

**ACADEMIA DE LAS CIENCIAS Y LAS ARTES
MILITARES**

**LA TRANSFORMACIÓN DIGITAL EN LOS
NUEVOS ESCENARIOS DE CONFLICTO: DEL
CAMPO DE BATALLA DIGITAL AL CAMPO DE
BATALLA INTELIGENTE**

DISCURSO PRONUNCIADO POR EL

DR. D. FÉLIX PÉREZ MARTÍNEZ

EN EL ACTO DE SU TOMA DE POSESIÓN COMO
ACADÉMICO DE NÚMERO
EL DÍA 8 DE FEBRERO DE 2023



MADRID MMXXIII

Excelentísimo Sr. Presidente de la Academia de las Ciencias y las Artes Militares (ACAMI)¹, Vicepresidente, Secretario, Almirante, Presidente de la Sección de Prospectiva de la Tecnología Militar.

Excelentísimos e Ilustrísimos Señores Académicos,

Excelentísimo y Magnífico Rector de la Universidad Politécnica de Madrid,
Presidente de la Real Academia de la Ingeniería,
Almirante Director de Armamento y Material,
Teniente General Jefe del Mando de Apoyo Logístico del Ejército de Tierra,
Teniente General Director de Centro de Sistemas y Tecnologías de la Información,
Autoridades civiles y militares,

Señores, señoras, queridos familiares, compañeros, compañeras, amigos y amigas todos,

Hoy tengo el honor de pronunciar el discurso de ingreso a esta Academia, un honor que culmina una trayectoria profesional de más de cuarenta años de actividades en gran medida ligadas al sector de la defensa. Ser acogido en una Academia cuyo fin es fomentar la cultura militar en el ámbito de la sociedad española colma todas mis expectativas y lo que puedo asegurar, Presidente, es que pondré todo mi esfuerzo en no defraudar la confianza que han depositado en mi persona.

Quiero empezar mi intervención agradeciéndoles a todos ustedes su presencia aquí, compartiendo conmigo este acto. Agradecimiento, como no, a la Academia por admitirme en su seno como Académico de Número y, en particular, a los Generales de División D. José Carlos de la Fuente Chacón, D. Juan Antonio Moliner González y D. José Manuel Roldán Tudela por avalar mi candidatura. Un reconocimiento especial al G.D. de la Fuente, querido Charlie, por aceptar ser mi padrino en esta ceremonia. Gratitud que quiero extender a todos los miembros de las Fuerzas Armadas y Cuerpos y Fuerzas de Seguridad del Estado por la consideración y cariño que siempre me han demostrado.

También quiero manifestar mi agradecimiento a la Universidad Politécnica de Madrid² y a la Escuela Técnica Superior de Ingenieros de Telecomunicación³ instituciones que siempre han apoyado mis actividades docentes, investigadoras, de transferencia de tecnología y de gestión en el ámbito de la defensa. A la Fundación Círculo de Tecnologías para la Defensa y Seguridad⁴ que me ha dado la oportunidad de compartir con centenares de personas del sector tanto nuestro

¹ ACAMI-PÁGINA WEB

² UPM-PÁGINA WEB

³ ETSIT-PÁGINA WEB

⁴ Fundación Círculo-PÁGINA WEB

cariño y admiración por la labor de nuestras Fuerzas Armadas como la posibilidad de colaborar en que exista una base tecnológica e industrial en nuestro país que les ayude a cumplir sus trascendentales misiones. Agradecimiento también al Colegio Oficial y la Asociación Española de Ingenieros de Telecomunicación⁵ y al Instituto de la Ingeniería de España⁶ que siempre me apoyaron en estos objetivos. Tampoco quiero olvidar a mis compañeros del Centro de I+D+i en Procesado de la Información y Telecomunicaciones⁷, en especial al grupo de investigación Microondas y Radar, uno de los grupos de investigación de nuestro país que más ha trabajado en el desarrollo de sistemas para la Defensa.

Por último, pero no menos importante, a mi familia que en todo momento me han acompañado en mi trayectoria profesional: a mi compañera de este viaje, Lalines, a mis hijas Paloma y Ana; y a mi hermano, el Profesor Jorge Pérez, con el que he compartido una buena parte de esta trayectoria en la Universidad Politécnica de Madrid.

Muchas gracias a todos los que lo habéis hecho posible, estéis aquí, o lo veáis en el canal de YouTube de la Academia.

El título que he escogido para mi discurso, *La transformación digital en los nuevos escenarios de conflicto: Del campo de batalla digital al campo de batalla inteligente*, resume varios artículos y ponencias propios, alguno de ellos realizados como Académico Correspondiente de la Academia que hoy nos acoge, complementado con un conjunto de reflexiones personales fruto de mi trato con personas vinculadas al sector de la Defensa en las instituciones y entidades mencionadas. El eje central del discurso será el impacto que las conocidas como tecnologías de la información y las comunicaciones –las denominadas TIC- han tenido y tendrán en las operaciones militares.

Un tema que abordé por primera vez hace veinte años en un trabajo que realicé mientras cursaba el Curso de Defensa Nacional, impartido en el Centro Superior de Estudios de la Defensa Nacional y que se publicó bajo el título “Las TIC en la Seguridad y Defensa Nacional” en el Boletín de Información de esta institución en el año 2002⁸. Posteriormente una versión actualizada se publicó la revista BIT en el año 2006⁹ y desde entonces se convirtió en un tema constante de interés por mi parte, en paralelo con mi actividad principal de diseñador de sistemas radar y de radiofrecuencia.

Sin más prolegómenos paso a desarrollar el tema central del discurso.

