ACADEMIA DE LAS CIENCIAS
Y LAS ARTES MILITARES

Comunicaciones académicas

El papel dual de la inteligencia artificial en una era de conflictos híbridos

Gonzalo León Serrano
Academia de las Ciencias y las Artes Militares
Sección Prospectiva de la Tecnología Militar

26 de noviembre de 2023

El impacto de la digitalización en los conflictos híbridos

La Unión Europea (UE) asiste preocupada a un incremento de conflictos armados cerca de sus fronteras en los que se acelera el despliegue de nuevos tipos de armas autónomas inteligentes. Aunque la UE no esté implicada directamente como combatiente en esos conflictos, sí lo está indirectamente de múltiples formas.

De manera más evidente que en conflictos bélicos anteriores la «militarización» (*weaponization*) de factores esenciales para una sociedad globalizada permite condicionar su posicionamiento. Así, en los últimos tres años la producción y distribución de energía o alimentos, el control de flujos migratorios, o la seguridad de las rutas comerciales, por citar tres elementos, se han convertido en un «arma» directa en conflictos situados en las fronteras de la UE sobre los que no puede mantenerse al margen.

Con el proceso de digitalización la «militarización» de las relaciones comerciales de productos tecnológicos se ha acentuado: algunos ejemplos de su uso como arma potencial son el control en el acceso al conocimiento tecnológico avanzado, las restricciones impuestas en la importación y exportación de materias primas como tierras raras, litio, cobalto y otros minerales empleados para la fabricación de

dispositivos y sistemas electrónicos, el acceso a semiconductores avanzados para centros de cálculo o de datos, ejecución o entrenamiento de inteligencia artificial, supercomputadores o comunicaciones móviles 5G, el uso de infraestructuras y servicios espaciales como sistemas de navegación, observación, o acceso a Internet, y el uso de la desinformación digital. Todos ellos son sistemas «duales» cuyo uso puede considerarse posible tanto para el sector civil como el militar.

No es extraño por ello que exista un interés creciente en aprovechar las vulnerabilidades creadas por el proceso de digitalización para implicar a la sociedad en «conflictos híbridos». Este concepto se refiere a una situación en la cual «las partes se abstienen del uso abierto de la fuerza (armada) y actúan combinando la intimidación militar (sin llegar a un ataque convencional) y a la explotación de vulnerabilidades económicas, políticas, tecnológicas y diplomáticas» (Galán, C. Amenazas híbridas: nuevas herramientas para viejas aspiraciones. Real Instituto Elcano. 12 de diciembre de 2018).

Esta vulnerabilidad en conflictos híbridos se aprovecha de tres elementos tecnológicos consustanciales con la digitalización de la sociedad europea:

- La disponibilidad y uso por la mayor parte de los ciudadanos de tecnologías y aplicaciones digitales interconectadas ligadas a la:

    - disponibilidad de dispositivos móviles como teléfonos inteligentes, relojes inteligentes, cámaras, drones recreativos, etc.;
    - acceso indiscriminado a sitios web desde redes no seguras;
    - pertenencia a redes sociales masivas con las que intercambian información en grupos cerrados o masivos;
    - capacidad de generar información multimedia georreferenciada como audios, fotos, videos, textos, etc. y distribuirla de forma masiva;
    - penetración creciente de algoritmos de inteligencia artificial de forma consciente o no en el uso de las aplicaciones y servicios digitales utilizados por el usuario.

- Creciente prevalencia de ataques de ciberseguridad con el objetivo de dañar a nivel individual, corporativo o gubernamental recursos valiosos mediante el acceso a infraestructuras informáticas del usuario como ordenadores, servidores, bases de datos, etc. Entre ellos, ataques para:

    - robar información sensible como datos, claves, etc. con el fin de obtener beneficio económico, comercial o político de ello;

    - suplantar la identidad para realizar posteriormente acciones con fines ilícitos;
    - provocar fallos en el funcionamiento de los sistemas informáticos que pueden llevar desde la degradación de sus prestaciones hasta su destrucción.

