del AI Summit Seoul 2024, a celebrarse en diciembre de ese año.

[6] Empresas vinculadas a la IA en la República de Corea.

[7] Interesante documento sobre la historia y perspectivas del mercado de la IA en Corea del Sur. En él se valora el mercado actual de la IA en la República de Corea en más de 1000 millones de dólares y se especula con un crecimiento anual del 15,3 % hasta superar los 3500 millones en 2032.

world/us-china-tech-war/?utm_source=pianodnu&utm_medium=email&utm_campaign=72&tpcc=dnu&pnespid=9febytrlurpi.lpjthysv_zk9xer.sflwg8iq1a2sk6vb.egdlikrmwpegs6bullgtknrw.

Hornung, J. W. *et al.* (2021). *Preparing Japan's Multi-Domain Defense Force for the Future Battlespace Using Emerging Technologies*. RAND Corporation. [Consulta: 2024]. Disponible en: https://www.rand.org/pubs/perspectives/PEA1157-1.html[8].

Kadidal, A. y Kumar N. (2023). Japan to develop AI wih US for loyal wingman UAVs. *JANES.* [Consulta: 2024]. Disponible en: https://www.janes.com/defence-news/news-detail/japan-to-develop-ai-with-us-for-loyal-wingman-uavs.

Kim, F. (2022). South Korea enhances Defense with robotics AI systems. *Indo Pacific Defense Forum*. [Consulta: 2024]. Disponible en: https://ipdefenseforum.com/2022/09/south-korea-enhances-defense-with-robotics-ai-systems/.

Korea Institute for Defense Analyses. (2023). *Defense Innovation 4.0 to build Robust ROK Armed Forces of AI Science and Technology.* [Consulta: 2024]. Disponible en: https://www.kida.re.kr/frt/board/frtPcrmBoardDetail.do?sidx=366&idx=2624&depth=3&searchCondition=&searchKeyword=&pageIndex=1&lang=en.

Korea Internet and Security Agency. (s.f.). [en línea]. [Consulta: 2024]. Disponible en: https://www.kisa.or.kr/EN.

Korea Science. [en línea]. (s.f.). [Consulta: 2024]. Disponible en: https://koreascience.kr/journal/OGJNBS.page[9].

Kyodo News Agency. (2023a). Japan's AI draft guidelines ask for measures to address overreliance. *The Japan Times*. [Consulta: 2024]. Disponible en: https://www.japantimes.co.jp/news/2023/10/15/japan/politics/ai-draft-guidelines/?utm_source=pianodnu&utm_medium=email&utm_campaign=72&tpcc=dnu&pnespid=5fpany5b_vox.qigvqggv_kf9q0gochvwxn3gks341yvw86k2.n4i5esanb7cf_tuloaoa.

— (2023b). Japan scientists create world's first mental images with AI tech. *The Japan Times*. [Consulta: 2024]. Disponible en: https://www.japantimes.co.jp/news/2023/12/16/japan/science-health/scientists-ai-mental-imaging/?utm_

[8] Empresa vinculada a la IA en la República de Corea.

[9] Se trata de una publicación de carácter trimestral a cargo del Korean Institute of Science and Technology Information (KISTI).

source=pianodnu&utm_medium=email&utm_campaign=72&tpcc=dnu&pnespid=op_zyywm7abiofojtg_2v.kj_kalu3z6lamkrec14lavozb0avdabm9wralqpnxruu6slg.

Lee, H. (2024). South Korean military integrates AI in frontline surveillance system. *Korea JoongAng Daily*. [Consulta: 2024]. Disponible en: https://koreajoongangdaily.joins.com/news/2024-01-09/national/defense/South-Korean-military-integrates-AI-in-frontline-surveillance-system/1954288.

Libre mercado. (2023). Nvidia planea establecer un centro de innovación sobre inteligencia artificial en Japón [en línea]. *Libre Mercado*. [Consulta: 2024]. Disponible en: https://www.libremercado.com/2023-12-06/nvidia-planea-establecer-un-centro-de-id-sobre-inteligencia-artificial-en-japon-7077041/.

López, J. C. (2023). NVIDIA va a montárselo por su cuenta en Japón. Y a darle prioridad frente a otros países. *Xataka*. [Consulta: 2024]. Disponible en: https://www.xataka.com/empresas-y-economia/nvidia-va-a-montarselo-su-cuenta-japon-a-darle-prioridad-frente-a-otros-paises.

Mainichi. (2023). G7 crafts 1st int'l principles covering AI users to mitigate risks [en línea]. *The Mainichi*. [Consulta: 2024]. Disponible en: https://mainichi.jp/english/articles/20231201/p2g/00m/0in/079000c.

Ministerio de Defensa de Japón. (2023). *Defense White Paper.* [Consulta: 2024]. Disponible en: https://www.mod.go.jp/en/publ/w_paper/index.html.

Ministry of National Defense Republic of Korea. (2023). *Defense White Paper 2022*. [Consulta: 2024]. Disponible en: https://www.mnd.go.kr/cop/pblictn/selectPublicationUser.do?siteId=mndEN&componentId=51&categoryId=0&publicationSeq=1057&pageIndex=1&id=mndEN_031300000000.

Noyes, M. (2023). Japan embraces AI to boost cyber defense, fight disinformation [en línea]. *Fox News*. [Consulta: 2024]. Disponible en: https://www.foxnews.com/world/japan-embraces-ai-boost-cyber-defense-fight-disinformation.

Office of National Security. (s.f.). *Estrategia de Seguridad Nacional de la administración del presidente Yoon Suk Yeol*. [Consulta: 2024]. Disponible en: https://www.president.go.kr/download/648037c2bf5e7.

Pérez, E. (2023). El G7 acuerda unas reglas a nivel mundial para la IA. La solución de Japón ha ganado [en línea].

Xataka. [Consulta: 2024]. Disponible en: https://www.xataka.com/legislacion-y-derechos/g7-acuerda-unas-reglas-a-nivel-mundial-para-ia-solucion-japon-ha-ganado/amp#amp_tf=De%20%251%24s&aoh=16987043136350&csi=0&referrer=https%3A%2F%2Fwww.google.com.

Protector indefinido. (2023). Canon presenta oficialmente su escáner de nanoimpresión para chips de 5 nm ¿competencia para ASML y EUV? [en línea]. *El chapuzas informático.* [Consulta: 2024]. Disponible en: https://elchapuzasinformatico.com/2023/11/canon-escaner-litografia-nanoimpresion-chips-5-nm/.

Republic of Korea National Cybersecurity Strategy [en línea]. (2023). *dig.watch*. [Consulta: 2024]. Disponible en: https://dig.watch/resource/south-korean-national-cybersecurity-strategy#313_Develop_next-generation_cybersecurity_infrastructure.

Samsung Research. [en línea]. (s.f.). Samsung Research AI Center [Consulta: 2024]. Disponible en: https://research.samsung.com/aicenter_seoul.

Secretaría del Gabinete. (2022). National Security Strategy of Japan [en línea]. [Consulta: 2024]. Disponible en: https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf.

Su, F. (2019). *Military developments in artificial intelligence and their impact on the Korean peninsula*. [Consulta: 2024]. Disponible en: https://www.jstor.org/stable/resrep24532.12.

Waldon, G. (2023). Japan USA to research AI in unmanned aircraft [en línea]. *Flight Global.* [Consulta: 2024]. Disponible en: https://www.flightglobal.com/defence/japan-usa-to-research-ai-in-unmanned-aircraft/156314.article.

Warren, A, Hunt, C. T. y Warren, M. (2023). AI cooperation between Australia, Japan and the United States. *Australian Institute of International Affairs*. [Consulta: 2024]. Disponible en: https://www.internationalaffairs.org.au/australianoutlook/ai-cooperation-between-australia-japan-and-the-united-states/.

Capítulo tercero

Análisis de la geopolítica mundial mediante inteligencia artificial (IA) y *big data*

Álvaro Ortiz, Tomasa Rodrigo

Resumen

La digitalización de la información y el desarrollo de la inteligencia artificial está propiciando un cambio sin precedentes en la disponibilidad de nueva información de manera no-estructurada (texto, vídeo...). Gracias al desarrollo de los modelos de procesamiento de lenguaje natural (NLP), el texto se ha convertido en una de las principales fuentes de información, y la posibilidad de trasladar «Texto a Números» se está convirtiendo en una poderosa herramienta de análisis en el campo de la ciencia política y las relaciones internacionales. En este artículo repasamos los distintos modelos y bases de datos que extraen y procesan texto de los medios de comunicación locales e internacionales para su uso en el análisis de las relaciones internacionales, incluyendo el seguimiento en tiempo real y la previsión de conflictos. Entre ellos, presentamos varios ejemplos desarrollados por el sistema de seguimiento geopolítico desarrollado en BBVA Research, incluyendo el análisis de flujos migratorios a Europa tras la crisis en Siria, la guerra entre Rusia y Ucrania, el conflicto armado Israel-Hamas y el impacto de los cuellos de botella y tensiones entre China y Taiwán en el sector estratégico de los semiconductores.

Palabras clave

Big data, Inteligencia artificial, Procesamiento del lenguaje natural, Geopolítica, Modelos de alerta temprana.

Analysis of global geopolitics through artificial intelligence (AI) and big data

Abstract

The digitisation of information and the development of artificial intelligence is bringing about an unprecedented change in the availability of new information in an unstructured form (text, video...). Thanks to the development of natural language processing (NLP) models, text has become one of the main sources of information, and the possibility of translating "Text to Numbers" is becoming a powerful tool for analysis in the field of political science and international relations. In this article we review the various models and databases that extract and process text from local and international media for use in the analysis of international relations, including real-time monitoring and conflict forecasting. Among them, we present several examples developed by the geopolitical monitoring system developed at BBVA Research, including the analysis of migration flows to Europe after the Syrian crisis, the war between Russia and Ukraine, the armed conflict between Israel and Hamas and the impact of shortgates and tensions between China and Taiwan in the strategic semiconductor sector.

Keywords

Big data, Inteligencia artificial, Natural Language Processing, Geopolitics, Early warning models.

1. La revolución en la inteligencia artificial y los modelos de procesamiento del lenguaje natural

El rápido desarrollo del proceso de digitalización y los crecientes avances en el campo de la inteligencia artificial (IA) están propiciando una revolución en el análisis de las ciencias sociales. Lo que conocemos como *big data* es el resultado de diferentes fuerzas que han venido operando simultáneamente desde hace tiempo y que se refuerzan entre sí: el rápido desarrollo de la capacidad de procesamiento de los ordenadores, el creciente volumen de información y el veloz desarrollo de los algoritmos.

La primera de ellas, la capacidad de procesar información de las computadoras, ha sido clave en el desarrollo de la IA. El rápido desarrollo de los ordenadores en las últimas décadas ha sido un fenómeno asombroso en el que el número de transistores, tal y como predijo Gordon Moore (1965: 114) hace seis décadas, ha venido casi doblándose cada dos años aproximadamente. Esto ha supuesto un aumento exponencial en el rendimiento y la capacidad de procesamiento, que ha venido acompañada de un descenso de tamaño considerable de los mismos (desde los primeros que ocupaban habitaciones enteras hasta los modernos dispositivos móviles que caben en la palma de nuestra mano), así como una disminución notable en su coste.

La mayor potencia de los ordenadores ha facilitado también el desarrollo de la gestión, procesamiento y análisis de cantidades masivas de datos a una velocidad antes inimaginable. Esto ha sido fundamental para la evolución y expansión de internet, que ha actuado como catalizador de la digitalización de la información. Entre otras cosas, internet ha supuesto una digitalización casi total de la información existente, facilitando el acceso a la misma, su distribución y su compartición a través de las redes globales.

El desarrollo de internet no solo ha mejorado la eficiencia, en términos de almacenamiento y distribución de la información, sino que también ha abierto nuevas vías para el análisis de datos como, por ejemplo, las tecnologías de computación en la nube. Estas han facilitado el acceso a una capacidad de procesamiento y almacenamiento de datos que hace años era simplemente inalcanzable. Todo ello, junto al rápido descenso de los costes de los ordenadores y dispositivos, ha permitido una democratización del acceso a tecnologías avanzadas sin precedentes.

Por último, el desarrollo de nuevos algoritmos está contribuyendo también al rápido avance de la inteligencia artificial (IA). Los algoritmos proporcionan las reglas y procedimientos que guían el aprendizaje y la toma de decisiones de las computadoras. A medida que evolucionan, también lo hace su capacidad de realizar tareas cada vez más complejas. Los algoritmos de aprendizaje profundo, por ejemplo, han permitido avances significativos en áreas como el reconocimiento de voz, de imágenes, la conducción autónoma... Los recientes desarrollos en los grandes modelos del lenguaje (LLM) e inteligencia generativa aventuran avances sin precedentes en el ámbito de análisis de las ciencias sociales, incluyendo el análisis geopolítico.

Todo ello forma parte de lo que, en este artículo, entendemos como *big data*. Esto es, el acceso al procesamiento de datos masivos gracias al desarrollo de la capacidad de procesamiento de los ordenadores y a los nuevos algoritmos que nos permite convertir esta información, muchas veces no estructurada, en datos que podemos utilizar para analizar cuestiones complejas en las ciencias sociales.

Dentro del amplio espectro de información no estructurada con potencial para ser utilizada en el campo del análisis de las ciencias sociales (imágenes, vídeo, audio etc.), y en particular de las relaciones internacionales, la información proveniente de los textos ha jugado un papel relevante. Aquí, el desarrollo de un conjunto de algoritmos conocidos como modelos de procesamiento del lenguaje natural (NLP) han permitido extraer texto en forma no estructurada y convertirlo en información estructurada numérica susceptible de ser procesada para el análisis de las relaciones internacionales.

El avance en los modelos de procesamiento del lenguaje natural ha sido también relativamente rápido y ha ido evolucionando en complejidad, desde el análisis de palabras individuales y su distribución en temas, a encontrar sentido a las palabras según el contexto que los acompaña; hasta inferir o predecir texto como en el caso de los nuevos modelos de procesamiento del lenguaje natural.

Los primeros modelos se centraron básicamente en palabras o *tokens* individuales. Estos primeros modelos se caracterizan por analizar la frecuencia de las palabras en las búsquedas booleanas. Aunque simples, estos algoritmos nos permiten, por ejemplo, analizar cuestiones como el grado de incertidumbre, simplemente

analizando búsquedas de palabras como «Incertidumbre» y el conjunto del campo de palabras asociadas al fenómeno que queremos aplicar. En el caso de la incertidumbre de política económica, un buen ejemplo de ello es el trabajo de Baker, Bloom y Davis (2016), mientras que, en el ámbito de las relaciones internacionales, Caldara y Iacovello (2022) han desarrollado índices de incertidumbre geopolítica al estilo de los que describiremos en los siguientes apartados.

Otros algoritmos sencillos hacen uso de técnicas asistidas por diccionarios específicos para interpretar el sentimiento de los textos. Estos algoritmos supervisados pueden ser utilizados para clasificar el carácter positivo o negativo de los textos, la polarización o armonía, etc... Existen múltiples diccionarios, desde aquellos más generales a diccionarios con terminologías específicas (economía, relaciones internacionales, medicina, legales...) desarrollados por expertos. Dentro del campo de las relaciones internacionales, algunos artículos se han centrado en la polarización de los discursos políticos (Gennaro y Ash, 2021), mientras otros autores han mostrado, por ejemplo, cómo la combinación de técnicas y análisis del sentimiento pueden ser utilizado para diseñar un modelo de radicalización en las redes sociales (Bermingam *et al*., 2009).

Con el tiempo, los algoritmos se sofisticaron y comenzaron a tener en cuenta el contexto global del texto a analizar. Nacieron así los modelos dinámicos de temas desarrollados por David Blei (2003), que resumen el texto en estructuras semánticas o temas latentes. Los analistas políticos o de relaciones internacionales han analizado varios textos como discursos, debates, iniciativas legales, contenido de los medios, etc. Son modelos probabilísticos cuyo resultado lo forman grupos de palabras con mayor o menor probabilidad de pertenecer a un grupo. La mayoría de esos modelos son de carácter no supervisado, pues es el analista el que debe etiquetar manualmente el conjunto de palabras incluidas en un grupo. Existen numerosos trabajos que utilizan los modelos temáticos dentro del ámbito de las relaciones internacionales o la ciencia política. Entre ellos cabe destacar los trabajos de Mueller y Rauh (2018), que utilizan la variación en los temas en periódicos nacionales para predecir conflictos armados y violencia política en distintos países, o Martin y McCrain (2019), que utilizan un modelo de temas para analizar cómo los cambios en la propiedad conducen a cambios en la cobertura de la política nacional o sesgos de orientación.

Un importante avance en los modelos de procesamiento del lenguaje natural se produjo con el desarrollo de los modelos de incrustación de palabras (*word embeddings*), que son el germen a los modelos generativos del lenguaje natural. Estos modelos están basados en la hipótesis de la distribución del lenguaje[1]. Esta hipótesis sostiene que las palabras que aparecen en contextos similares tienden a tener significados similares y es normalmente el contexto lo que proporciona a las palabras su significado. Esta propiedad se ha convertido en un concepto fundamental en el campo de la lingüística computacional y el procesamiento del lenguaje natural (NLP).

Una de sus aplicaciones más populares ha sido para el diseño de diccionarios y clasificación de sentimientos o temas de una manera semiautomática. De acuerdo con varios autores (Rodriguez y Stewart, 2023), los resultados en el campo de la ciencia política son satisfactorios y, en términos generales, estos modelos obtienen resultados relativamente buenos, a veces incluso mejores, que los que proporcionan los codificadores o etiquetadores humanos.

Si bien los modelos de incrustación de palabras avanzaron significativamente en la comprensión y análisis de las palabras con significados similares (sinónimos), tuvimos que esperar al desarrollo de los «Transformadores» (Vaswani *et al*., 2017) y los grandes modelos de lenguaje para poder distinguir significados distintos para una misma palabra (polisemia). Para ello, estos modelos necesitan «prestar atención»[2], lo que en términos computacionales significa poder valorar la importancia de cada vector de palabras incrustadas en cada caso. Estos modelos utilizan estructuras similares a las de las redes neuronales, capaces de valorar cuales son las palabras clave del contexto para averiguar la siguiente palabra o aquella que queremos interpretar[3].

---

[1] Este concepto se basa en el trabajo del lingüista Zellig Harris, quien en la década de 1950 propuso que la similitud semántica entre palabras podía ser determinada por sus patrones de ocurrencia conjunta en el lenguaje. La idea es que el significado de una palabra se construye y se refleja a través de su uso, y, por lo tanto, analizando los patrones de cómo las palabras se distribuyen en grandes cantidades de texto, se puede inferir su significado y sus relaciones semánticas con otras palabras.

[2] El título en inglés del famoso artículo de Vaswani (2017) es «Todo lo que necesitas es atención» (*Attention is all you need*).

[3] Un buen ejemplo de ello es el desarrollo y aplicación de los *Transformers* a la codificación automática de los modelos de alerta temprana de eventos de conflicto como «Polecat» que serán explicados en la próxima sección.

Los grandes modelos de lenguaje (LLM) han comenzado ya a utilizarse con éxito en el ámbito de las relaciones internacionales. Estos modelos han entrado recientemente en el debate público sobre inteligencia artificial, ya que posibilitan el uso de una nueva metodología fácil de usar para el estudio del lenguaje. Básicamente, los modelos LLM aprovechan técnicas de aprendizaje profundo, recursos computacionales a gran escala y enormes cantidades de datos de entrenamiento para generar textos coherentes y contextualmente relevantes. Su principal diferencia respecto a los anteriores modelos es que su objetivo es la predicción.

Mientras que los modelos LLM como GPT-3, BERT, LlaMA, BARD... han sido ampliamente utilizados en muchas aplicaciones, el reciente lanzamiento público de ChatGPT desarrollado por la empresa americana OpenAI ha abierto un debate sobre los posibles usos y abusos de los modelos de ciencia política y relaciones internacionales[4].

2. Análisis geopolítico con modelos de procesamiento del lenguaje natural: clasificación de eventos y sistemas de alerta temprana

La utilización de la inteligencia artificial para el campo de las relaciones internacionales está íntimamente ligado al desarrollo de los modelos de alerta temprana para conflictos. Este es un campo que ha evolucionado significativamente a lo largo del tiempo, integrando avances en tecnología, análisis de datos y teoría de relaciones internacionales.

El concepto de sistemas de alerta temprana ganó relevancia durante la Guerra Fría, enfocándose principalmente en amenazas militares. Estos sistemas fueron diseñados inicialmente para detectar y poder responder con anticipación a ataques nucleares.

Uno de los primeros esfuerzos académicos en alerta temprana de conflictos fue el *Conflict and Peace Data Bank* (COPDAB), desarrollado por Edward Azar (1980), a comienzos de la década de 1970 y finalmente publicado en 1980. Su objetivo era crear una base de datos completa de eventos de conflicto y cooperación internacionales y domésticos. El proyecto recopilaba datos de informes de noticias y cobertura mediática, abarcando una amplia gama

[4] Para un resumen del estado de la cuestión véase Linnegard (2023).

de eventos políticos desde disputas diplomáticas hasta conflictos armados. COPDAB empleaba su propio sistema de codificación que clasificaba las interacciones entre actores (como Estados, organizaciones internacionales y grupos no estatales) en una escala de conflicto a cooperación.

A COPDAB le siguieron los proyectos como WEIS (McLellland, 1976) y KEDs (Schrodt, 1994), desarrollado por Philip Schrodt en la década de 1990. Ambos fueron significativos en la automatización del código de datos de eventos a partir de fuentes de noticias. A comienzos del siglo XXI se desarrollaron varios proyectos como el Programa de Datos de Conflictos de Uppsala (UCDP), desarrollado por Sundberg y Melander (2013), el sistema de alerta temprana integrado de crisis (ICEWS) financiado por DARPA en 2007 y desarrollado por la empresa Lockeed Martin, bajo la dirección de Paul O'Brien (2010) y que ha sido mejorado y rebautizado como POLECAT (Haltermann *et al*., 2023) y actualmente financiado por la CIA, y el proyecto de la Base de Datos Global de Eventos, Lenguaje y Tono (GDELT), iniciado en 2011 y publicado en 2013 por Leetaru y Schrodt (2013), que utilizaremos posteriormente como base al sistema de seguimiento geopolítico desarrollado por BBVA Research y que utilizaremos en el resto del artículo.

Los programas UCDP (Programa de Datos de Conflictos de Uppsala), GDELT (Base de Datos Global de Eventos, Lenguaje y Tono), ICEWS (Sistema Integrado de Alerta Temprana de Crisis) y POLECAT son proyectos significativos en el campo de datos de eventos globales y análisis de conflictos, pero difieren en su enfoque, metodología y aplicaciones. Entre las principales diferencias:

- El programa de datos de conflictos de la Universidad de Uppsala (UCDP), se centra en datos de conflictos armados y eventos similares. Proporciona información detallada sobre guerras, conflictos no estatales y violencia unilateral y combina la información de expertos con la de los medios de comunicación para la recopilación y categorización de datos. Los datos son de frecuencia anual y se han utilizado ampliamente en investigaciones académicas sobre conflictos y relaciones internacionales. Mueller y Rauh (2018) utilizan por ejemplo la base de datos de UCDP en su trabajo sobre la relevancia de la información de los medios para la predicción de conflictos.
- La base de datos Global de Eventos, Lenguaje y Tono (GDELT), es una vasta base de datos que rastrea eventos, lenguaje y tono de los medios de comunicación globales. Cubre una

amplia gama de eventos, incluidos, pero no limitados a conflictos. Como en el caso de ICEWS utiliza técnicas computacionales avanzadas para procesar datos de medios a gran escala, incluyendo las técnicas de los modelos de procesamiento del lenguaje natural y análisis de big data. GDELT utiliza un sistema de codificación de eventos basado en el esquema CAMEO (del inglés Conflict and Mediation Event Observations), desarrollado por Gerner et al. (2002), para categorizar los eventos políticos. Sus aplicaciones son diversas, desde investigación académica en ciencias sociales hasta usos prácticos en periodismo, inteligencia empresarial y análisis de políticas.

- El Sistema Integrado de Alerta Temprana de Crisis (ICEWS), está diseñado como un sistema de alerta temprana para predecir crisis políticas. Cubre una gama más amplia de eventos políticos, no limitados a conflictos armados. Combina la recopilación de datos automatizada (usando PNL y aprendizaje automático) con análisis de expertos y, como GDELT, utiliza el esquema CAMEO para categorizar los eventos. Utiliza la base de datos para orientar a los policymaker en las políticas y para el desarrollo de modelos para anticipar y responder a crisis internacionales.
- El Sistema de clasificación de Eventos Políticos, Atributos y Tipos (POLECAT), ha reemplazado recientemente a ICEWS (Halterrmann et al., 2023). Utiliza la ontología PLOVER (Political Language Ontology for Verifiable Event Records) para la codificación de eventos, en lugar de CAMEO. De acuerdo con sus autores, esta ontología es más flexible y adaptable, permitiendo una clasificación más detallada y variada de los eventos. POLECAT integra tecnologías avanzadas de procesamiento del lenguaje natural, incluyendo la base de los más avanzados modelos de lenguaje (Transformers) al análisis automatizado de eventos, buscando mejorar la precisión y la cobertura de los datos. Aunque también es útil en la formalización de políticas y análisis de Defensa, tiene un enfoque más amplio que puede ser de interés para investigadores académicos, organizaciones internacionales y otros usuarios interesados en el análisis político global.

La información subyacente a los diferentes sistemas es diferente. En el caso de UCDP se utilizan varios criterios para la inclusión de eventos, normalmente conflicto y violencia, junto a una amplia gama de fuentes de información proveniente de informes de organizaciones internacionales, gobiernos, ONGs, medios de comunicación y estudios académicos. Los datos son sometidos a

un riguroso proceso de verificación para asegurar su precisión. La base de datos se actualiza anualmente, proporcionando una perspectiva actualizada de los conflictos en curso y recientes.

En el caso de GDELT, ICEWS y POLECAT se utiliza el sistema de codificación de eventos de CAMEO. Este sistema está diseñado para clasificar y analizar eventos políticos y particularmente a los relacionados con conflictos y mediación. Utiliza una estructura jerárquica para clasificar eventos, dividida en categorías y subcategorías, que describen la naturaleza de la acción política o del conflicto. Las categorías de eventos en CAMEO varían desde niveles muy generales hasta más específicos. No solo identifica eventos, sino también actores y acciones. Los actores involucrados en eventos pueden ser estados, organizaciones internacionales, grupos no estatales, líderes políticos, grupos terroristas, etc.… mientras que las acciones que realizan estos actores son codificadas según la naturaleza del evento, como declaraciones diplomáticas, acciones militares, protestas, atentados, acuerdos, etc.

El Sistema de codificación de CAMEO está asociado a la escala de Goldstein (2002) y suelen utilizarse conjuntamente. El proceso de codificación en CAMEO se realiza en distintas fases. En una primera fase se analiza el texto, que normalmente proviene de noticias. En ellas, el sistema de codificación identifica los actores y las acciones descritas en el texto asignándoles el código correspondiente en la clasificación, mediante la utilización de técnicas de procesamiento de lenguaje natural. Esta clasificación tiene una estructura jerárquica, desde categorías generales hasta acciones más específicas. En su estructura más amplia consta de cuatro grupos o categorías que podemos ordenar desde cooperación material, cooperación verbal, conflicto verbal y conflicto material. Cada una de estas categorías consta de diferentes eventos, que, a su vez, pueden descomponerse en subcategorías con eventos más detallados.

El gráfico 1 nos ayuda a entender la clasificación. En la primera escala vemos las cuatro categorías ordenadas de mayor a menor relevancia en términos de violencia. En el ejemplo podemos apreciar cómo dentro del gran grupo de violencia verbal encontramos la agrupación de protesta. Esta se puede subdividir en varias categorías de protesta, ordenadas según su intensidad. Una vez los eventos y acciones están clasificadas, la escala de Goldstein asigna valores numéricos a diferentes tipos de eventos políticos, reflejando el potencial de cada tipo de evento para contribuir a la

estabilidad o inestabilidad política. Los valores en la escala varían desde mayores puntuaciones en las acciones cooperativas materiales y verbales (con valores positivos) a acciones con valores negativos asociados al conflicto verbal y al material. El conflicto material se asocia a los valores más negativos y, en su caso, por la utilización de armas de destrucción masiva.

Agrupaciones	Eventos	Codigo	Escala de Goldstein
Cooperacion Material	Establecer Cooperación Material (6)	6	6
	Proporcionar Ayuda (7)	7	7
	Producir (26)	8	5
	Investigar (6)	9	-2
Cooperación Verbal	Realizar Anuncio Público (11)	1	0
	Apelar (28)	2	3
	Expresar intencion de Cooperar (29)	3	4
	Consultar (8)	4	1
	Establecer Cooperación Diplomática (9)	5	3.5
Conflicto Verbal	Demandar (27)	10	-5
	Desaprobar (13)	11	-2
	Rechazar (27)	12	-4
	Amenazar (23)	13	-6
	Protestar (27)	14	-6.5
Conflicto Material	Exhibir Postura de Fuerza (6)	15	-7.2
	Reducir relaciones (14)	16	-4
	Coaccionar (13)	17	-7
	Asaltar (14)	18	-9
	Luchar (8)	19	-10
	Usar Armas de Destrucción Masiva (8)	20	-10

Gráfico 1. Clasificación de CAMEO y escala de Goldstein. Fuente: GDELT y Goldstein

Más allá de clasificar los eventos, poder evaluar la intensidad de estos y geolocalizarlos con precisión, las técnicas de procesamiento del lenguaje natural permiten desarrollar multitud de análisis en diferentes campos de las ciencias sociales. Entre ellas, nos permite evaluar el sentimiento con que se producen los eventos, con la ayuda de diccionarios especializados o la descomposición de grandes corpus de información de texto en los temas más relevantes. Los nuevos modelos de procesamiento de lenguaje natural ofrecen oportunidades que son difíciles de imaginar.

3. De texto a números: seguimiento y análisis geopolítico en BBVA Research

En la sección anterior hemos mostrado cómo podemos utilizar las técnicas de procesamiento de lenguaje natural para examinar y analizar multitud de eventos. Esto nos ha ayudado a entender

mejor una situación geopolítica cambiante y cada vez más compleja. En BBVA Research hemos estado trabajando durante la última década con esta metodología. El proyecto comenzó con la idea de usar datos cuantitativos para observar y examinar conflictos geopolíticos, especialmente aquellos que podrían tener un impacto significativo en la economía mundial. Este sistema nos ha proporcionado una descripción de los eventos casi en tiempo real y en alta definición o granularidad. En este sentido, la combinación de *big data* de noticias mundiales y las técnicas de procesamiento del lenguaje natural nos han dado como resultado una herramienta de análisis muy valiosa para analizar las relaciones internacionales.

El sistema que hemos desarrollado está basado en la Base de Datos Global de Eventos, Lenguaje y Tono (GDELT) descrita en la sección anterior. GDELT es una fuente de código abierto que analiza noticias digitales en más de cien idiomas. Además, clasifica la información utilizando miles de taxonomías y temas, identificando emociones, organizaciones, ubicaciones y eventos, así como el tono promedio de las noticias, que varía de -100 a +100, indicando sentimientos negativos o positivos, respectivamente.

Para construir los índices capturamos tanto la cobertura como el sentimiento de los artículos de noticias diarios que mencionan conflictos y protestas. Hemos desarrollado un amplio conjunto de índices que incluyen el riesgo geopolítico, la estabilidad política, los índices de conflicto y protesta, el índice de incertidumbre de política económica y nuestro índice de sentimiento bilateral entre países. Para algunos de estos índices también podemos distinguir entre fuentes de medios extranjeros o locales. En esencia, capturamos cómo los medios de comunicación mundiales perciben la situación geopolítica[5].

Durante estos años hemos utilizado este conjunto de indicadores para el seguimiento de diferentes conflictos. En la siguiente sección mostramos algunos ejemplos, como el seguimiento del impacto de la crisis de Siria, en la emigración hacia Europa, las guerras entre Rusia y Ucrania y, la más reciente, entre Israel y Hamas, así como la evolución del sentimiento mundial del mercado de los semiconductores y su relación con las tensiones entre China y Taiwán.

[5] Todos nuestros índices están normalizados, lo que significa que muestran su rendimiento relativo en comparación con su propio historial, a lo que definimos como «señales». Además, les aplicamos una media móvil geométrica de 28 días para reducir el ruido, dando más peso a la información diaria más reciente.

3.1. El conflicto sirio y la crisis migratoria a Europa

Una de las primeras aplicaciones que llevamos a cabo fue el impacto de la guerra civil en Siria en el flujo de emigrantes hacia Europa. Una de las fuentes que se han utilizado para el seguimiento de los flujos migratorios son las noticias y su geolocalización (Ahmed, 2016). Para capturar información sobre el impacto de conflictos, cambios en políticas (por ejemplo, el cierre de fronteras) y otros eventos externos, los datos de noticias proporcionados por GDELT son muy útiles.

La geolocalización de los eventos permite al analista monitorear las noticias digitalizadas en todo el mundo y extraer información valiosa de los textos. Esta incluye información sobre entidades como, personas, lugares, organizaciones etc., en más de cien idiomas diferentes. Los documentos están anotados, aplicando técnicas de procesamiento de lenguaje natural de última generación. Entre las categorías monitorizadas en la base de datos de GDELT se puede realizar un conteo de arrestos, muertes, protestas, heridos y refugiados entre otros. Además, para cada artículo, se proporcionan las ubicaciones del evento y se utilizan algoritmos para corregir el conteo múltiple. Procesada correctamente, esta información es muy valiosa para el seguimiento de los flujos de refugiados.

La guerra civil siria comenzó en marzo de 2011 como parte de la Primavera Árabe. Inició con protestas a gran escala y manifestaciones prodemocracia contra el gobierno de Bashar al-Assad, que rápidamente se reprimieron violentamente, llevando a la formación de grupos rebeldes armados y escalando hacia una guerra civil completa. Los rebeldes lograron hacer avances significativos, pero la intervención militar de Rusia, en 2015, cambió el equilibrio del conflicto a favor del gobierno. Además, el Estado Islámico tomó control de grandes partes de Siria, lo que llevó a una campaña de bombardeos liderada por EE. UU. y el apoyo a las milicias kurdas YPG y sus aliados. Turquía, preocupada por la influencia kurda en sus fronteras, lanzó operaciones transfronterizas para combatir tanto al Estado Islámico como a las fuerzas kurdas.

El conflicto generó una crisis de refugiados masiva, con millones de sirios desplazados, tanto internamente como hacia países vecinos como Turquía, Líbano y Jordania. Muchos también han buscado asilo en Europa, contribuyendo a la crisis migratoria europea. La crisis ha sido descrita como una de las mayores

crisis de refugiados en la historia, exacerbada por violaciones de derechos humanos y condiciones severas en los campos de refugiados. La situación sigue siendo una crisis humanitaria significativa con millones de personas desplazadas y en necesidad de asistencia.

La figura 2 muestra la magnitud de esta crisis de refugiados en relación con la intensificación del conflicto. Utilizando GDELT hemos desarrollado dos gráficos. El primero de ellos muestra geográficamente aquellas zonas donde los conflictos, en relación con el total de eventos, han sido más intensos. Dentro de Europa y Oriente Medio, los focos de conflicto más intenso se concentran en Siria, Irak y Yemen, con focos de conflicto aislados en Egipto y algunas de las ciudades importantes del Norte de África y menor tensión acumulada en Turquía y Grecia. En el segundo, acumulamos las noticias sobre refugiados discriminando entre origen de los refugiados (color granate) y destino (amarillo) para visualizar el origen y destino de los refugiados.

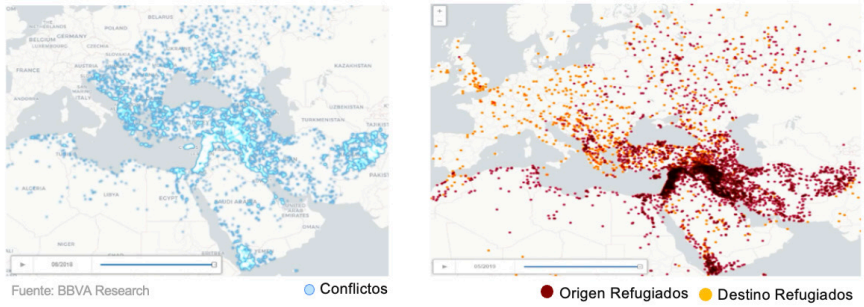


Gráfico 2. La guerra civil en siria y la emigración a Europa

Los principales destinos de los refugiados de la guerra civil siria han sido países vecinos y más allá, enfrentando una de las mayores crisis de refugiados en la historia. Turquía ha sido el país anfitrión más grande, albergando a más de 3,7 millones de refugiados sirios. Además, Líbano y Jordania recibieron incluso más en términos de porcentaje de la población, asentados, sobre todo, en campos de refugiados y comunidades urbanas.

Más allá de los países vecinos, los refugiados sirios buscaron asilo sobre todo en Europa, contribuyendo a la crisis migratoria europea. Estos países, y otros, han enfrentado desafíos significativos al tratar de acomodar y asistir a los refugiados sirios, lidiando con cuestiones de infraestructura, empleo, educación y tensiones sociales. Dentro de Europa, los principales destinos de los

refugiados sirios fueron aquellos países que ofrecieron políticas de asilo más accesibles y mejores condiciones de vida. Entre ellos destacan los países centroeuropeos (Alemania, Austria, Países Bajos y Francia), Escandinavia y el Reino Unido. Dentro de los países mediterráneos, Grecia e Italia experimentaron los mayores flujos de refugiados.

Turquía ha sido el principal receptor de refugiados sirios, con millones de sirios buscando refugio allí desde el comienzo del conflicto. El gobierno turco ha establecido campamentos de refugiados y ha ofrecido diferentes grados de apoyo y servicios a los refugiados, aunque las condiciones y el acceso a los derechos y servicios pueden variar considerablemente. En marzo de 2016, Turquía y la Unión Europea firmaron un acuerdo para frenar el flujo de migrantes hacia Europa. Según este acuerdo, Turquía aceptaría la devolución de todos los migrantes y refugiados que llegan a Grecia desde Turquía y, a cambio, la UE reaceptaría a un sirio de Turquía por cada sirio devuelto de las islas griegas.

Aunque la crisis se estabilizó a medida que el número de nuevos refugiados fue descendiendo en Siria, y que Isis comenzaba a perder influencia, muchos de los refugiados continúan en campos de refugiados o establecidos en países fuera de sus fronteras de origen.

3.2. El conflicto Rusia-Ucrania

Otra de las aplicaciones que se pueden desarrollar con GDELT es un análisis detallado de la evolución de los diferentes eventos dentro de un conflicto. En particular es posible monitorear, en tiempo real, las noticias sobre el enfrentamiento, tanto en términos generales o agregados como el análisis más detallado de eventos, de acuerdo con la clasificación de CAMEO, en términos de cooperación y conflicto material y verbal. Además, podemos monitorear la intensidad del conflicto a través de la escala de Goldstein.

Un ejemplo de esta aplicación en BBVA Research ha sido el monitoreo de eventos y su intensidad durante la guerra entre Rusia y Ucrania. Este ha sido un conflicto prolongado y complejo que ha evolucionado significativamente desde su inicio hace casi una década. En 2014, la tensión en la región se intensificó dramáticamente después de la anexión de Crimea por parte de Rusia y el estallido de la guerra en el este de Ucrania, en las regiones

de Donetsk y Luhansk. Estos eventos marcaron un cambio drástico en las relaciones entre Rusia y Ucrania, con un aumento en la intervención militar y una serie de sanciones internacionales impuestas a Rusia.

A lo largo de los años siguientes, el conflicto en el este de Ucrania se mantuvo en un estado de conflicto latente e intermitente. A pesar de los acuerdos de paz y los esfuerzos diplomáticos, como los Acuerdos de Minsk, las violaciones al alto el fuego fueron constantes y la región permaneció en un estado de inestabilidad crónica.

A lo largo de 2021 y principios de 2022, la situación se agravó significativamente cuando Rusia comenzó a acumular tropas en la frontera con Ucrania. Este movimiento generó una alarma internacional y temores de una invasión a gran escala. Las tensiones alcanzaron su punto máximo en febrero de 2022, cuando Rusia lanzó una operación militar a gran escala en Ucrania, marcando una escalada dramática en el conflicto. Esta acción fue condenada por la comunidad internacional y llevó a una nueva ola de sanciones contra Rusia, así como a un aumento significativo en el apoyo militar y humanitario a Ucrania por parte de países occidentales.

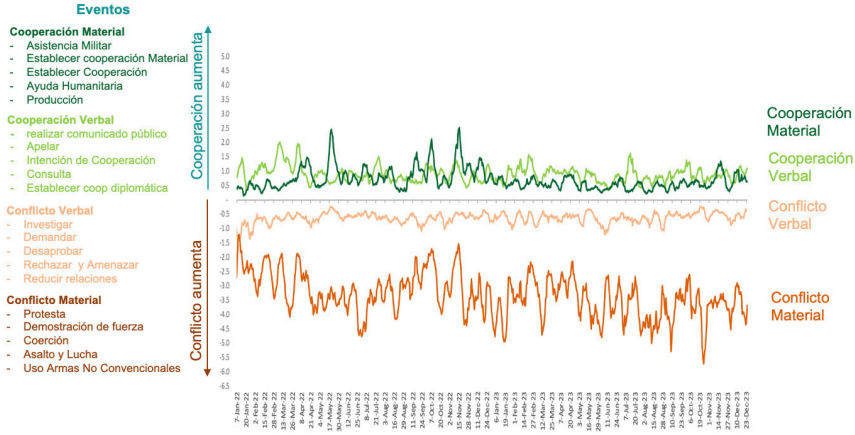
El siguiente gráfico resume la evolución de los distintos tipos de eventos en el conflicto desde la invasión de Rusia en febrero de 2022. Los cuatro índices reflejan la evolución ponderada de las cuatro grandes categorías de la escala de Goldstein (cooperación material y verbal y conflicto verbal y material). De acuerdo con esta clasificación, su intensidad y su evolución, las fases del conflicto han sido las siguientes:

- Inicio de la invasión (febrero a mayo 2022): con la invasión a gran escala de Ucrania en febrero de 2022 por parte de Rusia, el conflicto se disparó a los niveles más deteriorados de la escala de Goldstein, a medida que el número de eventos de conflicto material y su intensidad aumentaban. La reacción internacional fue en un principio de carácter verbal y pasó rápidamente a convertirse en material tras la ayuda, sobre todo, por EE. UU., pero también de Polonia, Reino Unido, Canadá, Noruega, Estonia y Letonia.
- Estabilización del conflicto y guerra de desgaste (primavera 2022 a finales de 2022): a medida que avanzaba la primavera de 2022, el conflicto se estabilizó en una guerra de desgaste, con un aumento inicial del índice de conflicto material y vaivenes en la intensidad de los enfrentamientos en la segunda mitad del año. Como refleja el índice de cooperación material,

se produjo una segunda ola de asistencia material a Ucrania y se intensificaron las sanciones a Rusia. A pesar de los esfuerzos diplomáticos internacionales, las negociaciones de paz no lograron detener el conflicto.

– Niveles de conflicto máximo (invierno de 2023): los primeros meses de 2023 fueron duros. El apoyo y la cooperación verbal sustituyó al material, mientras que el número e intensidad de los conflictos materiales alcanzaron niveles de máximo deterioro.
– Estancamiento del conflicto (finales 2023): los niveles de conflicto material continuaron en niveles de máxima tensión mientras comenzaba a apreciarse cierta mejora en los índices de cooperación material, tras haber permanecido en niveles mínimos durante todo el invierno.

En resumen, el conflicto se ha mantenido intenso, con esporádicos y limitados intentos de diálogo. En términos materiales, el continuo enfrentamiento militar y los ataques indican un sostenido nivel de conflicto material con oscilaciones alrededor de niveles de tensión elevados (aunque sin llegar a los niveles máximos de armamento no convencional). Verbalmente, aunque se hayan producido declaraciones ocasionales que sugieren la posibilidad de negociaciones, estas han estado a menudo acompañadas de condiciones previas y acusaciones mutuas, manteniendo un nivel bajo en la escala verbal de Goldstein. La guerra continuaba siendo un claro ejemplo de conflicto material y verbal, con pocas señales de cooperación significativa en cualquiera de los frentes.



Fuente: BBVA Research & Gdelt Project y Goldstein

Gráfico 3. Escala de eventos de la guerra Rusia-Ucrania (enero 2002-diciembre 2003). Número de eventos en cada categoría x la intensidad en escala de Goldstein

3.3. El conflicto entre Hamas e Israel

Una de las propiedades del sistema de alerta de señales geopolítico de BBVA Research es que incluye multitud de países y de índices de sentimiento extraídos de la base de datos GDELT. Esto supone una ventaja en aquellos conflictos en los que su situación estratégica puede tener implicaciones globales. Para capturar estas implicaciones, y su grado de transmisión o contagio, el sistema incluye índices de sentimiento geopolíticos, políticos, de incertidumbre de política económica, protesta y conflicto. Todo ello nos permite llevar a cabo un análisis detallado de las implicaciones de determinados conflictos en varias dimensiones y países, capturado en los diferentes medios de comunicación. Como hemos explicado anteriormente, este sistema de alerta nos permite analizar el sentimiento mediático según el origen de los medios de comunicación (local o extranjero), así como las relaciones bilaterales de los países.

Cuando Hamas atacó por sorpresa a Israel el pasado 7 de octubre de 2023, el sentimiento geopolítico mundial en los medios de comunicación era relativamente tranquilo. Desde el punto de vista geopolítico y en relación con el pasado reciente, el conflicto entre Rusia-Ucrania estaba todavía presente, pero su impacto mediático se había relajado notablemente. Como se aprecia en el gráfico 4, la mayoría de nuestros indicadores de sentimiento (geopolítico, político, incertidumbre de política económica, conflicto y protesta) mostraban una anormal neutralidad o tranquilidad tras meses de elevado riesgo durante los períodos más tensos del conflicto entre Rusia y Ucrania.

El efecto sorpresa también fue notorio en las noticias mundiales y, salvo una situación de conflicto histórico entre Israel y Hamas y los acuerdos Abrahams, que acercaban posturas entre Israel y Arabia Saudí, nada hacía presagiar un desenlace tan crítico.

El gráfico 4 muestra cómo los índices de sentimiento geopolítico de los países de Oriente Medio y de EE. UU. aumentaron súbitamente y alcanzaron niveles de riesgo extremo en cuestión de días. A excepción de EE. UU., cuyo índice de sentimiento geopolítico se fue moderando hacia un sentimiento más neutral a medida que las noticias comenzaron a digerirse tras la sorpresa inicial, la mayoría de los países del golfo han permanecido en zona de riesgo con algunos vaivenes alrededor de las treguas temporales.

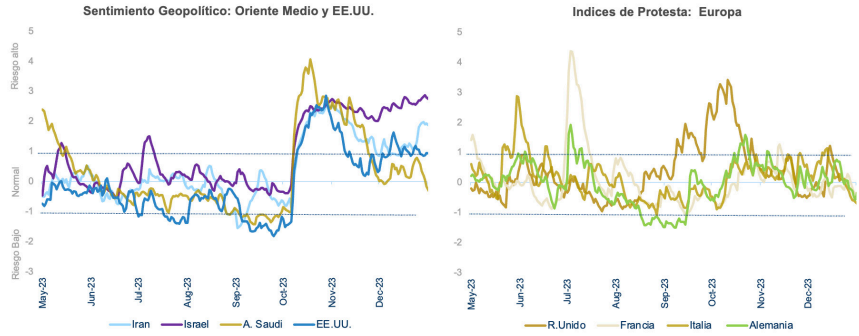


Gráfico 4. Indicadores de sentimiento: geopolítico y protesta (unidades de desviación típica)

Los efectos secundarios del conflicto en Europa también fueron evidentes desde el comienzo de la crisis, con estallidos de protesta en muchos países europeos, como se puede observar en el segundo gráfico 4b. El sentimiento se polarizó y el desencanto social comenzó a hacerse eco en las calles. Esto ha sido particularmente relevante en el Reino Unido y, en menor medida, en Francia, donde hemos asistido a una cierta polarización en el apoyo a los contendientes.

Pero no todos los indicadores reaccionaron de igual manera. Los siguientes diagramas en el gráfico 5 muestran un resumen gráfico de cómo evolucionaron los diferentes índices de sentimiento, incluyendo riesgo geopolítico, tensiones políticas, incertidumbre de política económica y protesta y conflicto desde el comienzo del conflicto.

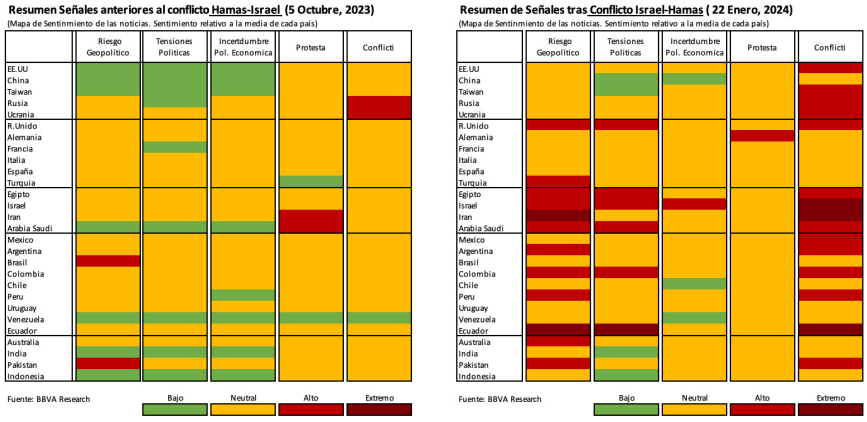


Gráfico 5. Indicadores de sentimiento: geopolítica, política, incertidumbre de política económica, protesta y conflicto antes y después del enfrentamiento Israel-Hamas

El riesgo geopolítico, la inestabilidad política, el conflicto y la protesta aumentaron en los países de Oriente Medio a niveles altos o extremos. Una excepción importante ha sido el sentimiento de protesta en Irán, que se mantuvo neutral. Esto es particularmente importante, ya que algunos analistas comentaron sobre la posibilidad de que la crisis movilizara al pueblo iraní y desestabilizara el régimen.