⁵ COIT-PÁGINA WEB

⁶ IIES-PÁGINA WEB

⁷ IPTC-PÁGINA WEB

⁸ Pérez, 2002

⁹ Pérez, 2006

La transformación digital se ha definido¹⁰ como la integración de las tecnologías digitales en todas las áreas de una empresa, entidad o institución, para generar cambios fundamentales en la forma en que éstas trabajan, incrementando su valor y el de sus clientes. Es un cambio cultural que requiere que las organizaciones desafíen continuamente el statu quo, experimenten con frecuencia y se sientan cómodas con el fracaso. ¿Qué ocurre cuando aplicamos este concepto de transformación digital al ámbito militar? ¿Qué ocurre cuando la empresa son las Fuerzas Armadas y el cliente es la Nación a la que hay que garantizar su defensa en un escenario de conflicto?

Permítanme que comience esta reflexión mirando hacia atrás, con los antecedentes de este proceso y concretamente con el fenómeno de la digitalización de las TIC y su evolución.

Los antecedentes: La digitalización de las TIC

La digitalización...

Las TIC, el conjunto de tecnologías que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de información, incluyen a la Electrónica, como tecnología básica, las Telecomunicaciones y la Informática¹¹.

Son tres tecnologías con orígenes y desarrollos diferentes pero que en los últimos cincuenta años han estado sometidas a un proceso de convergencia que las ha convertido en factores multiplicativos de las actividades humanas lo que explica su potencial transformador y ha propiciado su utilización masiva en la mayor parte de las actividades de todos nosotros, incluyendo las del ámbito de la defensa y la seguridad.

La clave de su convergencia fue la digitalización de la información introducida en las últimas décadas del pasado siglo. En castellano entendemos por digitalización tanto al proceso de convertir algo no digital en una representación digital, como al uso de tecnologías y datos digitales para optimizar una actividad haciéndola más eficiente, productiva y/o rentable. Permítanme que utilice esta segunda acepción a lo largo de esta exposición.

Lo primero que se digitalizó fue la representación de las cantidades, pasándolas del formato decimal al formato binario, para realizar cálculos de forma eficiente. De hecho, el término “digital” lo introduce George Stibitz, de los Laboratorios Bell, quien en 1940 patentó la primera computadora digital electromecánica realizada con

¹⁰ THE ENTERPRISERS PROJECT.

¹¹ Pérez, 1998

relés, aunque como concepto, los números binarios ya fueron definidos en 1703 por el filósofo y matemático Leibniz y utilizado antes que Stibitz, entre otros, por Boole y Shannon. Es relevante indicar, que uno de los grandes hitos en este camino es la construcción, a finales de los años cuarenta del pasado siglo, del primer computador digital electrónico de programación flexible, el bien conocido ENIAC, financiado por el Ejército de los Estados Unidos, concretamente por el Mando de Investigación y Desarrollo del Cuerpo de Artillería, con un coste total de unos 487.000 dólares.

En efecto, el desarrollo de los computadores digitales fue acelerado por la necesidad de predecir las trayectorias de artillería durante la segunda guerra Mundial y, posteriormente, serán las necesidades de cálculo en la carrera espacial y los requerimientos de proceso en tiempo real del radar y las comunicaciones seguras durante la Guerra Fría las que impulsaron el desarrollo de la microelectrónica y con ella la revolución digital¹². La conocida como la tercera revolución industrial utilizó como materia prima un intangible: la información y ha producido una transformación socioeconómica cuyos inicios cabe datarlos hace 60 años pues su comienzo puede situarse en el año en que se anuncia el primer microprocesador¹³.

Permítanme ahora una breve descripción del desarrollo de esta “revolución”, que, en mi opinión, lo fue –“revolución”- por sus consecuencias, pero no por su ritmo de implantación, aunque se haya escrito lo contrario en numerosas ocasiones.

La evolución de las TIC...

En efecto, en los años 70, de la mano de la microelectrónica, se generaliza el uso de la circuitería digital que se utilizó en la generación, almacenamiento, transmisión y procesamiento de datos digitalizados, y se aplicó a numerosas actividades: cálculo, gestión, comunicaciones, sensorización... Muy pronto comenzó el proceso de convergencia antes mencionado. La aparición del ordenador personal a mediados de los ochenta es un hito más que relevante porque muy pronto superará sus aplicaciones iniciales de cálculo y gestión de datos, para convertirse en uno de los elementos esenciales para el acceso universal a la información.

El otro elemento clave será la implementación y generalización del uso de internet que permitirá el acceso masivo de datos en tiempo casi real a millones de usuarios. En definitiva, por primera vez en la historia, la digitalización de las TIC permitió la ruptura de las barreras temporales en el acceso masivo a la información, transformando la sociedad y siendo una de las claves, junto con los avances en las tecnologías del transporte, de lo que hoy denominamos globalización.

¹² Ortega, 2007

¹³ Intel 4004-WIKIPEDIA

El siguiente hito se produce en la primera década de este siglo con la generalización del uso de las comunicaciones móviles digitales que añade la movilidad como una de las prestaciones básicas en el acceso a los datos, rompiendo las barreras espaciales en el acceso masivo a la información.

Por último, más recientemente y una vez rotas las barreras espaciales y temporales, la digitalización completa de los sistemas de información y comunicaciones independizan las técnicas de proceso de la información de sus fuentes (sensores, voz, imágenes...), permitiendo la estandarización de dispositivos y sistemas, y como consecuencia directa, su abaratamiento y la aparición de los teléfonos inteligentes que con los ordenadores cada día accesibles a la población hicieron posible lo que conocemos como «sociedad de la información», en la que hoy estamos. El grado de convergencia entre las tres tecnologías iniciales, Electrónica, Telecomunicaciones e Informática es tal que en estos momentos nos referimos a las TIC como “tecnologías digitales”.