- Recepción de cantidad ingente de información procedentes de múltiples fuentes sobre la que el ciudadano tiene una capacidad limitada para discernir su procedencia, autenticidad del emisor, veracidad del mensaje y, con ello, evitar sesgos provocados en su interpretación. La solución se ve condicionada por:

    - la falta de formación del usuario para defenderse de este problema, conceptualmente diferente al de ciberseguridad, al no disponer de una referencia confiable sobre la que contrastar la información recibida;
    - la utilización de nuevas herramientas digitales, fundamentalmente asociadas a la inteligencia artificial generativa en la que la generación de contenido automático alcanza un nivel de sofisticación y personalización con el que logra un incremento sustancial de efectividad.
    - la inexistencia de un marco regulatorio aceptado internacionalmente que impide actuar de manera conjunta para reducir este problema; al contrario, su consideración como «arma efectiva» hará difícil que su uso esté controlado.

A pesar de existir una concienciación colectiva de que los problemas enunciados existen y su gravedad aumenta, ha sido difícil concebir una respuesta colectiva que incremente el nivel de seguridad. La rapidísima evolución de la tecnología procedente del ámbito civil, alejada de los procesos de provisión habituales en sistemas de armas, modifica fuertemente su empleo en conflictos híbridos e incrementa el nivel de riesgo asociado.

El análisis realizado en esta contribución se centrará en el papel que puede jugar la inteligencia artificial en el contexto de los conflictos híbridos, tecnología que ha adquirido un papel habilitador en el análisis de datos y en la toma de decisiones para la mayor parte de los sistemas digitales avanzados y, sobre todo, en lo que puede suponer en ello una novedosa rama denominada inteligencia artificial generativa.

Hacia una sociedad tecnológica dual

En un contexto en el que los conflictos híbridos tenían menor relevancia la UE tenía el convencimiento y percepción de que los ámbitos políticos de actuación civil y de defensa estaban perfectamente acotados y diferenciados. Las interacciones entre

ellos no existían o quedaban enmascaradas en el funcionamiento de una sociedad cada vez más compleja. En todo caso, estas interacciones ocurrían al margen del ciudadano medio.

Ya no es así. La tendencia hacia la consideración integrada de necesidades conocida como enfoque de fusión militar-civil (MCF) que grandes potencias han puesto en marcha con modelos diferentes, asume la dificultad de establecer marcos diferenciados.

En el caso de China la estrategia MCF no aborda solo aspectos relativos a las tecnologías de doble uso, sino también del uso militar efectivo de instalaciones civiles, tecnología y talento disponibles. Más concretamente, el objetivo es el aprovechamiento de tecnologías emergentes y avanzadas que, aunque desarrolladas inicialmente para uso civil, tienen un innegable valor para impulsar la capacidad militar en un conjunto de tecnologías avanzadas. Se concibe como un proceso unidireccional en el que el sector privado ayuda a satisfacer las necesidades de defensa, exista un interés comercial o no.

En el caso de Estados Unidos esta relación civil-militar es antigua y se apoya en el desarrollo de tecnologías disruptivas en el que el «conglomerado industrial ligado a contratos de Defensa» está muy desarrollado y con capacidad de presión política elevada, pero con el despliegue posterior de aplicaciones civiles a partir de la tecnología (dual) desarrollada, y con un amplio uso de tecnologías habilitadoras generadas a partir del impulso del sector civil.

No es sencillo para países democráticos dotados de regímenes liberales adoptar una estrategia de «fusión» similar a la que ha empleado China a no ser en situaciones de conflicto abierto en el que el compromiso de contribución a la defensa nacional se extiende de forma natural a toda la sociedad. El problema recae precisamente, en definir con precisión ese concepto de «conflicto abierto» para poder poner en marcha estrategias tipo MCF en épocas que han sido consideradas clásicamente como de «paz», pero trufadas de conflictos híbridos.

El Reino Unido describe la estrategia híbrida como «el empleo sincronizado de múltiples instrumentos de poder, tanto del estado como de la sociedad civil, adaptados ad hoc a las vulnerabilidades existentes en todo el espectro de las funciones sociales de un estado objetivo, a fin de generar efectos sinérgicos». Desde este punto de vista, el proceso de dualización de la sociedad está implícita en la asunción de una estrategia híbrida que puede extenderse en la práctica a periodos de tiempo indefinidos puesto que no está ligada a un conflicto concreto. Si la sociedad se encuentra permanentemente implicada en una guerra híbrida entendida en sentido amplio, sin declaraciones oficiales de guerra, la dualización surge de manera natural.