La crisis se extendió rápidamente a algunos de los índices occidentales. De hecho, los indicadores geopolíticos y de conflicto se movieron deprisa hacia el área de alto riesgo en EE. UU. y algunos países europeos.

Afortunadamente, el índice de incertidumbre de política económica ha permanecido resiliente. Este ha sido un patrón generalizado. Hay algunas explicaciones aquí. Primero, el lenguaje del conflicto ha desplazado al económico. Segundo, el conflicto ha coincidido en tiempo con los Bancos Centrales clave, manteniéndose al margen después de un ciclo de endurecimiento muy agresivo y condiciones económicas razonables, lo que también ha impulsado un momento muy positivo en el mercado de valores.

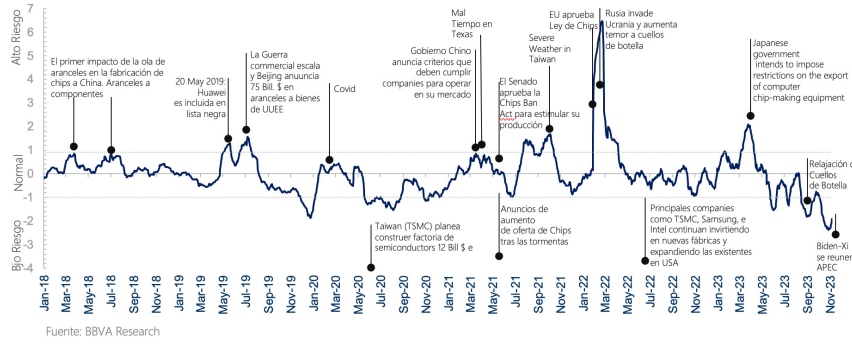
3.4. Las relaciones bilaterales entre países y los semiconductores: China, Taiwán y EE. UU.

Dentro del Sistema de Alerta diseñado en BBVA Research, una herramienta de análisis interesante es la posibilidad de analizar las tensiones en las relaciones entre países. Un ejemplo de ello es el análisis llevado a cabo sobre la crisis de los semiconductores provocada, entre otros factores, aunque no fue el único, por las tensas relaciones entre China y Taiwán y, por ende, entre China y EE. UU.[6].

La crisis de los semiconductores, que se extendió desde 2018 hasta finales de 2023, ha estado originada por varios factores a lo largo del tiempo. Para analizar el sentimiento mundial hacia la industria de semiconductores desarrollamos un indicador para monitorear el sentimiento mediático sobre los semiconductores a nivel mundial utilizando la base de datos GDELT para construir el índice de sentimiento de semiconductores de BBVA Research. Capturamos tanto la cobertura como el sentimiento de los artículos de noticias por día que incluyen cualquier mención de este tema.

[6] Para un análisis detallado de este apartado véase Hsu *et al.* (2023).

La evolución del Índice Global de Sentimiento de Semiconductores de BBVA Research se resume en el gráfico 6. Como se puede observar, la crisis de semiconductores y su posterior normalización han sido impulsadas por varios factores, como la guerra comercial entre EE. UU. y China, las escaseces relacionadas con el COVID-19 y los problemas de capacidad, el mal tiempo, las tensiones geopolíticas, pero también los avances en la diplomacia internacional que han operado con distinta intensidad durante los últimos años.



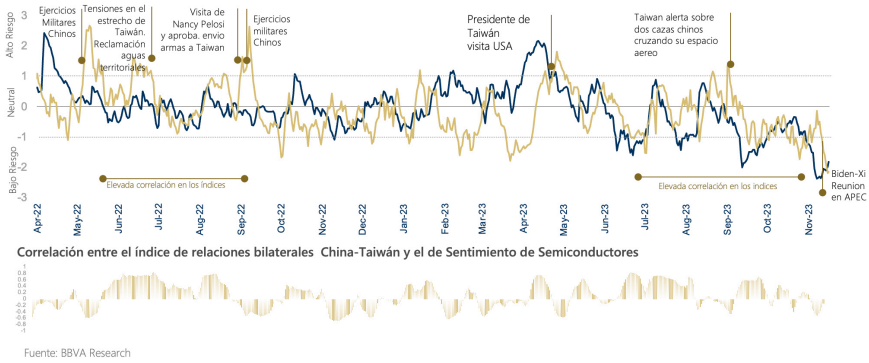
Fuente: BBVA Research

Gráfico 6. Índice Global de Sentimiento de Semiconductores (unidades de desviación típica)

Para entender mejor el impacto de los factores geopolíticos en la industria global de semiconductores, examinamos las interacciones entre China, Taiwán y Estados Unidos, centrándonos en el período entre 2022 y 2023. Este marco temporal nos ayuda a separar la influencia de estas relaciones de otros problemas como los problemas de capacidad relacionados con el COVID-19 y las interrupciones climáticas experimentadas durante 2020 y 2021. Los años 2022 y 2023 se caracterizaron por tensiones crecientes y complejas interacciones entre China, Taiwán y Estados Unidos, impulsadas por conflictos políticos arraigados e intereses estratégicos.

La relación entre China, Taiwán y Estados Unidos experimentó una tensión considerable en 2022. En abril, China intensificó su presencia militar cerca de Taiwán. Para junio, las tensiones escalaron aún más cuando el Ministerio de Relaciones Exteriores de Taiwán criticó a Pekín por reclamar el Estrecho de Taiwán como parte de su zona económica exclusiva. La situación empeoró con el apoyo de Estados Unidos a Taiwán mediante ventas de armas y la visita de la presidenta de la Cámara de Representantes, Nancy

Pelosi, en agosto, lo que llevó a China a realizar ejercicios militares en respuesta. Durante este período, el índice de relaciones bilaterales entre China y Taiwán pasó de neutral a una zona de mayor riesgo, mostrando una estrecha correlación con el índice global de semiconductores.



Fuente: BBVA Research

Gráfico 7. Relaciones bilaterales China-Taiwán e índice global semiconductores (unidades de desviación típica)

El año 2023 fue testigo de variados niveles de tensión. A principios de año, se observaron picos de tensión, particularmente alrededor de la visita de la presidenta Tsai a Estados Unidos. Las tensiones militares resurgieron en septiembre. Sin embargo, asistimos a una notable mejora en las relaciones más adelante en el año, a medida que los esfuerzos diplomáticos entre China y Estados Unidos se intensificaron en preparación para la reunión de Xi Jinping y Biden en la cumbre de APEC en noviembre.

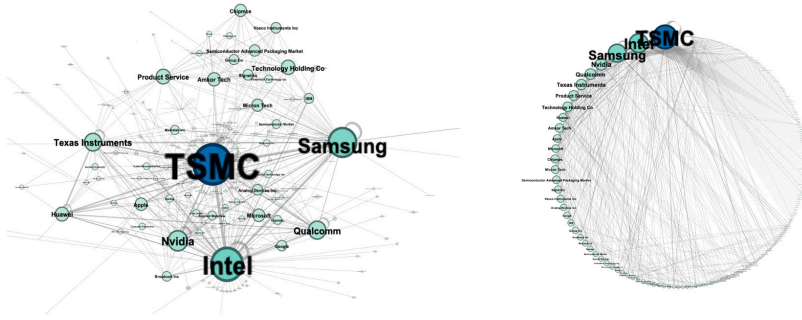
Estos desarrollos indican una fuerte correlación entre las relaciones China-Taiwán-EE. UU. y la estabilidad de la industria global de semiconductores. Comprender esta relación es crucial a la hora de diseñar políticas industriales que puedan limitar el impacto en una industria tan estratégica.

Los analistas de Ciencias Geopolíticas y Economía se han centrado en las posibles implicaciones económicas de un hipotético conflicto entre China y Taiwán. Un tema central en el análisis ha sido la relevancia de Taiwán en la industria mundial de semiconductores a través de la empresa Taiwán Semiconductor Manufacturing Company (TSMC), lo cual es, en particular, relevante para producir chips para los dispositivos más sofisticados.

Más que la evolución de las noticias de forma aislada para analizar el papel sistémico de TSMC en la industria de semiconductores,

construimos una red de noticias globales. Esta estrategia nos permite analizar las posibles relaciones en las noticias de la crisis de semiconductores de Taiwán con el resto de la industria. En esencia, analizamos quién está especialmente vinculado a TSMC en la industria de semiconductores. Para hacer esto, utilizamos la base de datos GDELT para analizar la co-ocurrencia de artículos de noticias de empresas de semiconductores, juntamente con TSMC.

Un gráfico de red o *Network* es una forma sencilla de representar datos de red donde los nodos (vértices) representan unidades (es decir, empresas) y una arista entre dos nodos indica que existe una relación entre ellos. Hay varias medidas de centralidad, incluyendo grados, cercanía e intermediación. Estas medidas evalúan el grado en que cada nodo juega un papel central en un gráfico. Como en este caso estamos interesados en analizar el papel sistémico de TSMC, implementamos un algoritmo para describir el tamaño de cada nodo, no solo en el número de aristas, sino también para considerar la relevancia de estas conexiones de aristas. La medida que usamos es la centralidad de auto vector, que tiene en cuenta la influencia transitiva de los nodos. Una alta puntuación de auto vector significa que un nodo está conectado a muchos nodos, que a su vez tienen altas puntuaciones, reflejando así mejor la naturaleza sistémica.



* La centralidad de vector es un algoritmo que mide la influencia transitiva de los nodos. Las relaciones que provienen de nodos con puntuaciones altas contribuyen más a la puntuación de un nodo que las conexiones de nodos con puntuaciones bajas. Una puntuación alta de vector propio significa que un nodo está conectado a muchos nodos que a su vez tienen puntuaciones altas

Fuente: BBVA Research

Gráfico 8. Red de relaciones industria de semiconductores

Los resultados de las noticias de 2022 revelan la importancia sistémica de TSMC y su relación con otras corporaciones en la industria de semiconductores. Grandes IDMs como Intel, Samsung, Texas Instruments y Micron Tech lideran, en términos de relevancia, subcontratando parte de su producción a TSMC

para tecnologías avanzadas. Empresas *fabless* como Nvidia y Qualcomm, seguidas por Broadcom y AMD, son clientes significativos de TSMC, diseñando y vendiendo *hardware* y chips mientras externalizan la fabricación. Grandes tecnológicas como Apple, Huawei y Microsoft dependen de TSMC para chips personalizados, aunque Huawei ha sido afectada por restricciones de EE. UU. Empresas OSAT[7] como Amkor Tech y Chipmos proporcionan servicios de empaquetado y pruebas para los semiconductores de TSMC, con Amkor recientemente anunciando que empaquetará chips fabricados en Arizona.

En resumen, la red de noticias muestra la centralidad de TSMC en la industria de semiconductores y su interconexión con importantes actores globales. La relación entre TSMC y estas empresas refleja la complejidad y la interdependencia del sector, destacando la influencia de TSMC en la cadena de suministro global y su papel crítico en la producción de tecnologías avanzadas. Estos vínculos son fundamentales para entender la dinámica del mercado y las posibles repercusiones de cualquier perturbación en la industria.

4. Conclusiones

En este artículo mostramos cómo la evolución de la digitalización de la información y el desarrollo de la inteligencia artificial, especialmente en el campo del procesamiento de lenguaje natural, están transformando radicalmente el análisis en las ciencias políticas y relaciones internacionales.

Hemos explorado diversos modelos que utilizan y procesan información no estructurada originada por los medios de comunicación internacionales y locales, a través de algoritmos de procesamiento de lenguaje natural y análisis de texto, que la convierten en valiosa información numérica, aplicable en el análisis geopolítico.

Adicionalmente, y basándonos en nuestra propia experiencia, mostramos cómo hemos utilizado este tipo de técnicas e información en BBVA Research a través de distintas herramientas aplicadas a diversos conflictos y eventos.

Desde el análisis de los flujos migratorios a Europa tras la crisis de Siria, al conflicto entre Rusia y Ucrania, las tensiones

[7] *Outsourced Semiconductor Assembly and Test.*

Israel-Hamas, y las implicaciones de las disputas entre China y Taiwán para el sector mundial de los semiconductores, estos ejemplos y otros en la literatura ilustran la capacidad de estos modelos para proporcionar análisis, realizar seguimientos detallados de los conflictos y, en algunos casos, llegar a poder a desarrollar sistemas de alerta temprana para anticipar conflictos.

La transformación del texto a números se perfila como una herramienta poderosa, ofreciendo una nueva perspectiva en el análisis político y de relaciones internacionales. Todo ello destaca la relevancia de las fuentes no estructuradas como herramientas analíticas en tiempo real. Este avance no solo permite un seguimiento en tiempo real de situaciones geopolíticas complejas, sino que también posibilita una comprensión más profunda de las dinámicas globales y regionales, contribuyendo significativamente a la formulación de políticas y estrategias más informadas y efectivas.

En conclusión, la integración de tecnologías avanzadas de IA y el procesamiento de lenguaje natural en el análisis de relaciones internacionales y las ciencias políticas abre un campo prometedor para investigaciones futuras y para la toma de decisiones estratégicas más informadas a nivel global.

Bibliografía

Ahmed, M. N. *et al.* (2016). A Multi-Scale Approach to Data-Driven Mass Migration Analysis. En: *SoGood@ECML-PKDD*.

Azar, E. E. (1980). The Conflict and Peace Data Bank (COPDAB) Project. *Journal of Conflict Resolution.* Vol. 24, n.º 1, pp. 143-152.

Baker, S. R., Bloom, N. y Davis, S. J. (2016). Measuring Economic Policy Uncertainty. *The Quarterly Journal of Economics*. Vol. 131, n.º 4, pp. 1593-1636.

Bermingham, A. *et al.* (2009). Combining Social Network Analysis and Sentiment Analysis to Explore the Potential for Online Radicalisation. En: *2009 International Conference on Advances in Social Network Analysis and Mining*.

Blei, D. M., Ng, A. Y. y Jordan, M. I. (2003). Latent Dirichlet Allocation. *Journal of Machine Learning Research.* Vol. 3, pp. 993-1022.

Caldara, D. y Iacoviello, M. (2022). Measuring Geopolitical Risk. *American Economic Review*. Vol. 112, n.º 4.

Gennaro, G. y Ash, E. (2021). Emotion and Reason in Political Language. *The Economic Journal.* Vol. 132, n.º 643, pp. 1037-1059.

Gerner, D. J. *et al.* (2002). Conflict and Mediation Event Observations (CAMEO): A New Event Data Framework for the Analysis of Foreign Policy Interactions. En: Goldstein, J. S. A Conflict-Cooperation Scale for WEIS Events Data. *Journal of Conflict Resolution.* Vol. 36, n.º 2, pp. 369-385.

Halterman, A. *et. al.* (2023). *PLOVER and POLECAT: A New Political Event Ontology and Dataset*. [Consulta: 2024]. Disponible en: https://osf.io/preprints/socarxiv/rm5dw.

Leetaru, K. y Schrodt, P. (2013). GDELT: Global data on events, location, and tone. En: *ISA Annual Convention*.

Martin, G. J. y McCrain, J. (2019). Local News and National Politics. *American Political Science Review.* Vol. 113, n.º 2, pp. 372-384.

Mclelland, C. A. (1976). World Event/Interaction Survey Codebook. *Ann Arbor: Inter-University Consortium for Political and Social Research.* ICPSR5211(4).

Moore, G. E. (1965). Cramming more components onto integrated circuits. *Electronics.* Vol. 38, n.º 8, p. 114.

Mueller, H. y Rauh, C. (2018). Reading Between the Lines: Prediction of Political Violence Using Newspaper Text. *American Political Science Review.* Vol. 112, n.º 2, pp. 358-375.

O'Brien, S. P. (2010). Crisis Early Warning and Decision Support: Contemporary Approaches and Thoughts on Future Research. *International Studies Review.* Vol. 12, n.º 1, pp. 87-104.

Rodriguez, P. L., Spirling, A. y Stewart, B. M. (2023). Embedding Regression: Models for Context-Specific Description and Inference. *American Political Science Review.* Vol. 117, n.º 4, pp. 1255-1274.

Schrodt, P. A., Davis, S. G. y Weddle, J. L. (1994). Political Science: KEDS—A Program for the Machine Coding of Event Data. *Social Science Computer Review.* Vol. 12, n.º 4, pp. 561-587.

Sundberg, R. y Melander, E. (2013). Introducing the UCDP Georeferenced Event Dataset. *Journal of Peace Research.* Vol. 50, n.º 4, pp. 523-532.

Vaswani, A. *et al.* (2017). Attention is all you need. *Advances in neural information processing systems.* Vol. 30.

Capítulo cuarto

La inteligencia artificial y la guerra de Ucrania

José Pardo de Santayana

Resumen

En el contexto geoestratégico de intensa rivalidad entre China y Estados Unidos, la lucha por la innovación tecnológica en el ámbito de la inteligencia artificial (IA) se presenta como la clave de la supremacía militar futura.

La guerra de Ucrania está acelerando el proceso de desarrollo de esta tecnología para fines bélicos y, aunque el carácter de esta contienda aún no esté determinado por la IA, dicho conflicto armado se asemeja a un laboratorio en el que las grandes potencias y las empresas del sector pueden entrenar y probar constantemente sistemas de IA para una amplia gama de capacidades, funcionalidades y aplicaciones.

La implicación de Washington —cuyas empresas dominan los avances de la IA— en esta guerra le da una ventaja sobre Pekín. China está siguiendo muy de cerca todo lo relativo a la guerra. Moscú aporta a Pekín información operativa sobre su experiencia en la guerra y, muy en particular, sobre la IA, mientras que China coopera con Rusia para el desarrollo militar de alta tecnología.

Dado que es probable que la guerra en Ucrania continúe durante algún tiempo, los bandos implicados están trabajando para lograr una ventaja sobre el otro y la IA desempeñará un papel cada vez más importante en la pugna militar.

Palabras clave

Inteligencia artificial, Guerra, Innovación, Rusia, Ucrania, China, Estados Unidos.

Artificial intelligence and the war in Ukraine

Abstract

In the geostrategic context of intense rivalry between China and the United States, the struggle for technological innovation in the field of artificial intelligence (AI) is emerging as the key to future military supremacy.

The war in Ukraine is accelerating the process of developing this technology for warfare purposes and, although the character of this war is not yet determined by AI, such armed conflict resembles a laboratory in which major powers and companies in the sector can constantly train and test AI systems for a wide range of capabilities, functionalities, and applications.

The involvement of Washington —whose companies dominate AI advances— in this war gives it an advantage over Beijing. China is thus closely following everything related to the war. Moscow provides Beijing with operational information on its expertise in this war and, most particularly, on AI, while China cooperates with Russia for high-tech military development.

Since the war in Ukraine is likely to continue for some time, the sides involved are working to gain an advantage over each other and AI will play an increasingly important role in the military contest.

Keywords

Artificial Intelligence, War, Innovation, Russia, Ukraine, China, United States.

1. Introducción

Vivimos en el alborear de una nueva era del modo de hacer la guerra debido al impacto de una serie de nuevas tecnologías, de las que la inteligencia artificial (IA) es la más crítica, con un gran impacto en los asuntos de seguridad globales.

Como se vio con el arma nuclear al final de la Segunda Guerra Mundial, el Estado que sea capaz de dominar esta tecnología de forma más rápida y eficaz para su empleo militar tendrá una enorme ventaja para poder imponerse en las próximas guerras. La predicción es que en diez años la IA sea el vector militar dominante (De Vynck, 2023).

Esta carrera armamentista de la era digital ya ha comenzado y hay quien teme que China pueda ir por delante tanto por razones puramente tecnológicas como de funcionamiento de un Estado autoritario que puede dirigir todas las energías y capacidades en la dirección deseada. En sentido contrario, a pesar de que las tecnológicas estadounidenses lideran el sector de la IA a nivel mundial, estas actúan conforme a sus propios intereses y no a los de su Gobierno, intentando zafarse del control estatal.

Por otra parte, existe igualmente un gran temor a que, de igual manera que la IA aporta muchos beneficios a la vida de las sociedades, también pueda tener un impacto negativo y peligroso, lo que está llevando a la necesidad de importantes regulaciones.

En la actualidad el debate sobre la peligrosidad de la IA está muy encendido y Kissinger (2023) llegó a afirmar que:

> «Estamos en la clásica situación previa a la Primera Guerra Mundial en la que ninguna de las partes tiene mucho margen de concesión política y en la que cualquier alteración del equilibrio puede tener consecuencias catastróficas […]. El destino de la humanidad depende de si América y China se puedan llevar bien […]. El rápido progreso de la inteligencia artificial, en particular, les deja sólo de 5 a 10 años para encontrar un camino».

El desarrollo de la IA en el ámbito de la Defensa tiene sus propias características. Para su uso militar no es suficiente con los datos procedentes de internet, la mayor parte de estos datos tiene que venir de las propias capacidades militares, los sensores y la colaboración con empresas tecnológicas. Además, los jefes militares necesitan saber cómo utilizar estos datos con fines bélicos.

En la actualidad, la guerra de Ucrania está atrayendo el foco del uso militar de la IA más que ningún otro conflicto armado, convirtiéndose así en el gran campo de pruebas de la guerra futura. La estrecha implicación del Gobierno y de las empresas de Estados Unidos en apoyo de Ucrania en este conflicto armado da ventaja a Washington sobre Pekín a la hora de extraer enseñanzas aplicables al uso militar de la IA.

De momento, la aplicación de esta tecnología ha permitido que Kiev, con una capacidad militar notablemente inferior a la de Moscú, le haya plantado cara seriamente. Téngase en cuenta que, antes de la guerra, se estima que Rusia gastaba unos 65 000 millones de dólares en Defensa mientras que Ucrania solo 6000.

Capacidades tecnológicas como drones, designación de objetivos con IA e inteligencia de imágenes, así como armas portátiles antiaéreas y antitanque de última generación, han permitido que Ucrania detuviera la embestida rusa e incluso contraatacara durante el primer año y medio de la guerra. Del mismo modo, la IA está teniendo un impacto significativo en la defensa de las infraestructuras críticas ucranianas contra los ataques rusos con drones y misiles.

En esta fase del desarrollo de la IA, aún se están explorando los parámetros de lo que es posible, pero la importancia capital de la respuesta militar a la tecnología de IA es innegable. A pesar de que mucha de la información sobre la materia no está accesible en fuentes abiertas, este documento pretende explorar el empleo que se está haciendo de la IA en la guerra de Ucrania y el impacto que esta circunstancia puede llegar a tener en el desarrollo del arte militar en los próximos años, reconociendo que en la guerra de Ucrania la IA se ha puesto de largo.

2. Marco estratégico

En este momento, solo hay dos superpotencias de IA: Estados Unidos y China, son los únicos países con el talento, las instituciones de investigación y la capacidad de computación masiva necesaria para entrenar los modelos de IA más sofisticados. Estos son los protagonistas de la película, aunque en la guerra de Ucrania haya una implicación muy desigual por ambas partes.

Antes del estallido de este conflicto armado, la IA ya había desencadenado una revolución de la seguridad que apenas estaba empezando a desarrollarse. El Ejército estadounidense utilizaba

la IA para optimizar todo, desde el mantenimiento de los equipos hasta las decisiones presupuestarias. Los analistas de inteligencia confiaban en la IA para escanear con rapidez montañas de información e identificar patrones relevantes que les permitieran tomar mejores decisiones y hacerlo más aceleradamente (Flournoy, 2023).

A parte de disponer de un instrumento muy útil para mejorar la eficiencia de la organización militar estadounidense, estaba la preocupación de que China consiguiera superar a Estados Unidos en IA, sobre todo en aplicaciones militares. En Washington se pensaba que, si lo conseguía, Pekín dispondría de un Ejército mucho más poderoso, capaz de aumentar el ritmo y el efecto de sus operaciones más allá de lo que Estados Unidos pudiera igualar.

Pekín no tiene la intención de ceder el dominio tecnológico a Washington y está trabajando duro para desarrollar sus propias aplicaciones militares avanzadas de IA. China está haciendo un enorme esfuerzo en muchos de los mismos ámbitos de uso de la IA que Estados Unidos, como la vigilancia, la identificación de objetivos y los enjambres de drones. La diferencia es que puede no estar sujeta a las mismas restricciones éticas que Estados Unidos y sus aliados, en especial cuando se trata de utilizar sistemas de armas totalmente autónomos.

> «China cuenta con algunas ventajas evidentes. A diferencia de Washington, Pekín puede dictar las prioridades económicas de su país y asignar los recursos que considere necesarios para alcanzar los objetivos de la IA. La política de seguridad nacional china anima a los hackers, funcionarios y empleados chinos a robar propiedad intelectual occidental, y Pekín no tiene reparos en intentar reclutar a destacados tecnólogos occidentales para que trabajen con instituciones chinas. Como China tiene una política de "fusión civil-militar", que elimina las barreras entre sus sectores civil y militar, el Ejército Popular de Liberación puede recurrir al trabajo de expertos y empresas chinos siempre que quiera. Y para 2025, China producirá casi el doble de doctorandos en ciencias, tecnología, ingeniería y matemáticas que Estados Unidos, lo que inundará la economía china de informáticos de talento» (Flournoy, 2023).

Así, el gigante asiático ya supera a Estados Unidos en IA de visión de computadora y en grandes modelos lingüísticos tipo ChatGPT.

En términos de implementación militar, está haciendo un esfuerzo diez veces mayor en los presupuestos de Defensa, en su conjunto la República Popular China gasta tres veces más que el Estado norteamericano, teniendo en cuenta que allí son las empresas tecnológicas las que soportan el mayor esfuerzo. También cuenta a favor de Pekín la supremacía en datos y, en una guerra dominada por la IA, todo depende de los datos, la nueva munición de las guerras del futuro (Bergengruen, 2023).

No obstante, Washington tiene ventajas frente a Pekín que se derivan principalmente del dinamismo y liderazgo tecnológico de sus empresas del sector, como Microsoft, Google, Amazon, Meta, OpenAI. Estas están inmersas en una lucha de gladiadores entre ellas que, sin duda, está impulsando la innovación.

Esta dinámica competitiva, en el contexto de la profunda desconfianza y la intensa rivalidad que enfrenta a ambas superpotencias, empuja a una carrera por la supremacía en la IA de uso militar. La parte que no ponga todo su empeño en ganarla tiene la derrota asegurada. La guerra de Ucrania, al prestarse como campo de pruebas, tiende además a acelerar este proceso.

Al mismo tiempo, hay muchas voces que están mostrando su preocupación de que esta nueva carrera de armamentos de la era digital termine teniendo consecuencias muy graves.

> «En los dos últimos años se han analizado estas cuestiones con un grupo de líderes tecnológicos que se encuentran en la vanguardia de la revolución de la IA y se ha llegado a la conclusión de que las perspectivas de que el avance ilimitado de la IA tenga consecuencias catastróficas para Estados Unidos y el mundo son tan apremiantes, que los líderes de los gobiernos deberían actuar ya» (Kissinger y Graham, 2023).

En las propuestas actuales sobre formas de contener la IA, se oyen muchos ecos del pasado nuclear. La petición del multimillonario Elon Musk de una pausa de seis meses en el desarrollo de la IA, la propuesta del investigador de IA Eliezer Yudkowsky de abolir la IA y la petición del psicólogo Gary Marcus de que la IA sea controlada por un organismo gubernamental mundial repiten esencialmente propuestas de la era nuclear que fracasaron. No son enfoques realistas, nunca en la historia una gran potencia, temiendo que un competidor pudiera aplicar una nueva tecnología para amenazar su supervivencia y seguridad, ha renunciado a desarrollar esa tecnología para sí misma (Kissinger y Graham, 2023).

En marzo de 2023, el presidente y consejero delegado de RAND, Jason Matheny, testificó ante el Comité de Seguridad Nacional y Asuntos Gubernamentales del Senado de Estados Unidos sobre los efectos de la IA en la seguridad nacional y la competitividad de Estados Unidos. Afirmó que la IA plantea graves retos para los que Estados Unidos no está preparado, entre otros, el desarrollo de nuevas armas cibernéticas, ataques de desinformación a gran escala y el diseño de armas biológicas avanzadas (RAND Corporation, 2023).

Surgen pues las preguntas:

> «¿Amenazarán las máquinas con capacidades sobrehumanas el estatus de la humanidad como dueña del universo? ¿Conseguirá la IA socavar el monopolio de las naciones sobre los medios de violencia masiva? ¿Permitirá la IA que individuos o pequeños grupos produzcan virus capaces de matar a una escala que antes era exclusiva de las grandes potencias? ¿Podría la IA erosionar las medidas de disuasión nuclear que han sido un pilar del orden mundial actual?» (Kissinger y Graham, 2023).

Mientras que los gobiernos lideraron el desarrollo de la tecnología nuclear, los emprendedores, tecnólogos y empresas privadas están impulsando los avances en IA. Cuando estos actores privados hacen cálculos entre riesgos y beneficios, los intereses nacionales quedan en un segundo plano. Además, la IA es digital, sus principales evoluciones se producen en la mente de los seres humanos. Su aplicabilidad evoluciona en los laboratorios y su despliegue es difícil de observar. Las armas nucleares son tangibles; la esencia de la inteligencia artificial es conceptual. Por último, la IA avanza y se extiende a una velocidad que hace imposible largas negociaciones.

Un peligro añadido se deriva de que sea la tecnología la que determine la ética, como ya defienden autores influyentes como Yuval Harari, y no la ética la que determine el empleo de la tecnología, como argumenta con gran solidez Eduardo Olier (2023) en su reciente libro.

Este grave dilema de la seguridad global exigiría, fundamentalmente, una nueva dinámica en las relaciones entre las grandes potencias antagónicas. La guerra de Ucrania no lo está facilitando en absoluto.

Por otra parte, lo que todos los conceptos de IA tienen en común es la visión de un campo de batalla verdaderamente conectado

en red, en el que los datos se mueven a la velocidad de la luz para conectar no solo los sensores con los tiradores, sino también la totalidad de las fuerzas y plataformas desplegadas.

Aunque todavía no ha cambiado el carácter de dicha guerra, Ucrania es el laboratorio en el que se está poniendo las bases para la próxima forma de guerra. No se trata de un laboratorio al margen, sino de un esfuerzo incesante y sin precedentes para perfeccionar, adaptar y mejorar los sistemas con IA o mejorados con IA para su despliegue inmediato. Ese esfuerzo está allanando el camino para la guerra de IA en el futuro (Fontes y Kamminga, 2023).

3. Aspectos generales

La IA se está perfilando como una baza importante en el actual conflicto ruso-ucraniano. A medida que evoluciona, su aplicación en los campos de batalla se está traduciendo en respuestas más precisas y potentes contra las fuerzas, movimientos y acciones del adversario. No obstante, hay que reconocer que la IA es un elemento facilitador y no el elemento determinante de este conflicto, ya que la guerra se está librando sobre el terreno con infantería, artillería y otras armas de una manera que recuerda más a la Primera que a la Segunda Guerra Mundial, donde el territorio se gana y se pierde en combates lentos y agotadores.

La guerra entre Rusia y Ucrania no se ajusta pues a estos escenarios futuros. Sin embargo, acerca claramente estas visiones futuristas de la guerra a la realidad. El conflicto es un campo de pruebas sin precedentes para la IA. En algunas áreas, su uso ha sido evidente. Por ejemplo, el empleo ya omnipresente de drones y municiones de merodeo —también conocidas como drones kamikaze/suicidas o misiles inteligentes— para ambos bandos ofrece capacidades autónomas mejoradas por la IA en vuelo, puntería y disparo.

Incluso antes de su inicio, la IA tuvo un impacto importante en la guerra, al ayudar a los analistas de inteligencia estadounidenses a predecir la invasión rusa de Ucrania con meses de antelación. Esto permitió a Washington advertir al mundo y negar al presidente ruso Vladimir Putin el elemento sorpresa.

Uno de los principales aspectos de la invasión rusa de Ucrania y la posterior guerra es la enorme cantidad de datos que están generando las distintas fuentes, en volúmenes muy superiores a

los que los seres humanos son capaces de analizar con rapidez y precisión. Esta circunstancia se presenta igualmente como una oportunidad para la experimentación y el desarrollo de una tecnología en expansión que necesita de esos volúmenes crecientes de datos específicos de calidad para poder crecer.

En la actualidad, el uso de la IA en Ucrania se centra en la actividad humana, y son los operadores los que, en última instancia, toman las decisiones finales sobre las unidades, las armas y los sistemas, con la ayuda de los análisis proporcionados por la IA. Este enfoque centrado en el ser humano es esencial para que se haga un uso ético de esta tecnología, al igual que la necesidad de llegar a un acuerdo sobre cómo pueden utilizar la IA Estados Unidos y sus aliados, tras su introducción inaugural en Ucrania.

La inteligencia artificial se utiliza para el análisis de datos con el fin de ayudar a la toma de decisiones en Ucrania; para analizar una cantidad masiva de imágenes y detectar objetos que con medios humanos sería inabordable; para vigilar un área y detectar cambios o movimiento y para los procesos logísticos más eficientes. En definitiva, para establecer una imagen operativa global del campo de batalla, con la intención de acceder rápidamente a las condiciones de combate en constante cambio y reaccionar ante ellas.

Además, la IA está desempeñando un papel importante en la guerra electrónica y el cifrado. Esto ilustra cómo los sistemas de IA se reentrenan y adaptan constantemente, por ejemplo, para hacer frente a idiosincrasias de forma personalizada (Fontes y Kamminga, 2023).

Un aspecto de enorme relevancia estratégica es el empleo de la IA para ayudar a advertir a los analistas norteamericanos sobre el movimiento de misiles con armas nucleares rusas que, en el pasado, a menudo eludían la detección. El Mando Estratégico de Estados Unidos está utilizando para ello un programa de IA desarrollada por Rhombus Power (Flournoy, 2023).

Un aspecto característico de esta guerra es la rápida evolución de las tecnologías de combate y la adaptación de tácticas y conceptos clave por ambas partes. Si la guerra se alarga mucho, es previsible que veamos al final un modelo operativo muy distinto al actual.

En particular, muchos de los drones rusos y ucranianos para misiones de reconocimiento y combate vuelan en grupos, con

uno o varios operadores pilotándolos. Una evolución esperada de estas tácticas es permitir que auténticos enjambres de UAVs vuelen de forma autónoma hacia los objetivos, gracias a tecnologías de IA. Estas tácticas podrían incluso surgir no solo de las instituciones oficiales de investigación y desarrollo militar, sino también de organizaciones de voluntarios que están ayudando a cada bando en el desarrollo y la adquisición de tecnología. Los drones utilizados incluyen UAVs de diseño militar, pero también drones comerciales como la serie Mavic de DJI, de fabricación china, que son mucho más baratos y fáciles de obtener.

La defensa antiaérea es otro ámbito donde se podrían producir avances importantes de la mano de la IA. Ello responde a la necesidad de combatir con eficacia al número creciente de vehículos presentes —tripulados y no tripulados— en el espacio aéreo y al cada vez menor tiempo de reacción, en particular, pero no exclusivamente, por el impacto de las armas hipersónicas. Esto supondría una verdadera revolución que terminaría transformando por completo la batalla aeroterrestre con algunos riesgos significativos de pérdida de control de los procesos de toma de decisiones.

En cualquier caso, hay que tener claro que los sistemas de armas mejorados con IA son solo la punta del *iceberg.* La mayor parte de la IA se despliega y se desplegará en sistemas alejados del campo de batalla, en sistemas de computación en nube y de análisis de datos relacionados con áreas como la planificación, la logística y el mantenimiento preventivo. Se trata de una faceta a menudo oculta de la revolución de la guerra impulsada por la IA que ya se ha puesto en marcha y no se detendrá.

4. El caso particular de la desinformación

En el período previo a la invasión rusa de Ucrania, y durante todo el conflicto en curso, las redes sociales han servido de campo de batalla para que Estados y actores no estatales difundan narrativas contrapuestas sobre la guerra y presenten el conflicto en curso en sus propios términos.

La desinformación está siendo utilizada masivamente tanto para fines operativos como en la batalla cognitiva por el relato. La capacidad para crear imágenes, audios y textos falsos, muy difíciles o incluso imposibles de distinguir de los reales, ha potenciado mucho este recurso.

Por ejemplo, al inicio de la invasión rusa de Ucrania, el Kremlin utilizó un video falso en el que el presidente Zelenskí llamaba al pueblo ucraniano a la rendición, que fue visto más de 120 000 veces en Twitter. Entonces, la tecnología no estaba suficientemente avanzada y la trampa no resultó creíble. Un video similar con Putin llamando a los rusos a rendirse tuvo 50 000 seguidores. Sin embargo, los avances están resultando tan rápidos y a precios cada vez más accesibles que el panorama ha cambiado en esencia (Pérez y Nair, 2022).

A medida que la guerra se prolonga, los ecosistemas digitales se han inundado de desinformación. Las campañas de propaganda estratégica, incluidas las de desinformación, no son nuevas en las guerras, pero el cambio hacia las redes sociales como principal canal de distribución está transformando la forma en que se libra la guerra de la información, así como quién puede participar en las conversaciones en curso para dar forma a las nuevas narrativas.

La IA y sus subcomponentes, como los algoritmos y el aprendizaje automático, están sirviendo como poderosas herramientas para generar y amplificar la desinformación sobre la guerra entre Rusia y Ucrania. Los algoritmos subyacentes, que las plataformas de redes sociales utilizan para determinar qué contenidos están permitidos y qué publicaciones son las más vistas, están generando diferencias en la percepción que tienen los usuarios de los acontecimientos. En los últimos años, tanto Facebook como YouTube han sido objeto de escrutinio por parte de los organismos reguladores de EE. UU. y la UE, preocupados por evitar que sus algoritmos den prioridad a los contenidos extremistas y por eliminar adecuadamente la desinformación.

La IA y sus herramientas también ofrecen medios eficaces para combatir la desinformación. El enorme volumen de información que se sube diariamente a las redes sociales hace esencial el desarrollo de herramientas de IA que puedan identificar y eliminar con precisión la desinformación. Lo cual tiene también sus propios peligros. ¿Quién controla al que nos controla?, ¿quién determina lo que es verdadero y lo que no?, ¿nos podemos fiar de nuestro propio «Gran Hermano»?

Los usuarios de Twitter suben más de 500 000 mensajes por minuto, mucho más de lo que los censores humanos pueden controlar. Las plataformas de redes sociales están empezando a combinar censores humanos con IA para controlar la

información falsa con mayor eficacia. Facebook, por ejemplo, desarrolló una herramienta de IA llamada SimSearchNet al comienzo de la pandemia de COVID-19 para identificar y eliminar mensajes falsos.

5. Inteligencia artificial en las operaciones ucranianas

En comparación con el uso realizado por los rusos, parece que Kiev está obteniendo mayor ventaja. Hasta ahora, Ucrania ha conseguido mantener un enfoque centrado en el ser humano, siendo los operadores quienes toman las decisiones finales (Benedett, 2023).

La utilización ucraniana de IA en combate está siendo posible gracias a los esfuerzos tanto del Gobierno como del sector privado, con la contribución esencial de las tecnologías y los conceptos para su empleo que sus aliados occidentales les ofrecen. Aunque el sector de alta tecnología del país consiguió desarrollar un *software* clave para compartir información, como Kropyva, incluso bajo el estrés de la guerra, así como una aplicación de notificación Reface para reconocer a las tropas rusas a partir de imágenes de satélite, es el apoyo recibido de fuera el que está resultando determinante.

Las empresas norteamericanas, los investigadores, los que trabajan en el desarrollo de estas tecnologías y los profesionales de los sistemas de información geográfica han hecho un gran esfuerzo, en dicho sentido, proporcionando información a Ucrania, a los Estados Unidos y sus aliados de la OTAN.

> «De hecho, el consejero delegado de Palantir, una de las principales empresas mundiales de IA, admitió recientemente que su empresa es responsable de la mayor parte de la designación de objetivos en Ucrania, como los tanques y la artillería, gracias a la información oportuna que obtienen de los satélites y las redes sociales para visualizar las posiciones amigas y enemigas, comprender los movimientos de las tropas y realizar evaluaciones de los daños en el campo de batalla. Empresas occidentales como Planet Labs, BlackSky Technology y Maxar Technologies también producen imágenes por satélite de conflictos y comparten datos y análisis con el Gobierno y el Ejército ucranianos» (Benedett, 2023).

Esto tiene gran impacto operativo, ya que un papel clave de la IA para la fuerza armada ucraniana es la integración del

reconocimiento de objetivos y objetos con imágenes por satélite, lo que ha llevado a los comentaristas occidentales a señalar que Ucrania tiene una ventaja en inteligencia geoespacial. La IA se utiliza igualmente para geolocalizar y analizar datos de fuentes abiertas, como el contenido de las redes sociales, para identificar soldados, armas, sistemas, unidades o movimientos rusos.

Según fuentes abiertas, las redes neuronales se utilizan para combinar fotos a ras de suelo, grabaciones de vídeo de numerosos drones y vehículos aéreos no tripulados, e imágenes por satélite para proporcionar análisis y evaluaciones de inteligencia más rápidos que produzcan ventajas estratégicas y tácticas de inteligencia.

Se está utilizando a gran escala un nuevo algoritmo de *machine learning* para evaluación de daños en áreas clave afectadas por las operaciones militares. De forma rápida se analizaron más de 2000 km^2 y se identificaron más de 370 000 estructuras, incluidas miles que no habían sido identificadas por otras fuentes abiertas de datos, focalizando dicha evaluación en Kiev, Járkov y Dnipro, proporcionando dicha información directamente a la amplia comunidad de IA (Wang, 2023).

La invasión rusa de Ucrania ha dado lugar al primer uso registrado de reconocimiento facial en combate: el ejército ucraniano utiliza Clearview AI, con sede en Estados Unidos, para identificar a soldados rusos muertos, descubrir a asaltantes rusos y combatir la desinformación. Los informes públicos también sitúan a la IA en el centro de los esfuerzos aliados en materia de guerra electrónica, ciberguerra y cifrado. La empresa estadounidense Primer ha desplegado su IA para analizar las comunicaciones de radio rusas no cifradas, utilizando el procesamiento del lenguaje natural para comprender las formas específicas que utilizan los soldados rusos para comunicarse. En 2022, la empresa estadounidense Microsoft informó de que las ciberdefensas ucranianas habían tenido éxito gracias a los avances en inteligencia sobre amenazas mejorada con IA y a la rápida distribución de *software* de protección a servicios en la nube y otras redes informáticas (Benedett, 2023).

Las soluciones comerciales de IA que ayudan a los esfuerzos ucranianos también son adoptadas rápidamente por los militares que necesitan pensar sobre la marcha, sin el lujo de largos ciclos de adquisición o programas de pruebas y evaluación de años de duración.

6. Inteligencia artificial en las operaciones rusas

Antes de la invasión de Ucrania, las Fuerzas Armadas rusas ya habían puesto mucho énfasis en la IA como herramienta de toma de decisiones y análisis de datos y parece que la utilizaron para dicho fin en la preparación de lo que Putin denominó Operación Militar Especial.

Sin embargo, en el lado ruso hay menos pruebas y aún menos información sobre el uso de la IA en la guerra propiamente dicha. Al igual que su homólogo ucraniano, el alto mando ruso espera que la IA proporcione análisis de datos y capacidad de toma de decisiones al combatiente con un enfoque centrado en el operador para orientarse y decidir mejor y más rápido en el campo de batalla.

No obstante, algunos expertos militares rusos prevén que la toma de decisiones en las operaciones de combate acabe siendo llevada a cabo por sistemas robóticos, eliminando al operador humano de funciones y responsabilidades clave. Así, el impulso hacia el uso de la IA en sistemas autónomos, no tripulados y robóticos es uno de los aspectos más visibles de los esfuerzos de investigación, desarrollo, ensayo y evaluación de alta tecnología del país.

La IA se ve como un medio para sustituir eventualmente a los combatientes humanos en situaciones peligrosas. Por ejemplo, la suplantación de los cazas tripulados por robots militares que pueden actuar con mayor rapidez, precisión y selectividad que las personas.

El ecosistema de investigación y desarrollo del Ministerio de Defensa ruso incluye la visión técnica, el reconocimiento de patrones, la aplicación de la IA en la robótica y la mejora de los sistemas de información que procesan grandes conjuntos de datos como la introducción más práctica de dicha tecnología durante las hostilidades en curso.

> «En junio de 2023, los canales de Telegram en ruso informaron que la munición de merodeo Lancet-3 utiliza redes neuronales convolucionales para recoger, clasificar y analizar las imágenes y el contenido de vídeo obtenidos por este UAV durante el vuelo. Utilizando dichas redes neuronales, un dron Lancet de reconocimiento puede detectar objetivos enemigos y transmitir sus imágenes al Lancet "kamikaze" que, a continuación, lleva a cabo un ataque […]. Tales afirmaciones

> carecen a menudo de pruebas definitivas o incluso del reconocimiento público del ministerio de Defensa, lo que dificulta determinar si la IA se está utilizando de aquella manera en el Ejército ruso» (Benedett, 2023).

El proyecto estrella ruso en visión por ordenador, procesamiento de lenguaje natural, navegación, movimiento autónomo y control de vehículos en grupo es el vehículo terrestre no tripulado de combate Marker. Este vehículo fue entregado a una organización de voluntarios con sede en el este de Ucrania para ser probado y evaluado en condiciones de combate real (Benedett, 2023).

El Ministerio de Defensa ruso también ha dejado constancia de que vigila la evolución de la IA en todo el mundo, lo que, lógicamente, incluye el uso de esta tecnología por parte de Ucrania.

Un aspecto esencial, aunque menos conocido, es la colaboración ruso-china en esta materia, y, muy en concreto, cómo China está aprovechando el conocimiento que se deriva de esta guerra. A raíz de la guerra arancelaria entre Washington y Pekín, iniciada por el presidente Trump en 2018, China y Rusia no solo ampliaron la cooperación militar, sino que también ampliaron la cooperación tecnológica a las telecomunicaciones de quinta generación, la IA, la biotecnología y la economía digital (Bendett y Kania, 2019). Desde entonces, la cooperación tecnológica en materia militar no ha dejado de profundizarse.

En una vista de Xi Jinping a Moscú, al poco de iniciarse la guerra de Ucrania, los presidentes de ambas potencias acordaron desarrollar nuevos modelos de cooperación en industrias como la IA, internet de las cosas, 5G, economía digital y economía baja en carbono y propusieron seguir mejorando su asociación estratégica en industrias específicas, combinando sus capacidades de investigación e industriales (Thurbon, 2023).

La guerra en curso está permitiendo una cooperación de doble dirección. Moscú aporta a Pekín el conocimiento de primera mano en las operaciones, mientras que China ayuda a Rusia a desarrollar sus propias capacidades de IA y ambas potencias procuran seguir muy de cerca los logros de la IA estadounidense.

7. Conclusiones

El desarrollo de la IA para fines bélicos se inició antes del conflicto armado de Ucrania en el contexto, principalmente, de la rivalidad

geoestratégica de China y Estados Unidos con el potencial de terminar transformando el modo de hacer la guerra.

La desconfianza entre ambas superpotencias está intensificando esta carrera armamentística digital y dificulta el necesario entendimiento entre las partes para reducir los peligros que se derivaban de esta dinámica.

La guerra de Ucrania está acelerando el proceso de desarrollo de la IA para fines militares y, aunque el carácter de la guerra aún no esté determinado por la IA, la guerra entre Rusia y Ucrania se asemeja a un laboratorio en el que muchas empresas y gobiernos pueden entrenar y probar constantemente sistemas de IA para una amplia gama de capacidades, funcionalidades y aplicaciones.

Las empresas del sector están obteniendo un acceso sin precedentes a la aplicación real de la IA en combate en un conflicto convencional entre adversarios similares, algo que antes únicamente era posible en simulaciones.

Es importante reconocer que el éxito ucraniano en la utilización de la IA ha sido posible gracias a la ayuda estadounidense y occidental.

El avanzado desarrollo por parte de Estados Unidos de tecnologías de IA civiles y militares está marcando el ritmo mundial de su utilización en combate.

Los logros de la IA estadounidense también son seguidos muy de cerca por el Ejército ruso, que está incorporando prácticas de desarrollo de inteligencia artificial estadounidenses.

China también está siguiendo muy de cerca todo lo relativo a la guerra y, muy en particular, a los desarrollos tecnológicos. Aunque apenas hay información sobre ello, se puede afirmar que existe una cooperación de doble dirección. Moscú aporta a Pekín información operativa sobre IA, mientras que China coopera con Rusia para el desarrollo militar de alta tecnología.

Dado que es muy probable que la guerra en Ucrania continúe durante algún tiempo, ambos bandos están trabajando para lograr una ventaja sobre el otro y la IA desempeñará un papel cada vez más importante en esta guerra.

Esta es la trágica paradoja. Cada día que el conflicto continúa, y los seres humanos pierden la vida de maneras horribles, los sistemas de IA se entrenan con datos reales de un campo de batalla

real, no para detener el sufrimiento y poner fin a la guerra, sino para ser más eficaces en la lucha contra la próxima: la guerra de la IA (Fontes y Kamminga, 2023).

Bibliografía

Benedett, S. (2023). Roles and Implications of AI in the Russian-Ukrainian Conflict. *Russia Matters*. [Consulta: 2023]. Disponible en: https://www.russiamatters.org/analysis/roles-and-implications-ai-russian-ukrainian-conflict.

Bendett, S. y Kania, E. (2019). A new Sino-Russian high-tech partnership. *ASPI*. [Consulta: 2024]. Disponible en: https://www.aspi.org.au/report/new-sino-russian-high-tech-partnership.

Bergengruen, V. (2023). Tech Leaders Warn the U.S. Military Is Falling Behind China On AI. *TIME*.

De Vynck, G. (2023). Some tech leaders fear AI. ScaleAI is selling it to the military. *The Washington Post*.

Flournoy, M. A. (2023). AI Is Already at War. How Artificial Intelligence Will Transform the Military. *Foreign Affairs*.

Fontes, R. y Kamminga, J. (2023). Ukraine A Living Lab for AI Warfare. *National Defense Magazine*. [Consulta: 2024]. Disponible en: https://www.nationaldefensemagazine.org/articles/2023/3/24/ukraine-a-living-lab-for-ai-warfare

Kissinger, H. (2023). Henry Kissinger explains how to avoid world war three. *The Economist*.

Kissinger, H. y Graham, A. (2023). The Path to AI Arms Control. America and China Must Work Together to Avoid Catastrophe. *Foreign Affairs*.