Finalizaré estos antecedentes resaltando dos aspectos de este proceso de digitalización que creo de especial relevancia:

- El desarrollo de las tecnologías digitales en las últimas décadas ha sido muy rápido y eficiente -fruto en última instancia de la famosa Ley de Moore del desarrollo de la microelectrónica¹⁴-, y los avances tecnológicos se han generado en la mayor parte de los casos en el ámbito civil, donde se han movilizado una cantidad de recursos muy superiores a los empleados en la introducción de estas tecnologías el ámbito de la defensa y la seguridad. La cuarta revolución industrial, la revolución 4.0, no está avanzado por vectores militares ni, como veremos a continuación, lo hará en el futuro.
- Las tecnologías digitales han sido tecnologías disruptivas y han generado “cambios profundos”, pero la denominada “revolución digital” lo ha sido por su impacto, no por su velocidad de implantación. Su desarrollo ha sido frenado por numerosas inercias consustanciales a los seres humanos que conforman la sociedad... han sido necesarios más de 50 años de digitalización para construir la sociedad de la información.

Tras esta aproximación histórica al tema, permítanme ahora unas reflexiones sobre algunos aspectos, tanto en el ámbito civil como en el militar, de esta sociedad de la información que todos compartimos.

¹⁴ Alamo, 2015

El presente: La sociedad de la Información y el campo de batalla digital

Comenzaré por las consecuencias en el ámbito civil de esta nueva sociedad.

Las economías digitales...

Entre otras muchas, una de las características de la actual sociedad de la información es que en ella se desarrollan economías digitales. Estas economías tienen una serie de características (globalización, transversalidad, estandarización, escalabilidad, adaptabilidad, eficiencia, etc.) que favorecen la innovación constante e incluso los cambios en los comportamientos sociales. Estos cambios generan a su vez nuevos modelos de negocio, lo que se ha traducido en el desarrollo exponencial de las mismas. Se trata de un cambio disruptivo que está afectando a todos los sectores económicos cuyo paradigma es la presencia de las grandes empresas tecnológicas asociadas al mundo digital en el ranking mundial de empresas por su capitalización bursátil.

El desplazamiento de las empresas tradicionales asociadas a los sectores de la química, mecánica, energía o construcción en el mencionado ranking es mucho más que una anécdota. Las organizaciones que no se adapten a las nuevas reglas de juego están llamadas a desaparecer. Es este contexto es en el que aparece la transformación digital como concepto aplicado primero a las empresas y posteriormente al resto de organizaciones, entre ellas las Fuerzas Armadas.

¿Qué ocurre en el ámbito militar?

La transformación digital de la Defensa...

En el ámbito de la defensa, la necesidad de adaptarse a los desarrollos tecnológicos fue reconocida desde los primeros momentos y se concretó durante la última década del siglo pasado en lo que se denominó la Revolución de los Asuntos Militares (*Revolution in Military Affairs* o RMA). Un concepto que recogía la necesidad de utilizar las nuevas tecnologías para mantener la eficacia de las Fuerzas Armadas de EEUU, que pronto derivó en un reconocimiento de que era necesaria una transformación profunda de las organizaciones militares y del campo de batalla como consecuencia del impacto práctico que las tecnologías digitales¹⁵.

De este modo, junto a los tradicionales dominios del campo de batalla -tierra, mar, aire y espacio ultraterrestre- aparecen dos nuevos dominios: el ciberespacio y, el más reciente, dominio cognitivo. A diferencia de los anteriores son dominios no

¹⁵ Martí, 2000

cinéticos, en ellos las acciones no son siempre observables y atribuibles al trabajar con un intangible: la información.

Está asumido que el ciberespacio es un dominio transversal a los cuatro dominios cinéticos porque, como muy bien expuso en esta misma sala hace unos meses en su discurso de ingreso nuestro Académico Manuel Esteve, lo que en este dominio ocurra tiene consecuencias en todos los dominios físicos¹⁶.

Por su parte, el dominio cognitivo ha estado siempre presente en los conflictos, pero es ahora cuando ha explicitado su importancia. Este dominio que nuestros compañeros académicos, Rubén García Servet y José Luis Calvo Alberó definen como “el que incluye las percepciones, creencias, comportamientos y toma de decisiones de los seres humanos, y la influencia externa que se puede ejercer sobre estos aspectos para modificarlos” y en el que “la actividad esencial es la influencia, que se consigue mediante la gestión de la información que los seres humanos y las sociedades reciben”¹⁷.

Son dos dominios cuya importancia está creciendo exponencialmente, como consecuencia directa del desarrollo de la sociedad de la información. En las actuales operaciones multidominio, la superioridad en estos dos dominios es imprescindible para asegurar el éxito en los conflictos. La actual Guerra en Ucrania, lamentablemente, lo está poniendo de manifiesto.

Nuestro país, y en particular nuestras Fuerzas Armadas, están involucradas en estos procesos. El Estado Mayor de la Defensa, los estados mayores de nuestros Ejércitos y la Armada, así como los organismos centrales del ministerio están inmersos en un proceso de transformación digital, que determinará un cambio radical de sus organizaciones y de la conducción de las operaciones en los futuros escenarios de conflicto^{18 19}.

De este modo, si bien, como decíamos, aunque la revolución 4.0, también denominada 4ª revolución industrial, no ha avanzado ni avanzará por vectores militares, sus aplicaciones en el sector de la defensa son imprescindibles. En último término, son aplicaciones que formarán parte del tsunami digital en el que está y estará inmersa la humanidad en las próximas décadas.

En los siguientes apartados de este discurso analizaré algunos aspectos de esta transformación digital, concretamente los asociados a los futuros campos de batalla.

¹⁶ Esteve, 2022

¹⁷ García, 2020

¹⁸ Millán, 2022

¹⁹ Gómez, 2022

El futuro: la sociedad del conocimiento y la defensa inteligente

Inteligencia por doquier...