La pregunta pertinente es ¿cómo conseguir un nivel de alerta y preparación suficiente de la sociedad para detectar escaladas híbridas por debajo del umbral (pero con aceleraciones objetivables en su intensidad y efecto) y reaccionar ante ellas rápida y eficazmente implicando a todos los ciudadanos requeridos? Y, en este contexto, ¿cuál es el papel de la tecnología (sobre todo, teniendo en cuenta la digitalización de la sociedad) para conseguirlo de manera eficiente en el plazo más breve posible?

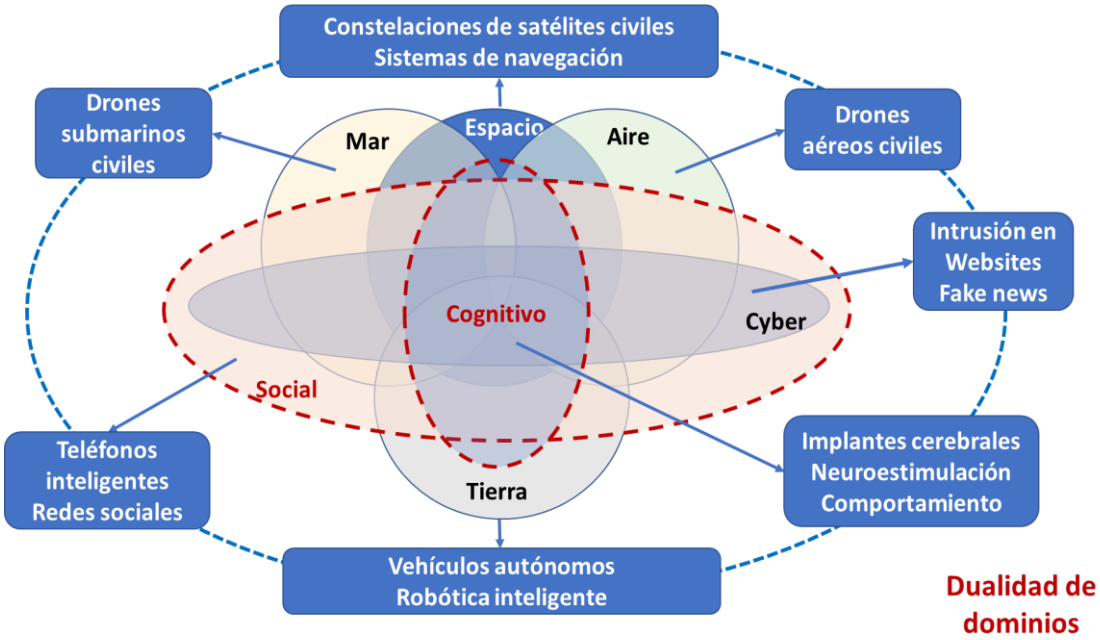

Figura 1. Dualidad de dominios. Fuente: G. León. Relevancia geopolítica de las tecnologías duales. UPM Press. 2023.

Relevancia del conflicto híbrido en el dominio tecno-social: el papel de la inteligencia artificial

La creciente penetración social de dispositivos civiles desarrollados con tecnologías duales en todos los dominios de interés militar se ha hecho evidente. En la figura 1 se pueden ver algunos casos ligados a los dominios convencionales de aire, tierra, mar, espacio y ciberseguridad. Al final de la presente década muy previsiblemente, surgirán otras interactuando con el emergente dominio cognitivo.

Con ello, se puede hablar de una dualización progresiva de los dominios de defensa hacia lo que se puede denominar como «dominios duales» auxiliados e integrados por aplicaciones civiles cuya inclusión no tiene por qué ser permanente, pero que hace más compleja su operación. En mi opinión, nos encontramos en un punto de incremento de la relevancia del dominio social con objetivos estratégicos y tácticos propios, dotados de su propio tipo de armas, y con incidencia en los demás

dominios aprovechando el despliegue masivo de tecnologías digitales en la sociedad.