Olier, E. (2023). *La debacle de Occidente. Las guerras del siglo XXI*. Sekotia.

Perez, C. y Nair, A. (2022). Information Warfare in Russia's War in Ukraine. *Foreign Policy*. [Consulta: 2024]. Disponible en: https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/.

RAND Corporation. (2023). U.S. Cooperation with China and Russia, Artificial Intelligence, War in Ukraine. *RAND Weekly Recap.* [Consulta: 2024]. Disponible en: https://www.rand.org/pubs/articles/2023/weekly-recap-march-10.html

Thurbon, R. (2023). Russia and China want to become world leaders in tech, security, and AI. *TECHSPOT*. [Consulta: 2024].

Disponible en: https://www.techspot.com/news/98032-russia-china-want-become-world-leaders-tech-security.html.

Wang, A. (2023). War, AI and the New Global Arms Race. *Ted Talk*. [Consulta: 2024]. Disponible en: https://www.youtube.com/watch?v=EpipswT-LuE.

Capítulo quinto

Inteligencia artificial en apoyo a la inteligencia militar. Eje fundamental del éxito o fracaso en la competición estratégica entre grandes potencias

Juan Luis Sánchez Sánchez

Resumen

La potencia de la inteligencia artificial, IA, en los futuros desarrollos tecnológicos impactará de manera drástica en el predominio mundial y en la competición estratégica entre grandes potencias, la forma de afrontar las crisis y conflictos híbridos y la utilización multidominio de las capacidades militares y su integración con las civiles. El uso avanzado de IA aplicado a la inteligencia permitirá la mejor y más rápida comprensión del entorno estratégico y operativo para adelantar, respecto a los competidores, las soluciones ejecutivas idóneas que permitan la supervivencia del modelo social, económico y político de nuestras sociedades democráticas liberales.

Palabras clave

Inteligencia, Información, Inteligencia artificial, OSINT, Guerra cognitiva, Operaciones especiales, Disciplinas de inteligencia, Ciclo de inteligencia, IMINT, SIGINT, Competición estratégica.

Artificial intelligence in support of military intelligence. Fundamental axis of success or failure in the strategic competition between great powers

Abstract

The power of artificial intelligence, AI, in future technological developments will impact deeply in the global preeminence and in the strategic great power competition, the way of face the crisis and hybrid conflicts and the multi domain military capabilities and their integration with the civil ones. The advanced use of AI applied to intelligence will allow a better and faster understanding of the strategic and operational environment in order to anticipate, in relation to competitors, the most appropriate management solutions that will allow the survival of the social, economic and political model of our liberal democratic societies.

Keywords

Intelligence, Information, Artificial intelligence, OSINT, Cognitive warfare, Special operations, Intelligence Disciplines, Intelligence cycle, IMINT, SIGINT, Strategic competition.

1. Una película muy real

Una crisis en el país X ha provocado la escalada de tensión interracial y la explosión de violencia. La embajada española en la capital recomienda a la población residente evacuarse, acudiendo a las instalaciones de la embajada para gestionarlo. En el interregno, una organización terrorista de una de las etnias sin identificar ataca la embajada matando a su servicio de seguridad y tomando un número indeterminado de rehenes. Las peticiones del grupo terrorista son inasumibles, se prevé una intención nihilista, y que asesinen a los rehenes inmolándose. Unidades de Operaciones Especiales del MOE[1] e Inteligencia españolas son requeridas para realizar una posible liberación de rehenes, de competencia legal nacional al ser territorio consular y ciudadanos españoles; el país X solo puede apoyar.

El equipo operativo alertado para realizar la operación de rescate, de manera inmediata, comienza la recopilación de información por parte de los especialistas de inteligencia. Estos buscan y administran el acceso a todas las bases de datos de Fuerzas Armadas utilizando IA de su LLM con *prompts* ensayados en otras incidencias parecidas a la situación real. La recopilación es autónoma y sistemática, bajándose en primer lugar cartografía y fotografía aérea para los sistemas digitales de planeamiento y navegación individuales y de equipo. Simultáneamente, en fuentes abiertas, con las debidas protecciones para no alertar de las intenciones, se ponen en marcha las capacidades de búsqueda OSINT: el equipo operativo, las unidades de inteligencia del MOE (nivel táctico) y del MCOE en el nivel operacional, apoyando el resto de niveles que tienen necesidad de conocer como el RINT n.º 1[2], J2[3] del MOPS[4] en el nivel operacional coordinando con X y aliados y, por supuesto, el CIFAS en el estratégico; la unidad de conducción y planeamiento estratégica en el Estado Mayor Conjunto del Jefe de Estado Mayor de la Defensa realiza también la coordinación en STRATCOM[5].

---

1 MOE. Mando de Operaciones Especiales del Ejército de Tierra (ET).

2 RINT n.º 1. Regimiento de Inteligencia n.º 1 de Fuerza Terrestre del ET.

3 J2. Jefatura de Inteligencia a nivel conjunto. Nomenclatura OTAN.

4 MOPS. Mando de Operaciones Conjunto de la Defensa. Encargados del mando y control de las operaciones exteriores y, en caso de un conflicto o crisis, se convertiría en el Mando de nivel Operacional.

5 STRATCOM. Comunicaciones Estratégicas. Encargada de la coordinación de campañas de información y de las medidas ejecutivas para el dominio cognitivo, con operaciones psicológicas, de «influencia» y de información pública entre otras.

La IA presenta en horas lo que antes necesitaba días, toda la información disponible en las bases de datos múltiples de inteligencia básica y mediante los *prompt* adecuados lanza peticiones automatizadas de información, RFI[6], al sistema de gestión centralizado del Sistema de Inteligencia de las Fuerzas Armadas, SIFAS, y recopila con IA los requerimientos de todas las unidades implicadas en la adquisición de inteligencia actual y reparte tareas de manera automatizada a sensores, planes de vuelo de UAV, satélites de control propio y, en su caso, de aliados, barcos, submarinos o aviones de guerra electrónica e inteligencia de imágenes.

Las IA del SIFAS alerta y suministra a todos los nodos implicados, informes y productos disponibles hasta el momento sobre la crisis adaptados a sus necesidades, con dos vértices: en el equipo operativo que deberá realizar la operación, el principal; y en el nivel político-militar de decisión.

Se recopila y resume información sobre las etnias, líderes, sus perfilaciones psicológicas indirectas, intencionalidades, capacidades, tipo de armamento disponible, red de apoyo de los grupos insurgentes o terroristas; se mapean las redes sociales del país, localidad y entorno de la embajada, se recopilan videos y material multimedia de los grupos insurgentes y se separan de los mismos datos biométricos como rasgos faciales, voz, iris o tatuajes y otros atributos distintivos de identidad, para investigar quiénes pueden ser los autores. La IA separa y secuencia actores hostiles con sus rasgos físicos y los equipos OSINT[7] del CIFAS recopilan información de *Identity Intelligence*[8] de los mismos: cuentas bancarias, teléfonos, direcciones IP y detalles de ordenadores, servidores, vehículos, familiares, amigos, domicilios, costumbres como rutas frecuentadas, bares, tiendas… todo ello con la prelación automatizada con IA de importancia relativa de esos actores. Adicionalmente se recopila la información física de españoles y trabajadores que pudieran o no estar ya en la embajada. No nos olvidamos de los planos de la embajada y edificios colindantes factibles de poderse utilizar para acceder por sorpresa en el asalto que se prepara.

---

6 RFI. *Request for Information*. Petición de información.

7 OSINT. Inteligencia de fuentes abiertas.

8 *Identity Intelligence*. Departamento y actividad que aglutina todas las características de identificación biométrica de individuos, junto con el resto de rasgos que definen esa «persona» como sus cuentas bancarias, vehículos, red de amigos y familiares, costumbres, personalidad o cualquier otra vinculada.

El mapa electrónico del objetivo, y de todas las vías de aproximación, se adquiere: qué radares hostiles o amigos a los que avisar del paso de helicópteros o apoyo aéreo en tiempo y forma; qué comunicaciones y repetidores gestionan la información de la embajada, se solicita al país anfitrión la interceptación de comunicaciones radio y móvil en la embajada y proximidades, ya que pudiera haber informantes cómplices de los asaltantes fuera. Mediante IA se traducen y transcriben las comunicaciones en tiempo real, se analizan y, en caso de interés, se trasladan a los órganos de inteligencia en los diversos niveles para que aprovechen la información.

Gracias a una imagen adquirida por un equipo HUMINT[9], de un agente local encubierto colaborador que se ha acercado a la embajada, se han logrado sacar unas fotos y videos de varios terroristas y se extrae entre las máscaras una nariz y algunas orejas, formas de andar y coger las armas que, analizadas con IA, han demostrado la identidad de algunos asaltantes, pertenecientes a una de las facciones insurgentes y cuyo líder se conoce por un video de propaganda; en niveles superiores se perfila psicológicamente al líder y se analizan con IA las posibilidades conductuales del mismo. El equipo HUMINT ha conseguido colocar con micro robots cámaras de video con micrófonos desatendidas, emisores-receptores wifi; todos los sensores son controlados desde España, y recopilan el número y posición dentro de la embajada de los activistas, sus comunicaciones y rutas… y, lo más importante: dónde se encuentran los rehenes, agrupados en varias habitaciones.

El equipo operativo, con la ayuda de programas informáticos de arquitectura administrados por IA, han recreado virtualmente las instalaciones, mobiliario, posiciones de terroristas y rehenes, accesos… información que se actualiza en tiempo real al ser adquirida. El equipo comienza a ensayar los planes de rescate con equipos de realidad aumentada y armas simuladas, donde se incorporan como en un video juego el resto de componentes y apoyos. Conforme el campo de ensayo se replica en real, el equipo ya tiene memorizadas las instalaciones y entrenadas todas las incidencias posibles sobre el plan de ataque, que, una vez en físico, se optimiza con IA para reducir tiempos, optimizar lugares de acceso, armas empleadas, y, sobre todo, riesgos para

9 HUMINT. Inteligencia de fuentes humanas.

los rehenes. Prima la seguridad y rapidez de liberación de estos sobre la del equipo de intervención.

El CIFAS recopila más información y analiza con sus expertos y los externos que se adscriben del mundo académico, diplomático y empresarial y, con ayuda de sus herramientas de IA, realiza modelos predictivos de los diversos escenarios de todo nivel: político-militar, estratégico a táctico, y la incidencia de las diversas posibilidades de actuación en adversarios, aliados y neutrales. La IA pondera variables, influencia de actores, instrumentos de poder de los sistemas intervinientes, las relaciona con todo el conjunto de evidencias, productos de inteligencia relacionados, predicciones, y actualiza sus algoritmos para reducir la incertidumbre y los sesgos cognitivos, y presenta posibilidades para que finalmente el componente humano tome las decisiones finales de valoraciones y recomendaciones para los decisores.

El gobierno y el gabinete de crisis donde la ministra de Defensa, el JEMAD[10] y otros actores importantes como el Departamento de Seguridad Nacional, CNI[11], el CIFAS, Ejércitos/Armada, MCCD[12] y MOE reciben la actualización de inteligencia del CIFAS en cuanto a la opción militar a realizar; finalmente el MOE expone la acción a desarrollar y se toma la decisión ejecutiva.

El equipo operativo se ha desplazado y está próximo a intervenir en las proximidades de la embajada en el país X, y continúa recibiendo, en tiempo real, gracias a su nube de combate, toda la actualización de inteligencia, el video en directo de los UAV[13] y satélites, actualización de inhibidores de comunicaciones y la situación actualizada dentro del objetivo, la IA reconoce los patrones de importancia y presenta al equipo solo la información de interés; mediante micro UAV en enjambre, robots capaces de anticiparse y reconocer zonas no controladas, identificar y transmitir la información entre ellos y en la nube y hasta España. Cada componente del equipo recibe alertas en tiempo real en sus visores holográficos ajustados a sus cascos, mientras que las constantes vitales y circunstancias del combate como direcciones de fuego, imágenes, reconocimiento e identificación de rehenes o terroristas o apoyos de fuego sobre lugares concretos son transmitidos de la nube de combate local a los helicópteros y cazas en

10 JEMAD. Jefe de Estado Mayor de la Defensa.
11 CNI. Centro Nacional de Inteligencia.
12 MCCD. Mando Conjunto del Cíber Defensa.
13 UAV, Unmanned Aerial Vehicle. Drones voladores.

espera para dar apoyo, y recibirán los orígenes de fuego hostil y parámetros de aterrizaje en tiempo real gracias a los diversos algoritmos de IA que sugieren alternativas de actuación en relación con la información recibida por todos los sensores.

Los rehenes son rescatados y los secuestradores neutralizados, y detenidos. Parte del equipo escolta a los rehenes a sus helicópteros de evacuación, mientras que otra parte se queda en la embajada para recopilar evidencias forenses, fotos, ADN, armas, teléfonos y ordenadores para su posterior análisis; se compartirán esos indicios con aliados y el país X, con los que se cruzarán datos para resolver la implicación de algunos de los terroristas en otros atentados con IED[14]. La utilización de IA ha sido clave para buscar con ciencia de datos entre miles de pistas y cruzarlas para convertirlas en indicios relacionales para desarmar redes delictivas y terroristas en las que militaron los finados.

Pero no termina ahí la labor de inteligencia porque hay que evaluar el impacto en RRSS[15], medios de comunicación y percepción en la sociedad del país X y otros de interés, junto a España. Se detectan campañas de desinformación y de guerra híbrida conducentes a desestabilizar y sacar beneficio de criticar los éxitos, maximizar los posibles errores producidos en la operación, victimizando y engrandeciendo al grupo terrorista como luchadores por la libertad. Se trabaja en la detección de la campaña de desinformación, sus narrativas, redes de difusión, detección de robots, procedimientos y verdaderos responsables, la IA es clave para realizar el trabajo en tiempo mínimo y contribuye a relacionar vínculos ocultos. Se realizan operaciones de *hacking* y detenciones físicas de responsables de esos entes cibernéticos para saber quién está detrás y qué intencionalidades han tenido o podrían tener en el futuro.

Para todo lo anterior, el MCCD y especialistas DOMEX[16] del MOE, RINT y CIFAS realizan la extracción de información de esos terminales informáticos, para lo que se rompen los códigos de encriptación y se analizan sus ficheros remotamente para encontrar instigadores y redes clandestinas en la *dark web* dedicadas a la financiación con criptomonedas, recluta, propaganda y adiestramiento de terroristas y grupos de crimen organizado relacionados

[14] IED, artefacto explosivo improvisado.

[15] RRSS, Redes sociales.

[16] DOMEX. Extracción de datos e información de documentación y medios informáticos/electrónicos capturados.

entre ellos. Y con J9/10 Influencia[17] y EMACON en su unidad de Comunicación Estratégica STRATCOM suministrar la información pertinente para desarrollar la contra campaña de infoxicación y desinformación con medidas dinámicas. Finalmente, gracias a las labores de inteligencia después de una operación, se detectan y previenen acciones hostiles futuras contra los intereses de España y sus aliados.

2. Una introducción

Con este relato, parecido al de un guion de película que bien pudiera ser real, hemos repasado de manera general los grandes efectos multiplicadores actuales de la IA en una operación militar de rescate de rehenes, quizás una de las más difíciles; y las intersecciones con la inteligencia como disciplina, responsable del éxito de las operaciones.

Efectivamente, la importancia creciente de la inteligencia en las crisis de todo tipo es incuestionable desde que se popularizó el paradigma *Intelligence leads operations*[18], aplastante corriente con la doctrina de contrainsurgencia (Kilcullen, 2010) tras la segunda guerra del Golfo y reflejo de la importancia de la inteligencia en las operaciones «quirúrgicas» tipo de las operaciones especiales y fuerzas de seguridad policiales, con sus *Intelligence Lead Policy* (ILP), en las que el detalle y contrastabilidad de la inteligencia condiciona y autoriza todas las operaciones[19] (Burcher y Whelan, 2018), todas ellas con supervisión legal final tras el proceso de recopilación de evidencias de inteligencia.

Si hay algo que caracteriza a esas operaciones quirúrgicas antedichas es la necesidad ingente de información e inteligencia, su proceso y análisis. Con la irrupción de la IA, somos capaces de abarcar más, con menos esfuerzo, de mejor manera, menos personal y más rápido.

---

17 Secciones del Estado Mayor J9 Información y J10 Influencia.

18 «La inteligencia lidera las operaciones». La traducción puede llevar a engaño, pues el verbo lead significa según el diccionario Cambridge: dirigir, liderar, ir ganando, conducir, llevar, conducir, llevar, … Su sentido invierte el paradigma de las fuerzas armadas burocratizadas de paz, acostumbradas a los ejercicios en el que el papel todo lo aguanta, que no han participado en situaciones bélicas de máximo esfuerzo y bajas; en estas últimas las Operaciones lideran y justifican todo el resto de las facetas de las funciones organizativas de Estado Mayor, incluida la Inteligencia.

19 *Intelligence-led policing* (ILP). Modelo para fuerzas de seguridad del estado policiales que busca colocar la inteligencia sobre el crimen al frente de las decisiones o las operaciones. Concepto manejado por los países anglosajones.

La utilización de la IA para la resolución de problemas de inteligencia está en relación con los desarrollos tecnológicos y a la revolución en los mismos, experimentada, sobre todo, en este primer cuarto de siglo XXI. En otros capítulos de este trabajo se expone la historia reciente de la IA, pero recordemos que el desarrollo de los ordenadores y los primeros algoritmos complejos nacieron de las necesidades bélicas durante la Segunda Guerra Mundial, en particular, de la inteligencia militar en descifrar los mensajes codificados por la herramienta analógica y mecánica Enigma; gracias a lo cual y a la interceptación de las comunicaciones, lo que llamamos SIGINT[20], los aliados consiguieron una ventaja estratégica, que favoreció su triunfo. En la actualidad, el visor de prospectiva de la IA en apoyo de las operaciones militares en su conjunto, y en particular de la Inteligencia, está sobre Ucrania, que se analiza expresamente en otro apartado del presente trabajo.

3. La IA como eje en la competición estratégica actual

Los EE. UU., desde la Segunda Guerra Mundial, han liderado todo lo concerniente a la innovación militar y, en particular, la IA no podía mantenerse ajena a la misma, si bien el entorno global de seguridad emplaza la competición estratégica entre EE. UU. y China. Podemos considerar que Rusia pasaría más a aliado del nuevo pretendiente a «hegemon» en el balance geopolítico mundial, aunque mantenga ese peso estratégico que le da el poder nuclear y no tanto el militar convencional y de desarrollo tecnológico, como se está constatando en su agresión a Ucrania.

China, a nivel económico, ya está a nivel de equilibrio, lo que le permite pasar a la última fase en su estrategia enunciada por Pillsbury del «Maratón de los 100 años»: la supremacía militar; y esta estará basada en encontrar su *Assessin's Mace*, el arma definitiva de su imaginario ancestral, que le dé el éxito frente a sus enemigos más poderosos (Pillsbury, 2016). Esas armas, estrategias (Aranda, 2023) o tecnologías disruptivas con las que China pretende superar a EE. UU., el actual hégemon, y sus aliados tienen como finalidad impedir que este y sus aliados le rodeen,

[20] SIGINT. Inteligencia de señales, dividida en las relativas a comunicaciones COMINT y firmas electrónicas ELINT.

como en el wo[21], y estrangulen la economía y salida estratégica de China con su superioridad aeronaval y espacial.

Para ello, en la búsqueda del arma definitiva, están creando una serie de sistemas de armas con una carga importante de IA en su desarrollo, diseño y C4I[22]. Tenemos ejemplos como los submarinos, las armas hipersónicas, los misiles anti satélites, los medios de interceptación y armas cíber, el *hacking* y todo lo concerniente a la guerra cognitiva. Todo ello fue introducido por los trabajos conceptuales chinos (Liang y Xiangsui, 1999), que probablemente inspiraron a Al Qaida y resto de las estrategias asimétricas que hoy llamamos de zona gris o guerra híbrida[23] (Pillsbury, 2016).

Pero, para el predominio tecnológico de China, uno de los ejes fundamentales ha sido el desarrollo de sus capacidades de copia y robo de tecnología utilizando sus importantes capacidades de espionaje, esto es inteligencia (Pérez, 2023), con infiltración tanto humana como tecnológica, con el uso extendido de las capacidades cíber para incluso acceder a información personal de gran parte de la población de EE. UU. (Clarín, 2020).

El nexo común que interrelaciona todas esas necesidades y capacidades está siendo el desarrollo de la IA, en el que se presume será el verdadero cemento de su pretendida supremacía mundial futura, que le ayudará a desarrollar su *Assessin's Mace*, junto con el conocimiento profundo e influencia en los sistemas de gobernanza mundiales, con superioridad en la prospectiva estratégica y el conocimiento gracias a la inteligencia y su gestión mediante IA, que pretende liderar para el 2030 (Knight, 2017).

Pero antes de continuar, aclaremos algunos términos.

4. Conceptos básicos: tipos de IA y de inteligencia

Entendemos como IA al proceso llevado a cabo por una máquina que puede analizar, organizar y convertir información en conocimiento

[21] Wo, juego ancestral chino, preferido al ajedrez, y en el que las piedras rodeadas del adversario son eliminadas; hay que rodear sin ser rodeado. En la educación china «Las 36 estratagemas» (Aranda, A. 2023) y las historias ancestrales de las luchas de los reinos chinos en guerra antes de la unificación, son la base de la estructura mental y cultural.

[22] C4I. Mando, Control, Comunicaciones, Computadoras e Inteligencia.

[23] La estrategia de la guerra irrestricta fue primeramente abrazada por Al Qaida, según múltiples analistas, ya que ejemplos de acciones descritas en este ensayo fueron realizadas muy poco después de su publicación, como el ataque a las Torres Gemelas el 11S, o atentados en África, además de existir constancias de asesores chinos en el Afganistán de los Talibanes y son previas a la famosa formulación de la guerra híbrida de Gerasimov.

(Jiménez, 2021). Estas IA utilizan programas, que son una representación de un algoritmo en un lenguaje de programación que puede ser interpretado y ejecutado por un ordenador. Y los algoritmos son la descripción del método mediante el cual se realiza una tarea; una secuencia de instrucciones que, ejecutadas correctamente, dan lugar al resultado que se busca. Los diseños de algoritmos están basados en procesos matemáticos que pueden ser trasladados a un ordenador, luego son computables e incluidos en la teoría de la computabilidad (Abellanas y Lodares, 1990).

4.1. Tipos de IA

Los tipos de campos de la IA, sin profundizar, los recordamos en las siguientes ramas de la IA, haciendo referencia al desarrollo de la aplicación de la materia o al campo de investigación de esta.

Estos campos de investigación de la IA son diversos (Russell y Norvig, 2004) en referencia al *test* de Turing en:

- Machine Learning (ML). Toman decisiones futuras utilizando la experiencia pasada.
- Procesamiento del lenguaje natural (PLN).
- Sistemas expertos. Proporcionarían una solución de un determinado problema.
- Visión artificial.
- Lógica difusa. Creando aproximaciones matemáticas para la resolución de problemas se producen resultados exactos mediante información imprecisa.
- Agentes inteligentes. Utilizando su propio conocimiento, ajustándose a los cambios del entorno, son capaces de realizar operaciones que satisfacen lo solicitado por un usuario.
- Deep Learning. Redes neuronales artificiales.
- Robótica.
- Algoritmos genéticos. Son aquellos inspirados en los procesos de la evolución genética y la supervivencia de las soluciones mejor adaptadas al medio.

Todos estos campos de la IA son de diversa aplicación a las actividades de inteligencia, como vamos a desarrollar a continuación.

4.2. Tipos de inteligencia

Los avances que en los últimos años se han producido en los campos de la IA son extraordinarios y tienen aplicación cada vez

mayor en la inteligencia. De una manera inmediata en lo que llamamos la inteligencia actual[24], gracias a la velocidad y automatismo de sus procesos, que permiten aproximar al tiempo real el que trascurre desde la captura de la información por el sensor al aprovechamiento de esta gracias a los mecanismos también autónomos en el procesado y preparación de los datos para transformarlos en inteligencia.

Pero para esa transformación final de la inteligencia se requiere una compilación de la información actual con la preexistente en forma de inteligencia básica. Hasta tiempo muy reciente, el uso de cierta IA se implementaba en los procesos de gestión y almacenamiento en bases de datos. Con la irrupción de la IA y técnicas tan específicas como el *Machine, el Deep Learning*, y el procesamiento del lenguaje natural (PNL), es posible el uso intensivo en cualquier base de datos de procesos estadísticos avanzados que permiten sacar segundos provechos de los datos almacenados.

Antes de la irrupción de la IA, era limitada la utilización masiva de datos y la mecanización con cómputo de tareas arduas y muy exigentes en cuanto a precisión; trabajo óptimo para robots. A lo anterior, unimos, desde hace poco más de un año, con la aparición de los LLM[25] o los grandes modelos de lenguaje natural como ChatGPT y su revolución conceptual y técnica global, que muchos han comparado con la invención de la rueda o internet (Leonhard, 2023), y, como no, también en el de la inteligencia como actividad genérica.

Vamos a analizar la situación actual y de desarrollo futuro, desde la perspectiva de la inteligencia, sus fases y disciplinas, y cómo la IA interviene o puede afectarles.

5. La IA en el ciclo de inteligencia

Pasemos ahora a revisar los procesos generales de inteligencia, en los cuales destaca el omnipresente ciclo de inteligencia, pero, de los diversos tipos existentes, cogeremos como referencia el de la doctrina OTAN y española: dirección, obtención, análisis y difusión.

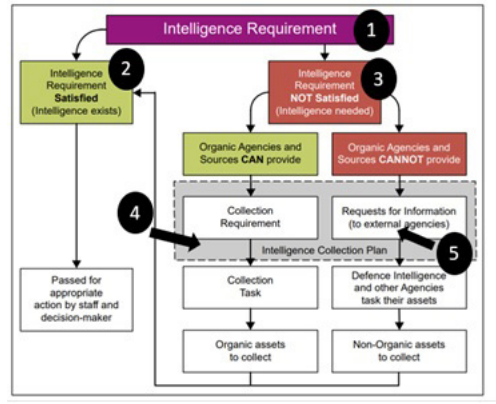
[24] Inteligencia actual. La del momento, muy vinculada a plazos inferiores a las 24 horas y cómo no la de tiempo próximo al real, gracias a la sensorización e intervención de IA en los procesos JISR.

[25] LLM. *Large Language Models*. En los que se inspiran los revolucionarios desarrollos de Open IA (ChatGPT) y del resto de gigantes tecnológicos en sus respectivos desarrollos todavía no tan avanzados.

5.1. Dirección

Esta fase de los procesos de inteligencia ha sido tradicionalmente la más reticente a la intervención robótica de la IA en los aspectos de decisión volitiva de los jefes. Pero la situación está cambiando por la irrupción de campos de la IA como el «Razonamiento Aproximado», la automatización de procesos que ya eran mecánicos en su realización humana, como gran parte de los que están bajo el paraguas conceptual de JISR[26] (Scott y Michell, 2022) y sus subprocesos de IRM[27], de gestión de las necesidades de inteligencia y CM, gestión de los medios de obtención. Interesante nueva aportación con un peso importante de IA es el centrado en la inteligencia, información, cíber, guerra electrónica y capacidades espaciales, I2CEWS[28] (Borne, 2019).

En estos procesos IRM se comparan los requerimientos e información necesarios para la elaboración de un producto de inteligencia y la IA puede cotejar de manera autónoma cuáles ya están en las bases de datos de inteligencia básica y, para los que no están, pasarlos a la siguiente estructura doctrinal, la gestión de la obtención CM, donde se dividen y preparan las necesidades de información para la elaboración de órdenes de obtención a los propios sensores y unidades o, en su defecto, solicitar esa información mediante peticiones de información a las unidades o entes de igual o superior nivel, con las RFI[29], según cuadro que se anexa y orden de procesos del uno al cinco.



Tareas y procesos para requerimientos de obtención. Collection Management (DCDC, 2011)

[26] JISR. *Joint Intelligence, Survaillance and Reconnaissance*. Inteligencia, vigilancia y reconocimiento conjuntos (cualquier dominio).

[27] IRM. *Intelligence Requirement Management.* CM, *Collection Managements.*

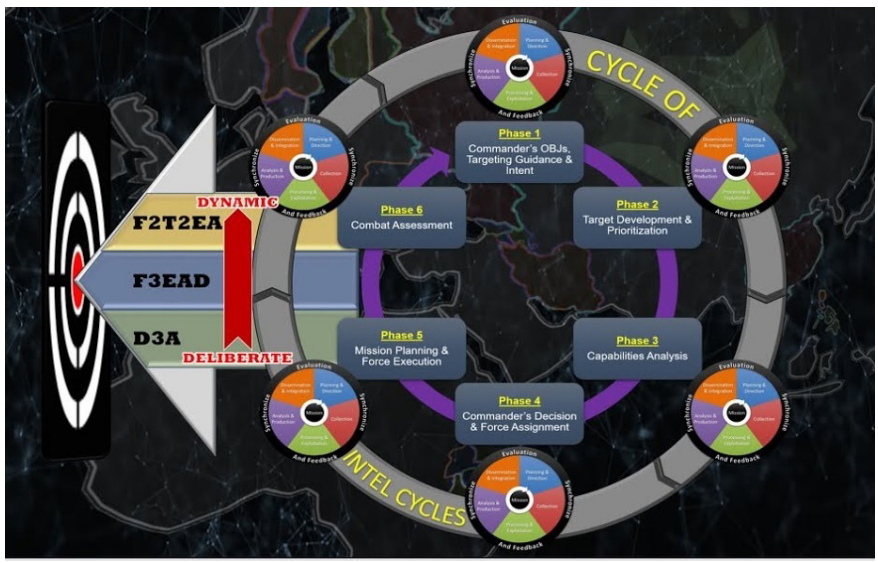
[28] I2CEWS. Concepto nuevo en implantación en EE. UU. *Intelligence, Information, Cyberspace, Electronic Warfare, and Space*

[29] RFI. *Request for Information.* Petición de información, con un formato determinado y estandarizado de circulación y uso común en todos los ejércitos y servicios occidentales. Ver en bibliografía presentación de la ONU.

La asignación automatizada con IA de misiones a sensores cada vez se puede realizar en tiempo próximo al real y el *dynamic re-tasking* (Saling, 1999) de los medios de obtención, esa reasignación de misiones una vez lanzados en ejecución, es más sencilla y está haciendo replantearse los plazos de petición y planeamiento de las mismas. De manera concurrente, la extensiva ocupación y sensorización del campo de batalla no continuo hace que la reasignación de misiones dinámica ya no sea excepcional, gracias a la intervención de la IA en la gestión administrativa y operativa necesaria para variar órdenes, rutas aéreas, sobrevuelos anunciados normalizados y gestiones de los espacios de batalla aeroterrestres y marítimos.

La IA aumenta la seguridad en esas reasignaciones dinámicas para evitar conflictos o colisiones. Algoritmos que soslayan los fallos humanos y aumentan la velocidad necesaria de trasvase de informaciones y cálculos de interés compartido complementario entre diversas plataformas/sensores u organizaciones; todas esas decisiones y gestiones necesitan la automatización para disminuir el tiempo de todos los procesos a tiempos inasumibles por el hombre.

Los plazos se minimizan gracias a la IA para solicitar y planear misiones para entrar en el ATO[30] de un determinado día.



Representación del ciclo conjunto de Targeting de la doctrina de EE. UU.

[30] ATO, *Air Tasking Order.* La publicación de las misiones aéreas con sus rutas, horarios y ocupación del espacio aéreo.

Esos ciclos de planeamiento se dinamizan y aceleran, debiendo imponerse a los del adversario, ya que son importantes para la coordinación del resto de ciclos como el de *targeting* (ATP 3-60) y JISR, y para la priorización de misiones, la asignación de sensores y medios para cada obtención. Estos procesos pueden ser también automatizados con IA.

De hecho, el modelo de la asignación de medios y misiones en los campos de la inteligencia y las operaciones enmarcados por el *targeting* moderno (Kyle, 1999) implica una automatización con IA para los TST[31], esos blancos de oportunidad típicamente desarrollados en las operaciones contra terroristas o insurgentes, como excepciones en las largas listas de objetivos, y que paraban todos los planes en marcha para reorientarlos a ese blanco sumamente importante que debía ser alcanzado lo antes posible cuando quiera que fuera localizado.

Otros campos de empleo de la IA pueden tener aplicación a esta fase, facilitando que no haya esa distinción de fases, sea todo fluido con el mérito de la rapidez y fiabilidad de la IA que nos permita desdibujar cuándo estamos en una u otra fase.

De esta manera, se pueden interconectar simultánea o secuencialmente una combinación de las diversas Necesidades de Información, NI, que se complementan y retroalimentan en tiempo próximo al real conforme se dan las condiciones y desarrollando nuevas NI, y adaptaciones de las Necesidades Críticas de Información del comandante, CCIR, que podrán ser más dinámicas conforme se sincronizan los ciclos de inteligencia, *targeting* (EE. UU. Joint Targeting School Guide, 2017) y operaciones: los ciclos de decisión, inteligencia, control y comunicaciones, C4ISR, se aceleran también por la IA para colapsar los ciclos del adversario.

¿Qué campos específicos de IA son de aplicación para este conjunto de actividades tan variopintas? Entre otros, los algoritmos adaptados a la resolución de decisiones complejas, problemas de decisiones secuenciales[32], sean estas parcialmente observables

[31] TST, *Time Sensitive Targets*. Objetivos de oportunidad de suma importancia.

[32] Richard Bellman, trabajando en la RAND Corporation desarrolló el concepto en 1949. *Dynamic Programming* (1957) para la resolución de problemas de horizonte infinito. Problemas de decisión secuencial en entornos inciertos, llamados, en inglés, por el acrónimo MDP, *Markov Decision Processes*, proceso que especifica los resultados probabilísticos de acciones y la función de premio que puntúa el mismo para cada caso.

o no[33]; también las redes dinámicas de decisión para adaptarse en sus estados de conocimiento conforme se recibe nueva información que complete la percepción de la realidad, para en último término inferir acciones posibles futuras; y, por último, también los conceptos adaptados de la teoría de juegos[34], entre otros.

Las necesidades específicas de inteligencia[35] (SIR), los elementos esenciales de información (EEI) e incluso las necesidades críticas de información del comandate (CCIR) se descomponen en variables y algoritmos de búsqueda de las que las necesidades prioritarias de inteligencia (PIR), se concretan en indicadores de escenarios; todos son indicadores (KPI) de diversos niveles de detalle que pueden ser relacionados como variables cualitativas transformables a cuantitativas y accionables con IA.

En definitiva, los sistemas de alerta de inteligencia necesitan la mecanización que permita monitorizar en tiempo real los cambios en las condiciones y, con sistemas de apoyo a la toma de decisiones (DSS), disminuir los tiempos de reacción de los decisores humanos. Estos procesos se aplican a cualquier actividad de respuesta a emergencias o civil, con la nomenclatura OTAN según las funciones que incluya (Delgado, 2020).

En este sentido, las Fuerzas Armadas españolas están implantando un sistema integral, el Sistema de Mando y Control Nacional, SC2N, (Ruiz, 2023) dentro del cual existe un subsistema dedicado a las labores de inteligencia, donde encontramos integradas las actividades del ciclo de inteligencia e interrelacionadas con el resto de sistemas como el de *targeting* u operaciones entre otros.

5.2. Obtención

En esta fase se explotan las fuentes, los sensores humanos o técnicos, y, por tanto, intervenidos en mayor o menor medida con IA, todos medios de obtención. También tenemos en esta fase los mecanismos para la entrega de la información obtenida a los

[33] POMDP. Acrónimo inglés referido a *Partial Observable* MDP, Problemas de decisión secuencial parcialmente observables.

[34] En la teoría de juegos se busca el equilibrio de Nash en el que no hay incentivos para las decisiones que se desvíen de una estrategia definida por humanos, y, por tanto, transformable en algoritmia controlada por humanos.

[35] SIR, *Special Intelligence Requirements;* EEI, *Essential Elements of Information*; CCIR, *Commander Critical Information Requirements*; PIR, *Priority Intelligence Requirements*; KPI, *Key Performance Indicator.*

órganos de análisis de la siguiente fase del ciclo de inteligencia, pero incluyendo un primer análisis eminentemente técnico del propio órgano recolector.

Esos sensores de los que hablamos son los medios JISR, en su mayor parte, que en la doctrina OTAN ha cobrado tal importancia como para fundamentar procesos específicos y la integración con los de mando control, comunicaciones, el conocido como JC4ISR, que vertebra esa sensorización masiva del campo de batalla, y que requiere de una gestión en la que la IA pasa de simple ayuda a ser protagonista imprescindible en ese *big data* autónomo.

Las creaciones conceptuales de la futura nube de combate de comunicaciones tipo 5G y 6G están haciendo que grandes empresas como Telefónica y GMV exploren soluciones para exportar el mundo tecnológico de la conectividad permanente a áreas remotas o denegadas por acciones hostiles y sacar ventaja de la superioridad tecnológica en los futuros conflictos.

Aquí vamos a dividir esa captura de información no elaborada en las disciplinas, campos y técnicas de explotación de inteligencia principales (no todas) que permiten dividir las facetas en las que la realidad puede ser diseccionada para su mejor asimilación.

5.2.1. OSINT. Inteligencia de fuentes abiertas

Empezamos por la disciplina que más ha crecido en su relación con la IA gracias a la digitalización con internet en la práctica totalidad de las actividades humanas.

Como ya avanzara Alvin Toffler en algunos de sus premonitorios libros de los noventa del siglo pasado, entre ellos *El cambio de poder* o *Las Guerras del Futuro*, la digitalización permitiría el paso de una sociedad de la segunda ola[36] a la tercera en la que el conocimiento, y por extensión la inteligencia, son las claves para el éxito y catalogación como sociedades avanzadas. En estas, su valor añadido lo da la calidad de la población fundamentalmente con el acceso a la educación avanzada para transformar por la tecnología la sociedad misma. Digamos que esta última reflexión casa muy bien con el efecto transformador de la IA en nuestra

[36] Teoría de las olas de Toffler de desarrollo de las sociedades. 1.ª ola con la revolución agraria, 2.ª ola con la revolución industrial y la 3.ª actual en la que la globalización y el cambio a sociedades del conocimiento con la irrupción de las tecnologías de la información.

sociedad actual, y que algunos teóricos ya catalogan como la 4.ª Revolución Industrial (Pérez y Sánchez, 2019).

La importancia actual del OSINT viene dado por el uso global de las fuentes abiertas, el *Open Source*, y la democratización de la tecnología que muchos teóricos iniciales de la IA preconizaban. Podemos decir que en el cajón de herramientas de un analista OSINT las que tienen un carácter de acceso abierto son preponderantes.

Prácticamente ningún servicio de inteligencia es capaz de competir con el *Open Source* mundial en el que individuos no adscritos a organización alguna y unidos por un sentido tribal de pertenencia a ese mundo de compartición avanzan sin restricciones. En él, los retos, trasvase de innovación y soluciones entre la comunidad de interés y hasta la compartición de código entre la colectividad OSINT hace que en cuestión de meses las herramientas que eran una solución factible se queden obsoletas o sean bloqueadas por sus desarrolladores para monetizarlas, pero son sustituidas inmediatamente por otras con el mismo carácter inicial llamémosle *Open Source*.

La unión tecnológica de las capacidades y necesidades del mundo cíber y del mundo OSINT es un hecho, y analistas o equipos OSINT integran capacidades de ingenieros y desarrolladores informáticos, así como diversos perfiles de científicos de datos y estadísticos. La necesidad de código específico y de *hacking* ético aúna los mundos que hasta hace poco estaban distantes. Así, cada vez se requieren más analistas de inteligencia, ya especializados en seguridad, ciencias políticas y relaciones internacionales, pero añadiendo conocimientos profundos informáticos y de cíber seguridad. Con este tipo de profesionales, el salto a la utilización de IA, ya sea propia o adaptada, potencia las capacidades OSINT a unos niveles de autosuficiencia técnica y de importancia capital para los servicios de inteligencia.

Ese hecho se constata por la mayor importancia de una disciplina que reivindica su papel clave para el resto, no solo para fundamentar el conocimiento de partida para otras disciplinas como el HUMINT, IMINT o el SIGINT, sino como fuente del conocimiento único sobre la mayoría de necesidades de inteligencia, ya sea por ser capaces de recopilar el conjunto disponible de información sobre las mismas, como por no haber otras disciplinas que tengan acceso al nicho donde se encuentra la información disponible.

Los informes de única disciplina, los OSINTREP, ya no son considerados un informe menor, sin distinción ni valor añadido en comparación a las otras disciplinas diferentes del OSINT, que suelen ser exclusivas de las capacidades militares y de servicios de Estado, estos son los que pueden pagar los medios y sensores tan caros que los soportan, como por ejemplo satélites, drones o pods de SIGINT, o la posibilidad de reclutamiento y adiestramiento de agentes HUMINT, los James Bond de nuestro imaginario cinematográfico colectivo.

Es extensiva la utilización por los investigadores periodísticos, o el mundo OSINT, de los informantes ocasionales que cuelgan en las diversas redes sociales sus videos y fotos, sus valoraciones o comentarios. Estas redes sociales, se sitúan en la web profunda, la *deep web*, aquella en la que la información no está indexada, no buscada ni catalogada por buscadores tipo google, yahoo: la *surface web* y que explotan solo del 4-8 % de toda la información que circula por internet. La inmediatez que posibilita tener testigos improvisados allá donde se da la noticia o evento de importancia, trasciende a nivel mundial gracias a la posibilidad de compartición de esa experiencia a nivel global. El que haya plataformas comerciales como las de empresas como Dataminr que hayan llegado a explotar esas capacidades con el uso intensivo de IA para extraer la información, verificar la veracidad de esta, contrastarla con otras fuentes disponibles, y todo en tiempo próximo al real, está posibilitando la irrupción de la empresa privada en el uso de estas tecnologías de conocimiento al servicio, antes exclusivo, de grandes corporaciones y Estados.

El que esas herramientas desarrolladas por empresas especializadas en inteligencia OSINT puedan ser adaptadas a las necesidades y preferencias de cada usuario las hace muy atrayentes para otras empresas en las que el uso de la información es vital para su negocio en campos tan dispares como el análisis de riesgos, el planeamiento estratégico de actividad, el marketing, o el impacto de la situación social, cognitiva, o política en sus actividades de negocio en determinados espacios geográficos o de modo global.

La revolución tecnológica actual hace que las capacidades que antes estaban solo al alcance de entidades oficiales y empresas poderosas, se extienda con la inteligencia económica y la irrupción de las necesidades de inteligencia en empresas para alerta temprana, evaluación del riesgo de sus inversiones en

lugares comprometidos y la seguridad del personal destacado. El OSINT es la disciplina que se ha extendido y está al alcance de cualquier empresa, ya sea de manera orgánica y permanente, o como servicio externo con asesorías de seguridad e inteligencia. Estamos ante tecnologías de doble uso: civil y militar (Toffler, 2001).

Portales como *Github, Google Colab* u otros de compartición o colaboración hacen que esa cesión de código en diferentes lenguajes minimice los esfuerzos de desarrollo de soluciones singulares y únicas adaptadas a las necesidades no solo de las organizaciones, sino de los equipos de analistas. Las capacidades de los mismos en OSINT se multiplica gracias a la implementación de soluciones *ad hoc* de IA para resolver problemas muy específicos.

Empleos efectivos del OSINT son cada vez más concluyentes e interesantes y la guerra en Ucrania está siendo un visor mundial del auge de la disciplina. El valor agregado de su democratización y las posibilidades que permite el acceso generalizado de la población con sus aplicaciones en *smartphones* y teléfonos a redes sociales por las que se difunden fotos, videos y comentarios directos, convierte a simples ciudadanos espectadores en agentes improvisados o testigos de primer orden, que rayan el «ciber HUMINT».

5.2.2. HUMINT. Inteligencia humana

Es la inteligencia de la información recolectada por operadores humanos del entorno físico y humano, de fuentes humanas.

Podríamos pensar que son actividades fuera de la cobertura de la IA, pero estos operadores humanos presentan limitaciones, prejuicios y sesgos cognitivos (Heuer, 1999), no controlan todos los idiomas de teatro en los que se pueden desplegar y a la hora de las entrevistas o interrogatorios, la ayuda de IA permitirá la interpretación de dialectos, lenguaje no verbal, detección de la mentira, entre otras necesidades, todas ellas en tiempo real.

Uno de sus cometidos son las misiones de reconocimiento, que perfectamente se pueden hacer a la vieja usanza con unos prismáticos o cámara y anotando incidencias, vehículos, personas… o bien expandiendo los usos de la IA con cámaras vinculadas en nube con algoritmos de reconocimiento y detección como si en

un circuito cerrado de televisión, CCTV, se tratara, pero pudiendo expandir las capacidades de imágenes visibles a infrarrojas o térmicas, reconocimiento automatizado de actores o vehículos, o implementando nuevas tecnologías de interpretación de señales wifi en el objetivo, cerca de él o por el propio equipo usando cámaras RGB, LiDAR, y radares portátiles o no para detectar movimientos y personas detrás de paredes (Newcomb, 2023) y en el que se utilizan algoritmos DensePose[37].

5.2.3. IMINT. Inteligencia de imágenes (De la Fuente *et al.*, 2022)

Es la inteligencia derivada de la adquisición de imágenes desde diferentes sensores y plataformas, ya sean basadas en tierra, aire o espacio. La adquisición de las citadas imágenes se puede realizar en el espectro visible, infrarrojo, multiespectrales, de detección de radiación electromagnética o en las imágenes obtenidas mediante señales radar.

El campo específico de la IA (Lauroba, 2021) que se ocupa de las imágenes está desarrollándose extensamente con set de datos de imágenes desde las diversas plataformas y ángulos de toma para detectar por ejemplo los expuestos por el INTA[38]:

– Detección de cambios

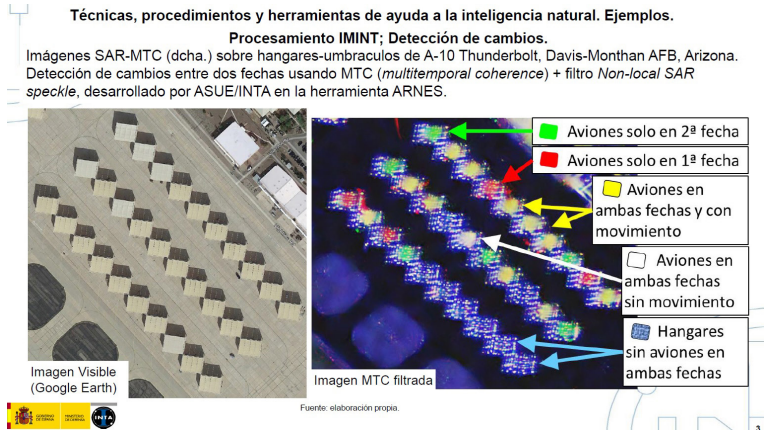


Figura 3

[37] Disponible en: densepose.org. Es parte de COCO and Mapillary Joint Recognition Challenge Workshop en ICCV 2019.

[38] INTA. Instituto Nacional de Técnica Aeroespacial.

Figura 4

– Detección de radares activos

Figura 5

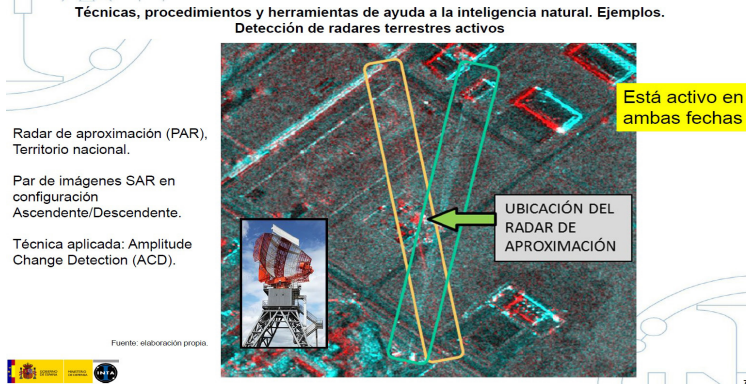


Figura 6

– Detección de movimiento

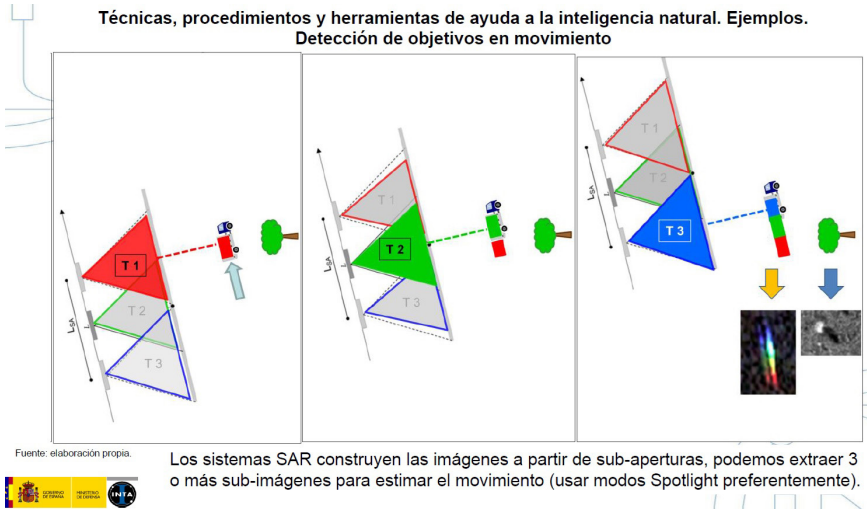


Figura 7

Y, por supuesto, todo el reconocimiento de objetos usando set de datos y fundamentalmente diversas técnicas de *Deep Learning* con redes neuronales combolucionales, con todo tipo de construcciones, aeronaves, etc.

La visión computerizada o artificial está en pleno desarrollo, pudiendo comprender su entorno, contribuyendo a la autonomía de los sistemas y aplicable a todo tipo de drones y es el nexo entre la disciplina IMINT clásica, que se circunscribía a imágenes aéreas, a poder integrar las de cualquier sensor terrestre y marítimos también, con lo que el campo de batalla envuelto en la nube[39] de combate, gracias a la computación en el borde[40] y en la niebla[41].