Superadas las barreras temporales y espaciales de acceso a la información y estandarizadas las técnicas de generación y proceso, el siguiente reto para las tecnologías digitales no es otro que la adaptación de los procesos de la información a las necesidades en tiempo real de los usuarios de estos servicios. Es el proceso que se desarrollará en los próximos años, cuando la capacidad y velocidad del procesamiento de datos lo hagan posible. De este modo, caminamos hacia lo que denominamos la sociedad del conocimiento, en la que las técnicas y los sistemas son inteligentes y los datos se comparten entre hombres y objetos en un entorno de hiperconectividad.

¿Cuáles son las tecnologías más relevantes que soportarán esta nueva “revolución”?

Para el Profesor José Ramón Casar²⁰, y comparto plenamente su análisis, son las siguientes:

- La implantación de la tecnología de 5G y, posteriormente la 6G, que desplegará nuevas infraestructuras de comunicaciones fijas y móviles que facilitaran el intercambio de cantidades masivas de información entre personas, vehículos y miles de millones de dispositivos fijos, con latencias muy bajas cuando sea necesario.
- La computación ubicua y distribuida, implementada en el borde de la red cuando sea necesario, y realizada sobre nuevas arquitecturas de nube. El desarrollo de las aplicaciones del “Internet de las Cosas” y el despliegue de las redes 5G y 6G, serán posiblemente los vectores de su rápida expansión.
- La introducción masiva de las técnicas de inteligencia artificial (IA) en las aplicaciones, servicios y negocios basados en los datos para incrementar exponencialmente sus capacidades y eficiencias.

Y, por último:

- Las interfaces y los nuevos modos “inmersivos” de interacción característicos de lo que ya conocemos como Metaverso.

Con estas tecnologías verán la luz, no solo nuevos sistemas de información, sino también sistemas ciberfísicos. Son sistemas conectados entre sí y conectados a un mundo virtual de la mano de las redes digitales cuyo objetivo principal es controlar e interactuar con un proceso en el mundo físico y adaptarse a la evolución de sus condiciones en tiempo real.

²⁰ Casar, 2022

¿Cómo será este mundo digital inteligente? En el año 2017, el prestigioso informe anual de Gartner sobre tecnologías emergentes²¹ ya presentaba como una de las tres “megatendencias” que definirían la economía digital en la siguiente década lo que etiquetaba como *IA en todas las partes* y en los sucesivos informes anuales también el desarrollo y las aplicaciones de las técnicas de IA han sido sus protagonistas. No tengo el tiempo que merecería este concepto tan popular que ha sido elegido “palabra del año” por la Fundación del Español Urgente de la Real Academia de la Lengua²². Me limitaré a tratar de explicar dónde estamos y hacia dónde nos encaminamos.

En efecto, hace solo unos años, la IA demostró sus posibilidades y se empezó a introducir extensivamente. Poco después, se hizo adaptativa, es decir, capaz de monitorizar y aprender de los cambios que se producen en el entorno para reentrenar continuamente los modelos, aprender de los datos nuevos y ajustar sus objetivos.

Y ahora, el último informe Gartner, define de nuevo como una de las “megatendencias” para la siguiente década de la economía digital, lo que denomina *la automatización acelerada de la IA*²³. Nuevas técnicas que aceleran la creación de modelos de IA especializados, que son desarrollados y entrenados utilizando, a su vez, técnicas de IA. La IA diseña IA. Como resultado las predicciones y decisiones son más rápidas, eficientes y precisas. No es fácil darse cuenta de lo que esto significa, pero obviamente, el papel de los humanos se está limitando a ser consumidores, asesores y, en el mejor de los casos, supervisores. Un proceso que produce vértigo.

Por otro lado, la IA se ha vuelto *generativa*²⁴, con solo unas pocas indicaciones de una persona, sus modelos ya generan textos, imágenes e incluso videos convincentes a partir de datos extraídos de internet. Es uno de los resultados de la iniciativa “*Open AI*”²⁵ que propugna una IA abierta que democratiza el acceso a estas tecnologías y las socializa... más vértigo.

El impacto en los medios de comunicación de uno de sus primeros productos, el popular ChatGPT, las reacciones y debates que está suscitando en estos días, quizá son exagerados, pero demuestran que estamos ante una tecnología disruptiva. A ChatGPT-3 no sólo se le atribuye la capacidad de explicar conceptos científicos complejos mejor que muchos profesores, escribir buena música y elaborar cualquier texto a gusto del usuario, también parece que tiene capacidad

²¹ Gartner, 2017

²² FUNDÉU, 2022

²³ Gartner, 2022

²⁴ MIT, 2022

²⁵ OPENAI, 2023

de generar código para programas. Algo que, como siempre, tiene muchísimas aplicaciones para hacer el bien y para hacer el mal.

Los ciberdelincuentes serán los primeros en encontrarle aplicaciones, por ejemplo, elaborando automáticamente código malicioso personalizado en cada una de las víctimas. También algunos de nuestros estudiantes tienen puestas sus esperanzas en estas aplicaciones y no precisamente para aprender más, al menos, con los estándares culturales que utilizamos.

Permítanme que me detenga brevemente en este punto.