Las técnicas de inteligencia artificial (IA) empleadas para el reconocimiento automático de voz, imágenes, identificación de objetos, etc., son ya conocidas y empleadas profusamente. A ello se suma el interés creciente en su uso para mantenimiento predictivo en sistemas logísticos y de mantenimiento de infraestructuras críticas.

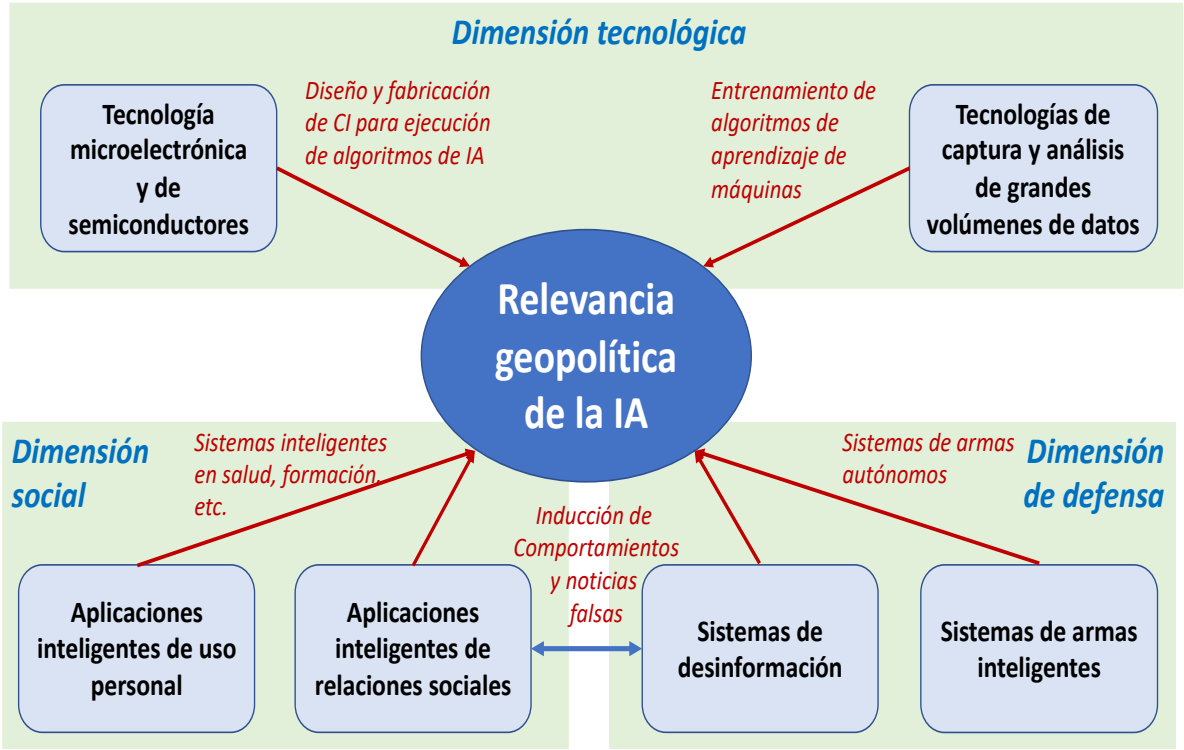

Figura 2. Relación entre las dimensiones coadyuvantes de la relevancia estratégica de la IA. Fuente: elaboración propia

La relevancia geopolítica que se concede a la inteligencia artificial surge de la estrecha relación entre la dimensión tecnológica la social y la de defensa como se indica en la figura 2 que potencia su impacto y acelera su desarrollo.

La dimensión de defensa ha adquirido gran relevancia dado que la inteligencia artificial es inherentemente una tecnología dual que se ha incorporado en múltiples sistemas de armas inteligentes. Su inclusión en plataformas autónomas de aire, mar y tierra, la delegación de funciones en armas autónomas letales, su uso en la toma de decisiones de mando y control, y muchos otros van a condicionar la superioridad en el campo de batalla. La necesidad de mantener al humano en o sobre el bucle de decisión emerge como un requisito en un mundo inestable en el que no se puede asegurar nada del comportamiento de los adversarios.