El procesamiento de imágenes incorpora potentes tarjetas gráficas que aportan potencia de cálculo para imágenes electroópticas e infrarrojas, con módulos de radio definidas por *software* (SDR) y PNT de posición, navegación y tiempo, que permiten la

[39] Servicios de computación en la red, internet u otra red propia.

[40] Estrategia de computacón distribuida que acerca la computación y almacenamiento de los datos a la ubicación donde se toman los datos y se necesita el cálculo, para reducir la latencia y el ancho de banda de comunicaciones requerido.

[41] Infraestructura descentralizada de computación en las que los ordenadores, datos y aplicaciones se sitúan entre la fuente de los datos y la nube.

comunicación e interacción de los sensores y sistemas entre sí para garantiza referencias únicas con el estándar de vetrónica de la OTAN. Todo ello permitirá la interactuación de sistemas de inteligencia con el FCAS, del Futuro Sistema Aéreo de Combate, y los enjambres de drones como fundamentales para los futuros campos de batalla.

El desarrollo de los sistemas espaciales está suponiendo un incremento de las funciones de ISR y su importancia para todos los dominios y sistemas autónomos, utilizando nuevas constelaciones de microsatélites.

Los satélites y plataformas espaciales de órbita intermedia (MEO) y sensores espaciales de órbita baja (LEO) con mayor intensidad de la señal y seguridad que mejorarán los sistemas de posicionamiento como el GPS, Galileo o el GNSS[42] y también mediante sensores inerciales, odómetros, cámaras, giroscopios. Todas estas mejoras implican computación a bordo e IA para fusionar datos con preprocesamiento de datos, reduciendo datos de comunicación con base, y autonomía ante procesos de navegación y superación de averías; pero con grandes limitaciones de espacio y energía necesaria, entretanto no lleguen los ordenadores cuánticos.

Las posibles supervisiones de robots o drones, mediante realidad virtual, aumentada o extendida, permitirán esa interactuación hombre-máquina que será la clave en la presentación de información e inteligencia accionable de manera inmediata a todos los niveles a todos los combatientes cualquiera que sea su función: de mando, asesoramiento, ejecutiva.

5.2.4. SIGINT. Inteligencia de señales

Es la inteligencia obtenida de las emisiones electromagnéticas. Su campo de actuación se divide en dos:

- Inteligencia de Comunicaciones (COMINT), cuando interviene la voz transmitida por cualquier medio electromagnético.
- Inteligencia Electrónica (ELINT), propia de las emisiones electromagnéticas que no pertenecen a la anterior.

Las posibilidades que da la IA de analizar, eliminar distorsiones, y comparar dichas señales, cualquiera que sea el tipo, asociando con análisis de redes actores y relaciones aumenta los éxitos ya

[42] GNSS: *Global Navigation Satellite System.*

cosechados en misiones contra insurgencia y contra terroristas, como en Iraq contra Al Qaida. En la actualidad, en Ucrania se ha hecho un uso combinado de esa localización, cíber jacking, extracción ISR de contenido de móviles, contactos, multimedia y la gestión de la información a unidades de operaciones psicológicas, de inteligencia y de SIGINT, artillería y planificadores. Esa información ha permitido desarrollar unas TTP por Rusia con la preparación de operaciones ofensivas sobre unidades previamente desmoralizadas y preocupadas por decepción masiva de sus combatientes, sus familias/amigos, noticias y fotos manipuladas para conseguir el efecto e inquietud justo antes del ataque convencional tradicional.

Este ejemplo expuesto denota el hecho de la tendencia en la convergencia de la ciberdefensa y la guerra electrónica en lo que llaman ciberelectromagnéticas (Porche *et al.,* 2013).

En España la ciberdefensa depende del MCCD[43] en todos sus aspectos, ofensivos, defensivos y de reconocimiento electrónico de sistemas, sin embargo, las intencionalidades de actores y su prospectiva en conjunción con el resto de disciplinas de inteligencia reside en los órganos del sistema de inteligencia, si son amenazas de entes designados como tales al más alto nivel: el JEMAD.

Por otro lado, la guerra electrónica (EW, por sus siglas en inglés) en cuanto a actividad de inteligencia SIGINT en sus dos subdivisiones tiene una responsabilidad máxima en los órganos de inteligencia nacionales en los diversos niveles con la cúspide en el CIFAS, pero la parte de acción ofensiva y defensiva de contramedidas, etc. depende de los mandos operativos en sí y de las unidades de EW con sus vehículos, drones y antenas especializadas que necesitarán mayores procesos de IA para su protección automática ya sea de ataques cíber, medidas o contramedidas electrónicas como chafs, etc. contra misiles o ataques de armas contra radiación. También cambiando las señales de perturbación adaptados a las amenazas de manera automatizada con IA.

La sucesiva presencia de la IA junto con sistemas de análisis de redes y grafos, entidades, acciones, etc. supone el descubrimiento e interconexión efectiva de masivas cantidades de datos, trazas electromagnéticas características, números de teléfono, repetidores, etc.

[43] MCCD. Mando Conjunto de Cíber Defensa.

5.2.5. ACINT. Inteligencia acústica

Es aquella que describe la inteligencia obtenida de señales acústicas emitidas, siendo siempre asociada al movimiento. Para el uso de esta disciplina de obtención hacen falta; grandes avances tecnológicos, como puede ser el sonar de última generación; sofisticados algoritmos de IA para el procesamiento y análisis de las señales adquiridas, la actualización de las BBDD correspondientes con la clasificación pertinente de lo encontrado; y, por último, una alta cualificación y entrenamiento de los operadores acústicos.

5.2.6. MASINT. Inteligencia de medidas y firmas

Es aquella derivada de análisis técnico de la información obtenida por instrumentos de detección y que finalmente asociaran a diversas fuentes emisoras. Toda la inteligencia obtenida se refiere a comparaciones con las dispuestas en una BBDD con información técnica conocida.

5.3. Elaboración

De manera general, el aprendizaje supervisado de ML, con sus algoritmos de regresión, produciendo valores medibles numéricos, y de clasificación, en los que se consiguen etiquetas dentro de un conjunto finito de posibles resultados, se pueden elegir alternativas cuando estén definidas; así, las incertidumbres puedan ser valoradas y cuantificadas. Además, se pueden hacer predicciones cuando se conocen las probabilidades de los efectos, dadas las causas, o al contario, conocer la probabilidad de las causas dados los efectos (algoritmos basados en la teoría de Bayes), simulando condiciones de incertidumbre y contrafactuales cuando no se sabe si la hipótesis enunciada es verdadera o falsa.

De otro lado, en la fase de elaboración, y en todos sus subprocesos, es donde tienen cabida los algoritmos de agrupación y de reducción de dimensionalidad del aprendizaje no supervisado de ML, enfrentándose al caos y encontrando patrones en grandes BBDD con todo tipo de información.

En esta fase, la información obtenida es transformada en inteligencia con los subprocesos siguientes que, con las nuevas tecnologías, no suponen que hayan de ser secuenciales necesariamente:

5.3.1. Compilación

De la información obtenida. Si cuando hablábamos de OSINT ya considerábamos la IA como solución para la «infosicación», la intoxicación provocada al producir y adquirir más datos de los que éramos capaces de asimilar, en esta etapa replicamos las soluciones habladas y con el uso de IA, agregamos toda la información necesaria referente a un evento, persona, lugar, investigación u objeto, en el sentido informático del término, que pueda dar sentido global e integrador de lo percibido en la realidad por nuestros sensores varios.

5.3.2. Evaluación

De la información y sus fuentes. Esta etapa cada vez más se realiza por cada disciplina de obtención si tiene entidad y capacidades para la misma, y forma parte del primer análisis de disciplina única por los especialistas y técnicos que están en contacto directo con la realidad. Aquí la toma en consideración de evaluaciones anteriores de las fuentes, pueden ser objeto de investigación dedicada para el resto de disciplinas, como pueda ser, por ejemplo, la categorización de una fuente HUMINT, reuniendo información por SIGINT y OSINT para verificar su veracidad, valía de las informaciones a las que tiene acceso, carácter personal o fracturas de seguridad de la misma como agente infiltrado o doble. Para todo ello el contar con extensos datos bien categorizados de las diversas fuentes, gracias a IA con técnicas de refuerzo profundo puede comprobar la veracidad a lo largo del tiempo de las informaciones recibidas. Así, de nuevo estamos hablando de un *big data* y la gestión del mismo para esta finalidad. Las informaciones sacadas de nuestras bases de datos dan la ventaja competitiva y la importancia de mimar la inteligencia básica de la organización.

5.3.3. Análisis de la información

En todas las fases del ciclo de inteligencia tenemos analistas en sus diversas funciones y grados de especialización, pero en esta parte del ciclo es donde se requieren capacidades analíticas más refinadas. El trabajo del analista consiste en encontrar las relaciones causa y efecto entre diferentes hechos, circunstancias, actores y situaciones, todo ello para tener un conocimiento de la situación y poder realizar sus predicciones a futuro (Heuer, 1999). Y en todos los procesos en los que intervienen humanos,

con su experiencia anterior, se producen errores motivados por estrategias simplificadas utilizadas por la mente de las personas para el procesamiento de información a los que se les denomina sesgos cognitivos (Heuer, 1999).

Podíamos hablar hace pocos años, cuando la palabra de moda en estos tipos de tecnología era el *big data*, que los procesos de inteligencia raramente incorporaban la IA a los razonamientos y procesos de análisis estructurado que desde la guerra de Iraq se han generalizado en los servicios de inteligencia.

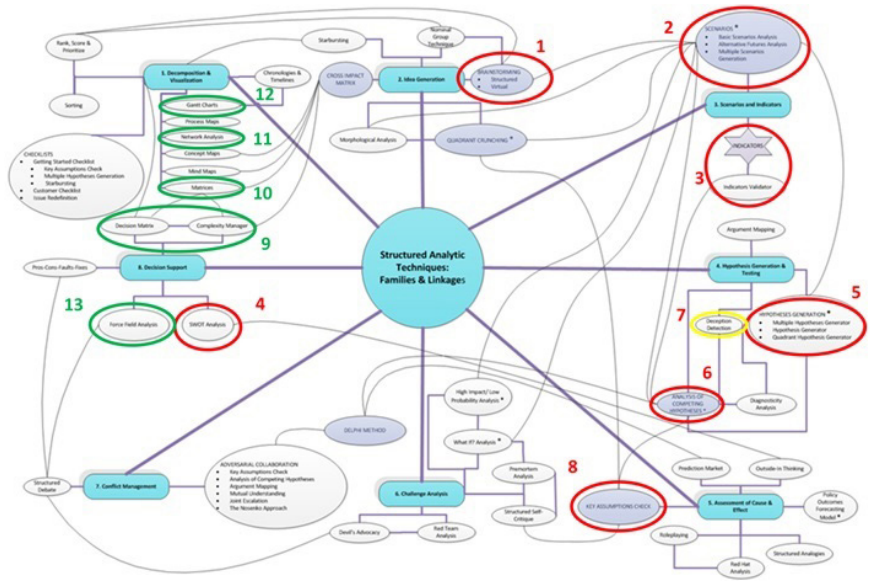
Estas técnicas estructuradas permiten la reducción de sesgos y la implantación de procesos de pensamiento y análisis científicos modulares y perfeccionables por equipos de analistas, utilizando las capacidades racionales y lógicas, su conocimiento de la realidad como expertos de un área, actividad o actor. Todo ese análisis estructurado da un valor añadido tendente a hacer una prospectiva, como producto final.

La irrupción de la estadística como campo en las ciencias sociales y políticas ha sido clave para trasladar el razonamiento científico y matemático a esferas colonizadas anteriormente por la intuición: ese olfato que daba la experiencia de esos asesores de inteligencia especializados.

El uso de la IA está posibilitando ir un punto más allá de las técnicas puramente estadísticas y gracias al M/DL poder sacar provecho de grandes cantidades de datos existentes o adquiribles por la sensorización del mundo y del campo de batalla para utilizar los set de datos en el entrenamiento de algoritmos de predicción, de inferencia que ayuden a los analistas y luego a los asesores a discernir las posibilidades de futuro y, por tanto, poder adelantar acciones correctoras al mismo mediante tareas ejecutivas en la organización. La IA no reemplaza a los analistas humanos, sino que ya los está empoderando.

Si tenemos en cuenta las técnicas de análisis estructurado podríamos dividir las que son más de razonamiento directo humano, que simplistamente podríamos catalogar de «analógicas», de las que permiten una digitalización y automatización mediante IA que potencia los resultados limitando el tiempo de análisis y mejorando la capacidad de asimilación de datos y variables en los procesos. Recordemos que uno de los inconvenientes de las técnicas de análisis estructurado es el tiempo necesario, su carácter predominante cualitativo frente al cuantitativo, ideal para medir con precisión los parámetros.

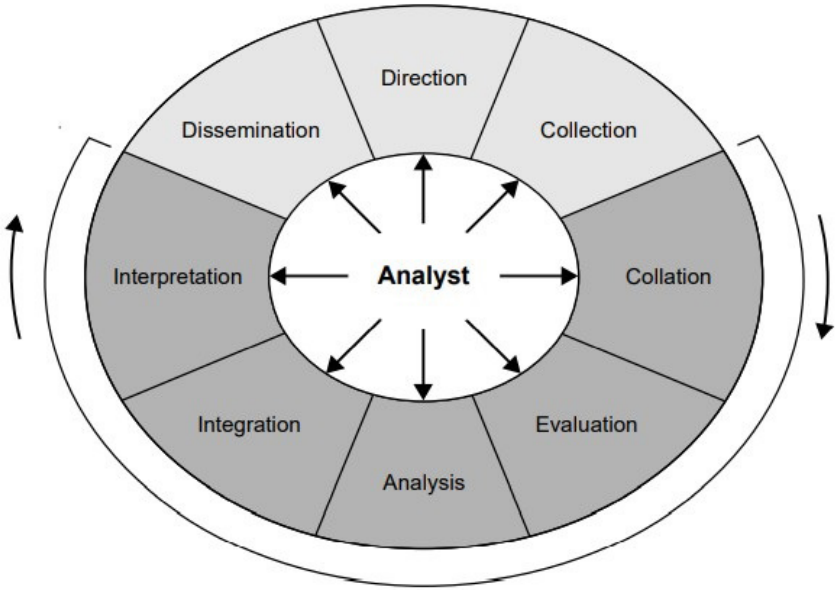
En el siguiente cuadro señalamos cuáles de las técnicas de la recopilación de técnicas de análisis estructurado (Heuer y Pearson, 2015) son más factibles de poder adaptarse a procesos con IA en contraposición a las técnicas más «analógicas» humanas, si bien todas las técnicas, de una manera u otra, podrían ser ayudadas con IA.



Técnicas de análisis estructurado factibles de automatizar con IA en verde y menos en rojo (Heuer y Pearson, 2015)

La incorporación de la IA en los procesos de análisis, y en sus subfases en los lugares adecuados, pueden ayudar a reducir esos sesgos cognitivos, ya que los procesos matemáticos y estadísticos informados en tiempo real por procesos de DSS e IA tienen la objetividad y prontitud de reducir la incertidumbre y presentar la realidad de una manera uniformada y similar en todas las ocasiones, o modificada para evitar errores anteriores de apreciación, evaluación o sesgo. En este campo los LLM modernos y los sistemas con algoritmos entrenados de manera autónoma o supervisada por humanos expertos en esas evaluaciones, son los de mayor avance, desarrollo y aplicación.

Existe un punto de inflexión en la historia de la inteligencia como actividad que fue la guerra del Golfo y los fallos achacados a la inteligencia en la justificación de la guerra sobre la existencia de armas de destrucción masiva, sin entrar en si fueran fallos



Fase de elaboración (DCDC, 2011)

reales en sí o manipulaciones para seguir un procedimiento[44] en la democracia americana de tergiversación o manipulación de sociedades democráticas para adherirse a medidas necesarias para una élite política, pero impopulares hasta ese momento, como era empezar una guerra.

Si bien en servicios de inteligencia tan dimensionados como el americano, no era nueva la aproximación a las ciencias sociales y a la aplicación de la ciencia para la resolución de problemas de prospectiva de inteligencia, sí fue el detonante para que a nivel mundial se abrazaran las técnicas de análisis estructurado como caja de herramientas a disposición de los analistas para justificar y modularizar sus análisis de modo lógico y secuencial para que la intervención de los decisores ya no dejase de atribuirse solo los logros exonerándose de los fracasos en una falta o fallo de inteligencia, un clásico.

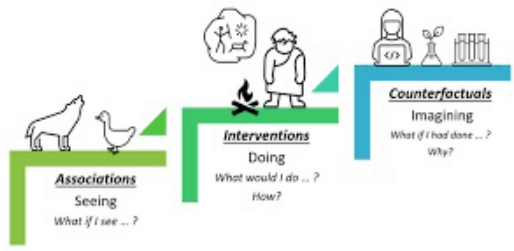
Así, esa modularidad permitía presentar las decisiones como un proceso en el que si el decisor, normalmente de especialidad de

[44] Hechos contrastados de ese tipo fueron la explosión fortuita o interesada del Maine que comenzó la campaña de prensa antiespañola y justificó la guerra de Cuba de 1898, o el análisis pretendidamente erróneo y ocultación de indicios e informes que alertaban de un ataque japonés a Pearl Harbour que justificaron y cambiaron el sentimiento popular americano para la entrada en la II Guerra Mundial.

operaciones o Estado Mayor, sin entender el porqué del análisis final se le exponían los pasos intermedios y la metodología científica empleada, si no estaba de acuerdo podía modificar y bajar al detalle de qué parte del proceso veía errónea, para rehacerla, insertarla de nuevo en el proceso general y dar un resultado analítico final, muchas veces igual al inicial, pero que ya daba confianza al decisor por su intervención directa.

Evidentemente en estos procesos modulares y técnicas diferenciadas, la aplicación de la IA es más que factible y con el paso de los años y el desarrollo de campos más ambiciosos de la IA, entre los que está la IA generativa y los modelos de LLM[45] que hacen obsoleto al cuadro de identificación de técnicas factibles de mecanizar (en verde) del imprescindible libro recopilatorio de Heuer y McPherson, en cuanto a técnicas eminentemente cualitativas y analógicas de intervención de expertos, equipos de trabajo multidisciplinar, mentes blancas, etc. de las que son factibles de transformar en cuantitativas y, por tanto, modelizables con algoritmia e intervención dinámica de la IA, con ciclos de análisis y reevaluación de parámetros más necesarios en tiempo próximo al real.

Por tanto, la incorporación de la IA a las técnicas de análisis, entre las que los profesionales de la inteligencia prefieren en gran medida las estructuradas, con la irrupción de las técnicas de análisis de la ciencia sociológica, política y estadística avanzada con ciencia de datos que va a revolucionar en muchas facetas la disciplina por cuanto reducirá los plazos de planeamiento, el esfuerzo y tiempo dedicado a análisis puntuales de materias, efectos, decisiones, escenarios prospectivos. Los análisis de amplio espectro de ambición estratégica pueden tener aprovechamiento, ya no operacional, sino táctico, en cuanto que la actualización de los mismos va a la par del ritmo y tempo de las operaciones a nivel táctico, más inmediato.



Representación de la escalera causal (Pearl y Mackenzie, 2018)

[45] LLM, *Large Lenguage Models.*

Punto que necesitaría un artículo aparte es la incorporación al mundo de la inteligencia de la llamada «revolución causal» (Pearl, 1981). La incorporación conceptual de la escalera causal a los niveles de interiorización y conocimiento profundo de la materia, lugar, personaje o circunstancia objeto de un análisis es para algunos profesionales de la inteligencia de muy correcta y necesaria implantación. Brevemente diríamos que esa escalera establece los límites en los que la mente humana establece el conocimiento de cualquier materia, siempre basado en procesos de causa y efecto, de experimentación y retroalimentación.

Primero tendríamos el primer escalón básico que Pearl llama de asociación (Pearl, 2009), en el que, mediante la observación de la realidad, con nuestros sensores intentamos hacernos una idea los más correcta posible de la realidad. Son hechos, eventos y evidencias que reuniríamos en nuestros mapas de situación, SITMAP, perfeccionando la alerta situacional del término *Situational Awareness* [46] y que la IA está revolucionando con la posibilidad de visualizar en una única pantalla los diversos sensores, cómo y dónde está el enemigo y las tropas propias, qué hacen… y somos capaces de ver lo que ocurre si uno de nuestros sensores localiza un fogonazo en una posición por un tipo de arma que impacta a los pocos segundos en otra localización y con un efecto, por ejemplo una batería artillera enemiga.

En definitiva, somos capaces de establecer variables y ver cómo se relacionan. En este peldaño se necesitan predicciones que se basan en observaciones pasivas (Pearl y Mackenzie, 2018), y cuya base matemática y estadística es la probabilidad condicional, la correlación y regresión para asociar efectos, variables y actores. Aquí necesitamos datos, cuantos más mejor, y, por tanto, la gestión de los mismos requiere la intervención de la IA, en definitiva.

En el segundo escalón causal, de intervención, hacemos una experimentación que demuestra cómo se comporta la realidad, resolvemos y somos capaces de conocer los procesos que dan lugar a ciertos resultados y, por tanto, seríamos capaces de diseccionar el conjunto de soluciones posibles y con metodología bayesiana podemos inferir qué efecto produciría en otro blanco si el disparo realizado por esa pieza de artillería, que hemos

[46] *Situational Awareness.* Conciencia situacional, término extendido en OTAN para denominar el conocimiento de la realidad que incluiríamos en nuestro concepto de inteligencia actual.

previamente visualizado en el primer escalón, le impactara. En este nivel no nos conformamos con ver, sino que modificamos lo que existe, alteramos el entorno. Aquí entran operadores estadísticos modernos como el *do* para probabilidades (P(destrucción de mi unidad | do (batería enemiga dispara)) que se adaptan a este tipo de condicionantes.

Por último, tenemos el tercer escalón causal, el de aplicación de contrafactuales, en el que utilizamos la capacidad humana única de imaginar, de comprender profundamente los procesos y somos capaces de enlazar los mismos para darnos cuenta de que la clave para minimizar el impacto de esa batería de artillería de nuestro ejemplo, ya que nos preguntamos ¿y si la batería no hubiera recibido información de cálculo de tiro o situación de nuestra posición?, ¿y si la información es errónea porque le damos un señuelo a los sensores del enemigo?, ¿qué pasaría si el camión o la cadena logística no le da los proyectiles que necesita a esa batería?, ¿y si el camino de acceso a la posición artillera se bloquea por unas minas lanzadas, qué ocurriría? Como vemos, integramos muchos tipos de conocimiento, además del balístico, para comprender profundamente las capacidades e incluso intencionalidades del problema, en este caso del enemigo. Aquí entran las matemáticas y una vez que entran estas, el paso a la algoritmia computacional es inmediato.

Los tres escalones causales son inteligencia pero la verdaderamente prospectiva, anticipatoria y eficaz implica un conocimiento de los contrafactuales que nos permiten establecer escenarios futuribles con base en indicios y KPI[47] comunes en el mundo de la inteligencia de negocios, BI, el *big data*, la toma de decisiones automatizada o ayudada por algoritmia, los paneles de mando interactivos informados, la utilización de *data warehouse* dedicados a una determinada temática, y, en definitiva, el empleo masivo de la IA.

5.3.4. Integración de la información

La utilización de las posibilidades que nos da el análisis de redes, el *link analysis*, y la utilización de las matemáticas matriciales y la teoría de grafos han permitido expandir la IA a campos en los que la integración de la información está disponible en diversas bases de datos, estructuradas o no. La utilización de

[47] KPI. *Key Performance Indicators*

herramientas o robots de búsqueda de conexiones de manera autónoma, buceando en nuestro *data lake*[48] también ha superado los límites de nuestros procesos de integración de información y aprovechamiento de la misma.

Ese *data lake*, en su terminología inglesa más aceptada, se refiere a la base de datos general en la que todos los datos y metadatos se encuentran disponibles para esos robots, esos algoritmos de IA que buscan lo que nosotros les digamos de una manera más eficiente, rápida y con menos errores, ya que permiten autónomamente recatalogar, renombrar, reorganizar la información a formatos entendibles por el metabuscador, siendo capaces de reducir drásticamente ese 70 % de tiempo que el científico de datos empleaba hasta ahora en la organización, reparación y preparo de los datos, de manera manual antes de aplicarles ciencia de datos, *Machine o Deep learning*, según la finalidad que buscase, tomemos por caso. La gestión de las diversas bases de datos y cubos OLAP/ROLAP son de las más solventes para la aplicación de las nuevas tecnologías (Jiménez, 2023; JFD, 2017; Gómez, 2021).

Volvamos a la importancia del análisis de redes sociales y la expansión de las herramientas iniciales en servicio de los analistas de inteligencia que buscaban entender, estructurar, visualizarlas de una manera coherente para con los principios de las matemáticas de grafos buscar la topofrafía, la cohesión y agrupamiento (*clustering*), los vínculos entre los nodos, su poder, centralidad y otros tantos conceptos que empezaron a analizarse con programas como UCINET, Netdraw, Pajek y ORA (Everton, 2012)[49], y, por supuesto, el *software* tan extendido entre servicios de policía, inteligencia y OTAN, casi estándar podríamos decir: Analyst Notebook, ANB, de i2 que ahora se han diversificado a librerías de IA en lenguaje javascript, R o Python, códigos democratizados en el mundo del *Open Source*, como expusimos en el apartado de OSINT.

Con la eclosión de la IA, las capacidades para extraer entidades, nexos, pesos de los mismos, acciones, sentimientos… posibilita la transformación automatizada masiva de informes al formato CSV y ANB, que en Afganistán necesitaba naves enteras de analistas junior 24/7, extrayendo y preparando esos grafos y tablas, que una vez relacionados por el programa posibilitaba a los analistas

48 *Data Lake*. Lago de datos.

49 ORA. *Organizational Risk Analyzer.*

de alto nivel hacerse una imagen espacial de las redes y sus interconexiones.

Es nuclear contar con sistemas informáticos que sean capaces de extraer datos de diversos tipos de bases de datos, materia en la que fueron pioneros la empresa americana de Palo Alto, Palantir, que desde hace tiempo buscó mecanizar el acceso a esas bases de datos que no se hablaban aunque físicamente tuvieran oficiales de enlace cada uno con su sistema en los centros de fusión de inteligencia, las *Intelligence Fusion Center*, que el general McCrystal plantó en Bagdad cuando el Surge del 2007, y que para muchos de nosotros fue una nueva revolución en la inteligencia y en la manera en la que se integraba la misma para aumentar el tempo y ritmo en las operaciones especiales para ser capaces de ganar colapsando a una guerrilla insurgente con el uso intensivo de nuevas aproximaciones y usos conjuntos e integrados de la inteligencia.

5.3.5. Interpretación

Esta puede que sea la subfase más humana e implica una experiencia, y, por qué no decirlo, arte, olfato de analista, para ver e intuir lo que no es a veces tan aparente, eso sí ayudado por las técnicas y el conocimiento científico que hay detrás de tantos procesos como los descritos.

5.4. Difusión

La entrega oportuna de los productos de inteligencia por los medios adecuados a los clientes que la requirieron o le pueda interesar. El factor tiempo es fundamental y la clasificación de seguridad adecuada. Muchas veces los productos son repetitivos y estandarizados, lo que permite la mecanización y el relleno de formatos, con la presentación de productos anteriores para dar un contexto y una sugerencia por IA de los eventos o puntos a incluir en informes descriptivos, por ejemplo.

La integración de los productos de inteligencia con los sistemas DSS será en las células de fusión de inteligencia, IFC, que preparan, dirigen y recopilan todas las misiones informativas y de elaboración conformadas en el ciclo de inteligencia para, posteriormente, integrarlas con el ciclo de operaciones y sus centros de operaciones conjuntos, JOC, donde, mediante sistemas informáticos, se pueden seguir y coordinar en los COP, *Common Operational Picture,* esos SITMAP enriquecidos, suministrando

acceso rápido a imágenes e inteligencia (JFD, 2017), donde se fusionan también los sistemas de alerta temprana, conocimiento de la situación de inteligencia (SA), con mapas de la situación para dar sentido al conjunto.

Todo ello, que es un EIS, se puede potenciar con IA para relacionar variables e indicadores, sean críticos o no, con procesos solo visibles bajo parámetros fijados por los usuarios, pero que detrás realizan multitud de procesos de manera automatizada y en tiempo real (Jiménez, 2021; DCDC, 2011).

6. Contrainteligencia y seguridad

En la OTAN está extendida la nomenclatura de J2X para unificar estas labores de inteligencia que tienen los mismos procedimientos y herramientas ya relatados, pero que tienen su foco mirando hacia el interior de nuestros países y organizaciones, en evitar las fugas de información hacia servicios externos, sean potencialmente hostiles o amigos, porque en la búsqueda de información todos buscamos de todo y de todos (Herraiz, 2023).

La interrelación de ciertos departamentos de seguridad para proteger la seguridad física de instalaciones, personas, documentación, etc. se complementa con la propiamente cíber de los sistemas informáticos, comprobando y certificando sistemas de seguridad y anti intrusión. No cabe duda de que la aplicación de sistemas de IA para la comprobación rutinaria de claves, vulneraciones de seguridad y automatización en las respuestas ya protocoladas, dará supervivencia y mantendrá nuestros secretos y datos a buen recaudo de espías externos.

Un campo que se toca con todas las relaciones forenses y de gran aplicación de los avances de IA, es todo lo que implica la subdisciplina de la inteligencia de personalidades e identidades, la *Identity Intelligence*, que ya explicamos anteriormente y que tiene grandes aplicaciones para la contra inteligencia y la seguridad. Solo subrayar un hecho, es en J2X donde existe un mayor nexo con otros servicios de inteligencia civiles y policiales con organismos internacionales como Interpol y Europol para la compartición de información y en donde la información biométrica, por ejemplo, no está clasificada y permite el intercambio ágil de esos datos técnicos, «ceros y unos», en los que se representan a las personnas; sin intervención ni ralentización judicial ni vulneración de derechos fundamentales.

7. Conclusiones

Empezamos este capítulo con el relato de una operación especial exponiendo la exorbitante cantidad de inteligencia que se maneja para el desarrollo y ejecución de ese ejemplo de misión y sus derivadas. Para terminar con las conclusiones, pongamos en esas unidades de operaciones especiales el devenir que se nos presenta de manera inquietante, en conflictos de alta intensidad dentro de la «competición estratégica entre grandes poderes por el dominio mundial» en la que nos vemos ya inmersos.

- PRIMERA. Cambio de paradigma para ampliar el foco de las amenazas a afrontar de las organizaciones no estatales insurgentes/terroristas a adversarios convencionales con estructura, medios y orden de batalla, doctrina y reglas de enfrentamiento de un Estado; esto es: una fuerza militar reconocible.
  Todo ello implica cambiar el tipo y metodología del sistema de *targeting*, obtención de inteligencia, reporte y asesoramiento a los decisores. La intensidad y ritmo de todos los procesos será la clave del éxito en todos los dominios. La IA permitirá automatizar procesos para acortar los ciclos de decisión, inteligencia y planeamiento respecto al competidor (Brown, 2022).
  Mantenemos la idea de ampliar el foco en tanto que no han desaparecido aquellas organizaciones insurgentes islamistas, u otras nuevas pueden continuar o aprovecharse como *proxies* de potencias Estado. En nuestro caso tendremos que operar en esa Zona Gris (Nieto, 2021), promoviendo resistencias armadas aliadas o como contrainsurgencias en nuestro terreno y todas ellas necesitarán fuerzas de inteligencia y operaciones especiales, entre otras, que sean capaces de operar en la zona gris.
  Allí, la superioridad de la información y comprensión de lo que implica la competición estratégica será facilitada por la IA en todos los aspectos: político, militar, económicos, social, de información y de infraestructura (PMESII), junto al diplomático, cultural y legal que necesita el acceso al máximo de conocimiento profundo de la realidad por los niveles más bajos tácticos: ese cabo estratégico (Krulak, 1999) o los guerreros autónomos del futuro (Toffler, 1991) como silogismo de los soldados de operaciones especiales e inteligencia con capacitación equivalente a la de diplomáticos con grados en economía, política, *marketing*/propaganda, psicología, sociología, medicina… y letales soldados; capaces de resolver situaciones al máximo nivel sin instrucciones.

- SEGUNDA. Lucha por todos los dominios: cognitivo, moral, físicos (tierra, mar, aire/espacial). La lucha por la narrativa y la legitimidad, así como la competición en la zona gris, será facilitada por la masiva irrupción de la IA en la coordinación de las acciones multidominio. Especial importancia por su desarrollo con las nuevas tecnologías es el cognitivo, con el impacto de las redes sociales y los enlaces e información residentes en la Deep y Dark web y la utilización de técnicas de ingeniería social ofensivas y defensivas para influir en las percepciones, sentimientos y actitudes de la población y entes políticos, mediante operaciones psicológicas y de información para modificar la moral, fundamental para la victoria. El empleo creciente de la IA para analizar el entorno de la información mediante OSINT será fundamental para prevalecer y adelantar escenarios de inteligencia para el posterior empleo defensivo/ofensivo que asegure los dominios cognitivo y de moral con la utilización de campañas, creación y manipulación de noticias, desinformación con las las fake news, deep fakes, si necesario para controlar finalmente los dominios cíber y físicos (tierra, mar, aire).
- TERCERA. Interconexión de sistemas y digitalización de manera automatizada con IA. Tecnología que pueda adquirir y fusionar información de esos sistemas en cualquier dominio[50] (Kyle, 2019) y nivel de conducción (estratégica, operacional o táctica) con acceso a sensores[51] para asegurar la aplicación de la medida, letal o no letal, más apropiada, una vez se ha seguido, identificado y adquirido el posible blanco. Como corolario, la hiper sensorización, informatización y análisis con IA de todos los entornos, principalmente urbanos, hace más complicadas la infiltración de agentes, y requieren de capacidades adicionales cíber para ser capaces de engañar o enmascarar perfiles y firmas físicas a esos sensores o sistemas, utilizando sistemas alternativos como OSINT e IMINT.
- CUARTA. Mayor letalidad por el uso de armas inteligentes y autónomas, cada vez más robotizadas y sin decisión final humana a la hora de la elección de misiones o blancos con ayuda de IA, con efectos letales o no. La guerra sin contacto directo[52] (Brown, 2022) en los diversos niveles desde drones a misiles hipersónicos, sistemas de armas integradas, que

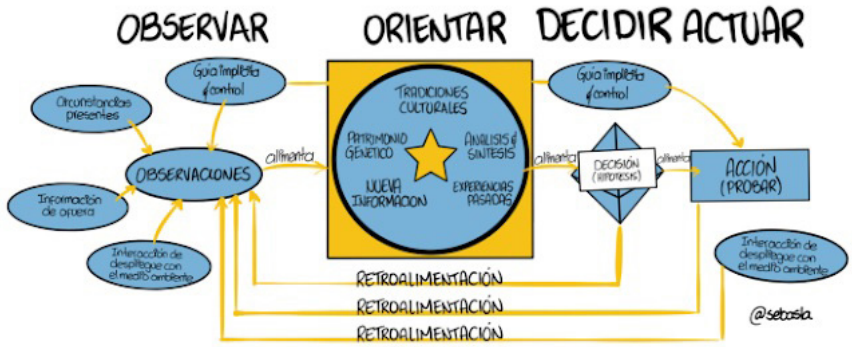
[50] *Joint All Domain Operations,* JADO.

[51] Concepto de *Internet of things* aplicado a las nubes de comunicación tácticas en zonas de operaciones donde se proyectan acciones militares de inteligencia.

[52] Concepto de *Contactless war.*

componen la adquisición y análisis autónomo con sensores de información útil para su operación en tiempo real, con cada vez menos necesidad de intervención humana desde su base por la intervención de IA en las diversas fases.

– QUINTA. Incremento de la velocidad y el tempo en las operaciones y crisis con la intervención de la IA en todo el proceso de orientación y toma de decisiones «OODA loop» (Boyd, 1987) en el que básicamente realizamos análisis causales encadenados en los que observamos, orientamos, decidimos y actuamos/ejecutamos y en los que los dos primeros son eminentemente responsabilidad del ciclo de inteligencia.



El OODA loop de Boyd. Observación, orientación, decisión y ejecución. Del original The Essence of Winning and Losing. Fuente: foto Sebasla Blog

La IA supondrá llevar al extremo la guerra de mando y control para colapsar la correspondiente capacidad del adversario. Si a esto unimos las hiperbólicas capacidades que darán los computadores y tecnologías cuánticas a lo que ahora conocemos, podemos inferir que la proyección a futuro de la aplicación automatizada de IA no ha de tener límites técnicos, sino éticos.

Fuel	Analytic Type	Observe	Orient	Decide	Act
Data Assets/Sensor Data ->	Descriptive - What happened?	X			
	Diagnostic - Why did it happen?	X	X		
	Predictive - What will happen?	X	X		
	Prescriptive - What should I do?	X	X	X	
	AI - Automation	X	X	X	X

Influencia del análisis de datos con IA en el ciclo de decisión OODA y su impacto causal

– SEXTA. Opinamos que no hay que tener miedo de la transformación que va a suponer IA en todos los ámbitos de la sociedad, también en el militar, pues permitirá un salto tecnológico y de capacidades que es difícil de valorar. Algunos analistas sostienen que el salto será equiparable a la invención de la rueda en la antigüedad, y sabemos qué pasó con las civilizaciones que no la aprovecharon.
  La híper regulación de la UE en muchos ámbitos, entre los que se encuentra la referente a la IA, puede constreñir la capacidad europea y occidental en la competición mundial por el desarrollo y aplicación de la IA, por loable que sea esta primera iniciativa de regulación en el mundo; algunas prácticas y usos de la IA estarán totalmente prohibidos, como la manipulación cognitiva conductual y el uso de sistemas de reconocimiento facial indiscriminado (Política Exterior 1358, 2024).
  El reglamento no se aplicará a ámbitos fuera del de aplicación del Derecho de la UE y no afectará a las competencias de los Estados miembros en materia de seguridad nacional. Tampoco se aplicará a los sistemas utilizados exclusivamente con fines militares o de Defensa, entre los que están las actividades de inteligencia; así como a los empleados con fines de investigación e innovación (Representación en España de la Comisión Europea, artículo 25/1/2024).
  Otros factores que habrá que evaluar son los que suponen la intervención humana en procesos de IA: *human OUT of the loop*, de autonomía total; *human ON the loop*, capacidad del operador de monitorizar y parar procesos; y *human IN the loop,* con control completo del operador humano. Para las labores de inteligencia, el riesgo de fatalidades es menor por ser labores no letales, y, por tanto, permiten el primer tipo, de máximo de desarrollo de la IA autónomamente.
– SEPTIMA. La IA tendrá un impacto significativo en los interfaces hombre-máquina y en el análisis de big data para aumentar la alerta situacional[53], reduciendo la carga cognitiva y aumentando los procesos de toma de decisiones asistidos a todos los niveles. Un buen ejemplo es el concepto Hyper-Enabled Operator (HEO), desarrollado por el USSOCOM[54], como un sistema innovador electrónico en el que se incluyen sensores, procesadores, realidad aumentada y enlace todo tiempo en la nube y con las bases donde radicarán las capacidades de cóm-

[53] *Situational Awareness,* SA*,* término de uso extendido en la jerga de OTAN.
[54] USSOCOM. Mando Conjunto de Operaciones Especiales de EE. UU.

puto y bases de datos para el procesamiento computerizado distribuido (MacCalman et al., 2019).

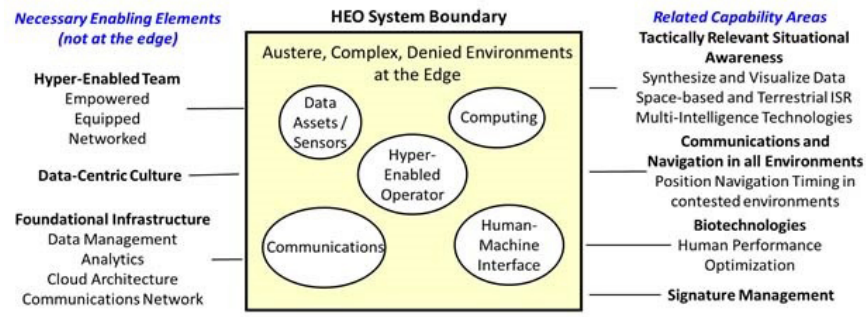


Diagrama del sistema de operadores hipercapaces (Hyper-Enabled Operators, HEO)

Su objetivo será proveer de la correcta información a cada combatiente, analista y decisor de manera oportuna sin saturarlo, enlazando todos los niveles de aprovechamiento (táctico a estratégico) de la inteligencia que es única para que cada eslabón humano realice las actividades con valor añadido y creativo que le son propias y diferenciadoras con la IA que le ayuda en el resto.

– OCTAVA. De forma global, la aplicación de la IA al ciclo de inteligencia posibilita mejores resultados.
  Tanto la IA por síntesis, que procesa grandes cantidades de datos para extraer información, como la IA lógica inductiva, que busca patrones en la información extraída, produciendo inteligencia dentro de los sistemas de apoyo de una forma concreta, benefician a los órganos decisores que utilizan el ciclo de inteligencia complejo. La intervención temprana de la IA en todas las fases permite el procesamiento acelerado para permitir su difusión inmediata.

Bibliografía

Abellanas, M. y Lodares, D. (1990). *Análisis de Algoritmos y Teoría de Grafos.* Ra-Ma.

Aranda Vasserot, A. (2023). *Las 36 estratagemas chinas. Manual Secreto del Arte de la Guerra*. Ariel.

Arévalo, A. (2018). *Inteligencia artificial, prioridad en la estrategia de defensa de EE. UU.* [Consulta: 2024]. Disponible en:_ http://hdl.handle.net/10654/21066.

Army Pubs. (2023). ATP 3-60 – Targeting, enlace doctrinal de EE. UU. En su versión para fuerzas terrestres. [Consulta: 5 de febrero de 2024]. Disponible en: https://www.armypubs.org/atp-3-60-targeting/.

Borne, K. D. (2019). Targeting in Multidomain Operations*. Military Review*. [Consulta: 5 de febrero de 2024]. Disponible en: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/Borne-Targeting-Multi-domain/.

Boussad, A., Kodjabachian, J. y Meyer, C. (s.f.). *CIA evasion attacks transferability between machine learning models.* [Consulta: 5 de febrero de 2024]. Disponible en:_ https://www.cesar-conference.org/wp-content/uploads/2018/11/articles/C&ESAR_2018_J1-08_B-ADDAD_CIA_evasion_attacks_transferability_between_ML_models.pdf

Boyd, J. R. (1995). La guerra de mando y control y la teoría del OODA Loop. *Dialnet.* [Consulta: 2024]. Disponible en:_ https://dialnet.unirioja.es>descarga>articulo https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiX-Ozw8bmEAxU1gv0HHbA0DiQQFnoECDIQAQ&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F4604097.pdf&usg=AOvVaw2z_dQaNnMqiwSTcu8tOkyg&opi=89978449.

Bringas, A. (2019). The Influence of Big Data in the Intelligence Cycle. *The Security Distillery.* [Consulta: 2024]. Disponible en:_ https://thesecuritydistillery.org/all-articles/the-influence-of-big-data-in-the-intelligence-cycle.

Brown, A. L. (ed.) *et al*. (2022). *A Perilous Future: High-Intensity Conflict and the Implications for SOF. Special Operations Forces and Great Power Competition.* CANSOFCOM Education&Research Centre. Canadian Special Forces Command. [Consulta: 2024]. Disponible en: https://jsou.edu/Press/PublicationDashboard/218.

Burcher, M. y Whelan, C. (2018). Intelligence-Led Policing in Practice: Reflections From Intelligence Analysts. *Police Quarterly*. Vol. 22. [Consulta: 4 de febrero de 2024]. Disponible en: https://www.researchgate.net/publication/327294043_Intelligence-Led_Policing_in_Practice_Reflections_From_Intelligence_Analysts. DOI: 10.1177/1098611118796890.

Clarín. (2020). EE. UU. acusó a cuatro militares chinos por el robo de datos de 145 millones de personas. [Consulta: 5 de

febrero de 2024]. Disponible en: https://www.clarin.com/mundo/ee-uu-acuso-militares-chinos-robo-datos-145-millones-personas_0_xjx5F8J7.html.

De la Fuente Chacón, J. C. *et al.* (2022). *Sistemas autónomos y robótica inteligente en Defensa*. Academia de las Ciencias y las Artes Militares. EEC.

Delgado Gamella, J. L. (2020). *Sistemas de Mando y Control y su función en la ayuda humanitaria.* GMV. [Consulta: 5 de febrero de 2024]. Disponible en:_ http://www.gmv.com/media/blog/defensa-y-seguridad/sistemas-de-mando-y-control-y-su-funcion-en-la-ayuda-humanitaria.

Dhamija, P. y Bag, S. (2020). Role of artificial intelligence in operations environment: a review and bibliometric analysis. *The TQM Journal*. ISSN: 1754-2731. [Consulta: 4 de febrero de 2024]. Disponible en: https://www.emerald.com/insight/content/doi/10.1108/TQM-10-2019-0243/full/html. DOI:10.1108/TQM-10-2019-0243.

EE. UU. Joint Targeting School Student Guide. (2017). [Consulta: 5 de febrero de 2024]. Disponible en: https://www.jcs.mil/Portals/36/Documents/Doctrine/training/jts/jts_studentguide.pdf?ver=2017-12-29-171316-067

Everton, S. F. (2012). *DIFUSIÓN disrupting Dark Networks.* Cambridge University Press.

Gómez de Ágreda, Á. *et al.* (2019). *Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R).* Vol. 04/2019.

Gómez González, Á. S. (2021). Tendencias de evolución de la inteligencia militar. *Documento de Opinión IEEE 35/2021.* [Consulta: 5 de febrero de 2024]. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO35_2021_ANGGOM_Inteligencia.pdf.

Heuer, R. J. (1999). *Psychology of Intelligence Analysis.* Central Intelligence Agency.

Heuer, R. J. y Pherson, R. H. (2015). *Técnicas analíticas estructuradas para el análisis de inteligencia*. Madrid, Plaza y Valdés, S. L.

Herraiz, P. (2023a). ¿Por qué filtraron secretos a EE. UU. los agentes del CNI? *El Mundo*. [Consulta:_ 3 de febrero de 2024]. Disponible en: https://www.elmundo.es/espana/2023/12/05/656e2433fc6c8367208b45b3.html.

Jiménez, Á. (2021). *Inteligencia Artificial y Machine Learning al servicio de la Inteligencia* [trabajo de fin de máster]. Universidad Nebrija y ESFAS.

Joint Force Development. (2017). *Joint and National Intelligence Support to Military Operations US Joint Publication 2-01.* Vol. 297.

Kilcullen, D. (2010). *Counterinsurgency*. Oxford University Press.

Knight, W. (2017). China planea utilizar la inteligencia artificial para obtener el dominio económico mundial en 2030. *MIT Technology Review.* [Consulta: 5 de febrero de 2024]. Disponible en: https://www.technologyreview.es/s/8475/china-planea-utilizar-la-inteligencia-artificial-para-obtener-el-dominio-economico-mundial-en.

Krulak, C. C. (1999). The Strategic Corporal: Leadership in the Three Block War. *Marines Magazine.* Air University. [Consulta: 23 de noviembre de 2023]. Disponible en: https://www.mca-marines.org/wp-content/uploads/1999-Jan-The-strategic-corporal-Leadership-in-the-three-block-war.pdf.

Lauroba, E. (2021). La importancia del IMINT. *Code Space*. [Consulta: 5 de febrero de 2024]. Disponible en: https://codespaceacademy.com/importancia-imint-ciberinteligencia/.

León, G. (2020). *Repercusiones estratégicas del desarrollo tecnológico. Impacto de las tecnologías emergentes en el posicionamiento estratégico de los países.* Madrid, Ministerio de Defensa.

Leonhard, G. (2023). *Revolución: el ChatGPT y su impacto similar a la invención de Internet*. [Consulta: 5 de febrero de 2024]. Disponible en: https://www.mdzol.com/mundo/2023/5/10/revolucion-el-chatgpt-su-impacto-similar-la-invencion-de-internet-336595.html.

Liang, Q. y Xiangsui, W. (1999). *Unrestricted Warfare: China's Master Plan to Destroy America*. Natraj Publishers. New Delhi.

MacCalman, A. *et al*. (2019). The Hyper-enabled Operator. *Small Wars Journal Online.* [Consulta: 5 de febrero de 2024]. Disponible en: https://smallwarsjournal.com/jrnl/art/hyper-enabled-operator.

Martínez, L. (2016). *El Ciclo de Inteligencia Complejo: una ágil herramienta para operar en red*. Instituto Español de Estudios Estratégicos, pp. 1-15.

National Defense Strategy. (2018). *Summary of the 2018 National Defense Strategy of The United States of America.*

[Consulta: 2024]. Disponible en: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Newcomb, T. (2023). Scientists Can Now Use WiFi to see Through People's Walls. *Popular Mechanics*. [Consulta: 5 de febrero de 2024]. Disponible en: https://www.popularmechanics.com/technology/security/a42575068/scientists-use-wifi-to-see-though-walls/.

Nieto, I. (2021). El papel de las Fuerzas Armadas en la zona gris. *Global Strategy Report*. N.º 41/2021. [Consulta: 5 de febrero de 2024]. Disponible en: https://global-strategy.org/el-papel-de-las-fuerzas-armadas-en-la-zona-gris/.

Parlamento Europeo. (2023). *Ley de IA de la UE: primera normativa sobre inteligencia artificial.* Temas. [Consulta: 5 de febrero de 2024]. Disponible en: https://www.europarl.europa.eu/topics/es/article/20230601STO93804/ley-de-ia-de-la-ue-primera-normativa-sobre-inteligencia-artificial.

Pearl, J. (2009). *Causality: Models, Reasoning, and Inference*. Cambridge University Press, Nueva York.

Pearl, J. y Mackenzie, D. (2018). *El libro del porqué. La nueva ciencia de la causa y el efecto*. Editorial Pasado&Presente, p. 39.

Pérez Triana, J. M. (2023). *¿Libertad para innovar en una autocracia? Duelo por la hegemonía tecnológica militar: China copia, roba y desarrolla, ¿pero podrá innovar?* [Consulta: 5 de febrero de 2024]. Disponible en: https://www.elconfidencial.com/tecnologia/2023-03-02/hegemonia-tecnologia-militar-eeuu-china-innovacion_3585169/.