Cuando empecé mis labores docentes, a finales de los años setenta del pasado siglo, un ejercicio intelectual, por ejemplo la realización de un simple trabajo evaluable en una asignatura, implicaba una labor ardua de búsqueda de información en libros y revistas disponibles en bibliotecas; una información que siempre era limitada. Posteriormente un trabajo muy personal de comprensión, análisis y redacción permitía obtener el producto. Los alumnos empleaban varias semanas en hacer un número muy limitado de trabajos a lo largo del curso. Ahora, en plena sociedad de la información, en el mismo periodo tiempo, los alumnos realizan numerosos trabajos de alcance similar, pero les lleva hacer cada uno de ellos sólo algunas horas gracias a sus dispositivos y a internet. Claro que tenemos algunas dudas sobre el proceso de aprendizaje que ello implica. ¿Qué pasará en los próximos años, con una herramienta similar al ChatGPT en la que con algunas indicaciones el alumno obtenga, en unos segundos, un trabajo de calidad equivalente o superior a la de los trabajos que ahora realizan? Algo similar ocurrirá en otras muchas actividades de carácter intelectual, cuando el incremento en la potencia de cálculo y el desarrollo de nuevos algoritmos permita optimizar este tipo de aplicaciones.

Lo que está ocurriendo en estos momentos con el ChatGPT es el indicador de una disrupción que tendremos que asimilar y que desembocará en cambios sociales muy profundos. Es solo el principio, la IA nos dará sorpresas similares en los campos de la visión artificial, robótica, programación, predicción, producción etc.

Son numerosos los documentos, incluso las denuncias que nos hablan de que las empresas que están utilizando técnicas de IA son cada vez más numerosas y pequeñas, son *startups*, que se comportan como en el “salvaje Oeste”, con apenas reglas que limiten el uso y desarrollo de esta tecnología. De hecho, los reguladores de todo el mundo están tratando de contenerlas, como es el caso del Reglamento sobre la Inteligencia Artificial que está tramitando la Unión Europea. Estamos, insisto, ante un típico fenómeno de disrupción.

El proceso es imparable y caminamos hacia la sociedad del conocimiento. Hablamos de hogar inteligente, ciudades inteligentes, salud inteligente, transporte inteligente... que tienen en común la aparición de un elemento disruptivo, la IA

habilitadora de unas tomas de decisión mucho más eficientes que las del operador humano, al menos en términos de velocidad de respuesta. Lo peor es que en muchos casos los algoritmos utilizan criterios no conocidos ni explicados, en algunos casos “decisiones ciegas”, como puede ocurrir con las técnicas de aprendizaje profundo. En definitiva, hablamos de la sustitución del operador humano – lo que por otra parte han estado haciendo de modo acelerado las tecnologías digitales durante los últimos cuarenta años- pero ahora, y es una diferencia muy relevante, hasta los niveles de decisión más críticos. Por ello la “explicabilidad” de la IA es uno de los retos que deben abordarse.

¿Y en el ámbito de la defensa y seguridad?, Imaginemos un sistema de mando y control automatizado, conectado de alguna manera a internet y otros servidores específicos, similar al ChatGPT, en que todos y cada uno de los mandos y soldados implicados en una operación militar puedan en cualquier momento consultar que hacer, y que los errores y sesgos en las informaciones e instrucciones recibidas sean inferiores a las que les suministrarían directamente sus mandos.

Obviamente las Fuerzas Armadas de todos los países y en particular, las nuestras y las de nuestros aliados, son conscientes de estos cambios, aunque el concepto de Defensa Inteligente no es todavía tan popular como en otros sectores de actividad donde se les atribuye el adjetivo inteligente con mucha más frecuencia.

Defensa Inteligente...

El concepto de Defensa Inteligente se ha utilizado para definir la aplicación de las tecnologías base de la “cuarta revolución industrial” a la optimización de las actividades de las Fuerzas Armadas y Fuerzas y Cuerpos de Seguridad del Estado. Su fin es maximizar el potencial de sus componentes y aliviar en lo posible la exposición a los peligros inherentes a sus misiones. En última instancia se trata de configurar unas Fuerzas Armadas menos numerosas pero dotadas de potentes medios basados en las últimas tecnologías.

Es importante resaltar que la Defensa Inteligente no solo implica desarrollar nuevas tecnologías para ser una “nación inteligente”, también obliga a la selección de aquellas por las que apostar. Un elemento esencial que considerar en esta elección es la dualidad de las tecnologías implicadas, lo que la convierte en una decisión estratégica que debe estar encaminada a apoyar las industrias de defensa nacionales. Es como se ha planteado en los países que la definen así y que coinciden con aquellos cuyas economías se están digitalizando más rápidamente.

Concretaré estas ideas en un ejercicio de prospectiva sobre como el desarrollo de estas tecnologías impactará en las futuras operaciones militares. Un ejercicio arriesgado por dos razones. En primer lugar, porque especular con unas tecnologías que están en permanente evolución siempre es muy complicado y posiblemente abocado al fracaso. En segundo lugar, porque para un profesor

universitario hablar de operaciones militares ante personas que han desarrollado su trayectoria profesional estudiando, diseñando y participando en operaciones militares, como es el caso de una buena parte de los aquí presentes, no es un reto, es un atrevimiento que espero superar entrando muy superficialmente en los temas no tecnológicos y contando con su indulgencia.

El nuevo campo de batalla inteligente: datificación, hiperconexión, autonomía e inteligencia

Es de todos conocido que, lejos ya los tiempos de la Guerra Fría, en los últimos años el contexto de los conflictos ha evolucionado hacia una gran complejidad, con la aparición de nuevos entornos de conflicto, como el ciberespacio y el dominio cognitivo ya mencionados, donde, además de los conflictos convencionales entre estados, aparecen nuevos tipos como los asimétricos, de creciente sofisticación a medida que se facilita y abarata el acceso a las tecnologías emergentes, y los híbridos donde los enfrentamientos se libran simultáneamente en los ámbitos militares y civil.