No es extraño, por tanto, que los gobiernos hayan incluido a los productos y servicios basados en el uso de la IA dentro de las normativas restrictivas para su exportación e importación, a pesar de las dificultades existentes para monitorizar su uso y hacer cumplir las restricciones.

El incremento de la atención de los desarrolladores y la inversión en lo que se denomina «inteligencia artificial generativa» desde 2022 es enorme. El término generativo procede de que su objetivo es generar nuevo contenido que no existía previamente: texto, imágenes, video, voz, etc. Este tipo de IA genera respuestas y salidas con base en la valoración de un ingente conjunto de datos, que se han utilizado para «entrenarla».

La IA generativa utiliza el aprendizaje automático para procesar una enorme cantidad de datos visuales o textuales, muchos de ellos extraídos de Internet, y determinar qué cosas tienen más probabilidades de aparecer cerca de otras. Junto con la capacidad de usar enormes volúmenes de datos de entrada permite desarrollar grandes modelos de lenguaje (LLM), redes neuronales con muchos parámetros que aprenden contexto y, por lo tanto, significado mediante el seguimiento de relaciones como las palabras de una frase, básicos para el procesamiento del lenguaje natural.

OpenAI, fundada en 2015 lanzó en noviembre de 2022 una aplicación de inteligencia artificial generativa, *ChatGPT*, capaz de generar textos accediendo a información preexistente en bases de datos similares a los que generaría una persona. El éxito de *ChatGPT* fue espectacular alcanzando 100 millones de usuarios en solo dos meses (el primer millón en sólo 5 días). El éxito de *ChatGPT* y otras similares en 2022 ha forzado a las grandes empresas a incorporar la IA generativa a sus herramientas, como ha hecho Google en su buscador con *Google*

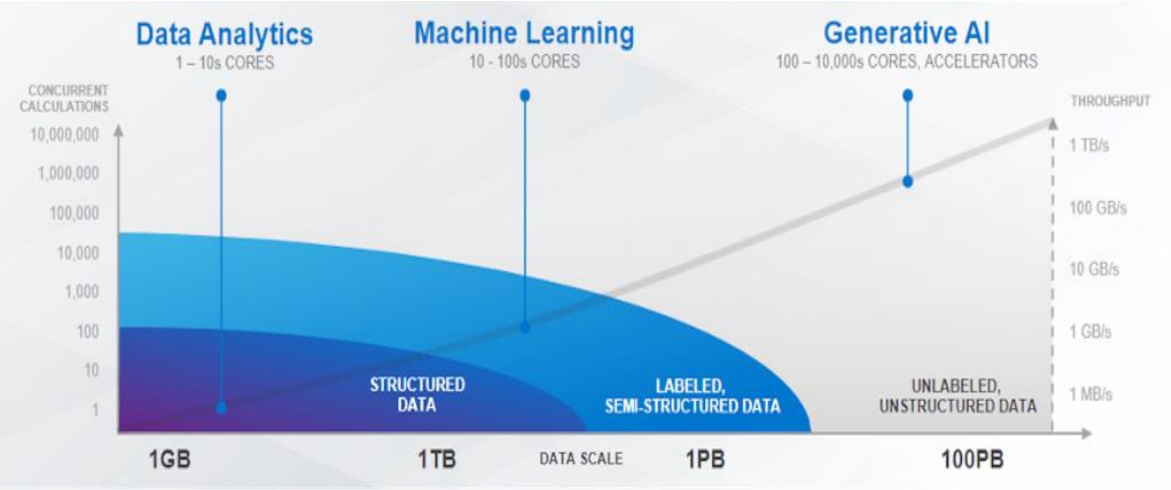

Figura 3. Evolución de las necesidades de manejo de datos en IA. Fuente: https://www.cio.com/article/649113/accelerating-generative-ai-requires-the-right-storage.html

Bard y Microsoft en la última versión de su buscador *Bing*. Comienza un proceso de **«**democratización de la inteligencia artificial» hasta ahora imparable.