Pérez González, N. y Sánchez, M. (2019). *Inteligencia Artificial: la cuarta Revolución Industrial.* [Consulta: 5 de febrero de 2024]. Disponible en: https://www.ayming.es/insights-y-noticias/noticias/inteligencia-artificial-la-cuarta-revolucion-industrial/.

Pillsbury, M. (2015). The *Hundred-Year Marathon. China's Secret Strategy to Replace America as the Global Superpower.* Henry Holt and Company. New York. Reedición con St. Martin's Griffin. 2016.

Política Exterior. (2024). Europa se abre paso en materia de IA. N.º 1358. [Consulta: 18 de febrero de 2024]. Disponible en: https://www.politicaexterior.com/articulo-completo/europa-se-abre-paso-en-materia-de-ia-342290/

Porche, I. R. *et al.* (2013). *Redefining Information Warfare Boundaries for an Army in a Wireless World*. Santa Monica, CA:

RAND Corporation. [Consulta: 5 de febrero de 2024]. Disponible en: https://www.rand.org/pubs/monographs/MG1113.html.

Rainer Granados, J. J. *et al*. (2019). *La inteligencia artificial aplicada a la defense.* Documentos de Seguridad y Defensa 79. Madrid, Ministerio de Defensa.

Representación en España de la Comisión Europea. (2024). *Las Claves de la nueva ley de Inteligencia Artificial*. Comisión Europea. Grupo independiente de expertos de alto nivel sobre Inteligencia Artificial. [Consulta: 4 de febrero de 2024]. Disponible en: https://spain.representation.ec.europa.eu/noticias-eventos/noticias-0/las-claves-de-la-nueva-ley-de-inteligencia-artificial-2024-01-25_es.

Request for information Management. (s.f.). [Consulta: 5 de febrero de 2024]. Disponible en: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiox63giZeEAxX_g_0HHZ2gDBEQFnoECBAQAQ&url=https%3A%2F%2Fresourcehub01.blob.core.windows.net%2Ftraining-files%2FTraining%2520Materials%2F042%2520PKISR%2520RTP%2F042-011%2520PKISR%2520RTP%2520Lesson%25203.4%2520RFI%2520Management.pdf&usg=AOvVaw0DO5ill-4zkGVFb0jcnBRW&opi=89978449.

Roldán, F. S. (2012). Opinión e Inteligencia. *Documento de opinión IEEE 1-4*. [Consulta: 2024]. Disponible en: http://www.ieee.es/contenido/noticias/2012/06/DIEEEO45-2012.html.

Roldán, J. M. *et al.* (2018). *La inteligencia artificial aplicada a la defensa*. Madrid.

Rosales, I. A. *et al*. (2005). *El papel de la inteligencia ante los retos de la seguridad y la defensa internacional.* Madrid, Ministerio de Defensa.

Rouhiainen, L. (2018). *Inteligencia Artificial: 101 cosas que debes saber hoy sobre nuestro futuro inteligencia artificial.* Barcelona, Editorial Planeta, S. A.

Ruiz Enebral, A. (2023). Defensa instala terminales del nuevo sistema de gestión de información clasificada [en línea]. *El Confidencial Digital.* [Consulta: 5 de febrero de 2024]. Disponible en: https://www.elconfidencialdigital.com/articulo/defensa/defensa-instala-terminales-nuevo-sistema-gestion-informacion-clasificada/20231218000000688906.html#emstrongrenovacion-tecnologica-strong-em.

Russell, S. y Norvig. P. (2004). *Inteligencia Artificial, Un enfoque moderno*. Madrid, PEARSON Prentice Hall. [Consulta: 2024].

Disponible en: Tendencias de evolución de la inteligencia militar (ieee.es).

Ruvalcaba, E. (2004). Sistemas de soporte a la decisión o DSS. *Gestiopolis*. [Consulta: 2024]. Disponible en: https://www.gestiopolis.com/sistemas-soporte-decision-dss/.

Saling, J. M. (1999). *Dynamic Re-Tasking: The JFACC and the Airborne Strike Package*. Defense Technical Information Center. [Consulta: 5 de febrero de 2024]. Disponible en: https://apps.dtic.mil/sti/citations/ADA398855.

Scott, B. y Michell, A. (2022). Enhancing Situational Understanding through Integration of Artificial Intelligence in Tactical Headquarters. *Army University Press.* [Consulta: 4 de febrero de 2024]. Disponible en: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2022/Scott/

Tariq, M. U., Poulin, M. y Abonamah, A. A. (2021). Achieving Operational Excellence Through Artificial Intelligence: Driving Forces and Barriers. *Frontiers in psychology*. Vol.º 12, p. 686624. [Consulta: 4 de febrero de 2024]. DOI: https://doi.org/10.3389/fpsyg.2021.686624. Disponible en: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8295597/.

UK Ministry of Defence (2011). *DCDC. Understanding and Intelligence Support to Joint Operations (JDP 2-00).*

Urquizu, P. (2009). ¿Qué es un DSS? [en línea]. *Business Intelligence.* [Consulta: 4 de febrero de 2024]. Disponible en: https://www.businessintelligence.info/dss/dss-apoyo-decisiones.html.

Capítulo sexto

Inteligencia económica (IE) e inteligencia artificial (IA)

Claude Revel

Resumen

La introducción de herramientas de inteligencia artificial en una disciplina tan relevante como la inteligencia económica es una evolución natural. La información y su tratamiento constituyen, en ambos casos, el punto de partida para la obtención de información útil para la toma de decisiones. El tratamiento automatizado que proporciona la inteligencia artificial permite alcanzar mayores grados de abstracción en los procesos de inteligencia económica frente a las técnicas tradicionales. Ante las ventajas de incorporar inteligencia artificial, surgen nuevos desafíos a los que será necesario hacer frente ante un nuevo campo de juego donde las buenas prácticas y la regulación, en muchos, casos, todavía no están desarrolladas.

Palabras clave

Inteligencia artificial, Inteligencia económica, Estrategia, Herramienta, Valor añadido.

Economic intelligence (EI) and artificial intelligence (AI)

Abstract

To incorporate artificial intelligence tools in a discipline as relevant as economic intelligence is a natural evolution. In both cases, information and its processing are the starting point for obtaining useful information for decision making. The automated processing provided by artificial intelligence makes it possible to reach higher levels of abstraction in economic intelligence processes compared to traditional techniques. Given the benefits of incorporating artificial intelligence, new challenges arise that must be addressed in a new environment where best practices and regulations have not yet been developed in many cases.

Keywords

Artificial intelligence, Economic intelligence, Strategy, Tool, Added value.

1. Introducción

La inteligencia económica (IE) y la inteligencia artificial (IA) tienen en común que ambas se basan en la información, más exactamente, en los datos. Ambas los utilizan como material para producir información relevante. Se basan en el análisis multidisciplinar, mientras que la IA es ante todo una herramienta. Los datos hoy deben considerarse como la principal fuente de riqueza como (eran) petróleo y gas fuentes materiales de energía fósil, aunque de forma inmaterial. La IE se basó en los datos mucho antes de que naciera la IA. Una cuestión interesante es cómo interactúan o pueden interactuar.

Inteligencia Económica es una traducción directa de *Intelligence économique*, un concepto francés que hace referencia a un doble significado del término inteligencia: es decir, la capacidad de aprehender las interrelaciones de los hechos presentados de tal manera que guíen la acción hacia un objetivo deseado (véase la definición de inteligencia en el diccionario Webster) y la información precisa y exacta recopilada por los «servicios de inteligencia (o secretos)». El término inteligencia económica tiene un alcance más amplio que los términos ingleses más próximos, *Business Intelligence* y *Competitive Intelligence*.

El objetivo común de la IE y la IA es gestionar la información para crear conocimiento y facilitar la toma de decisiones. Intentan ofrecer análisis predictivos. Pero la IE va mucho más allá: en primer lugar, pretende crear una cultura y unas competencias de gestión del conocimiento en la organización (empresa, Estado, otros...) y, en segundo lugar, y más importante, conecta este conocimiento con la prevención y la gestión de los riesgos económicos y con la estrategia de influencia de la organización. Es todo un proceso de ingeniería que alimenta constantemente a la organización con información fiable, analizada y operativa basada en el dominio de conceptos multidisciplinares e innumerables hechos para ayudar a anticipar y decidir en un mundo complejo y globalizado. Es importante mencionar que la IE se conceptualizó por primera vez para hacer frente a la creciente competencia internacional en los años noventa del siglo pasado. Tiene fines operativos. Debe ser valiosa para la organización.

En cuanto a la IA, según IBM[1], «la IA aprovecha los ordenadores y las máquinas para imitar las capacidades de resolución de

[1] Disponible en: https://www.ibm.com/topics/artificial-intelligence

problemas y toma de decisiones de la mente humana». Según la OCDE[2], «un sistema de IA es un sistema basado en una máquina que, con objetivos explícitos o implícitos, infiere, a partir de la información que recibe, cómo generar resultados tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales».

A primera vista, la IE es tanto una herramienta como una estrategia, mientras que la IA parece ser primero una herramienta. Sin embargo, la IA y la IE comparten un objetivo común: reducir la incertidumbre.

La aplicación de la IE se basa en tres pilares fundamentales: la recogida temprana, el análisis y el seguimiento de los datos y la información, con el fin de comprender y anticipar (o predecir) el entorno exterior. Este primer paso suele denominarse vigilancia y es indispensable para los otros dos. El segundo pilar es la seguridad, es decir, la protección de los activos económicos, especialmente los inmateriales. A menudo se denomina la vertiente defensiva de la IE. El tercer pilar es el «ofensivo», es decir, cómo influir en nuestro entorno exterior, en nuestro interés (reglamentos, normas, imagen...) y no solo depender pasivamente de él. En el mundo real, los tres pilares son interdependientes y se gestionan de manera conjunta. Un ejemplo: para una empresa, no anticiparse a una nueva norma europea crucial en su sector es el resultado de una mala vigilancia, puede poner a la empresa en una situación de alto riesgo y revela también una falta de influencia y de redes. Lo mismo ocurre con los Estados a nivel internacional y multilateral.

2. Interacciones IE/IA

En cuanto a la recopilación, el análisis y la predicción, lo primero es distinguir entre datos e información. En principio, el papel de la IE es extraer información inteligente de un sinfín de datos y construir a partir de ella análisis sólidos y, si es posible, predicciones, exactamente adaptadas a las necesidades y propósitos de la organización.

Lo que se suele decir de la IA es que permite predecir con mayor facilidad, disminuye el coste de todo el proceso y puede mejorar

[2] Véase en: https://www.oecd-ilibrary.org/sites/603ce8a2-es/index.html?itemId=/content/component/603ce8a2-es

su calidad. Esto es cierto, por ejemplo, para el diagnóstico médico, ya que la IA es capaz de dominar muchos más datos que un cerebro humano, y en muchos otros campos.

Desde el punto de vista de la IE, la IA es sin duda una poderosa herramienta para mejorar la cartografía, en todos los campos, incluidas las redes, las opiniones, etc. Su objetivo es hacer posible que no se olvide ningún detalle, ningún dato. Sin embargo, la pertinencia de un análisis no es sinónimo de mayor información, ni siquiera de recopilación de análisis y predicciones de alto nivel. En la IE, la pertinencia de un análisis se basa, en primer lugar, en su aportación precisa a la situación y las necesidades de la empresa (o el Estado o cualquier organización), que el analista debe comprender perfectamente de antemano; en segundo lugar, el análisis debe conducir a propuestas u orientaciones o incluso a una elección. Estos dos primeros requisitos pueden ser abordados por la IA, siempre que la pregunta se haya redactado de manera correcta.

Además, la cuestión de la calidad de los datos debe ser una preocupación constante para el analista. No solo la calidad técnica, sino también la cultural y la política. Al menos, los analistas deben ser conscientes del hecho de que la mayoría de los datos proceden de unas pocas fuentes nacionales, es decir, de países donde las fuentes de información son más numerosas (principalmente, Estados Unidos) y, además, son procesados por humanos, al menos al principio y a través de filtros a lo largo de todo el proceso. Si se supone que la IA generativa va a ser más autónoma, entonces la calidad de los datos se convierte aún más en un problema, con todos los posibles sesgos obvios (además, desde el punto de vista de la IE, esta es una razón principal para que los sistemas de IA europeos se desarrollen con sus propias normas y cerebros).

Una tercera necesidad es más difícil de responder. El valor añadido de la IE es poder identificar «señales débiles (o ligeras)», es decir, elementos que pueden estar presentes, pero no priorizados o mezclados con otros, o incluso ausentes. Por señales débiles se entiende datos/información que aparentemente no tienen ninguna relación con la pregunta o tienen una relación ínfima. Es función de los analistas multidisciplinares experimentados ser capaces de identificarlas entre un océano de datos. Aún más sutil, puede ser interesante recurrir a la imaginación (y luego comprobar la pertinencia de los resultados). Por eso cada vez más analistas (incluso del sector de Defensa) recurren a «expertos en creatividad», es decir, escritores, guionistas...

La gran novedad de la IA es que se basa en datos que ya existen o han existido.

> «[...] el acceso a grandes cantidades de datos es un activo más valioso para las organizaciones gracias a la IA [...]. El valor también depende de si los datos sólo están disponibles históricamente o si una organización puede recopilar información continua a lo largo del tiempo. La capacidad de seguir aprendiendo a través de nuevos datos puede generar una ventaja competitiva sostenida» (Agrawal, Gans y Goldfarb, 2018).

También se dice que cuantos más ejemplos pasados, más precisas serán las predicciones. Sin embargo, si los escenarios de desglose son extremadamente difíciles de construir por el cerebro humano, ¿son más alcanzables por la IA? Si por casualidad es así, tendrán que ser evaluados o completados por (múltiples) ojos humanos. De hecho, la palabra clave sigue siendo juicio. ¿Una IA es capaz de juzgar? Sí, lo es. ¿Qué juicio? Al final se convierte en una cuestión política: «El juicio es el proceso de determinar la recompensa de una acción concreta en un entorno determinado. Cuando se utiliza la IA para hacer predicciones, un humano debe decidir qué predecir y qué hacer con las predicciones» (Agrawal, Gans y Goldfarb, 2018). Esto es objeto de una profunda reflexión.

Parece entonces que un valor definitivo de la IA es reducir los costes de acceso a los datos y de almacenamiento, y aportar en primer lugar elementos fuertes. Sin embargo, no es suficiente. Es decir, tomando prestada una cita célebre, «necesaria pero no suficiente». Sin embargo, a medida que la IA se abarate, será cada vez más atractiva como solución para el análisis y la predicción, y probablemente sustituya a los humanos. Esto puede ir en detrimento de la precisión de los análisis y, por tanto, de las decisiones.

En cuanto al segundo pilar de la IE, es decir, la seguridad, el interés de la IA parece evidente. Constituye una ayuda significativa para identificar los riesgos y amenazas de mayor alcance, siempre y cuando se realice de nuevo un análisis humano de los resultados. La ciberinteligencia y la ciberseguridad son apuestas importantes. En primer lugar, para proteger los datos y los análisis, sobre todo cuando son estratégicos; en segundo lugar, para prevenir los ciberataques; en tercer lugar, si se producen, para hacerles frente con más información. Cabe mencionar un aspecto particular: los ataques a la reputación y la imagen. La IA puede

ayudar a predecir algunos de ellos, mediante un análisis profundo de todas las fuentes posibles, incluidos los competidores. También puede ayudar a atajarlos, mediante solicitudes semánticas sobre el uso de las palabras, por ejemplo. Luego viene la influencia.

El tercer pilar de la IE, la influencia, también se ve obviamente afectado por la IA, ya que esta es capaz de crear contenidos, extraer palabras adecuadas y tendencias profundas de las redes sociales, mapear las múltiples partes interesadas de las campañas, así como las personas pertinentes encargadas de elaborar textos, normas, estándares que puedan tener un impacto en la empresa (o el Estado). La IA puede ayudar a automatizar el proceso interno de comunicación.

Una vez más, es necesario un análisis profundo de los ecosistemas para construir acciones de influencia pertinentes y, una vez más, las señales débiles (o ligeras) son indispensables para adaptar correctamente la propia acción. La influencia es quizás incluso más que la seguridad necesariamente basada en la experiencia.

Por último, la IA es un problema para la IE en sí misma. La IE se basa en abordar la competencia y la IA puede cuestionar las estrategias competitivas de los sectores público y privado.

Por lo que respecta al sector privado, la IA puede repercutir en las prácticas competitivas, al menos a tres niveles: precios, patentes y normas.

La primera cuestión es que los algoritmos de fijación de precios pueden ayudar a las empresas a fijar los precios, pero también a coludir en torno a ellos. El reto clave consiste entonces en determinar la intención anticompetitiva. Al principio, esto es relativamente fácil. Pero una vez entrenados, ¿pueden los algoritmos de IA coludir entre sí sin que los humanos se den cuenta? ¿Pueden ser intencionados? Podría ser el crimen perfecto sin intención. Es una cuestión interesante para los expertos jurídicos y en inteligencia artificial.

En segundo lugar, es probable que la IA tenga un gran impacto en las estrategias competitivas a nivel mundial, a través de patentes y normas. En la actualidad, IBM es el líder en patentes, con casi 16 000 patentes relacionadas con la IA. Le siguen Intel, Samsung, Microsoft y la japonesa NEC (Dibiaggio *et al*., 2022). La batalla de las normas es también una gran preocupación. Quien fija las normas establece el terreno de juego. Esta cuestión afecta a las empresas, pero también a los Estados, que tradicionalmente desempeñan un papel más o menos activo en esta competencia normativa.

La importancia concedida a la IA por los Estados está provocando cambios significativos en conceptos jurídicos de la competencia, establecidos desde hace tiempo, incluso en la UE, donde cada vez son más las voces que reclaman normas europeas, incluso prioridades europeas. En Estados Unidos, además de sus gigantescos esfuerzos público-privados en I+D, el Gobierno interviene en los negocios privado-privados. Como ejemplo, Nvidia Corporation anunció que había recibido una carta del gobierno estadounidense el 31 de agosto de 2022, prohibiéndoles exportar chips avanzados de IA a China. AMD informa de lo mismo.

Por último, dada su crucial importancia estratégica, la IA se está convirtiendo en una cuestión de diplomacia empresarial. La IA puede contribuir al poder blando, por ejemplo, mediante la prestación de asistencia técnica y formación en los países en desarrollo. Algunos Estados, o actores privados que trabajan con ellos, como fundaciones y universidades, imparten programas de formación a naciones menos desarrolladas, especialmente en África, con cierta ventaja. El razonamiento subyacente es que en 2030 habrá cientos de millones de jóvenes en el mercado laboral africano y deben recibir formación, sobre todo en IA, de acuerdo con las normas y prácticas estadounidenses.

Es muy probable que pronto haya clasificaciones, y, por tanto, una nueva forma de competencia, para determinar qué Estados utilizan mejor la IA para gobernar; la cuestión entonces es cómo definir mejor, algo así como la clasificación *Doing Business* destinada a ayudar a evaluar el rendimiento normativo.

La IE y la IA están definitivamente vinculadas. Los agentes económicos privados y públicos deben aprender a gestionar sus interacciones.

Bibliografía

Agrawal, J., Gans, J. y Goldfarb, A. (2018). *La economía de la inteligencia artificial*. Informe de la Conferencia de la Oficina Nacional de Investigación Económica.

Dibiaggio, L. *et al. (2022). Intelligence artificielle, un sujet politique*. SKEMA PUBLIKA.

OCDE. (2019). La inteligencia artificial en la sociedad. *El panorama económico.*

Capítulo séptimo

Gestión de crisis mediante la utilización de IA

Juan Manuel Corchado

Resumen

En los últimos años se ha producido un desarrollo acelerado de la inteligencia artificial que, desde su nacimiento, ha experimentado ciclos de gran desarrollo seguidos de otros ciclos, denominados inviernos, motivados por limitaciones técnicas o tecnológicas. La gestión de crisis se verá muy beneficiada por la utilización de la inteligencia artificial para conseguir acciones más precisas. En particular, la inteligencia artificial generativa va a transformar la gestión de crisis con nuevos métodos con los que abordar los problemas, sujetos a una regulación en la que deberán tenerse siempre presentes los aspectos éticos de su uso y el cumplimiento de una legislación que se está desarrollando en paralelo con la implantación tecnológica.

Palabras clave

Gestión de crisis, Inteligencia artificial, Inteligencia artificial generativa, Modelos de lenguaje, Regulación.

Crisis management using AI

Abstract

In recent years, there has been an accelerated development of artificial intelligence which, since its birth, has experienced cycles of great development followed by other cycles, called winters, motivated by technical or technological limitations. Crisis management will benefit greatly from the use of artificial intelligence to achieve more precise actions. In particular, generative artificial intelligence will transform crisis management with new methods to deal with problems, according to regulations that always take into account the ethical aspects of its use and compliance with legislation that is developing in parallel with technological implementation.

Keywords

Crisis management, Artificial intelligence, Generative artificial intelligence, Large language models, Regulation.

1. Introducción

En la actualidad, la inteligencia artificial (IA) se ha convertido en un pilar fundamental en múltiples sectores, impulsando innovaciones y transformaciones a un ritmo sin precedentes. La aparición de la IA generativa marca un hito particularmente significativo en esta trayectoria. Esta nueva ola de IA no solo mejora procesos y sistemas existentes, sino que también abre puertas a posibilidades antes inimaginables (Corchado, 2023). Desde la creación de contenido hasta el análisis predictivo, la IA generativa está redefiniendo los límites de la tecnología y su aplicación práctica en la vida cotidiana y profesional.

La IA generativa destaca por su capacidad para manejar y extraer valor de datos no estructurados, una habilidad crucial en la gestión de crisis. En situaciones donde la información es vasta, compleja y a menudo caótica, como en el caso de conflictos armados, desastres naturales o crisis económicas, puede identificar patrones, predecir tendencias y proponer soluciones con una eficiencia y precisión que superan ampliamente los métodos tradicionales (Chui *et al.,* 2023). Su habilidad para procesar y analizar grandes volúmenes de datos en tiempo real permite una toma de decisiones más informada y rápida, aspectos críticos en la gestión de cualquier crisis.

Este capítulo se adentrará en el mundo de la IA generativa y su aplicación en la gestión de crisis. Comenzaremos explorando los orígenes y evolución de la IA, enfocándonos en el desarrollo y el impacto del invierno de la IA. A continuación, analizaremos cómo la IA del siglo XXI, especialmente la IA generativa, está remodelando la gestión de crisis, con un enfoque en conflictos no convencionales y guerras sin disparos. También abordaremos los desafíos éticos y de seguridad que surgen con su implementación, concluyendo con una mirada hacia el futuro de esta tecnología en la gestión de crisis.

La emergencia de la IA generativa no es solo un avance tecnológico; es un cambio de paradigma que está reconfigurando el mundo (Parikh *et al*., 2022). Su influencia se extiende más allá de la economía y lo social, alcanzando aspectos fundamentales de nuestra existencia, incluyendo cómo trabajamos, cómo resolvemos problemas y cómo nos preparamos para los desafíos futuros. Este capítulo no solo busca explorar las aplicaciones actuales de la IA generativa, sino también inspirar una reflexión sobre cómo esta tecnología podría moldear nuestro futuro en un espectro mucho más amplio.

2. Desde su origen hasta el invierno de la IA

La inteligencia artificial (IA) es un campo de la ciencia computacional dedicado a la creación de sistemas capaces de realizar tareas que normalmente requieren inteligencia humana, como el reconocimiento de patrones, el aprendizaje, la adaptación y la toma de decisiones. Sus orígenes se remontan a la década de 1950, cuando el término «inteligencia artificial» fue acuñado por John McCarthy (1956) en la famosa Conferencia de Dartmouth. Esta conferencia marcó el nacimiento oficial del campo y sus objetivos iniciales eran bastante ambiciosos: desarrollar máquinas que pudieran simular diversos aspectos de la inteligencia humana. En sus inicios, la IA se centró en problemas como la resolución de problemas y el razonamiento simbólico, con la esperanza de imitar la capacidad cognitiva humana en computadoras. Con el tiempo, el campo se ha expandido enormemente, abarcando áreas como el aprendizaje automático, la visión por computadora y el procesamiento del lenguaje natural, evolucionando mucho más allá de sus metas y métodos originales (Chamoso *et al*., 2019). En esta sección revisaremos los orígenes de la IA y su evolución desde mediados del siglo pasado hasta la actualidad y, posteriormente, analizaremos sus limitaciones y lo aprendido hasta primeros de este siglo. Con ello podremos entender cómo en la actualidad, con los sistemas de IA generativa, podemos atacar problemas que antes eran prácticamente inabordables con la tecnología existente. Problemas como las crisis de seguridad y militares que hoy en día nos afectan.

2.1. Historia de la IA: desde sus inicios hasta los periodos de estancamiento

La inteligencia artificial es una rama de la informática y la tecnología enfocada en crear sistemas computacionales capaces de realizar tareas que normalmente requieren habilidades humanas, como aprender, tomar decisiones, resolver problemas, percibir y entender el lenguaje. La pregunta fundamental de «¿Pueden las máquinas pensar?» fue planteada en los primeros días de la inteligencia artificial. Fue John McCarthy quien introdujo el término «inteligencia artificial» en la década de 1950 y jugó un papel clave en el desarrollo de lenguajes de programación importantes para este campo. Junto con figuras como Marvin Minsky, Lotfali A. Zadeh y John Holland, McCarthy fue pionero en el desarrollo

de conceptos, modelos y algoritmos que han sido fundamentales en la evolución de la inteligencia artificial, impactando en áreas como la medicina (Hernández *et al.,* 2023).

Con el tiempo, la inteligencia artificial se diversificó en varias ramas de especialización, incluyendo la lógica simbólica, los sistemas expertos, las redes neuronales, la lógica difusa, el procesamiento del lenguaje natural, los algoritmos genéticos, la visión por computadora, los sistemas multiagentes y las máquinas sociales (Pérez-Pons *et al*., 2023). Estas ramas, a su vez, se subdividen en áreas más especializadas, lo que demuestra el alto grado de especialización y profundidad que ha alcanzado la inteligencia artificial en la actualidad.

La mayoría de los sistemas complejos están influenciados por varios factores, están vinculados o generan diversas fuentes de datos, cambian a lo largo del tiempo y, en muchos casos, se benefician del conocimiento especializado. En este contexto, la combinación de sistemas simbólicos para modelar conocimientos con técnicas de análisis de datos que trabajan en diferentes niveles o con diversas fuentes parece ser una estrategia prometedora para soluciones integrales (Corchado *et al*., 2000). Un área donde esto es evidente es en la medicina, donde modelar el conocimiento es tan crucial como analizar los datos de los pacientes. Un ejemplo de esta integración es la plataforma Gene-CBR para el análisis genético, que combinaba un sistema de razonamiento basado en casos con redes neuronales y sistemas difusos para ayudar en el análisis del mieloma (Díaz *et al*., 2016; Hernandez-Nieves *et al*., 2021). Los años setenta y ochenta marcaron un período de significativo progreso en la inteligencia artificial y la informática distribuida (Chan *et al*., 2016; Pérez-Pons *et al*., 2021). Fue una era de transformación, marcada por el auge de internet, en un momento en que el mundo se acercaba a un nuevo siglo y el foco de la informática se inclinaba más hacia el potencial de internet que hacia el avance de la IA. La combinación de limitaciones en el *hardware*, la falta de interés de la industria en la IA y la escasez de ideas innovadoras llevó a un período de estancamiento en el campo, conocido como el «invierno de la IA».

2.2. Lecciones aprendidas de los inviernos de la IA

Durante el invierno de la IA se aprendieron varias lecciones cruciales que han moldeado el desarrollo futuro del campo (Hendler, 2008). Una de las más importantes fue la comprensión de que las

expectativas excesivamente optimistas sobre las capacidades de la IA pueden llevar a desilusiones y a una reducción en el apoyo y financiamiento. Se reconoció la necesidad de establecer objetivos más realistas y alcanzables. Además, este período subrayó la importancia de la robustez y escalabilidad en los sistemas de IA, así como la necesidad de un enfoque más integrado y multidisciplinario que combine diferentes áreas de la informática y la inteligencia artificial. También se destacó la importancia de los datos de calidad y la comprensión de que el *hardware* y los algoritmos necesitan evolucionar conjuntamente para lograr avances significativos. Estas lecciones han sido fundamentales para guiar la investigación y el desarrollo de la IA hacia enfoques más sostenibles y efectivos.

Ciertamente, para los que comenzamos a trabajar en el ámbito de la IA, en la década de los noventa nos encontramos con una tecnología con gran potencial, ilusionante, pero que a la vez había generado desilusión y desánimo en numerosos investigadores y en muchas empresas. Durante este tiempo, muchos proyectos de IA ambiciosos fracasaron, lo que llevó a un cuestionamiento generalizado de la viabilidad de la IA. Sin embargo, se aprendieron lecciones importantes que han ayudado a guiar el desarrollo de la IA en las últimas décadas posteriores.

Una de las lecciones más importantes aprendidas durante el invierno de la IA es que la IA es una disciplina compleja que requiere un enfoque sistemático y riguroso. En los años anteriores al invierno de la IA, muchos proyectos de IA se basaban en enfoques ingenuos que no tenían en cuenta los desafíos inherentes a la IA. Como resultado, estos proyectos a menudo fracasaron. Otra lección importante es que es importante desarrollar una comprensión clara de los límites de la IA.

La IA es una herramienta poderosa, pero no es omnipotente. Los algoritmos del siglo pasado escalaban mal y tenían limitaciones claras en algunos ámbitos, que, en algunos casos, se podrían haber resulto con técnicas de mezcla de expertos o con modelos de amplio alcance que incorporaran algoritmos complementarios; algo difícil de entender por la mayor parte de la comunidad científica, muy polarizada y especializada en áreas concretas de investigación.

En esta época, también empezó a quedar claro que la IA debe ser desarrollada de manera responsable y ética. Tiene el potencial de ser una fuerza poderosa para el bien o el mal. Es importante

desarrollarla de manera que se utilice para beneficiar a la humanidad y no para dañarla. Estas lecciones han ayudado a guiar el desarrollo de la IA en las décadas posteriores. Como resultado, ha progresado enormemente en los últimos años. Ahora se utiliza en una amplia gama de aplicaciones, desde la autoconducción hasta el reconocimiento facial o la gestión logística.

Parece claro que la IA continuará progresando en los próximos años. En todo caso, es importante recordar las lecciones aprendidas durante el invierno de la IA. Estas lecciones nos ayudarán a asegurar que se desarrolle de manera responsable y ética.

3. IA en el siglo XXI y su potencial

Tras un periodo de estancamiento, el campo de la inteligencia artificial experimentó un renacimiento a principios de siglo con el desarrollo del aprendizaje profundo y las redes neuronales convolucionales (CNNs). Esta innovación marcó un cambio significativo en el tratamiento de la información, utilizando técnicas de aprendizaje automático de maneras novedosas (Muñoz *et al.,* 2020). A diferencia de modelos anteriores, las CNN cuentan con múltiples capas ocultas que les permiten identificar características y patrones en los datos de entrada de forma cada vez más compleja y abstracta. Este enfoque único permite abordar problemas desde diversas perspectivas con un solo algoritmo.

Estos modelos han marcado un punto de inflexión, impulsando un cambio en nuestra manera de trabajar y abriendo las puertas a lo que se considera la quinta revolución industrial. Esta revolución se caracteriza por la fusión de tecnologías digitales, físicas y biológicas, aprovechando estos nuevos métodos de creación de conocimiento. En un mundo que ya evolucionaba rápidamente, ahora nos enfrentamos a una aceleración continua, ofreciendo a quienes se adapten a estos cambios oportunidades de negocio y creación de valor sin precedentes.

3.1. Desarrollos recientes y avances significativos en IA

El aprendizaje profundo, una rama del aprendizaje automático, se inspira en la estructura y función del cerebro humano, a través de lo que se conoce como redes neuronales artificiales. Estas redes, en particular las de múltiples capas, han demostrado ser extremadamente eficaces en una amplia gama de tareas de IA. Los modelos generativos basados en aprendizaje profundo tienen

la capacidad de aprender a representar datos y generar nuevos ejemplos que imitan la distribución de los datos originales.

Las redes neuronales convolucionales (CNNs) son un tipo especializado de redes neuronales diseñadas para procesar datos estructurados en forma de cuadrícula, como las imágenes, siendo clave en tareas de visión por computadora (Khedern y Ali, 2022). En el ámbito de la IA generativa, las CNN se han adaptado para la generación de imágenes. Un ejemplo destacado son las GAN (redes generativas antagónicas), que suelen emplear CNN en sus generadores y discriminadores para crear imágenes realistas.

Introducidas en 2014 por Ian Goodfellow y su equipo, las GAN constan de dos redes neuronales: un generador que crea datos (como imágenes) y un discriminador que intenta diferenciar entre datos reales y generados. A lo largo del entrenamiento, el generador mejora en su habilidad para crear datos que engañan al discriminador. Las CNN son comúnmente usadas en las GAN para tareas de imagen. Otro tipo de modelo generativo son los VAE (*autoencoders* variacionales), que modelan explícitamente una distribución de probabilidad de los datos y utilizan técnicas de inferencia variacional para el entrenamiento. Además, existen modelos basados en píxeles que generan imágenes píxel a píxel, empleando redes neuronales recurrentes o CNN (Aljojo, 2022).

El aprendizaje profundo, y en particular las redes convolucionales, han sido esenciales en el desarrollo y éxito de muchos modelos de IA generativa, especialmente en la generación de imágenes. Estas técnicas han permitido avances notables en la capacidad de los modelos para generar contenido casi indistinguible del real.

Por ejemplo, ChatGPT ha revolucionado nuestra vida cotidiana, desde su uso ocasional hasta su aplicación en proyectos de valor. Su habilidad para redactar textos, generar algoritmos y proponer ideas razonadas es solo la punta del *iceberg*. Ya se utiliza en atención al cliente, análisis de datos médicos, toma de decisiones y diagnóstico. Sin embargo, ChatGPT es solo uno de los muchos sistemas en este campo, junto con BARD, XLNet, T5, RoBERTa, entre otros (Adams *et al*., 2023; Likura *et al*, 2021). Estas tecnologías prometen avances en diagnósticos médicos precisos, telemedicina y monitoreo de pacientes crónicos en casa. Se están desarrollando algoritmos de gran interés en el ámbito médico, como *Transformers, Autoencoders* y modelos generativos basados en energía profunda (Janbi *et al*., 2022). La IA tiene el

potencial de cambiar radicalmente nuestra vida y trabajo, pero también presenta desafíos éticos en privacidad y seguridad que deben abordarse.

3.2. El papel de la IA en la sociedad moderna y su potencial expansivo

La inteligencia artificial (IA) tiene un papel central en la transformación digital de la sociedad actual y se espera que sus aplicaciones futuras impliquen grandes cambios. La IA ya está presente en nuestras vidas en diferentes ámbitos, como la salud, la educación, la agricultura, la administración pública y los servicios. Puede ayudar a mejorar la eficiencia y la precisión en la toma de decisiones, así como a reducir costos y tiempos en diferentes procesos. Sin embargo, también hay preocupaciones sobre su impacto en el empleo y la necesidad de adaptarse a los cambios que se avecinan. La IA tiene un potencial expansivo en diversos sectores y se espera que su democratización y crecimiento continúen en el futuro. La IA generativa tiene un gran potencial para resolver problemas muy diversos y de gran tamaño, con datos no estructurados y dinámicos, debido a sus características y capacidades. Algunas de las razones por las es tan versátil y efectiva incluyen:

- Modelos de aprendizaje profundo: utiliza modelos de aprendizaje profundo, que son capaces de procesar grandes cantidades de datos y encontrar patrones complejos, lo que permite a las computadoras aprender y adaptarse a nuevos datos de manera similar a como lo haría un ser humano.
- Capacidad para manejar datos no estructurados: puede procesar y extraer información útil de datos no estructurados, lo que permite abordar problemas en campos como la salud, la educación y la agricultura, donde los datos pueden ser heterogéneos y difíciles de analizar manualmente.
- Escalabilidad: es capaz de escalar rápidamente y adaptarse a nuevas tareas o problemas, lo que permite a las empresas y organizaciones aprovechar sus capacidades en diversos ámbitos.
- Generación de contenidos: puede ayudar en la creación de contenidos, como la generación de texto, música y videos, lo que permite a las empresas y los creadores de contenidos mejorar la calidad y la eficiencia de su trabajo.
- Superación de limitaciones de actualización: permite a los modelos de IA superar la limitación de depender de conjuntos

de datos estáticos, al integrar información en tiempo real, lo que mejora la relevancia y precisión de las respuestas generadas por IA.
- Toma de decisiones basada en datos: facilita la toma de decisiones informadas al proporcionar a los ejecutivos y analistas de datos acceso a una amplia gama de fuentes de datos, lo que permite una experiencia de usuario más rica y satisfactoria.
- Innovación en productos y servicios: permite a las empresas comprender mejor las tendencias del mercado y las necesidades de los clientes, lo que facilita la innovación y la creación de nuevos productos y servicios.

La inteligencia artificial (IA) está ya desempeñando un papel relevante y expansivo en la sociedad, permeando casi todos los aspectos de la vida cotidiana y profesional. Su influencia se extiende desde la mejora de la eficiencia operativa en las empresas hasta la transformación de la atención médica, la educación, el entretenimiento y más allá. A continuación, se detallan algunos ejemplos clave de su aplicación y potencial expansivo:

- Salud y medicina: la IA está revolucionando el campo de la medicina, desde el diagnóstico hasta el tratamiento y la gestión de la atención sanitaria. Por ejemplo, los algoritmos de IA pueden analizar imágenes médicas con una precisión que iguala o incluso supera a los radiólogos humanos, detectando enfermedades como el cáncer en etapas tempranas. Además, la IA en la genómica está permitiendo tratamientos personalizados basados en la genética del paciente.
- Negocios y finanzas: se utiliza para analizar tendencias del mercado, predecir el comportamiento del consumidor, optimizar las operaciones logísticas y automatizar tareas administrativas. En finanzas, los algoritmos de IA están transformando el trading y la gestión de riesgos, proporcionando análisis predictivos y automatización de procesos.
- Educación: está personalizando la experiencia de aprendizaje al adaptar el material educativo a las necesidades y habilidades de cada estudiante. Sistemas de tutoría inteligentes y plataformas de aprendizaje adaptativo están ayudando aal alumnado a aprender a su propio ritmo, mejorando la eficiencia y la efectividad de la educación.
- Transporte y automoción: está en el corazón de los vehículos autónomos y los sistemas de transporte inteligente. Los coches autónomos, que utilizan IA para navegar y tomar decisiones en tiempo real, tienen el potencial de reducir signi-

ficativamente los accidentes de tráfico, mejorar la eficiencia del tráfico y cambiar la naturaleza del transporte personal y público.
- Seguridad y vigilancia: se utiliza en sistemas de vigilancia para detectar actividades sospechosas o anómalas mediante el análisis de video en tiempo real. Esto no solo mejora la seguridad pública, sino que también ayuda en la gestión de emergencias y respuestas rápidas.
- Entretenimiento y medios de comunicación: está detrás de las recomendaciones personalizadas en plataformas de streaming como Netflix o Spotify, mejorando la experiencia del usuario al sugerir contenido basado en sus preferencias y hábitos de consumo anteriores.
- Medio Ambiente y sostenibilidad: ayudando en la lucha contra el cambio climático a través de la optimización de la energía, el análisis de grandes conjuntos de datos ambientales y la modelización del clima, lo que permite una mejor comprensión y respuesta a los desafíos ambientales.
- Investigación y desarrollo: acelera la investigación en campos como la química y la física, donde puede predecir las propiedades de nuevos materiales o fármacos, reduciendo significativamente el tiempo y los costos asociados con los experimentos tradicionales.

También en la gestión de crisis, la IA generativa ofrece importantes alternativas y tiene un extraordinario potencial. La IA generativa, una rama avanzada de la inteligencia artificial, tiene un potencial significativo para ayudar en la gestión de crisis en diversos ámbitos, como emergencias, seguridad, operaciones militares y catástrofes naturales (Farrokhi *et al*., 2020). Su capacidad para analizar grandes volúmenes de datos, generar simulaciones realistas y ofrecer soluciones innovadoras la convierte en una herramienta invaluable en situaciones críticas (Horowitz y Lin-Greenberg, 2022). A continuación, se detallan algunas de las formas en que la IA generativa puede ser aplicada en estos contextos:

- Simulación y modelado de crisis: puede crear modelos y simulaciones detalladas de situaciones de crisis, como desastres naturales o conflictos armados. Estas simulaciones pueden ayudar a los planificadores y responsables de la toma de decisiones a entender mejor las posibles consecuencias de diferentes cursos de acción, permitiendo una planificación más efectiva y la preparación de respuestas adecuadas.

- Análisis predictivo en emergencias: en situaciones de emergencia, como terremotos o inundaciones, la IA generativa puede analizar datos de múltiples fuentes para predecir el impacto y la evolución de la crisis. Esto incluye la identificación de áreas de alto riesgo, la estimación de daños potenciales y la optimización de los recursos para las operaciones de rescate y ayuda.
- Gestión de la seguridad y vigilancia: permite ser utilizada para analizar datos de vigilancia en tiempo real, identificando patrones anómalos o comportamientos sospechosos. Esto es crucial para prevenir ataques terroristas, delitos y otras amenazas a la seguridad.
- Operaciones militares: ofrece simulaciones avanzadas para entrenamiento y planificación estratégica. Además, analiza datos de inteligencia para predecir movimientos enemigos o sugerir estrategias óptimas, mejorando la eficacia y seguridad de las operaciones.
- Respuesta a catástrofes: es capaz de ayudar en la coordinación de respuestas a catástrofes, analizando datos de diferentes agencias y organizaciones para optimizar la distribución de recursos, la asignación de personal y la logística de las operaciones de rescate y recuperación.
- Comunicación en crisis: facilita la creación de sistemas de comunicación automatizados y personalizados que proporcionen información actualizada y relevante a las personas afectadas, mejorando la eficiencia y efectividad de las comunicaciones de emergencia.
- Reconstrucción y recuperación postcrisis: después de una crisis, la IA generativa puede analizar datos para ayudar en la reconstrucción y recuperación. Esto incluye la evaluación de daños, la planificación de la reconstrucción y la identificación de las necesidades de las comunidades afectadas para una recuperación más rápida y eficiente.

La IA moderna no solo está mejorando la eficiencia y la productividad en diversas industrias, sino que también está abriendo nuevas fronteras en la innovación y el desarrollo. Su capacidad para procesar y analizar grandes cantidades de datos, aprender y adaptarse a nuevas situaciones, y realizar tareas complejas de manera autónoma, la convierte en una herramienta poderosa con un potencial expansivo ilimitado.

La IA generativa tiene el potencial de transformar la gestión de crisis, ofreciendo herramientas avanzadas para la simulación, el

análisis predictivo, la planificación estratégica y la respuesta eficiente en situaciones de emergencia. Su capacidad para procesar y analizar grandes cantidades de datos y generar soluciones innovadoras puede mejorar significativamente la preparación y respuesta ante crisis, salvando vidas y minimizando daños. En este sentido, y dado su potencial, es crucial abordar también los desafíos éticos y de privacidad asociados con su uso, asegurando que su implementación sea responsable y respetuosa con los derechos individuales.

4. Por qué la IA generativa ofrece una alternativa casi perfecta en la gestión de crisis

La IA generativa es una alternativa adecuada en la gestión de crisis, especialmente en contextos de emergencias, seguridad, operaciones militares y catástrofes, debido a su capacidad única para analizar y sintetizar grandes volúmenes de datos de manera rápida y eficiente. En situaciones de crisis, donde el tiempo es un factor crítico y las decisiones deben tomarse rápidamente, la IA generativa puede procesar y analizar información procedente de diversas fuentes, como sensores, imágenes satelitales, informes en tiempo real y bases de datos históricas. Esta capacidad permite identificar patrones, predecir desarrollos y generar soluciones con una velocidad y precisión que superan, por mucho, las capacidades humanas (Nguyen *et al*., 2023). Por ejemplo, en el caso de desastres naturales, la IA generativa puede predecir la trayectoria de huracanes o inundaciones, estimar el impacto potencial y sugerir las rutas de evacuación más efectivas, ayudando a salvar vidas y reducir daños.

Además, puede crear simulaciones detalladas y realistas de situaciones de crisis, lo que es invaluable para la planificación y el entrenamiento. Estas simulaciones pueden ayudar a los equipos de emergencia y militares a prepararse para una variedad de escenarios, mejorando su capacidad de respuesta y eficacia en situaciones reales. En el ámbito de la seguridad, la IA generativa puede identificar amenazas potenciales, analizando patrones en datos de vigilancia, lo que es crucial para prevenir ataques o incidentes. En el proceso de recuperación postcrisis también puede analizar datos para optimizar la distribución de recursos y planificar la reconstrucción, asegurando una recuperación más rápida y eficiente. La IA generativa no solo mejora la capacidad de respuesta en situaciones de crisis, sino que también contribuye a

una mejor preparación, prevención y recuperación, lo que la convierte en una herramienta indispensable en la gestión moderna de crisis.

4.1. Definición y capacidades de la IA generativa

El aprendizaje profundo o *deep learning* es una rama del aprendizaje que ha permitido a la IA resolver problemas que eran imposibles o muy difíciles de resolver con los métodos de IA anteriores. Por ejemplo, el *deep learning* se utiliza en el reconocimiento facial, reconocimiento de voz, la traducción automática y el juego de ajedrez. El *deep learning* permitió salir a la IA de su invierno ya que:

- Ha facilitado el uso de datos no estructurados: los datos no estructurados son datos que no tienen un formato predefinido, como imágenes, videos, texto y audio (Hernández et al., 2021; González-Briones et al., 2018).
- Ha conducido a la IA aprender de datos complejos. Esto ha permitido a la IA resolver problemas que eran difíciles o imposibles de resolver con los métodos de IA anteriores.
- Ha hecho posible utilizar datos procedentes de numerosas fuentes (Verma et al., 2022; Alizadehsani et al., 2023).

Después de la revolución del aprendizaje profundo, ha llegado la IA generativa (Corchado *et al*., 2023), que ha facilitado el desarrollo de sistemas capaces de crear nuevos datos, sin copiarlos. La IA generativa utiliza técnicas de *deep learning* para generar imágenes, videos, texto y audio (Janbi *et al.*, 2022). Esto ha abierto nuevas posibilidades, como la creación de contenido de *marketing*, la producción de películas y la investigación científica. La IA generativa puede resolver problemas de una manera nueva, creando nuevas ideas y soluciones.

El aprendizaje profundo, en especial a través de las redes neuronales convolucionales, ha sido clave en el avance y éxito de numerosos modelos de IA Generativa, particularmente en la creación de imágenes (*Jara and Wowen*, 2022). Estas técnicas han logrado progresos notables, permitiendo a los modelos generar contenido que, en muchos casos, es casi indistinguible de lo real. Un claro ejemplo de esto es ChatGPT, que se ha integrado con sutileza en nuestra vida cotidiana. Mientras algunos apenas han oído hablar de él, otros lo han usado ocasionalmente, y muchos ya están implementando proyectos y generando valor con esta tecnología.

La habilidad de ChatGPT para redactar textos, generar algoritmos y formular propuestas coherentes es solo una muestra de su potencial. Actualmente, se utiliza en la creación de sistemas de atención al cliente, análisis de datos médicos, soporte en la toma de decisiones y diagnósticos, entre otros.

Sin embargo, ChatGPT es solo uno de los primeros en una creciente lista de sistemas similares que incluye a BARD, XLNet, T5, RoBERTa, Bedrock, Wu Dao, Nemo, LLAMA 2, entre otros. Estas tecnologías están allanando el camino para el desarrollo de sistemas de diagnóstico más precisos basados en evidencias y registros clínicos, la expansión de la telemedicina y el monitoreo de pacientes crónicos en sus hogares. En el ámbito médico, se están desarrollando algoritmos prometedores como *Transformers, Autoencoders*, modelos generativos basados en energía profunda, modelos de inferencia variacional de prototipos y sistemas de aprendizaje por refuerzo con inferencia causal.

La IA está en camino de transformar radicalmente nuestra forma de vivir y trabajar, aunque también presenta desafíos significativos en términos de ética, privacidad y seguridad que necesitan ser abordados cuidadosamente. En este contexto los grandes modelos de lenguajes, o *Large Language Models* (LLM) tienen mucho que decir, ya que son la base sobre la que se asientan las aplicaciones a desarrollar.

4.2. Grandes modelos de lenguaje

Los LLM son sistemas de inteligencia artificial especializados en procesar y generar lenguaje natural. Estos modelos, entrenados con extensas cantidades de texto, son capaces de realizar tareas lingüísticas complejas como traducción, creación de texto y respuestas a preguntas. Su popularidad ha crecido gracias a los avances en la arquitectura de transformadores y el incremento de la capacidad computacional, lo que les permite manejar una gran cantidad de parámetros y capturar la complejidad del lenguaje humano. Los LLM han marcado un hito en el procesamiento del lenguaje natural, y se caracterizan por:

- Gran cantidad de parámetros: por ejemplo, GPT-3, uno de los LLM más conocidos, cuenta con 175 mil millones de parámetros, lo que le permite modelar con precisión la complejidad del lenguaje.

- Entrenamiento en grandes corpus: se entrenan con vastos conjuntos de datos, incluyendo libros, artículos y sitios web, adquiriendo un conocimiento amplio y general.
- Capacidad de generación de texto: pueden crear textos coherentes y fluidos, desde ensayos hasta poesía, indistinguibles en muchos casos de los escritos por humanos.
- Transferencia de aprendizaje: tras el entrenamiento inicial, pueden adaptarse a tareas específicas con pocos datos adicionales.
- Uso de arquitectura de transformadores: utilizan mecanismos de atención para capturar relaciones complejas en los datos.
- Capacidad multimodal: algunos modelos recientes pueden procesar y generar múltiples tipos de datos, como texto e imágenes.
- Generalización a diversas tareas: pueden realizar una amplia variedad de tareas sin cambios arquitectónicos específicos.
- Desafíos éticos y de sesgo: existe preocupación por los sesgos inherentes a los datos de internet con los que se entrenan, lo que plantea desafíos éticos.