En un futuro próximo, y me refiero más o menos a un periodo de 10 a 15 años -al horizonte 2035 que utilizan nuestras Fuerzas Armadas-, el Jefe del Estado Mayor de la Defensa (JEMAD)²⁶ lo definió con tres elementos clave: como un entorno VUCA, caracterizado por su volatilidad, incertidumbre, complejidad y ambigüedad; en zona gris, con muchas actividades hostiles por debajo del umbral del conflicto, e hiperconectado por el uso extensivo de la digitalización. Un entorno que, en opinión del JEMAD, requiere unas Fuerzas Armadas, trabajando en un entorno multidominio, donde la superioridad de la información será un aspecto clave y su consecución se basa en la superioridad tecnológica. Por lo demás, son ideas similares a las que mantienen en la OTAN²⁷ y otras organizaciones militares.

Quédense, por favor con esta última idea expresada por el JEMAD, “la superioridad de la información será un aspecto clave y su consecución se basa en la superioridad tecnológica”, y permítanme que reflexione, e incluso especule, sobre algunos aspectos tecnológicos de estos nuevos escenarios de conflicto. Lo haré utilizando las cuatro palabras clave indicados en título de este apartado que definen funcionalidades de base tecnológica presentes en los futuros campos de batalla.

Empecemos por la *datificación*.

Datificación

²⁶ JEMAD, 2021

²⁷ OTAN, 2020

Este neologismo, todavía no recogido por la Real Academia de la Lengua en su diccionario, alude a la conversión de procesos que antes eran efímeros en datos que se almacenan y analizan²⁸. Estamos datificando la realidad y no solo con sensores electromagnéticos y electroópticos cada vez más eficaces, en términos de alcance, precisión y capacidad de identificación- y de menor coste.

En efecto, el número de teléfonos inteligentes en el mundo se calcula en cerca de 7.000 millones y el número de personas que usan internet ya supera los 5.000 millones. La potencia de sensorización y capacidad de distribución de los datos obtenidos es muy difícil de imaginar y, de hecho, la cantidad de información producida y distribuida por fuentes abiertas es enorme y está disponible. En los actuales y futuros escenarios de conflicto el potencial de sensorización de todas las personas involucradas en ellos será también enorme. De hecho, ya está ocurriendo en la Guerra de Ucrania donde los civiles reportan en tiempo casi real muchas incidencias de las operaciones.

Además, en pocos años veremos desplegarse los dispositivos y sistemas de lo que se denomina la IoT, la Internet de las Cosas, que no es más que conjuntos de objetos físicos que se comunican datos entre sí, con un control central o sin él, pero que trabajan coordinadamente sin la intervención explícita de un humano. En pocos años la Internet de las Cosas estará basada en tecnologías estandarizadas, lo que se traducirá en un radical abaratamiento que permitirá configurar centenares de miles de redes con millones de millones de conexiones fiables y seguras. Estas redes de sensores estarán disponibles en muchos escenarios de conflicto y, si no es el caso, se desplegarán.

Desde el punto de vista de las operaciones militares el reto es la necesidad y consecuencias del despliegue de unas tecnologías que convierten la realidad de un campo de batalla de datos. El problema no radicará tanto en la falta de información, como ocurre muchas veces en estos momentos, como es el exceso de ésta y su gestión requerirá nuevas herramientas y técnicas.

Continuemos con las palabras clave, *hiperconectividad*.

Hiperconectividad

Para anticiparse a las amenazas y aprovechar sus debilidades es necesario ser ágiles en la toma de decisiones y en la acción en el campo de batalla, lo que requiere coordinación en tiempo real de las actividades asociadas a las distintas operaciones. Además, se trabajará en un entorno multidominio, lo que, unido a lo anterior, exigirá una conectividad masiva entre todos los participantes en las operaciones, pero selectiva en cuanto a los contenidos intercambiados. En definitiva, romper las barreras espaciales y temporales, así como adaptar la

²⁸ FUNDÉURAE, 2022

información a las necesidades de los diferentes combatientes desplegados en los conflictos. Esto ya lo permiten los actuales sistemas de comunicaciones de última generación, en particular la tecnología 5G, pero las versiones más avanzadas de estos sistemas tardarán en desplegarse.

Por otro lado, además de la gran capacidad de transmisión de la información y la baja latencia de los datos, la principal novedad que incorporarán los nuevos sistemas de comunicaciones será en el procesamiento de la información mientras está siendo transmitida. La información se modificará mientras recorre las redes para adaptarla a las necesidades del combatiente. Las redes serán inteligentes y jugarán un papel esencial en la consecución de la superioridad de la información.

¿Qué tecnología se utilizará? Aunque por razones relacionadas con la seguridad y protección de las comunicaciones es un tema sometido a debate, estoy convencido que la tecnología 5G se impondrá y que al final habrá un estándar 5G militar que se desplegará en los campos de operaciones junto a otras redes redundantes de menores prestaciones.

Por supuesto que el uso de satélites será esencial, en muchos casos incorporando las tecnologías 5G. Hasta ahora no ha habido ningún conflicto explícito en el dominio del espacio ultraterrestre y, como está ocurriendo en la Guerra de Ucrania, los satélites mantienen la conectividad en grandes áreas con independencia de los combates en los otros dominios. Es muy posible que el primer conflicto explícito en dominio ultraterrestre esté relacionado con el control de las comunicaciones satelitales.

La dualidad de las tecnologías implicadas y el hecho de que su vector de innovación esté en el mundo civil constituye un importante reto para el mundo militar que debe de ser capaz de introducirlas muy rápidamente para evitar la obsolescencia anticipada en su implantación.

En este sentido es relevante lo que está ocurriendo en el conflicto de Ucrania. Llama la atención la robustez y resiliencia que los sistemas de telefonía móvil y la internet están teniendo, pero todavía más sorprendente es el papel que las redes de telefonía móvil están teniendo en las operaciones militares²⁹. La lección aprendida, según el General de Brigada Director de la Escuela de Guerra del Ejército es que, y cito literalmente, “la decisión de qué hacer con la red de telefonía móvil en la zona de combate debe ser uno de los elementos básicos contemplados en todo plan de operaciones en el campo de batalla moderno”. Permítanme que vaya lejos, en los futuros campos de batalla las redes civiles y militares – estas últimas basadas en tecnologías civiles- librarán un enfrentamiento decisivo para la resolución del conflicto.