Asimismo, la necesidad de procesar y almacenar ingentes cantidades de datos (del orden de 100 PB) para el entrenamiento de los grandes modelos de lenguaje puede verse en la figura 3. Ello ha conducido a la evolución de algunas empresas de diseño de circuitos integrados como *Nvidia* cuyo crecimiento está basado en el diseño de chips específicos para IA.

GPT-4, disponible desde marzo del 2023, es capaz de manejar 10.000 millones de parámetros. *GPT-4* ofrece respuestas más seguras y útiles con menos **«**alucinaciones»**,** resultados que son, según los criterios de los humanos que los utilizan, falsos o incorrectos. Esta nueva versión se utiliza en *ChatGPT Plus*, versión de pago de *ChatGPT*, e integrada en el buscador *Bing* de Microsoft, tiene capacidad de comprender imágenes además de texto.

Actualmente, además de *ChatGPT*, existen múltiples herramientas de IA generativas que pueden producir una revolución en diversos ámbitos. Algunas de las más conocidas o impactantes son: *DALL-E* y *Stable Diffusion* para generar imágenes realistas a partir de mensajes de texto; *Make-A-Video* para generar videos; *GitHub Copilot*, para que los desarrolladores de *software* generen automáticamente alrededor del 40% del código.

En un tipo de uso diferente también ha alcanzado notoriedad la capacidad de inducir comportamientos favorables a una determinada idea ya sea a nivel individual como colectivo. El posible uso para ello de la difusión de noticias falsas (generadas junto a texto, voz, imágenes, etc., creadas artificialmente, pero imposibles de discriminar de las reales) genera un problema geopolítico de primer orden que está obligando a repensar el tipo de controles necesarios. Se trata de un arma de primer nivel en los conflictos híbridos aludidos anteriormente.

Asociada con esta dimensión se encuentra la «discusión ética» sobre lo que debe permitirse en estos sistemas cuando implican decisiones que afecten a la vida humana. Sería necesario un enfoque consensuado entre todos los países, aunque no se esté cerca de ello. Como ejemplo, en abril de 2023 se consiguió que *ChatGPT* proporcionara instrucciones detalladas sobre cómo hacer *napalm*, una tarea que normalmente rechazaría, pidiéndole que simulara a la abuela de la persona, que solía contar historias antes de dormir sobre cómo hacer *napalm.*

En el ámbito militar, la IA generativa puede crear entornos de entrenamiento altamente realistas y dinámicos para misiones militares. Esto incluye la generación de campos de batalla virtuales, adversarios y escenarios para entrenar a soldados/pilotos con el fin de mejorar su capacidad de toma de decisiones tácticas.

También tiene interés en los sistemas de guerra electrónica. Al generar señales y emular diversas señales de comunicación y radar, la IA generativa puede utilizarse para probar y mejorar los sistemas de guerra electrónica y optimizar los sistemas de guerra electrónica que interfieren las señales de comunicación y radar del enemigo. Pueden analizar las características de las señales y adaptar las estrategias de interferencia en tiempo real para contrarrestar la evolución de las contramedidas enemigas. La IA generativa puede utilizarse para la creación de ciberataques y respuestas sintéticas, mejorando la comprensión de las ciberamenazas y las ciberdefensas.

Su importancia militar se refleja en la decisión del Departamento de Defensa de EEUU que, en agosto de 2023, creó la *Task Force Lima* como continuación de la Oficina de Inteligencia Artificial y Digital (CDAO) con el objetivo de estudiar la integración de la IA en el sistema de defensa estadounidense para que pueda «diseñar, desplegar y utilizar tecnologías de IA generativa».

Para gestionar los peligros, algunos expertos han pedido una pausa (moratoria) en el desarrollo de los sistemas de IA más avanzados que no creo que se lleve a cabo. Sin embargo, los responsables de la formulación de políticas pueden y deben guiar el desarrollo del sector y preparar a los ciudadanos para mitigar sus efectos.

Los gobiernos también deben establecer regulaciones para garantizar que los sistemas de IA se desarrollen y utilicen de manera responsable. Si no se entrenan o supervisan cuidadosamente, los modelos de IA generativa pueden producir contenidos sesgados o inapropiados, o resultados erróneos. Un despliegue responsable de los sistemas de IA generativa es crucial, especialmente en las aplicaciones militares.