El desarrollo de los LLM ha experimentado un crecimiento exponencial, con empresas como OpenAI y Google liderando la creación de modelos cada vez más grandes y versátiles. Por otro lado, META, con su modelo Llama 2, ha generado interés por sus versiones adaptadas a diferentes capacidades de procesamiento. Los modelos de lenguaje de gran escala (LLM) como Llama 2 tienen la capacidad de especializarse mediante estrategias de ajuste fino o *fine tuning*, lo que les permite convertirse en herramientas altamente especializadas para abordar problemas específicos con gran precisión y eficacia. Esta especialización puede aplicarse en una variedad de contextos, como el diagnóstico médico, el análisis de datos complejos y el soporte en la toma de decisiones.

Al ajustar estos modelos a necesidades concretas, pueden procesar y analizar información relevante de manera más efectiva, proporcionando *insights* y soluciones adaptadas a situaciones particulares. Esta capacidad de adaptación y especialización hace que los LLM sean herramientas excepcionales para la gestión de crisis, donde la capacidad de responder rápidamente con información precisa y relevante es crucial para mitigar riesgos, coordinar esfuerzos de respuesta y tomar decisiones informadas en escenarios de alta presión y cambio constante. Las estrategias de *fine tuning* y adaptación incluyen entre otras:

- Selección de datos: la elección de un conjunto de datos adecuado y relevante para el problema específico es fundamental para entrenar un modelo de IA. Los datos deben ser representativos del problema que se desea resolver y deben estar en el mismo lenguaje que el modelo de IA.
- Ajuste de parámetros: los modelos de IA pueden ajustar sus parámetros y algoritmos internos para adaptarse a un nuevo problema. Esto puede incluir la modificación de las ponderaciones de las diferentes capas del modelo, la selección de diferentes funciones de activación o la modificación de los tamaños de los kernels en las capas de convolución.
- Entrenamiento en múltiples tareas: los modelos de IA pueden entrenarse en múltiples tareas o problemas simultáneamente, lo que les permite adaptarse a diferentes situaciones y aplicaciones. Esto puede mejorar la flexibilidad y la eficiencia de los modelos de IA, permitiéndoles adaptarse a nuevos problemas sin necesidad de reentrenar desde cero.
- Transferencia de conocimiento: es una técnica en la que se reutiliza un modelo de IA entrenado en un problema para resolver un problema diferente. Este enfoque puede ser útil cuando no hay suficientes datos para entrenar un modelo de IA desde cero en un nuevo problema.
- Regularización: es un proceso en el que se añade un término de penalización al error de entrenamiento para controlar la complejidad de los modelos de IA. Esto puede ayudar a evitar que los modelos se ajusten de manera excesiva a los datos de entrenamiento, lo que puede mejorar su generalización y capacidad para adaptarse a nuevos problemas
- Optimización de hardware: puede mejorar la eficiencia y el rendimiento de los modelos de IA, lo que puede resultar en una mejor adaptación a diferentes tareas y aplicaciones

La especialización de estos LLM es la base para la construcción de los sistemas de ayuda a la toma de decisiones en momentos de crisis. Se trata de modelos que pueden especializarse, aprender del pasado, integrar datos desestructurados de forma constante, recibir información de numerosas fuentes y explicar sus propuestas. Los problemas relacionados para la construcción de estos sistemas de ayuda a la toma de decisiones son el coste computacional, el tiempo y la experiencia para ponerlos en marcha y la necesidad de disponer de datos e información sobre crisis pasadas y sus resoluciones. Con los recursos adecuados, estos sistemas se presentan como la mejor alternativa para construir sistemas de este tipo.

5. El futuro de la gestión de crisis con IA generativa

Una crisis se refiere a una situación de extrema dificultad o peligro que afecta la seguridad y estabilidad de individuos, comunidades o naciones. En temas militares y de seguridad, las crisis pueden manifestarse en varias formas, por ejemplo: conflictos militares y guerras, atentados terroristas, ciberataques, delincuencia organizada, inestabilidad política o crisis humanitarias. En todos estos casos, las crisis se caracterizan por su naturaleza urgente, su potencial para causar daño significativo y la necesidad de respuestas rápidas y efectivas para mitigar sus efectos. La gestión de estas crisis requiere un enfoque multidisciplinario que incluya inteligencia, estrategia, recursos tecnológicos y humanos, y una comprensión profunda de las dinámicas sociales, políticas y económicas involucradas.

5.1. IA generativa en la gestión de crisis

En el mercado actual, existen diversas herramientas profesionales diseñadas para la gestión de crisis en varios ámbitos, incluyendo emergencias, seguridad, respuesta a desastres y operaciones militares (Farrokhi *et al*., 2020). Estas herramientas varían en función y complejidad, pero todas tienen el objetivo común de facilitar una respuesta eficaz y coordinada a situaciones críticas. Algunas de las herramientas más destacadas incluyen:

- Software de comunicación en crisis: herramientas como Everbridge, AlertMedia o OnSolve proporcionan plataformas para comunicar información crítica rápidamente a las personas afectadas o involucradas en una crisis. Permiten enviar alertas, instrucciones y actualizaciones en tiempo real a través de múltiples canales.
- Sistemas de gestión de emergencias: plataformas como WebEOC, Incident Command System (ICS) y Emergency Operations Center (EOC) ayudan a coordinar la respuesta operativa durante emergencias, permitiendo a los equipos de respuesta compartir información, asignar recursos y gestionar tareas de manera eficiente.
- Herramientas de inteligencia y análisis de datos: soluciones como Palantir Gotham, Deepint y IBM i2 Analyst's Notebook ofrecen capacidades avanzadas para recopilar, analizar y visualizar grandes volúmenes de datos, lo que es crucial para entender la situación, predecir desarrollos y tomar decisiones informadas (Corchado et al., 2021).

- Software de mapeo y SIG (sistemas de información geográfica): herramientas como ArcGIS de Esri y QGIS permiten visualizar datos geoespaciales, lo que es esencial para la planificación y respuesta en situaciones como desastres naturales, donde la geografía juega un papel crucial.
- Plataformas de redes sociales y monitoreo de medios: herramientas como Hootsuite, TweetDeck y Dataminr permiten monitorear las redes sociales y los medios de comunicación para obtener información en tiempo real, lo que puede ser vital para evaluar la opinión pública y detectar emergencias emergentes.
- Software de simulación y capacitación: programas como Simtable y ADMS (Advanced Disaster Management Simulator) ofrecen entornos simulados para entrenar a los equipos de respuesta en escenarios de crisis, mejorando su preparación y capacidad de respuesta.
- Herramientas de gestión de recursos humanitarios: plataformas como ReliefWeb y Humanitarian Data Exchange (HDX) proporcionan información y recursos para la gestión de crisis humanitarias, incluyendo datos sobre desplazamientos de población, necesidades de recursos y coordinación de ayuda.
- Aplicaciones móviles para gestión de crisis: aplicaciones como CrisisGo y Zello facilitan la comunicación y coordinación en dispositivos móviles, lo que es crucial para equipos de respuesta que necesitan coordinarse sobre el terreno.

Estas herramientas, combinadas con la experiencia y conocimientos de los profesionales de la gestión de crisis, son fundamentales para una respuesta efectiva y eficiente en situaciones de emergencia y crisis. La elección de la herramienta adecuada dependerá de la naturaleza específica de la crisis, los recursos disponibles y los objetivos de la respuesta. Los LLM especializados puede complementar y mejorar significativamente la eficacia de las herramientas de gestión de crisis existentes de varias maneras clave:

- Análisis predictivo mejorado: la IA generativa (LLM) puede procesar y analizar grandes volúmenes de datos de diversas fuentes para predecir la evolución de una crisis. Por ejemplo, en el contexto de desastres naturales, puede prever la trayectoria de tormentas o inundaciones, ayudando a los sistemas de gestión de emergencias a planificar respuestas más efectivas.
- Simulaciones realistas para la capacitación: las herramientas de simulación pueden ser mejoradas con LLMs espe-

cializados para crear escenarios de crisis más realistas y detallados. Esto permite una formación más efectiva para los equipos de respuesta, preparándolos mejor para situaciones reales.
- Generación automatizada de informes y comunicaciones: los LLM pueden automatizar la creación de informes detallados y comunicaciones durante una crisis, liberando a los equipos para que se concentren en tareas críticas. Por ejemplo, puede generar automáticamente actualizaciones para el público o informes para coordinadores de emergencia, asegurando que la información sea precisa y oportuna.
- Mejora en la coordinación de respuestas: integrada con sistemas de gestión de emergencias, la IA generativa puede optimizar la asignación de recursos y la coordinación de tareas. Puede sugerir la distribución óptima de equipos y suministros, basándose en el análisis de las necesidades y condiciones actuales.
- Análisis de sentimientos y monitoreo de redes sociales: al analizar datos de redes sociales y medios de comunicación, la IA generativa puede identificar tendencias de opinión pública, detectar pedidos de ayuda no atendidos y monitorizar la propagación de información durante una crisis.
- Mejora en la toma de decisiones: al proporcionar análisis y recomendaciones basados en datos, la IA generativa puede apoyar a los tomadores de decisiones en la elección de estrategias más efectivas. Esto es especialmente útil en situaciones de rápida evolución donde las decisiones deben tomarse bajo presión.
- Personalización de respuestas humanitarias: en crisis humanitarias, la IA Generativa puede ayudar a personalizar la asistencia, analizando las necesidades individuales y las condiciones locales para asegurar que la ayuda sea relevante y efectiva.
- Integración con sistemas de información geográfica (SIG): la IA generativa puede enriquecer los análisis SIG con predicciones y visualizaciones avanzadas, lo que es crucial para la planificación espacial y la respuesta en situaciones de crisis.

La IA generativa tiene el potencial de transformar la gestión de crisis al mejorar la precisión del análisis predictivo, la eficiencia de la comunicación, la efectividad de la capacitación y la calidad de la toma de decisiones. Al integrarse con las herramientas existentes, puede proporcionar una comprensión más profunda y una respuesta más ágil en situaciones críticas.

5.2. Aspectos éticos

El uso de la IA generativa en la gestión de crisis plantea importantes consideraciones éticas que deben ser cuidadosamente evaluadas. Uno de los principales desafíos es garantizar que estas tecnologías no perpetúen ni amplifiquen sesgos existentes en los datos, lo cual podría llevar a respuestas desiguales o injustas en situaciones de crisis. Además, la privacidad y la seguridad de los datos son de suma importancia, en especial cuando se manejan informaciones sensibles relacionadas con la salud, la seguridad y el bienestar personal. Es crucial que se establezcan protocolos rigurosos para la protección de datos y se respeten las normativas de privacidad. Otro aspecto ético relevante es la transparencia en la toma de decisiones automatizada; los usuarios y las partes afectadas deben entender cómo la IA generativa toma decisiones y en qué datos se basan estas. Por último, es esencial considerar el impacto humano y social de la automatización en la gestión de crisis, asegurando que la tecnología apoye, pero no reemplace, el juicio humano crítico y la empatía necesaria en situaciones de emergencia. Abordar estos aspectos éticos es fundamental para fomentar la confianza y asegurar el uso responsable y efectivo de la IA generativa en la gestión de crisis.

El uso de la IA generativa y los LLM reentrenados en la ayuda a la resolución de crisis plantea una serie de desafíos éticos que deben tenerse en cuenta. Estos desafíos incluyen:

- Precisión y fiabilidad: es importante garantizar que la información proporcionada por la IA generativa y los LLM reentrenados sea precisa y fiable. Esto es especialmente importante en situaciones de crisis, donde la información errónea puede tener consecuencias graves.
- Objetividad: es importante que la IA generativa y los LLM reentrenados sean objetivos en su presentación de la información. Esto es importante para evitar sesgos que puedan influir en las decisiones de los responsables de la toma de decisiones.
- Respeto a la privacidad: es importante proteger la privacidad de los individuos cuando se utiliza la IA generativa y los LLM reentrenados. Esto incluye evitar la recopilación de datos personales sin el consentimiento de los individuos.
- Respeto a los derechos humanos: es importante respetar los derechos humanos cuando se utiliza la IA generativa y los LLM reentrenados. Esto incluye evitar el uso de la IA generativa y los LLM reentrenados para fines discriminatorios u opresivos.

Para abordar estos desafíos éticos, es importante que los desarrolladores y usuarios de la IA generativa y los LLM reentrenados tengan en cuenta los siguientes principios:

- Transparencia: es importante ser transparente sobre cómo se desarrolla y utiliza la IA generativa y los LLM reentrenados. Esto incluye proporcionar información sobre los datos que se utilizan para entrenarlos, así como sobre cómo se utilizan los resultados.
- Responsabilidad: es importante que los desarrolladores y usuarios de la IA generativa y los LLM reentrenados sean responsables de sus acciones. Esto incluye ser conscientes de los posibles riesgos y beneficios del uso de la IA generativa y los LLM reentrenados, y tomar medidas para mitigar los riesgos.
- Rendición de cuentas: es importante que los desarrolladores y usuarios de la IA generativa y los LLM reentrenados sean responsables ante los usuarios y la sociedad. Esto incluye estar sujetos a la supervisión y el control de las autoridades competentes.

El cumplimiento de estos principios ayudará a garantizar que el uso de la IA generativa y los LLM reentrenados en la ayuda a la resolución de crisis sea ético y responsable.

Algunos ejemplos específicos de cómo se pueden aplicar estos principios incluyen:

- Precisión y fiabilidad: los desarrolladores de IA generativa y LLM reentrenados pueden utilizar técnicas de verificación de datos para garantizar que la información proporcionada sea precisa. También pueden utilizar técnicas de control de calidad para garantizar que los modelos sean robustos y no se vean afectados por sesgos.
- Objetividad: los desarrolladores de IA generativa y LLM reentrenados pueden utilizar técnicas de debiasing para evitar que los modelos reflejen los sesgos de los datos de entrenamiento. También pueden proporcionar a los usuarios información sobre los datos de entrenamiento para que puedan evaluar la objetividad de los resultados.
- Respeto a la privacidad: los desarrolladores de IA generativa y LLM reentrenados pueden utilizar técnicas de anonimización para proteger la privacidad de los individuos. También pueden proporcionar a los usuarios información sobre cómo se recopilan y utilizan los datos personales.
- Respeto a los derechos humanos: los desarrolladores de IA generativa y LLM reentrenados pueden evitar el uso de la IA

generativa y los LLM reentrenados para fines discriminatorios u opresivos. También pueden proporcionar a los usuarios información sobre cómo se pueden utilizar los resultados de la IA generativa y los LLM reentrenados para proteger los derechos humanos.

Es importante que los desarrolladores y usuarios de la IA generativa y los LLM reentrenados tengan en cuenta estos principios éticos para garantizar que esta tecnología se utilice de manera responsable. En paralelo, el sentido común es un elemento fundamental a la hora de interpretar y poner en uso los resultados proporcionados por estos sistemas, que deben ser siempre vistos como herramientas de ayuda a la toma de decisiones.

5.3. Legislación

La legislación está adaptándose para regular el uso de la IA de varias maneras. Una de las formas más comunes es mediante la creación de nuevas leyes y reglamentos específicos para la IA. Por ejemplo, la Unión Europea ha aprobado la Ley de Inteligencia Artificial, que establece normas para el desarrollo, el uso y la comercialización de la IA en la UE.

Otra forma de regular la IA es mediante la aplicación de leyes y reglamentos existentes a la IA. Por ejemplo, la Ley de Protección de Datos de la UE se puede aplicar a la IA que recopila o utiliza datos personales. En algunos casos, la legislación se está adaptando para abordar los riesgos específicos asociados con la IA. Por ejemplo, los Estados Unidos están considerando la aprobación de una ley que prohibiría el uso de la IA para desarrollar armas autónomas. La legislación sobre este campo aún se encuentra en sus primeras etapas de desarrollo, pero es probable que siga evolucionando a medida que se desarrolle esta tecnología. Es importante que la legislación sobre la IA se mantenga al día con los últimos avances tecnológicos y aborde los riesgos y beneficios asociados con la IA. Algunos de los principios clave que se están incorporando a la legislación incluyen:

- Transparencia: la legislación debe exigir que los desarrolladores y usuarios de la IA sean transparentes sobre cómo se desarrolla y utiliza la IA. Esto incluye proporcionar información sobre los datos que se utilizan para entrenar los sistemas de IA, así como sobre cómo se utilizan los resultados.
- Responsabilidad: la legislación debe responsabilizar a los desarrolladores y usuarios de la IA por sus acciones. Esto incluye

ser conscientes de los posibles riesgos y beneficios del uso de la IA, y tomar medidas para mitigar los riesgos.
- Rendición de cuentas: la legislación debe garantizar que los desarrolladores y usuarios de la IA sean responsables ante los usuarios y la sociedad. Esto incluye estar sujetos a la supervisión y el control de las autoridades competentes.

El cumplimiento de estos principios ayudará a garantizar que el uso de la IA sea ético y responsable.

6. Conclusión

El potencial de la IA y en concreto de la IA generativa en la gestión de crisis es extraordinario, abarcando desde emergencias naturales y desastres hasta situaciones de seguridad y conflictos militares gracias a su capacidad para analizar grandes volúmenes de datos, generar simulaciones realistas y ofrecer soluciones innovadoras que pueden mejorar drásticamente la eficiencia y efectividad en la respuesta a crisis. Sin embargo, también existen desafíos éticos y prácticos inherentes a su implementación, incluyendo la necesidad de abordar los sesgos en los datos, proteger la privacidad y la seguridad, y mantener un equilibrio entre la automatización y el juicio humano. A medida que avanzamos, es claro que la IA generativa no es solo una herramienta tecnológica avanzada, sino un facilitador clave para una gestión de crisis más informada, ágil y adaptativa. Su integración en las estrategias de gestión de crisis representa no solo una evolución en la tecnología, sino también en nuestra capacidad para enfrentar y superar los desafíos complejos de nuestro mundo.

La IA generativa redefinirá el campo de la gestión de crisis, ofreciendo herramientas revolucionarias que transforman la forma en que respondemos a emergencias y desafíos complejos. Estos sistemas avanzados, capaces de manejar datos no estructurados y crear espacios de latencia donde billones de conceptos y parámetros están interconectados, abren nuevas posibilidades para generar soluciones y estrategias de respuesta innovadoras. Aunque el desarrollo de grandes modelos de lenguajes (LLM) requiere una inversión significativa, su aplicación en la gestión de crisis democratiza el acceso a tecnologías poderosas para una variedad de usos, desde la coordinación de respuestas en emergencias hasta el apoyo en decisiones críticas y análisis predictivos.

Esta transformación tecnológica tiene un potencial enorme para cambiar la manera en que abordamos las crisis, mejorando la eficiencia y efectividad de nuestras respuestas. Sin embargo, es crucial enfrentar estos avances con una perspectiva equilibrada, estableciendo medidas normativas y de control para asegurar un desarrollo ético y responsable. La regulación de cómo las grandes corporaciones y entidades gubernamentales utilizan esta tecnología es vital para prevenir abusos y garantizar que su uso beneficie al bien común, especialmente en situaciones de crisis humanitaria y emergencias globales.

Existe el riesgo de que estas herramientas sean utilizadas para manipular o exacerbar situaciones de crisis, concentrando poder y control en manos de unos pocos. Por lo tanto, es imperativo actuar con rapidez y cautela para implementar salvaguardas que minimicen estos riesgos. Nos encontramos al borde de una era de cambios significativos en muchos ámbitos y en concreto en la gestión de crisis, y es esencial estar preparados y ser proactivos para manejar las implicaciones de esta poderosa tecnología.

Bibliografía

Adams, L. C. *et al.* (2023). What Does DALL-E 2 Know About Radiology? *Journal of Medical Internet Research*. Vol. 25, p. e43110.

Alizadehsani, Z. *et al.* (2023). DCServCG: A data-centric service code generation using deep learning. *Engineering Applications of Artificial Intelligence*. Vol. 123, p. 106304.

Aljojo, N. (2022). *Predicting financial risk associated to bitcoin investment by deep learning.*

Chamoso, P. *et al.* (2019). Social computing in currency exchange. *Knowledge and Information Systems*. Vol. 61, pp. 733-753.

Chan, W. H. *et al.* (2016). Identification of informative genes and pathways using an improved penalized support vector machine with a weighting scheme. *Computers in biology and medicine*. Vol. 77, pp. 102-115.

Chui, M. *et al.* (2023). *The economic potential of generative AI.*

Corchado J. M. (2023). *El Despertar de la Inteligencia Artificial Global.* Salamanca, Real Academia de Medicina. Depósito legal: S. 000-2023.

Corchado, J. M. *et al.* (2000). *Redes neuronales artificiales. Un enfoque práctico.* Servicio de Publicacións da Universidade de Vigo.

Corchado, J. M. *et al.* (2021). Deepint. net: A rapid deployment platform for smart territories. *Sensors*. Vol. 21, n.º 1, p. 236.

Corchado, J. M. *et al.* (2023). Generative Artificial Intelligence: Fundamentals. *Advances in Distributed Computing and Artificial Intelligence Journal*. Vol. 12, n.º 1, pp. e31704-e31704.

Díaz, F., Fernández-Riverola, F. y Corchado, J. M. (2006). gene-CBR: A Case-Based Reasonig Tool for Cancer Diagnosis Using Microarray Data Sets. *Computational Intelligence*. Vol. 22, n.º 3-4, pp. 254-268.

Farrokhi, A. *et al.* (2020). Using artificial intelligence to detect crisis related to events: Decision making in B2B by artificial intelligence. *Industrial Marketing Management*. Vol. 91, pp. 257-273.

González-Briones, A. *et al.* (2018). Multi-agent systems applications in energy optimization problems: A state-of-the-art review. *Energies*. Vol. 11, n.º 8, p. 1928.

Hendler, J. (2008). Avoiding another AI winter. *IEEE Intelligent Systems*. Vol. 23, n.º 2, pp. 2-4.

Hernández, G. *et al.* (2021). Video analysis system using deep learning algorithms. En: *Ambient Intelligence–Software and Applications: 11th International Symposium on Ambient Intelligence*. Springer International Publishing, pp. 186-199.

Hernández, M. *et al.* (2023). Machine Learning and Deep Learning Techniques for Epileptic Seizures Prediction: A Brief Review. En: Fernández-Riverola, F. *et al.* (ed.). *Practical Applications of Computational Biology and Bioinformatics, 16th International Conference (PACBB 2022). PACBB 2022.* Lecture Notes in Networks and Systems. Springer. Vol. 553. [Consulta: 2024]. Disponible en: https://doi.org/10.1007/978-3-031-17024-9_2.

Hernández-Nieves, E. *et al.* (2021). CEBRA: A CasE-Based Reasoning Application to recommend banking products. *Engineering Applications of Artificial Intelligence.* Vol 104, p. 104327.

Horowitz, M. C. y Lin-Greenberg, E. (2022). *Algorithms and influence artificial intelligence and crisis decision-making.* International Studies Quarterly. Vol. 66, n.º 4, p. sqac069.

Iikura, R., Okada, M. y Mori, N. (2021). Improving bert with focal loss for paragraph segmentation of novels. En: *Distributed Computing and Artificial Intelligence, 17th International Conference*. Springer International Publishing, pp. 21-30.

Instituto Nacional de Estadísticas de España (INE). (s.f.). *Cifras INE, series detalladas desde 2002, resultados nacionales, Población residente por fecha, sexo, grupo de edad y país de nacimiento.* [Consulta: 15 de abril de 2023]. Disponible en: https://www.ine.es/jaxiT3/Tabla.htm?t=9675&L=0

Janbi, N. *et al*. (2022). Imtidad: A Reference Architecture and a Case Study on Developing Distributed AI Services for Skin Disease Diagnosis over Cloud, Fog and Edge. *Sensors*. Vol. 22, n.º5, p. 1854.

Jara, J. D. Z. y Bowen, S. (2022). Learning Curve Analysis on Adam, Sgd, and Adagrad Optimizers on a Convolutional Neural Network Model for Cancer Cells Recognition. *Advances in Distributed Computing and Artificial Intelligence Journal*. Vol. 11, n.º 3, pp. 263-283.

Kheder, M. Q. y Ali, M. A. (2022). IoT-Based Vision Techniques in Autonomous Driving: A Review. *Advances in Distributed Computing and Artificial Intelligence Journal*. Vol. 11, n.º 3, pp. 367-394.

Kothadiya, D. *et al*. (2022). Deepsign: Sign language detection and recognition using deep learning. *Electronics*. Vol. 11, n.º 11, p. 1780.

McCarthy, J. (1956). *The inversion of functions defined by Turing machines.* Automata studies, pp. 177-181.

Muñoz, F., Isaza, G. y Castillo, L. (2020). Smartsec4cop: smart cyber-grooming detection using natural language processing and convolutional neural networks. En: *International Symposium on Distributed Computing and Artificial Intelligence*. Springer International Publishing, pp. 11-20.

Nguyen, X. P. *et al*. (2023). Robust Adaptive Fuzzy-Free Fault-Tolerant Path Planning Control for a Semi-Submersible Platform Dynamic Positioning System With Actuator Constraints. *IEEE Transactions on Intelligent Transportation Systems.*

Parikh, V. *et al*. (2022). Deep Learning Based Automated Chest X-ray Abnormalities Detection. En: *International Symposium on Ambient Intelligence.* Springer International Publishing, pp. 1-12.

Pérez-Pons, M. E. *et al*. (2021). Deep q-learning and preference based multi-agent system for sustainable agricultural market. *Sensors*. Vol. 21, n.º 16, p. 5276.

Pérez-Pons, M. E. *et al*. (2023). OCI-CBR: A hybrid model for decision support in preference-aware investment scenarios. *Expert Systems with Applications*. Vol. 211, p. 118568.

Verma, S. *et al*. (2022). A Novel Framework for Ancient Text Translation Using Artificial Intelligence*. Advances in Distributed Computing and Artificial Intelligence Journal*. Vol. 11, n.º 4, pp. 411-425.

Capítulo octavo

La IA en el espacio: un catalizador para los cambios geopolíticos en la economía espacial

Marco Lisi

Resumen

Este artículo investiga la intersección de la inteligencia artificial (IA) con la economía espacial y sus profundas implicaciones geopolíticas. La IA está impulsando cada vez más las misiones espaciales, las redes de satélites y la utilización de recursos, lo que está reconfigurando el panorama de la industria espacial mundial. Se explora cómo los avances impulsados por la IA están alimentando las oportunidades económicas y la competencia entre las naciones en las industrias relacionadas con el espacio, y los consiguientes efectos geopolíticos. Desde los servicios basados en satélites hasta la exploración lunar y de Marte, la IA está llamada a ser una fuerza motriz en la configuración del equilibrio de poder en el ámbito espacial, lo que la convierte en un tema crítico para responsables políticos, estrategas y líderes de la industria por igual.

Palabras clave

Inteligencia artificial, Espacio, Economía espacial, Geopolítica.

AI in space: a catalyst for geopolitical changes in the space economy

Abstract

This article investigates the crossover of artificial intelligence (AI) with the space economy and its far-reaching geopolitical implications. AI is increasingly powering space missions, satellite networks, and resource utilization, thus reshaping the global space industry landscape. It explores how AI-driven advances are fuelling economic opportunities and competition among nations in space-related industries, and the consequential geopolitical effects. From satellite-based services to lunar and Martian exploration, AI is set to be a driving force in shaping the balance of power in the space arena, making it a critical issue for policymakers, strategists and industry leaders alike.

Keywords

Artificial intelligence, Space, Space economy, Geopolitics.

1. Introducción

Localización y temporización ubicuos, detección ubicua, conectividad ubicua, modelado digital basado en la inteligencia artificial (IA): estas cuatro tendencias tecnológicas principales están desencadenando una transición trascendental en la historia de la humanidad, caracterizada, por un lado, por la integración y fusión de diferentes tecnologías e infraestructuras espaciales y terrestres, con el objetivo de una representación nueva y mejorada de nuestro mundo físico; por otro, por una desmaterialización progresiva de los productos y por su transformación en servicios.

El mundo de la fabricación se va a transformar de manera drástica, tanto en términos de paradigmas organizativos (Industria 4.0) como de tecnologías radicalmente nuevas (por ejemplo, la fabricación aditiva).

Estas tecnologías emergentes provocarán transformaciones radicales de nuestra sociedad, como las relacionadas con la conducción autónoma y con un amplio uso de vehículos aéreos no tripulados (UAV) en aplicaciones comerciales (y no solo militares).

En este «Nuevo Mundo Digital», el futuro de las tecnologías espaciales depende de dos palabras: integración y fusión.

Con su papel fundamental en localización y temporización, teledetección y comunicaciones, las tecnologías espaciales pueden desempeñar un papel esencial en la prestación de servicios digitales ubicuos (y de banda ancha).

A modo de ejemplo, la conectividad ubicua que requiere la internet de las cosas (IoT), a pesar de la amplia difusión de las redes inalámbricas y las promesas de la 5G (y la próxima 6G), nunca se logrará plenamente sin el apoyo de las comunicaciones móviles por satélite.

La misma consideración se aplica también a la conducción autónoma y a los vehículos aéreos no tripulados (más en general, al mundo de las cosas autónomas, AuT), donde los satélites no solo proporcionan comunicaciones ubicuas, sino también posicionamiento y temporización ubicuos.

La inteligencia artificial está desempeñando un papel esencial en la apertura de un nuevo panorama para las actividades espaciales, lo que comúnmente se denomina «Nueva Economía Espacial».

La IA se ha integrado a la perfección en diversas facetas de las actividades espaciales, convirtiéndose en un catalizador de un cambio sin precedentes en la economía espacial.

Naciones, organizaciones e industrias aprovechan cada vez más la IA para mejorar las operaciones de los satélites, procesar los grandes datos recogidos desde el espacio, mejorar el diseño de las naves espaciales y revolucionar la exploración espacial.

Al mismo tiempo, la IA introduce dinámicas geopolíticas que están remodelando profundamente el panorama geopolítico de las actividades espaciales.

2. La economía espacial emergente

La nueva economía espacial (NSE), también denominada Espacio 4.0, es un término que hace referencia a la comercialización y democratización de la exploración espacial. Se trata de tender un puente entre la exploración espacial y las inversiones de capital riesgo, de modo que esta nueva economía abra oportunidades para que las entidades privadas inviertan y hagan negocio en actividades espaciales.

Tradicionalmente, la exploración espacial era dominio de las agencias espaciales gubernamentales, alimentada por las ambiciones de las superpotencias e impulsada por la búsqueda del conocimiento científico, pero en las últimas décadas se ha producido un cambio hacia una mayor comercialización. Este cambio se debe, en gran medida, a los avances tecnológicos, que han reducido el coste de acceso al espacio y el tamaño y la masa de los satélites

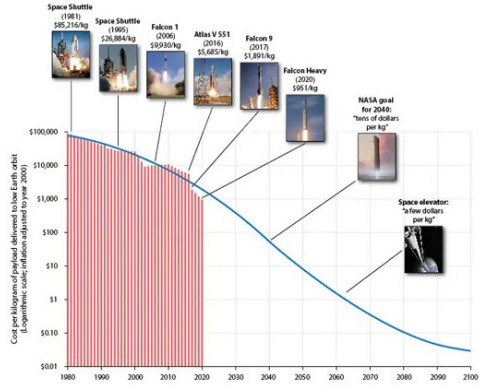


Figura 1. Coste por kilogramo de carga útil entregada en órbita terrestre baja. Fuente: FutureTimeline.net, 2018

(pequeños, micro y nanosatélites, o Cubesat), haciendo factible la participación de empresas privadas.

A modo de ejemplo, en los últimos años los costes de los lanzamientos pesados en órbita terrestre baja (LEO) han bajado de 65 000 dólares por kilogramo a 1500 dólares por kilogramo (en dólares de 2021), una disminución superior al 95 %.

Esta drástica reducción de costes fue paralela a la aparición de nuevos proveedores de lanzamientos comerciales (por ejemplo, Space X) que priorizan la eficiencia y desarrollaron componentes reutilizables para los vehículos de lanzamiento.

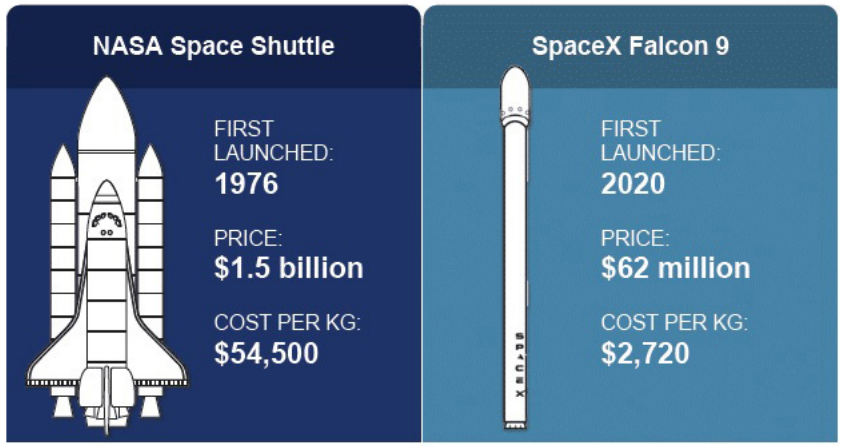


Figura 2. Reducción de costes de lanzamiento con lanzadores reutilizables. Fuente: Eversana. Disponible en: https://www.eversana.com/insights/a-spacex-philosophy-to-launching-in-pharma/

En cuanto al *hardware*, el diseño asistido por ordenador, la impresión en 3D y otras innovaciones (incluida la inteligencia artificial) han contribuido a la reducción de costes al agilizar el proceso de fabricación y mejorar las cadenas de suministro.

Son bien conocidos algunos ejemplos notables de éxito y ruptura tecnológica a través de empresas privadas.

SpaceX (*Space Exploration Technologies Corp*.), fundada por Elon Musk, es una empresa privada pionera en la fabricación aeroespacial y el transporte espacial. Es conocida por sus cohetes Falcon y Starship, la nave espacial Dragon y el desarrollo de la constelación de satélites Starlink para la cobertura mundial de internet de banda ancha. SpaceX ha logrado importantes

hitos, como ser la primera nave espacial de financiación privada en alcanzar la órbita, la primera nave espacial de financiación privada en acoplarse a la Estación Espacial Internacional (ISS) y la primera empresa privada en lanzar astronautas al espacio.

Figura 3. Dos propulsores reutilizables, Falcon Heavy de SpaceX, realizan un aterrizaje simultáneo tras poner en órbita el primer cohete Falcon Heavy el 6 de febrero de 2018. Fuente: Space.com

Un competidor en cierto modo directo de SpaceX es Blue Origin, fundada por Jeff Bezoz, fabricante aeroespacial privado y empresa de servicios de vuelos espaciales. Se centra en el desarrollo de tecnologías de cohetes reutilizables para abaratar el acceso al espacio. El cohete suborbital New Shepard de Blue Origin está diseñado para el turismo espacial, y su cohete orbital New Glenn está destinado al lanzamiento de satélites comerciales y otras misiones.

Otra empresa dedicada al turismo espacial es Virgin Galactic, fundada por Sir Richard Branson, que pretende ofrecer vuelos espaciales suborbitales a clientes de pago, permitiéndoles experimentar la ingravidez y ver la curvatura de la Tierra.

Dos empresas, entre muchas otras, en el negocio de, respectivamente, las telecomunicaciones y la observación de la Tierra: OneWeb y Planet Labs.

OneWeb es una empresa mundial de comunicaciones centrada en la construcción de una constelación de satélites en órbita

terrestre baja (LEO) para ofrecer servicios de internet de alta velocidad y baja latencia. El objetivo es reducir la brecha digital y ofrecer conectividad en regiones remotas y desatendidas. Ha lanzado hasta ahora numerosos satélites como parte de su red de banda ancha, y es probablemente el competidor más directo de la constelación Starlink de SpaceX.

Planet Labs se especializa en la obtención de imágenes de la Tierra a través de su flota de pequeños satélites. Estos CubeSats capturan imágenes de alta resolución de la superficie terrestre y las ponen, previo pago, a disposición de todos los usuarios potenciales. El objetivo de la empresa es crear un mapa «vivo» de la Tierra, actualizado diariamente.

El NSE asiste a una expansión mundial, con un número récord de países y agentes comerciales que invierten en programas espaciales. El aumento del interés queda patente en el hecho de que ya hay satélites de más de ochenta naciones registrados en órbita.

Este creciente interés por las actividades espaciales está estimulando inversiones económicas que van más allá de las infraestructuras espaciales tradicionales, con repercusiones en muy diversos sectores de la economía mundial.

Según un informe de 2022, el valor de la nueva economía espacial asciende al menos a 469 000 millones de dólares, generados en su mayor parte por la facilitación o mejora de actividades en la Tierra, pero en el futuro podría surgir un valor significativo de funciones que se desarrollen íntegramente en órbita, como los servicios en órbita, la investigación y el desarrollo, la fabricación y la extracción de minerales de asteroides.

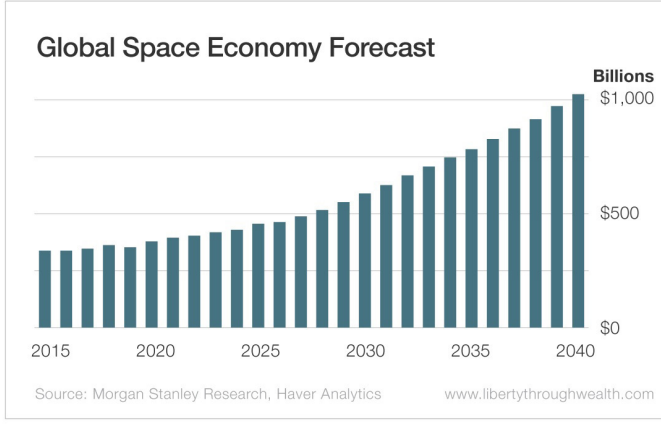


Figura 4

Las oportunidades económicas de la economía espacial están creciendo exponencialmente. En el centro de estas oportunidades se encuentran los servicios basados en satélites.

Los satélites, ya sea en órbita terrestre baja o geoestacionaria, se han convertido en herramientas indispensables para las telecomunicaciones, la radiodifusión televisiva, el posicionamiento global y la observación de la Tierra. Permiten conexiones a internet de alta velocidad en regiones remotas, proporcionan datos meteorológicos en tiempo real y facilitan la navegación de precisión.

Los datos y las imágenes por satélite han revolucionado sectores como la agricultura, la silvicultura y la gestión de catástrofes. Ofrecen información sobre los cambios medioambientales, la salud de los cultivos y la gestión de los recursos, lo que los convierte en herramientas inestimables para los responsables de la toma de decisiones en todo el mundo.

Los beneficios económicos de estos servicios son considerables, ya que mejoran la eficiencia y la asignación de recursos, al tiempo que reducen costes y riesgos.

La industria espacial comercial también se está aventurando en el turismo espacial, con empresas que desarrollan activamente la infraestructura necesaria para ofrecer viajes suborbitales y, con el tiempo, orbitales a los turistas espaciales. El turismo espacial representa un mercado incipiente pero potencialmente lucrativo, con el potencial de hacer el espacio más accesible a un mayor número de personas.

Uno de los aspectos clave del NSE es la democratización del espacio. En el pasado, solo un puñado de países disponía de los recursos y la tecnología necesarios para emprender misiones espaciales. Hoy en día, un abanico mucho más amplio de actores, incluidas las economías emergentes, las empresas privadas e incluso los particulares, pueden contribuir a la exploración espacial. Esto ha llevado a un aumento del número de satélites en órbita, sondas espaciales a planetas lejanos y planes para misiones tripuladas a la Luna y a Marte y el establecimiento de puestos avanzados permanentes en el espacio y colonias fuera de la Tierra.

Una característica marcada de la nueva economía espacial es la colaboración internacional: gobiernos e industrias privadas se unen para desarrollar y comercializar tecnologías espaciales, con el objetivo común de hacer negocio. Estas asociaciones

dan lugar a inversiones, tecnologías y oportunidades compartidas. Los esfuerzos conjuntos son esenciales no solo para compartir costes, sino también para aprovechar los conocimientos y la experiencia colectivos. Esta colaboración también fomenta la diplomacia en la gobernanza espacial, ya que las naciones tratan de crear un entorno espacial estable y predecible para las actividades económicas.

El NSE también presenta varios retos, como la cantidad de basura espacial que orbita la Tierra, que según la NASA es actualmente del orden de 9000 t. La basura espacial, debido al creciente número de satélites en órbita alrededor de la Tierra y a la llegada de las llamadas «Mega Constelaciones», podría suponer una amenaza, tanto para las naves espaciales tripuladas como para las no tripuladas.

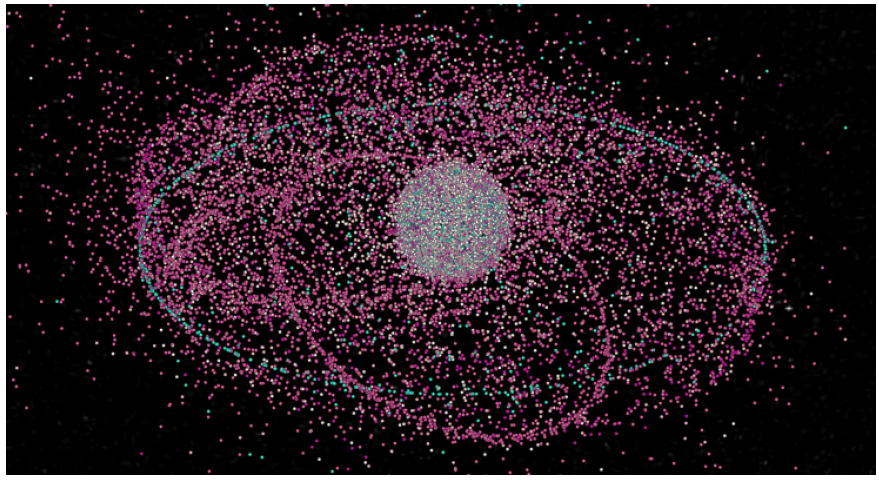


Figura 5. La asombrosa cantidad de objetos espaciales que rodean el planeta. Fuente: HPC Wire, 2022

Otras posibles cuestiones a tener en cuenta son las legales y reglamentarias, ya que el actual marco político y jurídico internacional no se diseñó pensando en la NSE.

En el contexto de la nueva economía espacial, la inteligencia artificial (IA) se perfila como un catalizador clave de las futuras actividades espaciales.

La unión de la inteligencia artificial y la exploración espacial está abriendo nuevos horizontes, acelerando la innovación y mejorando la eficacia de las misiones espaciales.

3. Inteligencia artificial

Antes de describir el papel de la inteligencia artificial, convendría establecer algunas definiciones básicas y acordar una taxonomía común.

La inteligencia artificial (IA) se refiere al desarrollo de sistemas informáticos o programas que pueden realizar tareas que simulan las funciones cognitivas humanas y adaptarse a diferentes situaciones, lo que normalmente requiere la intervención humana.

La IA como disciplina no es nueva y la investigación sobre ella se ha desarrollado a lo largo de más de cincuenta años.

La primera aproximación a la IA fue la de los sistemas basados en reglas (también denominados sistemas expertos), los cuales funcionan con reglas y lógica predefinidas, es decir, instrucciones explícitas, para tomar decisiones y realizar tareas.

Para superar las limitaciones de los sistemas expertos, principalmente la necesidad de un conjunto de definiciones muy detallado y exhaustivo para cada dominio de aplicación, se desarrolló un enfoque más flexible y evolucionado, el aprendizaje automático (*machine learning*, ML).

El ML consiste en entrenar un modelo sobre los datos para que reconozca patrones y haga predicciones o tome decisiones sin estar explícitamente programado. La fase de entrenamiento puede ser supervisada, es decir, con intervención humana, o no supervisada.

Un subconjunto del aprendizaje automático y su evolución posterior es el aprendizaje profundo (*deep learning*, DL).

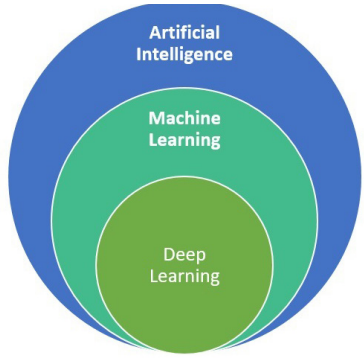


Figura 6. Inteligencia artificial, aprendizaje automático y aprendizaje profundo. Fuente: Nadia Berchane, M2 IESCI, 2018

El DL utiliza redes neuronales con múltiples capas (redes neuronales profundas) para analizar y aprender de los datos. En la red neuronal, las dos fases, de entrenamiento a partir de los datos y de definición del modelo, se producen al mismo tiempo, a costa, eso sí, de una mayor potencia de cálculo, un mayor conjunto de datos de entrada y un periodo de aprendizaje más largo.

En comparación con los sistemas expertos, los enfoques de aprendizaje automático (y aprendizaje profundo) requieren menos estructura: simplificando al extremo, introducimos datos en la máquina y vemos qué conclusiones obtiene.

En otras palabras, los algoritmos de *machine learning* tienen una característica peculiar: superan el paradigma de programación estándar, ya que el programador no tiene que pensar en todas las eventualidades en las que se puede encontrar la máquina para hacerla actuar en diferentes situaciones. La máquina, en cambio, se entrena y, por tanto, se vuelve capaz de adaptarse por sí misma a diferentes contextos, adquiriendo cierta autonomía y mostrando algunos comportamientos que se asemejan a la inteligencia de un ser humano.

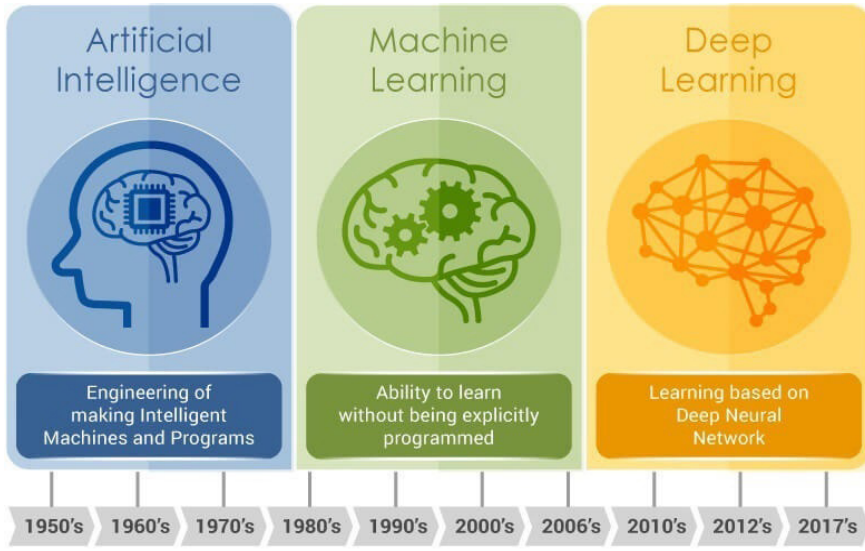


Figura 7. Evolución de la IA. Fuente: Edge ai+visión Alliance. Disponible en: https://www.embedded-vision.com

Las aplicaciones de la IA se están disparando en diversos sectores, como la sanidad, las finanzas, la educación, la seguridad y la fabricación, entre otros.

Sin embargo, aunque la IA presenta enormes oportunidades de innovación y eficiencia, también plantea problemas éticos y sociales, como el desplazamiento de puestos de trabajo, el sesgo de los algoritmos y cuestiones de privacidad.

4. La IA en el espacio: habilitar la economía espacial

La sinergia dinámica entre la IA y la economía espacial se manifiesta principalmente en cinco sectores diferentes:

1. Operaciones y comunicaciones por satélite.
2. Robótica y exploración espaciales.
3. Análisis de datos en tiempo real y fuera de línea.
4. Diseño, pruebas y adquisición de naves espaciales.
5. Seguridad.

En los párrafos siguientes se analizará en detalle cada uno de los sectores.

4.1. Operaciones y comunicaciones por satélite impulsadas por la IA

La IA está dotando a los satélites, más que nunca, de la capacidad de gestionar de forma autónoma diversas tareas, desde los ajustes de órbita hasta la evitación de colisiones y la transmisión de datos.

La IA ha revolucionado las operaciones por satélite, haciéndolas más ágiles, adaptables y resistentes. Los procesos autónomos de toma de decisiones son el núcleo de esta transformación. Los satélites están ahora equipados con algoritmos de IA que les permiten realizar multitud de tareas con una intervención humana mínima, por ejemplo, ajustes de órbita, evitación de colisiones y gestión de recursos.

Los algoritmos autónomos de toma de decisiones permiten a las naves espaciales identificar obstáculos, adaptarse a retos imprevistos y navegar por los complejos campos gravitatorios de los cuerpos celestes. Este nivel de autonomía reduce la necesidad de supervisión e intervención humanas constantes, lo que permite realizar misiones más ambiciosas y rentables.

Especialmente eficaz es la adopción de la IA en la optimización de trayectorias. En el espacio, cada gota de combustible importa.

Los algoritmos de IA tienen en cuenta múltiples variables, como las fuerzas gravitatorias, la dinámica orbital y los objetivos de la misión, para calcular las trayectorias más eficientes en términos de consumo de combustible.

Los riesgos de la misión se reducen sustancialmente al aumentar el nivel de conocimiento de la situación en torno a la nave espacial. Las técnicas de IA utilizadas para fusionar datos procedentes de múltiples sensores, como cámaras, radares y espectrómetros, pueden identificar posibles colisiones con otras naves espaciales o desechos espaciales, proporcionando alertas tempranas.