²⁹ Frías, 2022.

La siguiente palabra clave que definirá el futuro campo de batalla inteligente es *autonomía*.

Autonomía

Entre otras acepciones, la Real Academia Española (RAE) define autonomía como la condición de quien, para ciertas cosas, no depende de nadie; lo que es coherente con la definición de sistemas autónomos realizada por Watson D.P. y Scheidt D.H. en su artículo seminal de 2005³⁰ quienes los definen como aquellos que cambian su comportamiento en respuesta a hechos imprevistos. Una definición incompleta pero muy clara.

La autonomía permite aumentar las distancias entre los combatientes y reducir los riesgos y el número de bajas. La autonomía implica conocer el entorno mediante sensores, su análisis con procesadores y la realización de acciones con actuadores no controlados directamente. Los sistemas autónomos requieren mucha potencia de cálculo en tiempo real, lo que será posible aprovechando las nuevas arquitecturas de los sistemas de información y comunicaciones, utilizando por ejemplo arquitecturas de computación en la nube, en el borde y en la niebla (*cloud, edge and fog computing*).

No creo equivocarme si afirmo que en los próximos años el desarrollo de los sistemas autónomos se caracterizará por dos líneas de fuerza: la utilización masiva de técnicas de IA y un espectacular desarrollo de sistemas ciberfísicos, ya mencionados, conectados entre sí y con el mundo virtual a través de las redes digitales globales. El coche autónomo es uno de sus paradigmas en el ámbito civil, otro los futuros sistemas de armas inteligentes a las que luego me referiré.

La última palabra clave, *inteligencia*.

Inteligencia

Como se ha indicado, los avances en la IA permitirán automatizar y dotar de inteligencia a los sistemas militares. La autonomía con mínima supervisión será una realidad en los vehículos y las armas. La toma de decisiones asociada a los sistemas de mando y control también sufrirá una transformación radical al basarse en asesores digitales. Lo mismo ocurrirá con los sistemas de guerra electrónica, los de reconocimiento y vigilancia, las plataformas logísticas, los medios de transporte, etc. De hecho, la inteligencia, en muchos casos de origen algorítmico, será transversal a todos los sistemas de defensa y seguridad como lo serán en el resto de los sectores de actividad pues la dualidad de las tecnologías será un elemento esencial en este proceso.

³⁰ Watson, 2005

No quiero insistir más, pero lo cierto es que se ha llegado a un punto en que la IA superará, si no lo ha hecho ya en muchos campos, al poder cognitivo de los seres humanos. Los algoritmos pueden tomar decisiones muy rápidamente y cambiarlas en función de la evolución de la amenaza, permitiendo una acción más rápida para combatirla. Por eso la IA se ha convertido en uno de los principales objetivos de los casi todos los países que están aumentando significativamente sus inversiones en este ámbito del conocimiento. Se ha llegado a afirmar que, en el campo militar, el equilibrio internacional estará determinado por los proyectos de IA.

Datiificación, hiperconectividad, autonomía e inteligencia. Nótese las interdependencias y sinergias entre las cuatro funcionalidades de base tecnológica con las que he tratado de describir las futuras operaciones militares: sin inteligencia, la autonomía no puede llegar lejos; sin datos, no hay inteligencia; sin conectividad, no hay datos. Por otro lado, es muy importante ver la simbiosis que existe entre ellas. A modo de ejemplo, la introducción de IA en los sistemas requiere enormes volúmenes de datos, pero, a su vez, la introducción de la IA en los sistemas de adquisición y transmisión de datos facilita la obtención de estos.

¿Cuándo y cómo se introducirán estas nuevas funcionalidades? ¿Cuándo su papel será relevante en el campo de batalla? ¿Estamos ante futuros escenarios similares a los que describen las películas de ciencia ficción en que combaten las máquinas? Las respuestas a estas preguntas implican un elevado grado de especulación que asumiré.

Seguro que la realidad se parecerá muy poco a las imágenes que nos presentan las películas, pero estoy convencido que la mayor parte de los implicados en los combates, hombres y máquinas, lo harán con elevados grados de autonomía y mínima supervisión. Además, sus decisiones estarán fuertemente condicionadas por asesores inteligentes que irán definiendo sus acciones a partir de los datos extraídos dinámicamente de la realidad.

Los requerimientos tecnológicos de la introducción de inteligencia, autonomía e hiperconectividad implicarán un gran esfuerzo de ingeniería, pero no será la limitación más importante. En los próximos años, los desarrollos de estas tecnologías en el ámbito civil asegurarán su disponibilidad en el ámbito militar, con el único riesgo, nada desdeñable, de su velocidad de obsolescencia, fruto de las necesidades de innovación en los ecosistemas inteligentes civiles, poco compatibles con los actuales ritmos de introducción de cambios tecnológicos en el ámbito militar.

Los sistemas militares son mucho más exigentes que los civiles, deben trabajar en unas condiciones mucho más duras, sus tolerancias al fallo son muy pequeñas y tienen ciclos de vida mucho más elevados. Cabe, pues, esperar que la introducción de las innovaciones sea bastante más lenta en el ámbito militar. Además, como se

ha mencionado, las principales dificultades que puede paralizar el desarrollo de estas técnicas no radicarán en estos componentes técnicos o tecnológicos. Los retrasos más significativos en su implantación vendrán de elementos de índole socioeconómica, así como el factor humano de resistencia al cambio.