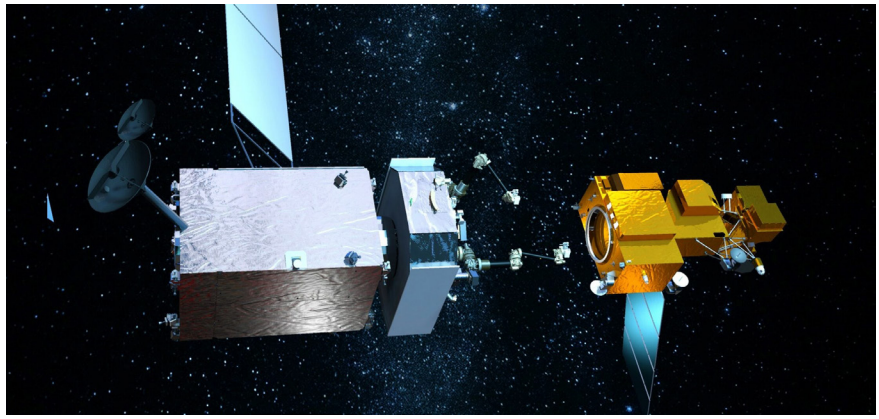


Figura 8. Nave espacial robótica de mantenimiento, ensamblaje y fabricación en órbita 1 (OSAM-1) basada en IA. Fuente: NASA

También es necesario un cambio de paradigma cuando se consideran las operaciones en tierra: mientras que la miniaturización de la tecnología ya ha permitido una reducción significativa del coste del segmento espacial, el coste del segmento terrestre no escala con el tamaño y la masa del satélite. Una vez más, la IA puede simplificar los sistemas terrestres y reducir el número de operadores especializados y altamente cualificados que trabajan por turnos las 24 horas del día, los 7 días de la semana.

El resultado es una infraestructura espacial que funciona eficazmente incluso en los escenarios más complejos y dinámicos.

Además, la IA mejora la propia columna vertebral de las redes de comunicaciones espaciales. La velocidad y eficacia con que se transmiten los datos entre la Tierra y el espacio ha aumentado en los últimos años, debido también a la adopción de tecnologías avanzadas, como las comunicaciones ópticas. Los algoritmos de

IA optimizan la recepción de señales, ajustan los patrones de los haces en tiempo real y asignan los recursos de comunicación de forma inteligente. De este modo se maximiza la velocidad de transmisión de datos, se minimiza la latencia y se mantiene la fiabilidad de la comunicación, incluso ante interferencias o cambios en las condiciones ambientales. Este nivel de sofisticación de las comunicaciones es decisivo para permitir no solo la observación de la Tierra y la investigación científica, sino también servicios críticos como la predicción meteorológica y la conectividad global a internet.

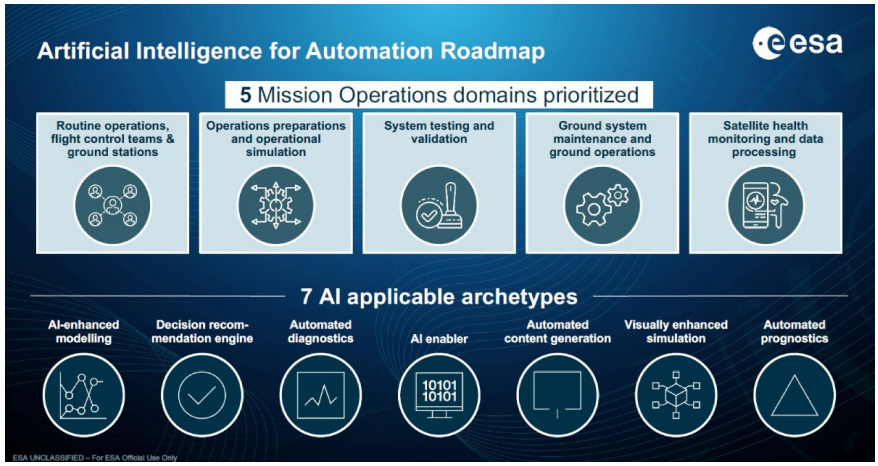


Figura 9. Hoja de ruta de la ESA para la aplicación de la IA a las operaciones de las misiones espaciales. Fuente: ESA

4.2. Avances en la exploración espacial impulsados por la IA

En el campo de la exploración espacial, las aportaciones de la IA son impresionantes.

La exploración espacial requiere niveles muy altos de autonomía y automatización. El control remoto total desde la Tierra es difícil, si no imposible, debido a las estrictas restricciones de las comunicaciones: ventanas de comunicación limitadas, largas latencias de comunicación y ancho de banda limitado. Por ejemplo, una señal de radio tarda entre cinco y veinte minutos en recorrer la distancia entre Marte y la Tierra, dependiendo de la posición de los planetas.

La IA permite a las naves espaciales realizar tareas rutinarias y tomar decisiones sin comunicación constante con la Tierra, reduciendo así la dependencia de las comunicaciones.

Las exploraciones del espacio profundo pueden ser de tres tipos:

- Predecibles (pero a menudo extremadamente complejas).
- Impredecible.
- Que requieren una respuesta en tiempo real.

La navegación autónoma, facilitada por algoritmos de IA, permite a las naves espaciales navegar lejos de la Tierra, aterrizar en cuerpos celestes, afrontar y adaptarse a situaciones inesperadas con un grado de confianza bastante alto.

Las misiones robóticas se benefician enormemente de la IA, ya que permite a los vehículos exploradores y de aterrizaje explorar de forma autónoma las superficies planetarias y realizar tareas complejas como la recogida y el análisis de muestras. Estos robots utilizan la IA para el análisis del terreno, el reconocimiento de objetos y la navegación, lo que les permite tomar decisiones en función de su entorno.

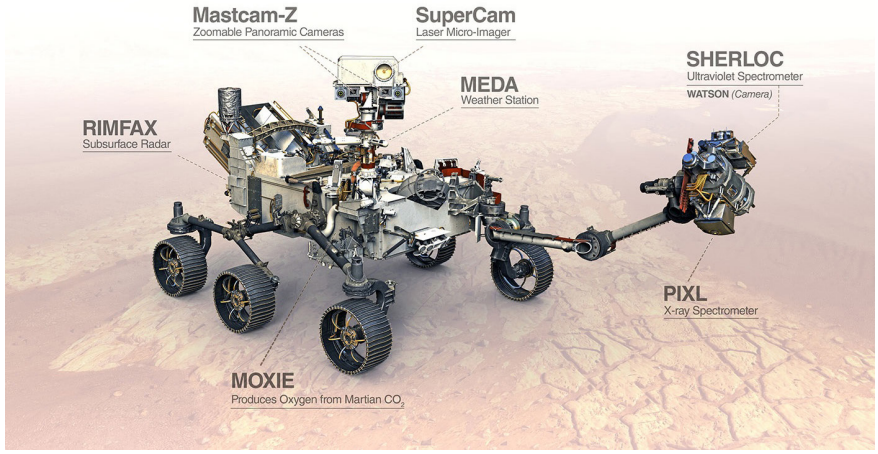


Figura 10. Mars Perseverance Rover de la NASA, basado en IA. Fuente: NASA

Además, el análisis de datos basado en IA acelera el proceso de descubrimiento científico, ya que tamiza el enorme volumen de datos recogidos durante las misiones y ayuda a los científicos a descifrar los fenómenos cósmicos.

La IA también ha dejado su huella en el ámbito de la utilización de recursos y la sostenibilidad. A través de la utilización de recursos *in situ* (ISRU), la IA desempeña un papel vital en la extracción y el procesamiento de recursos en los cuerpos celestes, desbloqueando potencialmente una gran cantidad de recursos

para futuras misiones a la Luna, Marte y más allá. Esto es fundamental para mantener a largo plazo los esfuerzos de exploración y colonización humana en el espacio.

El concepto de utilización de recursos *in situ* (ISRU) está a la vanguardia de estos avances. La robótica y las tecnologías mineras impulsadas por la IA están a punto de revolucionar la extracción de recursos en los cuerpos celestes, proporcionando potencialmente las materias primas necesarias para la exploración y la habitación humana a largo plazo. La Luna y Marte, con su abundancia de recursos, son objetivos privilegiados para la ISRU.

4.3. IA y análisis de datos espaciales

La inteligencia artificial muestra todo su potencial como herramienta de procesamiento y análisis de datos de teledetección por satélite.

La observación de la Tierra por satélite ya se basaba, en gran medida, en técnicas de tratamiento digital de imágenes para analizar datos procedentes, por ejemplo, de sensores ópticos o de radar de apertura sintética (SAR), pero la fotointerpretación, la fase del proceso que más valor añadido aporta, seguía siendo terreno de la experiencia humana hasta hace pocos años.

Las técnicas de IA hacen posible una «Integración y Fusión de Datos» eficaz, es decir, la integración de datos procedentes de múltiples sensores de satélite y la combinación de datos de satélite con observaciones terrestres u otras fuentes, mejorando la precisión y pertinencia de la información extraída de las imágenes de satélite.

El tratamiento de datos de satélite con técnicas de IA permite extraer información de forma más eficaz y precisa y analizar los datos casi en tiempo real, lo que abre nuevas aplicaciones en diversos campos, como:

- Reconocimiento y clasificación de imágenes, donde se emplean algoritmos de IA para identificar y clasificar objetos, características y patrones en imágenes de observación de la Tierra, incluida la identificación automática de tipos de cobertura del suelo, zonas urbanas, vegetación, masas de agua y cambios a lo largo del tiempo.
- Detección de cambios y anomalías, es decir, detección de cambios en la superficie terrestre a lo largo del tiempo. Comparando imágenes de satélite u otros datos de obser-

vación de la Tierra en distintos momentos, los modelos de aprendizaje automático pueden identificar cambios como la deforestación, la expansión urbana, los cambios en el uso del suelo, los efectos de catástrofes naturales, o identificar sucesos como vertidos de petróleo, incendios forestales o condiciones medioambientales anómalas que pueden requerir atención inmediata.

- Cartografía de la cubierta terrestre, para crear mapas detallados de la cubierta y el uso del suelo. Los algoritmos de IA pueden clasificar los tipos de ocupación del suelo en imágenes de satélite, distinguiendo entre categorías como bosques, zonas urbanas, masas de agua y tierras agrícolas. Esta información es crucial para la vigilancia del medio ambiente, la gestión de los recursos, la ordenación del territorio y la planificación urbana, la gestión del transporte y el seguimiento de las actividades humanas. Además, las mismas técnicas ayudan a detectar y analizar cambios en el medio ambiente a lo largo del tiempo, como la deforestación, la expansión urbana o las alteraciones en las masas de agua.
- Supervisión de cultivos y agricultura de precisión: en este caso, la IA se aplica a la supervisión y gestión de las actividades agrícolas. Los datos de satélites y drones, combinados con algoritmos de aprendizaje automático, permiten una agricultura de precisión al proporcionar información sobre la salud de los cultivos, predecir el rendimiento y optimizar la asignación de recursos.
- Investigación atmosférica y climática, donde la IA se utiliza en el análisis de datos atmosféricos y climáticos obtenidos de satélites de observación de la Tierra, lo que permite una vigilancia medioambiental eficaz y con capacidad de respuesta.

Figura 11. Aprendizaje profundo para imágenes de satélite. Fuente: Deepsense.ai

4.4. Diseño, pruebas y adquisición de IA y naves espaciales

La IA extiende su influencia al diseño y las pruebas de las naves espaciales, así como a la adquisición de piezas de la cadena de suministro de los subcontratistas, lo que contribuye a aumentar la eficacia, la rentabilidad y la innovación.

El diseño generativo, basado en algoritmos de IA, puede explorar numerosas posibilidades de diseño y optimizar los componentes de las naves espaciales en función de objetivos y restricciones predefinidos. Por ejemplo, aplicada a las estructuras de las naves espaciales, la IA puede optimizar su diseño, mejorando la integridad estructural y minimizando al mismo tiempo el peso y el coste.

La simulación basada en IA se utiliza para simular y modelar distintos aspectos del diseño de naves espaciales, como el análisis térmico, la integridad estructural, la compatibilidad electromagnética (CEM) y la aerodinámica. Esto permite a los ingenieros predecir y optimizar el comportamiento de las naves espaciales en diversas condiciones. En términos más generales, la IA simplifica el desarrollo de «gemelos digitales», modelos digitales sofisticados y completos que pueden utilizarse para simular el comportamiento de una nave espacial en una misión fuera de la Tierra en la seguridad y comodidad de un centro de control de misión.

Una fase esencial, pero tradicionalmente larga y costosa, del proceso de desarrollo de una nave espacial es la de las pruebas y la validación.

El competitivo entorno comercial de la nueva economía espacial exige que los productos estén en el mercado en el momento y al precio adecuados. Para lograr este objetivo es necesario reducir los plazos de desarrollo y despliegue.

Por otra parte, la realización de grandes constelaciones de satélites para comunicaciones móviles o multimedia exige producir un gran número de naves espaciales en un plazo notablemente breve. Los conceptos tradicionales de producción espacial ya no son adecuados para satisfacer los requisitos de estos proyectos innovadores.

Es necesario un cambio de paradigma en la forma de diseñar y producir satélites, con el objetivo de ofrecer un producto mejor

y más flexible, a menor coste y en menos tiempo (el *Time-to-Market* es el rey).

En cuanto a los métodos de ensamblaje, integración y pruebas/verificación (AIT/AIV), se requiere un estilo de producción en cadena, junto con instalaciones de producción expresamente diseñadas para la fabricación en serie.

Aquí la IA viene al rescate, contribuyendo a la automatización de los procesos de prueba, lo que permite la evaluación rápida y completa de los componentes y sistemas de las naves espaciales. Esto incluye pruebas funcionales, pruebas de estrés y pruebas de rendimiento, garantizando la fiabilidad antes del lanzamiento.

Además, durante las pruebas, la IA puede detectar anomalías o comportamientos inesperados en los sistemas de las naves espaciales. Esta detección temprana ayuda a los ingenieros a resolver los problemas con prontitud y mejora la fiabilidad general de la nave espacial.

La IA se está aplicando eficazmente a la evolución de los subsistemas a bordo de un objeto espacial (por ejemplo, un satélite). Un ejemplo representativo es el de los sistemas autónomos de vigilancia de naves espaciales.

Los sistemas de monitorización de la salud de las naves espaciales (HM), también denominados sistemas FDIR (*Fault, Detection, Isolation, and Recovery*), son esenciales para alcanzar los objetivos de disponibilidad, fiabilidad y seguridad de las naves espaciales.

La tecnología anterior se basaba en el conocimiento experto, que verificaba si los valores de telemetría estaban dentro de unos límites predefinidos o se salían de ellos (técnica *Out-of-Limits*, OOL).

En comparación con los sistemas expertos, los FDIR basados en IA pueden aprender continuamente de nuevos datos y experiencias, mejorando con el tiempo las capacidades de detección y recuperación de fallos. La IA puede integrar el conocimiento del dominio y las reglas expertas con los nuevos datos recopilados a lo largo de la vida operativa y, a continuación, emplear el razonamiento de diagnóstico para determinar la causa raíz de un fallo. Esto puede ser especialmente útil en sistemas complejos en los que la relación entre los síntomas y las causas profundas no siempre es directa.

4.5. IA y seguridad de los sistemas espaciales

La IA desempeña un papel importante en la mejora de la seguridad de los sistemas espaciales.

A medida que evoluciona la tecnología, los sistemas espaciales se hacen más complejos, interconectados y vulnerables a diversas amenazas.

Las tecnologías espaciales, con su papel en la localización y la temporización, la teledetección y las comunicaciones, son esenciales en la prestación de servicios digitales a escala mundial y vitales para el rendimiento y la supervivencia de nuestras infraestructuras críticas. Por estas razones, los sistemas espaciales deben estar garantizados y protegidos contra ataques intencionados y no intencionados, en términos de confidencialidad, disponibilidad, integridad, continuidad y calidad de servicio.

La convergencia entre defensa y espacio era ya uno de los temas más debatidos en todo el mundo.

La guerra de Ucrania ha demostrado dramáticamente con toda su evidencia que las preocupaciones y disposiciones en materia de seguridad deben extenderse a todos los activos espaciales. La percepción comúnmente compartida es que el espacio corre el riesgo de convertirse en el escenario de una futura guerra, si no lo ha sido ya.

Además de los ciberataques, dirigidos principalmente contra las infraestructuras del segmento terreno (centros de control, estaciones terrestres de control, instalaciones de lanzamiento), hoy en día son posibles varias amenazas físicas, que van desde las «armas antisatélite de energía cinética» hasta las «armas de energía directa» y las interferencias de radiofrecuencia.

Un arma antisatélite cinética puede ser un misil lanzado desde la Tierra al espacio hasta interceptar un satélite ya en órbita y destruirlo por impacto, o un satélite «asesino» que se pone en órbita y permanece allí a la espera de ser utilizado, modificando su órbita.

En ambos casos, a un ataque de «energía cinética», basado en el impacto físico con un satélite «objetivo» y su destrucción, le sigue también la consecuencia inevitable de la producción de «desechos», que siguen permaneciendo en órbita, aumentando la ya preocupante cantidad de basura espacial alrededor de la Tierra.

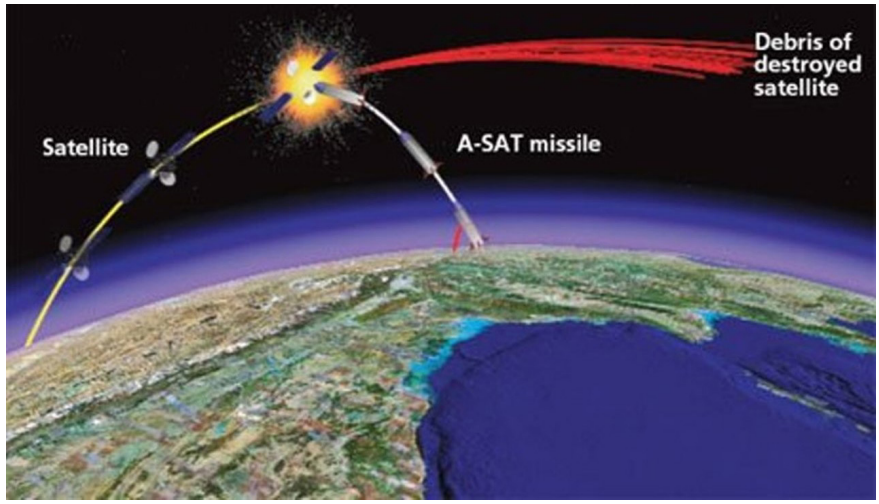


Figura 12. Ataque físico cinético antisatélite (A-SAT) de ascenso directo. Fuente: Centro de Estudios Estratégicos e Internacionales

Las armas de energía directa suelen dirigirse contra activos en órbita y pueden realizarse como rayos láser de alta energía o haces de radiofrecuencia generados en tierra, capaces de «cegar» satélites y dañar sus equipos electrónicos. También pueden generarse «destellos» destructivos de energía de radiofrecuencia mediante la explosión de pequeñas bombas nucleares en la ionosfera (pulso electromagnético, EMP).

La integración de la IA en la seguridad de los sistemas espaciales podría llegar a ser esencial para garantizar la resistencia y la protección de estos sistemas frente a una amplia gama de

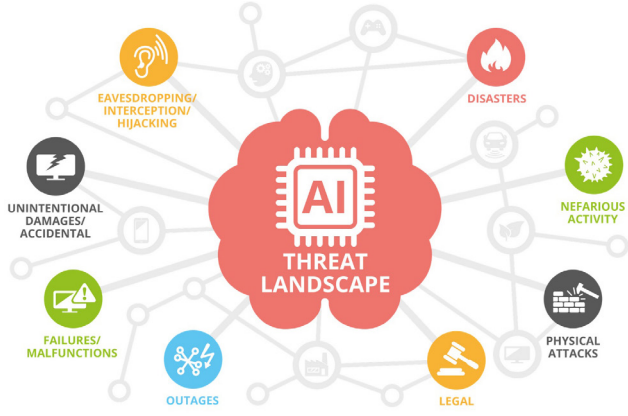


Figura 13. Panorama de las amenazas de la IA. Fuente: Agencia de Ciberseguridad de la Unión Europea - ENISA

amenazas intencionadas y no intencionadas, incluidos los ciberataques, los accesos no autorizados, los ataques físicos y los peligros medioambientales.

Un ámbito clave en el que la IA puede aportar una mejora sustancial es el de la detección y el análisis de amenazas.

Los algoritmos de IA pueden analizar grandes conjuntos de datos para identificar anomalías o patrones inusuales que puedan indicar una amenaza para la seguridad. Esto es especialmente importante para detectar accesos no autorizados o posibles ciberataques contra sistemas espaciales. Además, los sistemas de IA pueden reconocer patrones asociados a actividades maliciosas, ayudando a detectar y responder a incidentes de seguridad con mayor rapidez y eficacia.

En lo que respecta a la ciberseguridad, los algoritmos de IA ayudan a identificar vulnerabilidades en el *software* y la infraestructura de red del sistema espacial. Esto permite tomar medidas proactivas para abordar las debilidades potenciales antes de que puedan ser explotadas. La IA también se utiliza para desarrollar sistemas avanzados de detección y prevención de intrusiones, que pueden identificar y neutralizar ciberataques en tiempo real.

En el segmento espacial, la IA mejora, en primer lugar, el conocimiento de la situación espacial. Como ya se ha mencionado, la IA puede rastrear eficazmente los objetos espaciales, predecir sus trayectorias e identificar posibles colisiones o anomalías. Esto es crucial para evitar colisiones en entornos orbitales abarrotados, pero también posibles ataques cinéticos.

En términos más generales, los sistemas de IA embarcados pueden programarse para responder de forma autónoma a las amenazas a la seguridad, minimizando el tiempo de respuesta y reduciendo el riesgo de error humano. Estos sistemas pueden adaptarse a la evolución de las amenazas, aprendiendo y actualizando continuamente sus mecanismos de defensa. Esta adaptabilidad es esencial para adelantarse a las ciberamenazas sofisticadas.

Una última aportación de la IA a la seguridad espacial, aunque no por ello menos importante, es su contribución al desarrollo de protocolos de comunicación seguros, técnicas de cifrado y mecanismos de autenticación para proteger la integridad y confidencialidad de los datos transmitidos entre sistemas espaciales.

La IA puede emplearse para desarrollar y mejorar algoritmos de cifrado, incluidas técnicas criptográficas avanzadas, y para establecer sistemas de gestión de claves que adapten dinámicamente las claves de cifrado, dificultando así que los adversarios comprometan la seguridad de los canales de comunicación por satélite.

5. Implicaciones geopolíticas de la IA en el espacio

La integración de la inteligencia artificial (IA) en las actividades espaciales es más que un avance tecnológico, es una fuerza revolucionaria con implicaciones que van más allá de las oportunidades económicas, pues conlleva profundas implicaciones geopolíticas. A medida que las naciones y organizaciones aprovechan el poder de la IA en el ámbito espacial, no solo están configurando el futuro de la exploración espacial, sino también redefiniendo el equilibrio de poder mundial, desencadenando la competencia y necesitando nuevos enfoques diplomáticos y normativos.

Entre las consideraciones geopolíticas que exigen atención, la seguridad nacional es una preocupación primordial.

Los activos espaciales mejorados con IA desempeñan un papel vital en la vigilancia, el reconocimiento y las comunicaciones militares. Garantizar la seguridad de estos activos se convierte en una prioridad, lo que exige medidas de protección frente a posibles amenazas.

Las naciones están aprovechando la IA para la vigilancia y el reconocimiento desde el espacio. Los sistemas de IA pueden analizar grandes cantidades de datos procedentes de satélites y proporcionar información sobre posibles amenazas a la seguridad.

Aparte del uso en tiempo real o casi real de las imágenes de satélite, la IA puede ayudar a extraer enormes archivos de imágenes, a menudo de código abierto, recopilados a lo largo de los años (por ejemplo, las bases de datos de constelaciones de Copérnico, disponibles gratuitamente para todos los usuarios potenciales). La situación se asemeja, en cierto modo, a descubrir y traducir textos antiguos en latín y griego, copiados a mano por monjes medievales y conservados durante siglos en las bibliotecas de los monasterios.

Esta revisión de las imágenes satelitales históricas contribuirá a vigilar las zonas de conflicto y las regiones fronterizas, detectando cambios en el terreno, las infraestructuras o las actividades

militares, pero también a descubrir recursos naturales (minerales, petróleo, gas) o explotar nuevos servicios orientados al usuario.

No hay que subestimar el cambio potencial en el poder económico provocado por la IA, que permitirá a los países emergentes competir con las economías establecidas en determinados sectores, de los que estaban excluidos por falta de acceso al espacio. Al desarrollar capacidades autóctonas de IA, los países emergentes pueden reducir su dependencia de tecnologías extranjeras y reforzar su soberanía tecnológica.

En el plano político, el espacio vuelve a ser, como en los años sesenta, el campo de batalla de la competencia y las rivalidades entre las naciones que realizan actividades espaciales. El desarrollo y despliegue de la IA en la exploración espacial contribuyen al liderazgo tecnológico de una nación, mejorando su estatus en la comunidad espacial mundial.

Estados Unidos y China están inmersos en una competitiva carrera espacial, en la que ambas naciones invierten grandes sumas en tecnologías de IA para la exploración del espacio, las operaciones por satélite y las capacidades basadas en el espacio.

Los países de la Unión Europea, colectivamente, a través de la Agencia Espacial Europea (ESA) y la Agencia de la Unión Europea para el Programa Espacial (EUSPA), y a nivel de agencias espaciales nacionales individuales, están llevando a cabo, de manera activa, iniciativas espaciales impulsadas por la IA. Cabe mencionar, a modo de ejemplo, el programa Copernicus, que utiliza la IA para el análisis de datos procedentes de satélites de observación de la Tierra.

Otros países, como Rusia, con su larga y gloriosa tradición espacial, e India, Japón, Corea del Sur y los Emiratos Árabes Unidos (EAU) también están invirtiendo en iniciativas espaciales impulsadas por la IA.

Las empresas espaciales privadas, en particular las de Estados Unidos (por ejemplo, SpaceX, Blue Origin), están contribuyendo sustancialmente al desarrollo de iniciativas espaciales impulsadas por la IA, a menudo liderando la innovación.

Aunque la competencia es evidente, tanto a nivel nacional como privado, también hay casos de colaboración internacional en iniciativas espaciales impulsadas por la IA.

La diplomacia desempeñará un papel cada vez más importante en la gobernanza del espacio: las naciones y los consorcios

industriales se embarcan en misiones complejas, comparten trayectorias orbitales y pretenden explotar recursos fuera de la Tierra, por lo que la necesidad de normas, directrices y acuerdos claros adquiere gran importancia.

Es necesaria una nueva gobernanza espacial, con acuerdos internacionales y marcos de gobernanza que regulen las tecnologías espaciales de la IA en sectores controvertidos, como la gestión del tráfico espacial, la reducción de los desechos orbitales y la asignación del espectro.

Hasta ahora, el único derecho internacional que rige las actividades espaciales y proporciona algunos principios éticos y jurídicos generales es el Tratado sobre el Espacio Exterior (TES) de las Naciones Unidas.

El Tratado sobre el Espacio Ultraterrestre, formalmente conocido como *Tratado sobre los Principios que Deben Regir las Actividades de los Estados en la Exploración y Utilización del Espacio Ultraterrestre, incluso la Luna y otros Cuerpos Celestes*, fue adoptado por la Asamblea General de las Naciones Unidas y abierto a la firma el 27 de enero de 1967, y entró en vigor el 10 de octubre de 1967.

En síntesis, el TSO prohíbe el uso de recursos espaciales en conflictos bélicos; promueve la cooperación y el uso pacífico del espacio en beneficio de toda la humanidad; prescribe evitar la contaminación nociva del espacio y los cuerpos celestes y los cambios adversos en el medio ambiente de la Tierra; busca la coordinación de las actividades espaciales entre los Estados.

Algunas recomendaciones del Tratado sobre el Espacio Ultraterrestre son, sin embargo, obsoletas y corren el riesgo de ser superadas en la práctica por los hechos. Un ejemplo es la recomendación de que la Luna y otros cuerpos celestes no sean objeto de apropiación nacional por ningún medio, lo que contrasta evidentemente con los proyectos de minería comercial ya previstos, destinados a extraer y procesar materias primas en los asteroides.

También es necesaria una mayor gobernanza del espacio a escala internacional y nacional tras la creación de fuerzas espaciales o comandos espaciales dentro de los países, como respuesta a la evolución de la importancia estratégica del espacio y al reconocimiento de que las capacidades espaciales son fundamentales para la seguridad nacional. Varios países, como Estados Unidos,

China, Rusia, Reino Unido, Francia, Brasil y Japón, han creado entidades militares o de defensa dedicadas a las operaciones espaciales.

En el ámbito comercial, Estados Unidos cuenta con la *Commercial Space Launch Act*, aprobada originalmente en 1984 y modificada desde entonces, una ley que otorga al Departamento de Transporte de Estados Unidos la supervisión reguladora de los vuelos espaciales comerciales, indemniza a las empresas por grandes daños a terceros e informa las regulaciones para los vuelos espaciales humanos comerciales. En 2015, también se aprobó la Ley de Competitividad del Lanzamiento Espacial Comercial de EE. UU., diseñada para fomentar los vuelos espaciales comerciales y la innovación. Por cierto, esta ley concede a las empresas privadas el derecho a poseer los recursos recogidos en el espacio, como los materiales procedentes de la minería de asteroides, lo que contrasta de forma evidente con el Tratado sobre el Espacio Ultraterrestre de las Naciones Unidas.

Recientemente, el 23 de enero de 2024, durante la Conferencia Espacial Europea, funcionarios de la Comisión Europea anunciaron que están preparando la publicación, para marzo de 2024, de un borrador de la primera Ley Espacial Europea Completa.

Con el objetivo de construir un verdadero mercado único espacial en la UE, la ley debería ayudar a armonizar el actual «régimen espacial muy diverso» dentro de la UE, donde once Estados miembros tienen sus propias leyes nacionales sobre el espacio. La legislación propuesta se centrará en tres ámbitos: seguridad, resistencia y sostenibilidad, pero es probable que también contenga disposiciones sobre el uso de la inteligencia artificial en el espacio.

6. Conclusión

De lo expuesto hasta ahora se desprende que la IA, como en todos los demás ámbitos de nuestra sociedad, tiene el potencial de influir radicalmente en el futuro de las actividades espaciales y de convertirse en un poderoso catalizador de profundos cambios geopolíticos en la economía espacial.

A medida que las naciones aprovechan cada vez más las capacidades de la IA para la exploración espacial, las operaciones de satélites y los esfuerzos estratégicos, han surgido nuevas oportunidades de competencia, colaboración e innovación que refuerzan aún más el progreso de la nueva economía espacial.

Es probable que las naciones con capacidades avanzadas de IA obtengan una ventaja estratégica, no solo en la exploración del cosmos, sino también a la hora de asegurar sus intereses nacionales mediante capacidades espaciales mejoradas. La confluencia de la IA y las tecnologías espaciales está remodelando la dinámica de poder tradicional y fomentando una nueva carrera espacial en la que la destreza tecnológica en IA podría convertirse en sinónimo de influencia geopolítica.

Las implicaciones geopolíticas de la IA son aún más evidentes a nivel estratégico. A medida que el espacio se militariza cada vez más, la importancia estratégica de proteger los activos espaciales mediante tecnologías basadas en la IA adquiere una importancia capital. Las naciones están invirtiendo mucho en conocimiento de la situación espacial, ciberseguridad y sistemas autónomos para proteger su infraestructura espacial. El desarrollo y el despliegue de la IA en este contexto contribuyen a un creciente dominio de la seguridad nacional que se extiende más allá de las fronteras terrestres.

Junto a las numerosas ventajas, la IA también plantea muchas dudas e introduce nuevos riesgos potenciales, incluso en las actividades espaciales.

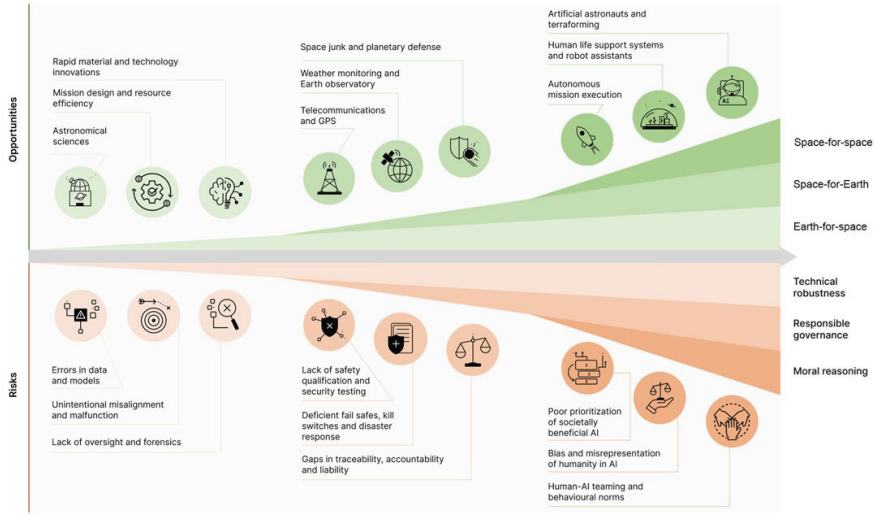


Figura 14. IA en el espacio: riesgos y oportunidades. Fuente: Frontiers. Disponible en: https://doi.org/10.3389/frspt.2023.1199547

El principal problema de los sistemas basados en la IA es que corren el riesgo de convertirse en «cajas negras», sistemas de los que podemos conocer los datos a la entrada y los resultados

o decisiones consiguientes, sin ninguna o poca visibilidad sobre el proceso decisorio. En esta situación, también es difícil, si no imposible, validar un proceso y corregir sus errores, o mejorarlo, porque el diagnóstico de un problema es difícil de realizar. Como consecuencia, esta falta de transparencia podría disminuir la confianza en los sistemas basados en IA, sobre todo en aplicaciones como las espaciales, donde la seguridad, la fiabilidad y la responsabilidad son esenciales, lo que plantea problemas éticos y normativos.

En términos más generales, la necesidad de explicabilidad en la IA es crucial en todas las aplicaciones en las que las decisiones afectan a las personas o a la sociedad en general.

Para arrojar algo de luz sobre el proceso de toma de decisiones de los algoritmos de IA, se está desarrollando la XAI.

XAI son las siglas de *Explainable Artificial Intelligence* (Inteligencia Artificial Explicable). Se refiere a un conjunto de técnicas y enfoques en inteligencia artificial (IA) y aprendizaje automático (AM) que pretenden hacer que los procesos de toma de decisiones de los sistemas de IA sean más comprensibles e interpretables por los humanos.

La XAI se centra en desarrollar modelos de IA que produzcan resultados fácilmente comprensibles e interpretables por los humanos, haciendo más transparente el funcionamiento interno del sistema de IA.

Los futuros marcos reguladores del espacio tendrán que incluir requisitos legales de transparencia y explicabilidad en los procesos de toma de decisiones, especialmente cuando los sistemas de IA afecten a la vida de las personas, a grandes responsabilidades económicas y a grandes riesgos financieros.

En general, el mayor riesgo asociado a la IA procede de sobreestimar sus potencialidades o de subestimarlas.

Los sistemas de IA nunca serán una alternativa completa al pensamiento humano: son como «sabios idiotas», con capacidades y habilidades fabulosas, derivadas del entrenamiento y el procesamiento de cantidades masivas de datos.

Van a cambiar radicalmente nuestras vidas, nuestra sociedad y el escenario geopolítico, en la Tierra y en el espacio, pero, como cualquier otra herramienta tecnológica, depende de nosotros utilizarlas sabiamente y mantenerlas bajo control.

Bibliografía

Agencia Espacial Europea. (2018). *Artificial intelligence for autonomous space missions*. [Consulta: 2024]. Disponible en: https://www.esa.int/Applications/Technology_Transfer/AIKO_Artificial_Intelligence_for_Autonomous_Space_Missions.

Agencia Espacial Europea. (2022). *Artificial intelligence in space*. [Consulta: 2024]. Disponible en: https://www.esa.int/Enabling_Support/Preparing_for_the_Future/Discovery_and_Preparation/Artificial_intelligence_in_space.

Boden, M. A. (s.f.). *Artificial Intelligence, a very short introduction*. Oxford University Press.

Carter, M. (s.f.). *Minds and computers*. Edinburgh University Press.

Cinelli, I. (2020). The Role of Artificial Intelligence (AI) in Space Healthcare. *Aerospace Medicine and HumanPerformance*. Asociación Médica Aeroespacial. Vol. 91, n.º 6, pp. 537-539(3).

Copeland, B. J. (2024). Artificial intelligence. *Enciclopedia Británica*. [Consulta: 2024]. Disponible en: https://www.britannica.com/technology/artificial-intelligence.

Fourati, F. y Alouini, M. (2021). *Artificial Intelligence for Satellite Communication: A Review*. [Consulta: 2024]. Disponible en: https://doi.org/10.48550/arXiv.2101.10899

Gal, G. A. *et al*. (2020). *Artificial intelligence in space*. ArXiv.

Garanhel, M. (2022). *AI applications in space exploration*. AI Accelerator Institute.

Hays, D. (2023). *AI Revolution in the New Space Economy: Transforming Business Strategies*.

Ieracitano, C. *et al.* (2022). *The use of artificial intelligence for space applications.* Springer.

Mazzolin, R. (2020). Artificial Intelligence and Keeping Humans «in the Loop». En: *Modern conflict and artificial intelligence.* Centre for International Governance Innovation.

Oficina de Asuntos del Espacio Ultraterrestre de las Naciones Unidas. (2022). *Space Law Treaties and Principles*. [Consulta: 2024]. Disponible en: https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties.html

Pandya, J. (2019). Geopolitics of artificial intelligence. *Forbes*.

Reiss, L. (2023). *4 Geopolitical Risks of the Rise of Artificial Intelligence (AI) for the Global Security*. Informe Atlas.

Richards, C. E. *et al*. (2023). *Safely advancing a spacefaring humanity with artificial intelligence.* Frontiers in Space Technologies.

Suess, J. (2019). *Jamming and cyberattacks: How space is being targeted in Ukraine*. Londres, Reino Unido. Royal United Services Institute.

Taulli, T. (2019). Artificial intelligence basics. *Apress*.

Weinzierl, M. y Sarang, M. (2021). The comercial space age is here. *HarvardBusinessReview.* [Consulta: 2024]. Disponibleen: https://hbr.org/2021/02/the-commercial-space-age-is-here,%202021.

Capítulo noveno

La huella medioambiental de la IA

David Ramírez Morán

Resumen

El impacto de la inteligencia artificial sobre el medioambiente es fruto de un amplio conjunto de factores bastante interrelacionados. Los requerimientos de energía, capacidad de procesado y refrigeración son los tres más directos, aunque hay otros factores, como la huella climática de las múltiples cadenas de suministro, las infraestructuras disponibles e incluso la regulación, que constituyen dimensiones relevantes en su desarrollo e implantación.

La sensibilidad existente actualmente en la población y en las organizaciones motiva que las empresas que proporcionan servicios estén haciendo constantes esfuerzos para reducir la huella climática de su actividad, a la vez que intentan minimizar los costes. Los esfuerzos se dirigen tanto a la optimización de sus propias operaciones como a la reducción de la huella en las cadenas de suministro. El objetivo es mostrar públicamente compromiso con el planeta, conseguir que el uso de sus servicios no afecte negativamente a la huella climática de la actividad de sus clientes y que incluso la reduzca, promoviendo así el uso intensivo.

Los escenarios futuros parecen augurar un crecimiento importante del uso de IA en muchos sectores, con soluciones que

pueden imponer restricciones adicionales como latencia limitada, necesidad de confinar geográficamente los datos o medidas que aseguren el estricto cumplimiento de las normas de privacidad y no discriminación.

Todos estos factores configuran un entorno de competencia internacional en el que pueden estar en juego la autonomía y soberanía estratégica de los países.

Palabras clave

Inteligencia artificial, Medioambiente, Huella de carbono, Competencia internacional.

Environmental footprint of artificial intelligence

Abstract

The impact of artificial intelligence on the environment is the result of a wide range of interrelated factors. Energy requirements, processing capacity and cooling are the three most direct, although there are other factors, such as the climate footprint of multiple supply chains, available infrastructures and even regulation, which constitute relevant dimensions in its development and implementation.

The current sensitivity of the population and organisations means that companies providing services are making constant efforts to reduce the climate footprint of their activity, while at the same time trying to minimise costs. Efforts are directed both at optimising their own operations and reducing the footprint in supply chains. The aim is to publicly show commitment to the planet, to ensure that the use of their services does not negatively affect the climate footprint of their customers' activity and even reduce it, thus promoting intensive use.

Future scenarios seem to portend significant growth in the use of AI in many sectors, with solutions that may impose additional constraints such as limited latency, the need to geographically confine data, or measures to ensure strict compliance with privacy and non discriminatory regulations.

All these factors shape an environment of international competition in which autonomy and strategic sovereignty of the countries may be at stake.

Keywords

Artificial intelligence, Environment, Carbón footprint, International competition.

1. Introducción

El impacto sobre el medioambiente de las actividades humanas ha recibido una creciente atención durante las últimas décadas. En la actualidad, la emergencia climática se ubica con frecuencia en los primeros puestos de las encuestas a la población sobre los factores de riesgo para las sociedades, y es tema de discusión en la práctica totalidad de los foros internacionales.

La inteligencia artificial irrumpe en este contexto con unos antecedentes que, entre la población general, despiertan preocupación. El elevado consumo de energía necesario para el minado de criptomonedas basadas en pruebas de trabajo, como bitcoin o ethereum, ha generado alertas sobre las consecuencias que los elevados requerimientos de capacidad de cálculo de la inteligencia artificial pueden suponer para el medioambiente. Esto ha llevado a los principales actores a tomar medidas para reducir la huella medioambiental relacionada con los centros de datos en los que se alojan los dispositivos que realizan las operaciones necesarias. Se persigue reducir la cantidad de energía necesaria tanto para la computación de los resultados como para refrigerar los dispositivos que los evalúan. Esta reducción se traduce en una menor emisión de gases de efecto invernadero y también en una reducción de los costes asociados.

El problema no se puede circunscribir a los centros de datos y a actuar sobre lo que albergan, sino que se está dando un paso más. Las mejoras marginales que se obtienen actualmente con nuevos desarrollos en estas infraestructuras deben coordinarse con medidas adicionales relacionadas con las cadenas de suministro de energía y equipamiento, así como con la gestión del ciclo de vida de este.

En la búsqueda de soluciones, son muy diversas las aproximaciones adoptadas, sin ser exhaustivo, desde el desarrollo de procesadores más eficientes, el diseño de los centros de datos, el uso de refrigeración líquida, el origen de la energía utilizada, hasta la ubicación de los centros de datos para el aprovechamiento de fuentes de energía, naturales o artificiales, o de otros recursos o infraestructuras. Cada una de estas soluciones llega en muchos casos acompañada de problemas adicionales que limitan la viabilidad y el impacto sobre la huella de carbono que permiten alcanzar.

Por otro lado, la inteligencia artificial en sí misma también puede contribuir a la reducción de la huella climática de la actividad

humana desde varios frentes. Como consumidor importante de energía, puede jugar un papel estabilizador en el aprovechamiento de las fuentes renovables, pues su consumo es menos cíclico que el de la actividad humana y puede aprovechar el exceso de capacidad energética de una región cuando el resto de consumos se reduce. La conectividad global también permite trasladar el procesado de un lugar a otro con relativa facilidad, por lo que es posible aprovechar capacidad de proceso remota para conseguir una menor huella medioambiental.

La generalización del uso de la IA y la creciente dependencia de la disponibilidad de estas infraestructuras impone un requerimiento adicional en la resiliencia ante fallos y averías, que se traduce, a su vez, en necesidades de equipamiento adicional que también puede contribuir a la reducción de la huella energética de las instalaciones, entre otras ventajas que puede aportar la IA en la reducción de la huella climática de la actividad humana.

Los resultados proporcionados por la IA también contribuyen a la reducción de la huella medioambiental de la actividad humana. Sus capacidades de tratamiento de la información permiten identificar e implantar mecanismos para optimizar e incrementar la eficacia de las actividades y gestionar mejor la distribución y consumo, controlando cómo y de dónde se consume la energía.

La introducción paulatina de la IA en ámbitos de la sociedad alejados de la propia tecnología hace que la reducción de su huella medioambiental resulte, a su vez, de interés para aquellas empresas que hacen uso de ella. Cada vez hay una atribución más precisa de la huella de carbono de la aplicación de IA a lo largo de las cadenas de suministro y es necesario contabilizarla para evaluar la huella de carbono global de las organizaciones. Una huella nula o negativa del proceso de inteligencia artificial, junto con la optimización, fruto de su aplicación, de los procesos de las actividades principales de las organizaciones constituyen una ventaja competitiva e incrementa la sostenibilidad.

Sin embargo, no es posible alcanzar la eficiencia máxima porque otros factores también afectan a la viabilidad técnica o regulatoria de la implantación de soluciones que reducen la huella medioambiental. La menor latencia con la que hay que enviar resultados a los terminales está haciendo que la capacidad de cálculo se desplace desde los centros de datos al borde de la red, acercándola al terminal. La desconcentración de la capacidad de cálculo hace menos viables medidas de escala en la reducción de consumo u optimización de la refrigeración de los equipos.

Las regulaciones de protección de datos y privacidad también imponen limitaciones a la circulación de los datos. Pueden restringir la zona geográfica donde pueden ser almacenados y procesados. Así, deja de ser posible elegir dónde procesar la información sobre la base de criterios medioambientales y hay que tener en cuenta las limitaciones adicionales para ubicar el tratamiento de la información.

La preocupación creciente por la seguridad y privacidad de la información impone también restricciones de diversa naturaleza a la utilización de soluciones en la nube cuya implementación, por efectos de escala puede alcanzar mayores grados de eficiencia que la de centros de datos privados más pequeños.

Las soluciones aplicadas también dependen de la disponibilidad de equipamientos o infraestructuras que permitan implantarlas de forma viable en términos económicos.

El libre acceso a tecnologías, la disponibilidad de infraestructuras, las normativas de aplicación y las condiciones naturales se convierten así en dimensiones estratégicas que configuran los límites en los objetivos a los que pueden optar los diferentes países en la implantación y uso de la inteligencia artificial en su territorio.

Por último, no hay que olvidar las cuestiones políticas y geográficas que imponen condiciones de contorno infranqueables como el clima de la propia ubicación, la posibilidad de uso de energía nuclear o el acceso a agua o a fuentes renovables.

2. El consumo de la inteligencia artificial

La Agencia Internacional de la Energía cifra el consumo energético de los centros de datos, las criptomonedas y la inteligencia artificial, en 2022, en 460 TWh a nivel mundial, lo que supone un 2 % de la demanda global de energía (Agencia Internacional de la Energía, 2023). Esta cantidad se vería incrementada en un consumo equivalente al de toda Suiza o Alemania de cumplirse las previsiones de incremento para 2026.

A esta cantidad sería necesario incorporarle los consumos de los equipamientos involucrados en el ciclo de la información. La IA multiplica la cantidad de información que se puede procesar, lo que hace viable considerar un volumen de información mucho más amplio y diverso para la toma de decisiones. Pero, para poder actuar, es necesario recopilar la información para su procesado y uso. Es preciso establecer una cadena completa formada

por los sensores que captan la información, los dispositivos que la registran y transmiten a un nodo central cuando es pertinente y el nodo que recibe la información, la procesa y hace accesibles los resultados para que otros procesos los puedan utilizar. Ejemplo de estos equipamientos son las cámaras que recogen la actividad de las ciudades, sensores de variables meteorológicas o lumínicas, etc. así como toda la infraestructura necesaria para el transporte de la información que generan hasta donde es procesada.

Según un informe de PitchBook, para 2025, el 3,2 % de todas las emisiones de carbono del mundo provendrán de granjas de servidores de IA y «su costo ambiental no hace más que crecer a medida que la industria crece de una manera que prioriza la expansión en lugar de la eficiencia» (Bécares, 2023).

Las virtudes de la IA generativa se basan en procesados muy intensivos de la información, tanto en el proceso de entrenamiento como en la generación de resultados a petición de los usuarios. Ambas escalas no son comparables pues las dimensiones en las que generan cifras preocupantes son diferentes. En el caso del entrenamiento, requiere una elevada capacidad de procesado puntual, una vez, mientras que, para la generación de resultados, el riesgo proviene del número de peticiones realizadas por los usuarios. Por bajo que sea el consumo necesario para la generación de un resultado, cada vez serán más sistemas y cuestiones las que hagan uso de IA, resultando en un número de peticiones siempre creciente. Incluso las cuestiones más básicas podrían responderse recurriendo a IA, haciendo que cualquier actividad requiera gran número de consultas (Ramírez Morán, 2023).

Comparando las búsquedas tradicionales con consultas a modelos grandes de lenguaje como ChatGPT, un representante de Alphabet estimaba un coste diez veces superior con un consumo de hasta 3 Wh. Si cada búsqueda pasase a ser una consulta, la electricidad necesaria para dar las respuestas ascendería a 29,3 TWh al año, equivalente al consumo de un país como Irlanda (Robinson, 2023). Ante estos datos preocupantes, también hay motivo para albergar cierta esperanza pues entre 2010 y 2018 se quintuplicó la carga de trabajo de los centros de datos aunque el consumo de electricidad solo se incrementó en un 6 % (Chernicoff, 2023).

Respecto al consumo de energía de la utilización de sistemas ya entrenados, un estudio elaborado por profesores de universidades

americanas concluye que las emisiones de carbono asociadas a la escritura e ilustración son menores para la inteligencia artificial que para los seres humanos cuando se tiene en cuenta el consumo de los dispositivos utilizados (Tomlinson *et al.,* 2023). Una revisión crítica de este estudio destaca cómo se ha obviado la energía requerida por el entrenamiento de los sistemas de inteligencia artificial, los que generan el texto y las imágenes, que debe repercutirse en la elaboración de los contenidos (Mann, 2024).

Pero la energía no es el único consumo que está disparando las alertas medioambientales. El mercado de refrigeración de centros de datos en Europa alcanzó en 2020 los 3500 millones de dólares y se estimó un incremento anual de 2021 a 2027 de un 15 % adicional cada año (*Savills research*, 2023). El uso de agua para la refrigeración de los centros de datos es cada vez con más frecuencia un recurso escaso, especialmente cuando debe cumplir ciertos requisitos de calidad (Hidalgo García). En 2018, los centros de datos figuraban entre los diez principales consumidores de agua de los Estados Unidos, con un consumo de 513 millones de m^3, de los que una cuarta parte se utilizaban directamente para labores de enfriamiento directo (Siddik *et al.,* 2021).

CNDCP, una iniciativa autoregulatoria, presentó a la Comisión Europea un objetivo para 2040 de reducir el consumo de agua a 400 ml por MWh de energía de computación, objetivo muy ambicioso, pero que permite dirigir el trabajo y hacer un seguimiento de la evolución del sector (*Savills research*, 2023).

El problema del consumo de agua no se ha limitado a los ámbitos profesionales, sino que está llegando a la prensa general con noticias sobre los impactos[1] de centros de datos ubicados en zonas donde se producen sequías con frecuencia[2]. Tomando como ejemplo la costa oeste norteamericana, se observa cómo cerca de los polos tecnológicos de California, el problema de sequias es muy grave y puede afectar directamente a la instalación de centros de datos en esas zonas.

Tanto Meta como Intel declaraban que perseguían hacerse positivos en agua, proporcionando más agua de la que consumían, para 2030 (Robinson, 2022).

[1] Disponible en: https://www.newsweek.com/google-building-2-data-centers-which-require-heavy-water-use-drought-stricken-town-1647727.

[2] Véase en: https://time.com/5814276/google-data-centers-water/.

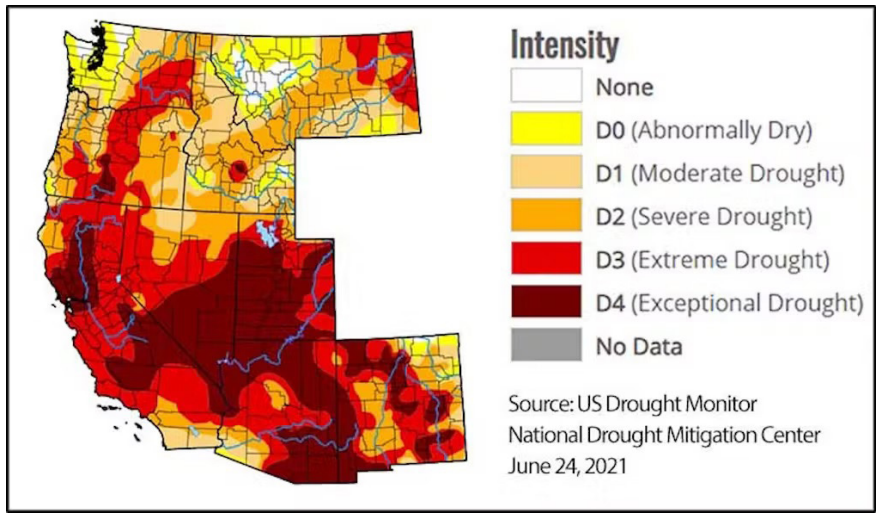


Figura 1

El informe del *think tank* Center for Data Innovation alerta sobre los riesgos que un exceso de regulación sobre la inteligencia artificial puede suponer para el compromiso entre los requerimientos de energía del modelo y la seguridad del sistema, con la implementación de técnicas de eliminación del sesgo y de salvaguardas que comprueben que los contenidos generados por los LLM no sean dañinos o contrarios a la ley (Castro, 2024: 13). Estos mecanismos imponen un consumo adicional de recursos que no contribuye directamente a la obtención de los resultados.

3. Reduciendo la huella medioambiental de la IA

La reducción de la huella de carbono de los centros de datos es un fin de los proveedores de servicios para que la utilización de sus productos no suponga un incremento de la huella de carbono de aquellas empresas que los incorporen a sus procesos de producción. Supondría una barrera a salvar para la incorporación de la tecnología a los procesos, mientras que el aún incipiente catálogo de funcionalidades que llevará a cabo la inteligencia artificial permite prever un uso cada vez más intensivo y extensivo de la tecnología. Los esfuerzos de los proveedores constituyen, a su vez, una barrera por cuanto conseguir los elevados niveles de eficiencia energética fruto de su creciente experiencia resulta en muchos casos inalcanzable para equipos que desarrollaran las funcionalidades de inteligencia artificial en sus propios centros de

datos. Se fomenta así la migración a la nube frente al desarrollo e instalación local de la tecnología.

A la hora de evaluar la huella medioambiental de la actividad de una organización, se definen tras ámbitos diferenciados, *scopes,* en inglés, correspondientes a la huella de la propia actividad de la compañía, *scope* 1, a la huella ambiental de los proveedores de recursos energéticos, o *scope* 2, y a la huella ambiental asociada a los proveedores de la empresa, *scope* 3, que aglutina la huella de fabricación y transporte de los productos que la empresa adquiere para realizar sus actividades. A través de estos ámbitos, es posible atribuir con precisión el origen de la huella medioambiental a lo largo de la cadena de valor de los productos y servicios.

Una actuación concienciada respecto al respeto al medioambiente es necesaria en todos los puntos de la cadena de valor. Desde la fabricación y distribución a la operación y posterior deshecho, es preciso mantener, en todo momento, una aproximación sostenible, tendente a la economía circular, en la que se minimizan los residuos, se favorece el reciclado y la recuperación de materiales y se persigue la minimización de los residuos que finalmente no pueden ser aprovechados o tratados.

3.1. Reducción de la huella de las fuentes de energía

El origen de la energía que alimenta el centro de datos también está tomando una importancia sustancial ante las crecientes imposiciones legales o voluntarias en relación con la huella de carbono. La generación de gases de efecto invernadero se evalúa en distintas dimensiones del modelo de negocio. La primera contribución proviene de la energía estrictamente necesaria para llevar a cabo las operaciones requeridas para la prestación del servicio.

Equipos más eficientes energéticamente y algoritmos más optimizados permitirán reducir el consumo exigido para el cálculo de los resultados de las peticiones. En un segundo escalón se sitúa el consumo auxiliar imprescindible para el funcionamiento de los sistemas. Dentro de esta categoría se incluirían consumos como el necesario para la refrigeración del centro de datos, así como la eficiencia energética de la infraestructura en términos de pérdida de energía por su transformación, su aseguramiento con sistemas de alimentación ininterrumpida o las pérdidas propias de la distribución a los múltiples equipos existentes en el centro

de datos. En un tercer escalón entra en juego la huella climática asociada a los proveedores de equipos, de construcción del centro de datos, de los suministros y el reciclaje de los residuos, etc.

En Estados Unidos se está planteando la construcción de los centros de datos en las proximidades de centrales energéticas ya existentes para reducir la carga sobre la red de distribución general que supone un centro de consumo tan intenso, mediante la construcción de conexiones dedicadas entre el centro de datos y la central. Se reducen así las pérdidas de energía debidas a su transporte a larga distancia, y se consigue también un incremento de la fiabilidad de la fuente de energía al utilizar infraestructuras dedicadas con las que se eliminan riesgos como la demanda variable y, por su menor complejidad, los asociados al mantenimiento.

Dos son las aproximaciones nucleares, por su reducida huella de carbono, que se están considerando. La primera es ubicar los centros de datos en las proximidades de centrales cuya capacidad no está plenamente explotada, de forma que la construcción de una línea dedicada que conecte la central eléctrica al centro de datos sea viable económicamente.

Por otro lado, las propuestas de nuevas centrales nucleares de un tamaño menor, bajo el modelo de reactores modulares pequeños, plantean la posibilidad de ubicar la central energética nuclear junto al propio centro de datos, en lo que se denomina colocalización (Chernicoff, 2023), con las ventajas antes reseñadas de emisión nula de carbono, menores pérdidas de transmisión, bajo coste y fiabilidad. Actualmente, el concepto de SMR (*Small Modular Reactors*), como los que alimentaban buques de guerra americanos desde los años cincuenta, no está completamente desarrollado, aunque, de resultar de interés en sectores como el del procesado de información, con las expectativas de crecimiento y estabilidad de demanda que presenta, podría acelerar el desarrollo de soluciones. En la actualidad hay varios SMR en construcción o esperando licencia en Argentina, Canada, China, Francia y Corea del Sur, aunque se encuentran todavía a años vista de su pleno rendimiento (Mann, 2022).

En todo caso, la contratación de suministros de energía de fuentes renovables a los proveedores tradicionales ya contribuye a limitar el impacto sobre el medioambiente de los centros de datos. La instalación de fuentes renovables en las propias instalaciones o en las proximidades también contribuye a la reducción de la huella energética de los centros de datos.

3.2. Mejora de las prestaciones de los equipos

La carrera tecnológica que se está produciendo en las dimensiones de los transistores que forman los circuitos integrados que procesan la información también tiene un trasfondo energético. Un menor tamaño del dispositivo reduce su capacidad eléctrica, por lo que la carga que es necesario inyectar o extraer del dispositivo cada vez que conmuta su valor lógico es más pequeña. La reducción de la carga que debe moverse conlleva una reducción de las corrientes que deben circular por los conductores de los circuitos integrados y, por tanto, una reducción de las pérdidas de energía que se traducen en calor. En definitiva, una tecnología de menor tamaño permitirá hacer las mismas operaciones con un menor consumo de energía o, equivalentemente, realizar más operaciones ante la misma disipación de calor, ser más eficientes. Pero no es posible reducir sin límite el tamaño de los dispositivos porque ya se está alcanzando el límite físico por el que los transistores, que deben funcionar como interruptores abiertos o cerrados, dejan de realizar correctamente su función debido a efectos cuánticos asociados al reducido número de átomos que forman los elementos semiconductores y aislantes de los dispositivos.

3.3. Reducción del impacto de fabricación

En un solo trimestre, una fábrica de chips produce casi 15 000 t de residuos, el 60 % peligrosos, así como un consumo de 927 millones de galones de agua, suficientes para llenar 1400 piscinas olímpicas (Belton, 2021). Cifras como estas justifican el importante esfuerzo realizado por las compañías para reducir el impacto. En 2022, Intel informaba de una reducción de un 4 % de generación de gases de efecto invernadero, en la senda de reducirlos un 10 % de 2019 a 2030, mientras que la energía que consumía provenía ya en un 93 % de fuentes renovables. También para 2030 se había fijado como objetivo reducir a cero la generación de gases de efecto invernadero de su cadena de suministro.

3.4. Optimizar la refrigeración de los centros de datos

Incluso evaluar el consumo instantáneo de los equipos dentro del centro de datos se convierte en un problema cuando se imponen las condiciones necesarias para asegurar la privacidad de la

información. Los equipos actuales incorporan numerosos mecanismos para poder evaluar su consumo instantáneo. El problema surge ante la necesidad de comunicar esta información hacia los dispositivos de control ambiental y de consumo eléctrico en un contexto donde la privacidad de los datos limita las conexiones que pueden realizar los equipos hacia el exterior.

Para hacer frente al problema que supone optimizar la refrigeración del centro de datos sin tener información sobre el consumo instantáneo de cada uno de los equipos que están operando en su interior, se recurre nuevamente a la IA con proyectos como el llevado a cabo por IBM en colaboración con la empresa japonesa NTT (Sharwood, 2024). Consiste en estimar el consumo de los equipos del centro de datos a partir de medidas de temperatura, humedad y flujo del aire en el centro de datos externas a los propios equipos de procesado de información. De esta forma, se conserva el aislamiento de los datos de los equipos a efectos de cumplimiento, desde la no conexión de dispositivos ajenos, la preservación del cifrado y la desconexión de redes ajenas a aquellas por las que circulan los datos. También se elimina la necesidad de que los equipos determinen su temperatura y la transmitan a los equipos de control de refrigeración del centro de datos.

En esta búsqueda de soluciones óptimas, Meta ha estado probando a elevar la temperatura de sus centros de datos hasta alrededor de 32° para reducir la necesidad de enfriamiento y, con ello, el consumo de agua y energía (Robinson, 2022).

3.5. Reducción de la emisión directa

Los centros de datos requieren la generación de energía en sus propias instalaciones para poder hacer frente a una pérdida del suministro de energía eléctrica. Para ello, deben contar con generadores que tradicionalmente han utilizado como combustible gasóleo. Se están probando nuevas soluciones para reducir las emisiones de estos equipos, que van desde la utilización de biocombustibles (Miller, 2022) hasta la instalación de pilas de combustible alimentadas por hidrógeno (Roach, 2020).

3.6. Deshacerse del calor del centro de datos

En lugar de disipar el calor residual del centro de datos, emitiéndolo sin más al ambiente, se consideró aprovechar este calor para otros fines. Son varios los proyectos que trabajan en esta

línea proporcionando agua caliente y o calefacción a ciudades cercanas a la ubicación del centro de datos. Sin embargo, no se trata de una solución aplicable de forma general pues requiere una infraestructura importante para llevar el calor desde el centro de datos a los destinatarios[3]. Esta infraestructura existe en algunas ciudades del norte de Europa y es allí donde se han implantado soluciones.

En esta línea, la Unión Europea, en la última revisión de la Directiva de Eficiencia Energética[4], estipula que los centros de datos con capacidad de procesado igual o superior a 1 MW deberán «tener en cuenta las mejores prácticas del código de conducta europeo en eficiencia energética de centros de datos», lo que significa implementar sistemas de recuperación de calor o demostrar que no era viable.

El Instituto Uptime estimaba (Smolaks, s.f.) en sesenta el número de proyectos de recuperación de calor en territorio europeo, mientras que en Estados Unidos solo hay seis proyectos actualmente y once se encuentran en desarrollo.

En Corea del Sur también se ha adoptado una aproximación novedosa por la que se colocalizan centros de datos y plantas de tratamiento de aguas residuales para reducir la energía necesaria para el tratamiento y aprovechar parte de las aguas tratadas para el enfriamiento del centro de datos (Robinson, 2022).

3.7. Inmersión de centros de datos en masas de agua

La inmersión del equipamiento de computación en grandes masas de agua es otra de las alternativas que se ha estudiado para eliminar el consumo y los costes de la refrigeración. Microsoft lideró una iniciativa, el proyecto Nattick[5], para evaluar las ventajas y la viabilidad de una solución técnica en este sentido. Los resultados fueron bastante buenos pues, no solo se consiguió el correcto funcionamiento del sistema durante todo el experimento, sino que se comprobó cómo los equipos incluidos en el contenedor habían tenido un número de averías inferior al de los ubicados en centros de datos tradicionales.

[3] Disponible en: https://www.theregister.com/2023/12/08/reusing_datacenter_heat_is_tricky/.

[4] Véase en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2023_231_R_0001&qid=1695186598766.

[5] Disponible en: https://natick.research.microsoft.com/.

3.8. El deshecho del material de computación

No puede olvidarse que todo sistema tiene un ciclo de vida desde su incepción hasta su eliminación. Los equipos e instrumentos que posibilitan y dan soporte a una tecnología tienen un ciclo de vida que requiere una evaluación de su impacto medioambiental desde la obtención de las materias primas, a partir de las que se construirán los equipamientos, hasta la eliminación de los residuos que se generan.

La basura tecnológica es un problema identificado. Frente a este se plantea la solución del reciclaje, aunque, debido a la escala y complejidad que conlleva, es una solución que, aunque factible, no está siendo explotada actualmente en su máxima expresión. De hecho, son muchos los problemas que este tipo de basura está generando a nivel internacional porque aquellas tareas asociadas a la separación y reciclado de los materiales están siendo desdeñadas por los países más desarrollados. Se están estableciendo procedimientos para el deshecho de este tipo de materiales sin efectuar su reciclado en origen, enviándolos por diferentes procedimientos a otras zonas del globo en las que se tratan de manera menos eficiente. En estas zonas se genera una extracción menos respetuosa con el medio ambiente y con menor eficiencia. Sin embargo, la diferencia de costes de mano de obra, dado que se recurre a personal de muy baja cualificación en condiciones de trabajo insalubres, en muchos casos, se utiliza como argumento para justificar estas medidas que, orquestadas alrededor del reciclaje, son realmente malas soluciones a un problema complejo.

Sería necesaria una normativa que introduzca la simplificación del proceso de reciclado en el desarrollo de productos con tiempos de vida relativamente limitados, como son los aparatos electrónicos. Además de promoverse el reciclado de acuerdo con normativas que eviten la generación de basura tecnológica descontrolada, debería simplificarse el propio proceso de reciclaje y que sea posible incluso construir una industria a su alrededor que, de forma respetuosa con el medio ambiente, se aproveche de la reciclabilidad por diseño, para conseguir un elevado porcentaje de recuperación de materiales. Son materiales en muchos casos de gran valor, como son los metales preciosos o las tierras raras. Además, se encuentran en concentraciones muy elevadas y sometidos a procesos tanto físicos como químicos conocidos, lo que permitiría diseñar procesos de separación y purificación muy específicos y eficientes.

Los materiales recuperados resultantes podrían reintroducirse en las cadenas de producción para la fabricación de nuevos equipos sin necesidad de recurrir a las costosas operaciones de obtención en la naturaleza. Los plásticos con los que se fabrican las carcasas y soportes de los dispositivos son un ejemplo de cómo se está orientando la industria hacia estos objetivos, rescatando incluso residuos plásticos costeros para su fabricación[6].

Para las empresas, el coste asociado a la implantación de estas técnicas de diseño, donde deben quedar documentados los procesos aplicados a las materias primas, deben generar un beneficio que puede provenir por la vía de una reducción de la huella ambiental de la empresa, por la bajada de precios de las materias primas o por los beneficios que pueden obtener de encargarse de la gestión del reciclaje de sus propios equipos, añadiendo una actividad más al ciclo de prestación de servicios de sus productos. En caso de no poder alcanzarse este objetivo, podrían ser los Estados los encargados de implantar la normativa que obligara a la aplicación de estas medidas. Sin embargo, esta última vía se presta nuevamente a la aparición de contrastes por la aplicación de normativas de carácter nacional o regional diferentes en lugares distintos del globo.

4. Intereses y limitaciones nacionales

Ante el elevado incremento del consumo energético dedicado a tecnologías de la información, son necesarias medidas gubernamentales para dar soporte a la necesidad de generación y distribución de la energía eléctrica necesaria.

Son varios los países que han implantado moratorias a la instalación de centros de datos en sus territorios, en atención al incremento del consumo energético que conllevan, así como a la mayor demanda que depositan sobre las redes de distribución. Los derechos de consumo industrial se están convirtiendo en objeto codiciado por las diferentes empresas dedicadas a los centros de datos.

Aquellos países con redes eléctricas más eficientes y actualizadas pueden ser polos de atracción para los nuevos centros de datos debido a la mayor fiabilidad que la provisión de energía proporciona. Por el contrario, los países que cuentan con infraestructuras de generación y distribución de la energía más precarias podrían ver mermado su atractivo para las empresas.

[6] El plástico reciclado llega a ordenadores y periféricos. Veáse en: https://plasticos-reciclados.es/2022/07/recycled-plastic-arrives-to-computers/.

España se está haciendo hueco entre los principales anfitriones de centros de datos europeos, al lado de países como Holanda, Alemania, Francia, Italia… Los motivos para ello son su ubicación geográfica estratégica, que hacen del país un lugar propicio para la terminación de grandes cables submarinos, así como para la implantación de fuentes de energía renovables como paneles solares o generadores eólicos o en el mar.

La ubicación geográfica de España la situa en una excelente posición para competir internacionalmente. De hecho, se espera un crecimiento a altas tasas los próximos años debido a su ubicación, que motiva, a su vez, su conectividad a traves de multiples cables submarinos, la elevada capacidad de energía renovable y la creación reciente de regiones de nube por los principales proveedores. Todo ello con el respaldado gubernamentalmente con el plan España Digital (DatacenterDynamics).

La Comunidad de Madrid ha expresado su preocupación ante las limitaciones que la red nacional de distribución de energía puede suponer para el atractivo industrial de la región para la implantación de nuevos centros de datos en su territorio (Álvarez *et al.,* 2023). El consumo de este tipo de instalaciones requiere de una red de transporte que le de soporte y, en la actualidad, no hay suficiente provisión para hacer frente a la solicitud por parte de distintos operadores de autorizaciones de consumo de energía. Se trata de una muestra de la importancia que la red de distribución, de titularidad pública, en la mayor parte de los casos, supone para un sector tan eminentemente privado como es el de los centros de datos.

En el caso de los Países Bajos se han dado los primeros casos de rechazo social a la implantación de centros de datos que pueden afectar a la disponibilidad energética por el creciente consumo de energía. Los planes de Meta para construir allí un centro de datos se han trasladado a la localidad de Talavera de la Reina (Jiménez Arandia, 2024). Se beneficia así España de las restricciones de otros países por motivos energéticos o de otro tipo (DatacenterDynamics).

5. Contribución de la inteligencia artificial al medio ambiente

En contraste con el impacto que la inteligencia artificial tiene sobre el medioambiente, también proporciona mecanismos que permiten reducir la huella climática de la actividad humana.

La aplicación de esta tecnología a cuestiones como el control ambiental y lumínico de edificios o la optimización de los consumos de energía para adaptarlos a las condiciones climáticas o de las infraestructuras resultan en beneficios para el medioambiente basados en dos premisas: la reducción del consumo total y la optimización del consumo para aprovechar al máximo las capacidades disponibles y ajustarlo a las condiciones específicas de cada momento.

La irrupción de la red inteligente o smart grid para la gestión de la energía supuso un punto de inflexión. El control tradicional de los equipamientos se hacía generalmente por franjas horarias definidas y mediante la aplicación de márgenes de temperatura controlados por termostatos. La introducción de la inteligencia artificial permite introducir nuevos paradigmas en la gestión de instalaciones como son el confort térmico y lumínico. En lugar de fijar una temperatura óptima general, esta se irá adaptando a las condiciones climáticas de forma automatizada, mediante algoritmos que determinan la temperatura y humedad óptimas.

Pero el consumo y la huella de carbono de los centros de datos no es la única relación de la inteligencia artificial con su huella. La propia IA se puede utilizar para la optimización de procesos industriales. Son muchas las soluciones que se están proponiendo en esta línea. El control del consumo de energía por intervalos se ha convertido en una medida de optimización de la generación eléctrica porque es posible controlar la carga de forma que, en los momentos de más demanda, algunos de los principales consumidores puedan reducir consumos instantáneos para descargar la red, o bien aprovechar momentos de alta capacidad de generación pero bajo consumo para realizar tareas con altos requerimientos de energía a precios más reducidos y aprovechando la capacidad disponible.

Para las redes de suministro, tan importante como las fuentes de energía son los consumidores que la demandan. Por tratarse de un sistema que debe estar equilibrado, en el que el consumo instantáneo debe coincidir con la energía generada:

> «En algunos sistemas eléctricos, los centros de datos pueden ser capaces de ayudar a balancear es sistema o proveer otros servicios. En Irlanda, por ejemplo, la eólica ostenta un significativo y creciente porcentaje de la generación de energía (28 % en 2018). Sin embargo, gran parte de esta potencia eólica se genera por la noche, cuando la demanda de

> energía es baja en los sectores comercial y residencial. Con demanda nocturna sostenida, los centros de datos pueden absorber el exceso de suministro e incrementar la utilización de la electricidad de fuentes eólicas».

Además, los centros de datos podrían jugar un importante papel en la respuesta por el lado de la demanda. Aunque típicamente tienen un perfil de petición de energía estable, los grandes centros de datos están altamente automatizados y monitorizados, haciéndolos potencialmente más flexibles y adaptables en comparación con instalaciones industriales tradicionales. La regulación y las señales de precios pueden ayudar para sacar partido a este potencial (Kamiya *et al.,* 2019).

El Gobierno de Irlanda, dentro de los requisitos para la autorización de la construcción de un centro de datos, impone tres condicionantes relativos al suministro de energía de los que el tercero va precisamente en esta línea, requiriendo la flexibilidad de la demanda de energía, reduciéndola cuando así lo solicite un operador del sistema eléctrico (Agencia Internacional de la Energía, 2023).

Con la llegada de la IA y otras tecnologías habilitadoras aplicadas a la mejora de la eficiencia y sostenibilidad, se abren nuevos caminos como la denominada *Twin Transition,* clave para una industria digital y descarbonizada, o las ciudades inteligentes, que permitirán reducir la contaminación ambiental con medidas como la mejor gestión del tráfico y de los transportes públicos.

6. La economía de la empresa en la gestión de la inteligencia artificial

Cuestiones que se separan de la tecnología también tienen su impacto sobre la huella medioambiental de la IA. Detrás de las soluciones actuales se encuentran empresas privadas cuyo objetivo son los beneficios. Por ello, van a gestionar el negocio de forma que se maximicen sus intereses, lo que dará lugar a políticas que aumenten la salud financiera de la empresa, que reduzcan sus costes y de las que podrán hacer uso mediante una conveniente comunicación a la sociedad para respaldar su forma de actuar.

La preocupación por los riesgos en los que se incurre con la implantación de la IA es generalizada. Hay dos cuestiones especialmente relevantes en las que la regulación está incidiendo

más con respecto a la IA generativa actual. Son la eliminación de sesgos por motivos como la raza, la religión o la ideología, y la prohibición de la generación de contenidos ilegales o fraudulentos.

Sin entrar en detalles tecnológicos sobre cómo abordar estos problemas, es necesario implantar en los sistemas de IA los mecanismos que aseguren el cumplimiento normativo a estos efectos, sin menospreciar el impacto social que podría suponer un flagrante incumplimiento de alguno de los principios. Los mecanismos requieren la aplicación de algoritmos que filtren las peticiones inapropiadas y que evalúen los resultados generados antes de remitirlos al usuario. La capacidad de cálculo que necesitan no contribuye directamente a la generación de resultados y suponen un uso adicional de recursos de computación para cada petición servida. Las empresas han destacado este último mensaje (Castro, 2024), incidiendo sobre el aumento del consumo de energía y de necesidad de refrigeración que supone, para abogar por un proceso legislativo que tenga en cuenta el impacto para el medioambiente que puede tener una legislación demasiado estricta.

El compromiso entre las restricciones impuestas y su viabilidad técnica queda también relacionado con los costes en necesidad de infraestructura y de consumo de energía para computación y refrigeración en que tienen que incurrir las empresas.

En términos puramente económicos, las empresas también están implantando políticas que responden a una maximización de la eficiencia de costes. La adquisición y amortización de los equipos informáticos constituyen dos de las principales cuentas en los balances de las empresas. Pequeñas variaciones en cualquiera de estos ámbitos, debido al elevado volumen que manejan en su operación, suponen diferencias sustanciales en los resultados empresariales y, por tanto, en la evolución en los mercados de las empresas. Su madurez en el competitivo mercado actual contribuye a que hayan alcanzado un grado de eficiencia elevado, que reduce las opciones aún disponibles a las que pueden recurrir para mejorar su cuenta de resultados mediante medidas de fondo económico.

La extensión del plazo de amortización del equipamiento informático supone utilizar los mismos equipos durante más tiempo, asumiendo el creciente riesgo de mal funcionamiento debido a su mayor antigüedad antes de ser sustituidos. Permite retrasar

la adquisición de nuevo equipamiento y, a lo largo de los años, reducir la cantidad de equipamiento adquirido para prestar los servicios. Son varios los hiperescalares[7] que han recurrido a estas medidas recientemente, entre los que se encuentran Amazon (Sharwood, 2024), Alphabet (Sharwood, 2024) o Cloudflare (Sharwood, 2024).

Esta medida también tiene sus efectos sobre el impacto ambiental debido a la rápida evolución tecnológica. Los nuevos dispositivos son más eficientes en términos de consumo de energía y de generación de calor gracias a nuevas arquitecturas más adaptadas a la resolución de algoritmos de inteligencia artificial y a la utilización de nuevos nodos tecnológicos (tamaño en nm) en la fabricación de los transistores, que reducen el consumo eléctrico y el calor generado.

Alargar la amortización del equipo supone su funcionamiento durante más años y que las ventajas de los nuevos equipos tarden más tiempo en poblar los centros de datos de las empresas. Durante este tiempo, los algoritmos estarán utilizando más energía de la que sería estrictamente necesaria si se compara con las prestaciones que los últimos dispositivos pueden proporcionar. La sustitución de un servidor antiguo por uno con las últimas tecnologías puede reducir hasta en un 30 % el consumo de energía necesario para realizar las mismas operaciones, lo que supondría un ahorro de alrededor de 480 $ durante un ciclo de vida de cuatro años, típico de este tipo de equipos[8].

Por el contrario, en favor de esta medida, los dispositivos fabricados estarán funcionando durante más tiempo, reduciendo el impacto de su fabricación en términos de consumo de materias primas y energía y de residuos generados durante su fabricación, así como el impacto que supone la retirada y reciclaje de los equipos decomisionados.

7. Conclusiones

El desarrollo de la IA no puede obviar el impacto medioambiental que su funcionamiento puede suponer. Los elevados consumos de energía y agua son factores muy importantes para la

[7] Proveedores de servicios de computación, comunicaciones y almacenamiento masivos.

[8] Disponible en: https://www.datacenterfrontier.com/voices-of-the-industry/article/11430647/waste-management-taking-out-the-trash-in-your-data-center.

implantación de la IA porque afectan a dimensiones sensibles como el calentamiento global y la huella de carbono. Las tecnologías de la información, y dentro de ellas aquellas dirigidas a soportar la inteligencia artificial, suponen un consumo energético significativo con respecto al consumo energético global por lo que la optimización de estas infraestructuras y los algoritmos que en ellas se ejecutan son una obligación para conseguir la sostenibilidad del sistema en términos tanto económicos como ambientales. La creciente sensibilización sobre la sostenibilidad y el riesgo que la implantación de nuevas necesidades de consumo de energía supone para el calentamiento global es una cuestión que debe estar presente en toda nueva estrategia de trabajo.

Las empresas del sector tienen muy presente el impacto ambiental y muchas de sus decisiones técnicas y de negocio se encuentran guiadas tanto por la sostenibilidad como por la reducción de costes económicos y medioambientales de sus operaciones.

Las fuentes de generación de energía juegan un papel muy relevante en la huella climática de un centro de datos cuyo consumo, al menos, se va a mantener, si no crecer, a lo largo del tiempo. El uso de fuentes renovables como el viento o la luz solar permiten reducir la huella de carbono de las instalaciones. La energía nuclear también se considera como una fuente de energía sin huella de carbono, aunque no todos los países pueden recurrir a ella. Se están aplicando otras tecnologías para la reducción de la huella ambiental como la sustitución de combustibles fósiles por biocombustibles en los sistemas de respaldo dentro de la política de reducir al máximo la huella de carbono de los centros de datos.

La geopolítica juega un papel importante en la huella climática de la inteligencia artificial, por cuanto afecta a qué soluciones resultan de aplicación y cómo de efectivas pueden resultar en cada territorio. Factores técnicos como las fuentes de generación disponibles, así como su tecnología —renovable, no renovable, nuclear…—, la disponibilidad y fiabilidad de la red de distribución o la distribución geográfica de las poblaciones en el territorio, no reducen la importancia de otros factores como la soberanía tecnológica, la autonomía o las regulaciones de protección de datos. Se genera así un mercado donde la competencia no se rige únicamente por los costes, sino que hay que incluir otros factores para determinar la viabilidad técnica y económica de las soluciones.

Bibliografía

Agencia Internacional de la Energía. (2023). [Consulta: 2024]. Disponible en: Electricity 2024 - Analysis and forecast to 2026 (iea.blob.core.windows.net). Pp 32-33.

Castro, D. (2024). *Rethinking Concerns About AI's Energy Use.*

DatacenterDynamics. (2022). Spain now a key data center hub for Southern Europe - Quark's Ricardo Abad. Disponible en: https://www.datacenterdynamics.com/en/marketwatch/spain-now-a-key-data-center-hub-for-southern-europe-quarks-ricardo-abad/

Hidalgo García, M. M. (2022). El consumo de energía y agua en los centros de datos: riesgos de sostenibilidad [en línea]. *Documento de Análisis IEEE 69/2022.* [Consulta: 2024]. Disponible en: El consumo de energía y agua en los centros de datos: riesgos de sostenibilidad (ieee.es)

Kamiya, G. y Kvarnström, O. (2019). *Data centres and energy – from global headlines to local headaches?*

Mann, T. (2024). *Think tank funded by Big Tech argues AI's climate impact is nothing to worry about.*

Ramírez Morán, D. (2013). Large Language Models: los nuevos actores de acceso al conocimiento [en línea]. *Documento de análisis 86/2023.* [Consulta: 2024]. Disponible en: Large Language Models: the new actors for knowledge access (ieee.es)

Robinson, D. (2023). AI processing could consume 'as much electricity as Ireland' [en línea]. *The Register.* [Consulta: 2024]. Disponible en: AI processing could consume 'as much electricity as Ireland' • The Register.

Savills research. (2023). European Data Centres 2023: the watershed for data centre water usage.

Sharwood, S. (2024a). *Alphabet just banked $3B by stretching life of its servers.*

—. (2024b). *Amazon extends the life of its servers to six years, expects $900m benefit in 90 days.*

—. (2024c). *Cloudflare joins the 'we found ways to run our kit for longer' club.*

—. (2024d). IBM Japan and NTT think they can make datacenter aircon adjust to different workloads [en línea]. *The Register.* [Consulta: 2024]. Disponible en: https://www.theregister.com/2024/02/07/ntt_ibm_datacenter_heat_ai/.

Smolaks, M. (s.f.). *Heat Reuse: A Management Primer*. [Consulta: 2024]. Disponible en: https://uptimeinstitute.com/resources/research-and-reports/heat-reuse-a-management-primer

Tomlinson, B. *et al*. (2023). *The Carbon Emissions of Writing and Illustrating Are Lower for AI than for Humans.*

Composición del grupo de trabajo

Presidente:	**Eduardo Olier Arenas** *Profesor honorífico del CESEDEN* *Presidente del Instituto Choiseul España*
Vocal y coordinador:	**Francisco Márquez de la Rubia** *Teniente coronel del Ejército de Tierra* *Analista principal del IEEE*
Vocales:	**Ángel Gómez de Ágreda** *Coronel del Ejército del Aire y del Espacio* *Doctor en Ingeniería, Universidad Politécnica de Madrid*
	Álvaro Ortiz *BBVA research* *Responsable de análisis económico con IA y Big Data*
	Tomasa Rodrigo *BBVA research* *Lead economist de análisis económico con IA y Big Data*
	José Pardo de Santayana y Gómez de Olea *Coronel del Ejército de Tierra* *Acting director, IEEE*
	Juan Luis Sánchez Sánchez *Coronel del Ejército de Tierra* *Centro de Inteligencia de las FAS (España)*
	Claude Revel *Former interministerial delegate for economic intelligence to the french prime minister*

Juan Manuel Corchado
Rector de la Universidad de Salamanca
Catedrático del Departamento de Informática y Automática de la Universidad de Salamanca

Marco Lisi
Board member at ASI (Agenzia Spaziale Italiana)
Ex director de Departamento de la Agencia Espacial Europea

David Ramírez Morán
Analista del IEEE
Científico superior de la Defensa

Cuadernos de Estrategia

01 La industria alimentaria civil como administradora de las FAS y su capacidad de defensa estratégica

02 La ingeniería militar de España ante el reto de la investigación y el desarrollo en la defensa nacional

03 La industria española de interés para la defensa ante la entrada en vigor del Acta Única

04 Túnez: su realidad y su influencia en el entorno internacional

05 La Unión Europea Occidental (UEO) (1955-1988)

06 Estrategia regional en el Mediterráneo Occidental

07 Los transportes en la raya de Portugal

08 Estado actual y evaluación económica del triángulo España-Portugal-Marruecos

09 Perestroika y nacionalismos periféricos en la Unión Soviética

10 El escenario espacial en la batalla del año 2000 (I)

11 La gestión de los programas de tecnologías avanzadas

12 El escenario espacial en la batalla del año 2000 (II)

13 Cobertura de la demanda tecnológica derivada de las necesidades de la defensa nacional

14 Ideas y tendencias en la economía internacional y española

15 Identidad y solidaridad nacional
16 Implicaciones económicas del Acta Única 1992
17 Investigación de fenómenos belígenos: método analítico factorial
18 Las telecomunicaciones en Europa, en la década de los años 90
19 La profesión militar desde la perspectiva social y ética
20 El equilibrio de fuerzas en el espacio sur europeo y mediterráneo
21 Efectos económicos de la unificación alemana y sus implicaciones estratégicas
22 La política española de armamento ante la nueva situación internacional
23 Estrategia finisecular española: México y Centroamérica
24 La Ley Reguladora del Régimen del Personal Militar Profesional (cuatro cuestiones concretas)
25 Consecuencias de la reducción de los arsenales militares negociados en Viena, 1989. Amenaza no compartida
26 Estrategia en el área iberoamericana del Atlántico Sur
27 El Espacio Económico Europeo. Fin de la Guerra Fría
28 Sistemas ofensivos y defensivos del espacio (I)
29 Sugerencias a la Ley de Ordenación de las Telecomunicaciones (LOT)
30 La configuración de Europa en el umbral del siglo XXI
31 Estudio de «inteligencia operacional»
32 Cambios y evolución de los hábitos alimenticios de la población española
33 Repercusiones en la estrategia naval española de aceptarse las propuestas del Este en la CSBM, dentro del proceso de la CSCE
34 La energía y el medio ambiente
35 Influencia de las economías de los países mediterráneos del norte de África en sus respectivas políticas de defensa
36 La evolución de la seguridad europea en la década de los 90
37 Análisis crítico de una bibliografía básica de sociología militar en España. 1980-1990
38 Recensiones de diversos libros de autores españoles, editados entre 1980-1990, relacionados con temas de las Fuerzas Armadas
39 Las fronteras del mundo hispánico
40 Los transportes y la barrera pirenaica
41 Estructura tecnológica e industrial de defensa, ante la evolución estratégica del fin del siglo XX

42 Las expectativas de la I+D de defensa en el nuevo marco estratégico
43 Costes de un ejército profesional de reclutamiento voluntario. Estudio sobre el Ejército profesional del Reino Unido y (III)
44 Sistemas ofensivos y defensivos del espacio (II)
45 Desequilibrios militares en el Mediterráneo Occidental
46 Seguimiento comparativo del presupuesto de gastos en la década 1982-1991 y su relación con el de Defensa
47 Factores de riesgo en el área mediterránea
48 Las Fuerzas Armadas en los procesos iberoamericanos de cambio democrático (1980-1990)
49 Factores de la estructura de seguridad europea
50 Algunos aspectos del régimen jurídico-económico de las FAS
51 Los transportes combinados
52 Presente y futuro de la conciencia nacional
53 Las corrientes fundamentalistas en el Magreb y su influencia en la política de defensa
54 Evolución y cambio del este europeo
55 Iberoamérica desde su propio sur. (La extensión del Acuerdo de Libre Comercio a Sudamérica)
56 La función de las Fuerzas Armadas ante el panorama internacional de conflictos
57 Simulación en las Fuerzas Armadas españolas, presente y futuro
58 La sociedad y la defensa civil
59 Aportación de España en las cumbres iberoamericanas: Guadalajara 1991-Madrid 1992
60 Presente y futuro de la política de armamentos y la I+D en España
61 El Consejo de Seguridad y la crisis de los países del Este
62 La economía de la defensa ante las vicisitudes actuales de las economías autonómicas
63 Los grandes maestros de la estrategia nuclear y espacial
64 Gasto militar y crecimiento económico. Aproximación al caso español
65 El futuro de la Comunidad Iberoamericana después del V Centenario
66 Los estudios estratégicos en España
67 Tecnologías de doble uso en la industria de la defensa
68 Aportación sociológica de la sociedad española a la defensa nacional

69 Análisis factorial de las causas que originan conflictos bélicos
70 Las conversaciones internacionales Norte-Sur sobre los problemas del Mediterráneo Occidental
71 Integración de la red ferroviaria de la península ibérica en el resto de la red europea
72 El equilibrio aeronaval en el área mediterránea. Zonas de irradiación de poder
73 Evolución del conflicto de Bosnia (1992-1993)
74 El entorno internacional de la Comunidad Iberoamericana
75 Gasto militar e industrialización
76 Obtención de los medios de defensa ante el entorno cambiante
77 La Política Exterior y de Seguridad Común (PESC) de la Unión Europea (UE)
78 La red de carreteras en la península ibérica, conexión con el resto de Europa mediante un sistema integrado de transportes
79 El derecho de intervención en los conflictos
80 Dependencias y vulnerabilidades de la economía española: su relación con la defensa nacional
81 La cooperación europea en las empresas de interés de la defensa
82 Los cascos azules en el conflicto de la ex-Yugoslavia
83 El sistema nacional de transportes en el escenario europeo al inicio del siglo XXI
84 El embargo y el bloqueo como formas de actuación de la comunidad internacional en los conflictos
85 La Política Exterior y de Seguridad Común (PESC) para Europa en el marco del Tratado de no Proliferación de Armas Nucleares (TNP)
86 Estrategia y futuro: la paz y seguridad en la Comunidad Iberoamericana
87 Sistema de información para la gestión de los transportes
88 El mar en la defensa económica de España
89 Fuerzas Armadas y sociedad civil. Conflicto de valores
90 Participación española en las fuerzas multinacionales
91 Ceuta y Melilla en las relaciones de España y Marruecos
92 Balance de las primeras cumbres iberoamericanas
93 La cooperación hispano-franco-italiana en el marco de la PESC
94 Consideraciones sobre los estatutos de las Fuerzas Armadas en actividades internacionales
95 La unión económica y monetaria: sus implicaciones

96 Panorama estratégico 1997/98
97 Las nuevas Españas del 98
98 Profesionalización de las Fuerzas Armadas: los problemas sociales
99 Las ideas estratégicas para el inicio del tercer milenio
100 Panorama estratégico 1998/99
100-B 1998/99 Strategic Panorama
101 La seguridad europea y Rusia
102 La recuperación de la memoria histórica: el nuevo modelo de democracia en Iberoamérica y España al cabo del siglo XX
103 La economía de los países del norte de África: potencialidades y debilidades en el momento actual
104 La profesionalización de las Fuerzas Armadas
105 Claves del pensamiento para la construcción de Europa
106 Magreb: percepción española de la estabilidad en el Mediterráneo, prospectiva hacia el 2010
106-B Maghreb: percepción espagnole de la stabilité en Méditerranée, prospective en vue de L'année 2010
107 Panorama estratégico 1999/2000
107-B 1999/2000 Strategic Panorama
108 Hacia un nuevo orden de seguridad en Europa
109 Iberoamérica, análisis prospectivo de las políticas de defensa en curso
110 El concepto estratégico de la OTAN: un punto de vista español
111 Ideas sobre prevención de conflitos
112 Panorama Estratégico 2000/2001
112-B Strategic Panorama 2000/2001
113 Diálogo mediterráneo. Percepción española
113-B Le dialogue Méditerranéen. Une perception espagnole
114 Aportaciones a la relación sociedad - Fuerzas Armadas en Iberoamérica
115 La paz, un orden de seguridad, de libertad y de justicia
116 El marco jurídico de las misiones de las Fuerzas Armadas en tiempo de paz
117 Panorama Estratégico 2001/2002
117-B 2001/2002 Strategic Panorama
118 Análisis, estrategia y prospectiva de la Comunidad Iberoamericana
119 Seguridad y defensa en los medios de comunicación social

120 Nuevos riesgos para la sociedad del futuro
121 La industria europea de defensa: presente y futuro
122 La energía en el espacio euromediterráneo
122-B L'énergie sur la scène euroméditerranéenne
123 Presente y futuro de las relaciones cívico-militares en Hispanoamérica
124 Nihilismo y terrorismo
125 El Mediterráneo en el nuevo entorno estratégico
125-B The Mediterranean in the New Strategic Environment
126 Valores, principios y seguridad en la comunidad iberoamericana de naciones
127 Estudios sobre inteligencia: fundamentos para la seguridad internacional
128 Comentarios de estrategia y política militar
129 La seguridad y la defensa de la Unión Europea: retos y oportunidades
130 El papel de la inteligencia ante los retos de la seguridad y defensa internacional
131 Crisis locales y seguridad internacional: El caso haitiano
132 Turquía a las puertas de Europa
133 Lucha contra el terrorismo y derecho internacional
134 Seguridad y defensa en Europa. Implicaciones estratégicas
135 La seguridad de la Unión Europea: nuevos factores de crisis
136 Iberoamérica: nuevas coordenadas, nuevas oportunidades, grandes desafíos
137 Irán, potencia emergente en Oriente Medio. Implicaciones en la estabilidad del Mediterráno
138 La reforma del sector de seguridad: el nexo entre la seguridad, el desarrollo y el buen gobierno
139 Security Sector Reform: the Connection between Security, Development and Good Governance
140 Impacto de los riesgos emergentes en la seguridad marítima
141 La inteligencia, factor clave frente al terrorismo internacional
142 Del desencuentro entre culturas a la Alianza de Civilizaciones. Nuevas aportaciones para la seguridad en el Mediterráneo
143 El auge de Asia: implicaciones estratégicas
144 La cooperación multilateral en el Mediterráneo: un enfoque integral de la seguridad
145 La Política Europea de Seguridad y Defensa (PESD) tras la entrada en vigor del Tratado de Lisboa

145-B The European Security and Defense Policy (ESDP) after the entry into Force of the Lisbon Treaty

146 Respuesta europea y africana a los problemas de seguridad en África

146-B European and African Response to Security Problems in Africa

147 Los actores no estatales y la seguridad internacional: su papel en la resolución de conflictos y crisis

148 Conflictos, opinión pública y medios de comunicación. Análisis de una compleja interacción

149 Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio

150 Seguridad, modelo energético y cambio climático

151 Las potencias emergentes hoy: hacia un nuevo orden mundial

152 Actores armados no estables: retos a la seguridad

153 Proliferacion de ADM y de tecnología avanzada

154 La defensa del futuro: innovación, tecnología e industria

154-B The Defence of the Future: Innovation, Technoligy and Industry

155 La Cultura de Seguridad y Defensa. Un proyecto en marcha

156 El gran Cáucaso

157 El papel de la mujer y el género en los conflictos

157-B The role of woman and gender in conflicts

158 Los desafíos de la seguridad en Iberoamérica

159 Los potenciadores del riesgo

160 La respuesta del derecho internacional a los problemas actuales de la seguridad global

161 Seguridad alimentaria y seguridad global

161-B Food security and global security

162 La inteligencia económica en un mundo globalizado

162-B Economic intelligence in global world

163 Islamismo en (r)evolución: movilización social y cambio político

164 Afganistán después de la ISAF

165 España ante las emergencias y catástrofes. Las Fuerzas Armadas en colaboración con las autoridades civiles

166 Energía y Geoestrategia 2014

166-B Energy and Geostrategy 2014

167 Perspectivas de evolución futura de la política de seguridad y defensa de la UE. Escenarios de crisis

167-B Prospects for the future evolution of the EU‘s security and defence policy. Crisis scenarios

168 Evolución del mundo árabe: tendencias

169 Desarme y control de armamento en el siglo XXI: limitaciones al comercio y a las transferencias de tecnología

170 El sector espacial en España. Evolución y perspectivas

171 Cooperación con Iberoamérica en materia de defensa

172 Cultura de Seguridad y Defensa: fundamentos y perspectivas de mejora

173 La internacional yihadista

174 Economía y geopolítica en un mundo globalizado

175 Industria Española de Defensa. Riqueza, tecnología y seguridad

176 Shael 2015, origen de desafíos y oportunidades

177 UE-EE.UU.: Una relación indispensable para la paz y la estabilidad mundiales

178 Rusia bajo el liderazgo de Putin. La nueva estrategia rusa a la búsqueda de su liderazgo regional y el reforzamiento como actor global

179 Análisis comparativo de las capacidades militares españolas con las de los países de su entorno

180 Estrategias para derrotar al DAESH y la reestabilización regional

181 América Latina: nuevos retos en seguridad y defensa

182 La colaboración tecnológica entre la universidad y las Fuerzas Armadas

183 Política y violencia: comprensión teórica y dearrollo en la acción colectiva

184 Una estrategia global de la Unión Europea para tiempos difíciles

185 Ciberseguridad: lal cooperación público-privada

186 El agua: ¿fuente de conflicto o cooperación?

187 Geoeconomías del siglo XXI

188 Seguridad global y derechos fundamentales

189 El posconflicto colombiano: una perspectiva transversal

190 La evolución de la demografía y su incidencia en la defensa y seguridad nacional

190-B The evolution of demography and its impact on defense and national security

191 OTAN: presente y futuro

192 Hacia una estrategia de seguridad aeroespacial

193 El cambio climático y su repercusión en la Defensa

194 La gestión del conocimiento en la gestión de programas de defensa

195 El rol de las Fuerzas Armadas en operaciones posconflicto
196 Oriente medio tras el califato
197 La posverdad. Seguridad y defensa
198 Retos diversos a la seguridad. Una visión desde España
199 Gobernanza futura: hiperglobalización, mundo multipolar y Estados menguantes
200 Globalización e identidades. Dilemas del siglo XXI
201 Limites jurídicos de las operaciones actuales: nuevos desafios
202 El SAHEl y G5: desafios y oportunidades
203 Emergencias pandémicas en un mundo globalizado: amenazas a la seguridad
204 La dualidad económica Estados Unidos-China en el siglo XXI
205 La no proliferación y el control de armamentos nucleares en la encrucijada
206 Las ciudades: agentes críticos para una transformación sostenible del mundo
207 Repercusiones estratégicas del desarrollo tecnológico. Impacto de las tecnologías emergentes en el posicionamiento estratégico de los países
208 Los retos del espacio exterior: ciencia, industria, seguridad y aspectos legales
209 Minerales: una cuestión estratégica en el siglo XXI
210 Redes transeuropeas: vectores vertebradores de la España del siglo XXI
211 El futuro de la OTAN tras la Cumbre de Madrid 2022
211-B The future of NATO after the Madrid 2022 summit
212 China: el desafío de la nueva potencia global
213 El Mediterráneo: un espacio geopolítico de interés renovado
214 Terrorismo internacional: mutación y adaptación de un fenómeno global
215 La Unión Europea hacia la autonomía estratégica
215-B The European Union Towards Strategic Autonomy
216 Asia Central: de pivote a encrucijada
217 La amenaza biológica
218 El Ártico: la región para la colaboración (o las disputas)
219 Asia Oriental, la interdependencia como causa de confllicto
220 África: la ambición de las potencias sobre el continente
221 Irán en la encrucijada global

222 Crisis migratorias como elemento de coerción internacional
223 Retos y respuestas frente a la amenaza química
224 Geopolítica del poder militar
225 Potencias medias: Transitando hacia un orden multipolar

PUBLICACIONES
Pd
DE DEFENSA

GOBIERNO
DE ESPAÑA

MINISTERIO
DE DEFENSA

SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

SUBDIRECCIÓN GENERAL
DE PUBLICACIONES
Y PATRIMONIO CULTURAL