En mi opinión serán necesarias entre una y dos décadas para que todo esto se haga realidad, pero las consecuencias de su implantación serán más profundas de lo que en estos momentos podemos imaginar.

Lo que parece claro es que serán los sistemas de mando y control los primeros en que se aplicarán técnicas de IA para la ayuda a la toma de decisiones, lo que se traducirá en un incremento exponencial de los niveles de la autonomía en el mando y control de las operaciones. En este contexto, los algoritmos serán en gran medida los responsables del éxito de las operaciones. Las ventajas estratégicas y tácticas asociadas a la velocidad y adaptabilidad de las tomas de decisiones lo hacen inevitable³¹.

Los sistemas de ciberdefensa y guerra electrónica serán también de los primeros en incorporarlas, entre otras causas, por la reducción de tiempos de respuesta que se requerirá. Sin duda serán los sistemas donde se desarrollará antes y con gran intensidad el combate algorítmico. Después irán los sistemas de reconocimiento y vigilancia, los sistemas de transporte, los sistemas logísticos, etc.

Naturalmente, también los sistemas de armas serán inteligentes. Se convertirán en sistemas ciberfísicos, en muchos casos sistemas de sistemas, que en los próximos años estarán dotados de elevados niveles de autonomía por el uso masivo de técnicas de IA. Es el caso, por ejemplo, de los programas VCR 8x8 "Dragón", la fragata F-110 o el concepto FCAS, el futuro sistema de combate aéreo en desarrollo por varios países europeos, entre ellos el nuestro.

Son sistemas cuyo objetivo final es la destrucción y, por tanto, muy susceptibles de producir daños colaterales. Ello conlleva una serie de precauciones de índole ético, jurídico y humanitario que pueden limitar y retrasar la introducción de técnicas que supongan altos niveles de autonomía.

Un comentario especial merece lo que denominamos sistemas de armas autónomas letales, en los que el operador no elige más que aproximadamente las coordenadas espaciales y temporales del objetivo a batir y por tanto entraña un mayor riesgo de pérdida del control humano.

¿Cuál será el grado de autonomía que se implementará en los sistemas de armas del futuro? El problema radica en que, como ya he reiterado, las técnicas de IA ya han demostrado su superioridad frente al ser humano, especialmente cuando se requiere agilidad y eficiencia en las operaciones, cualidades esenciales en esta

³¹ Haga, 2020

aplicación y que serán mucho más necesarias cuando se reduzcan los tiempos de respuesta con la llegada a los campos de operaciones de las armas hipersónicas y de las armas de energía dirigida. Aunque es un tema sujeto a controversia, mi opinión es que inevitablemente se evolucionará a que en muchas situaciones el combate sea autónomo, donde el papel del operador sea de «control» y no de «ejecución».

¿Cómo asegurar los estándares éticos que exigen nuestras sociedades democráticas? Quizá la solución venga de la propia IA. Lo que cabe esperar es la generación de algoritmos inteligentes de control predictivo del «funcionamiento correcto» de estas armas. Algoritmos que lleven la probabilidad de error a unos límites asumibles por los criterios éticos y jurídicos.

Permítanme ahora una breve reflexión sobre el papel de otras tecnologías emergentes en el campo de batalla inteligente.

De lo digital a lo cuántico y lo biotecnológico

Por supuesto que hay otras tecnologías, no digitales, que impactarán en las operaciones el futuro campo de batalla. La OTAN ha definido las tecnologías emergentes y disruptivas de especial relevancia en el ámbito de la Defensa³². De hecho, en febrero de 2021, los ministros de Defensa de la OTAN respaldaron una estrategia de innovación sobre tecnologías emergentes y disruptivas que se concreta en nueve áreas tecnológicas, tres de las cuales han sido objeto de análisis en los párrafos anteriores. Curiosamente son áreas que ya se han definido como disruptivas y las primeras en que las correspondientes estrategias han sido aprobadas^{33 34}.

Del resto de áreas tecnológicas emergentes, las que potencialmente tienen mayores posibilidades de ser disruptivas serán las tecnologías cuánticas y las biotecnologías, y en particular la neurotecnología, que conectará el cerebro humano con los sistemas de información y, a través de ellos, con las entidades físicas. No son el objeto de este discurso, pero permítanme apostillar que las sinergias de estas tecnologías con las digitales son muy importantes y que, dado su grado de desarrollo, cabe esperar que tarden en impactar significativamente en las operaciones militares varias décadas, aunque cuando lo hagan las pueden transformar radicalmente.

³² OTAN, 2022

³³ OTAN, 2021

³⁴ OTAN, 2022

...Y finalizo,

El contenido de los párrafos anteriores sólo tiene una conclusión posible, la aplicación de los últimos avances de las tecnologías digitales permitirá que los sistemas utilizados en las futuras operaciones militares sean varios órdenes de magnitud más eficientes que los actualmente operativos.

Y permítanme que finalice este discurso, agradeciendo de nuevo a todos ustedes su atención y con una cita propia extraída de dos documentos publicados por esta Academia^{35 36}:

“En definitiva, en los próximos años se producirá una brecha digital en la IA entre los países que dispongan de una “Defensa Nacional Inteligente” potente -con unos sistemas militares dotados de IA, personal capacitado para diseñarlos, producirlos y operarlos, y recursos invertidos en su despliegue- y otros que no. Las decisiones que se tomen ahora definirán a que grupo se pertenecerá en el futuro... y también el peso de cada país en la nueva economía digital globalizada”

He dicho.

Referencias

1. ACAMI-PÁGINA WEB. <https://www.acami.es/>.
2. UPM-PÁGINA WEB. <https://www.upm.es/>.
3. ETSIT-PÁGINA WEB. <https://www.etsit.upm.es/>.
4. Fundación Círculo-PÁGINA WEB. <https://www.fundacioncirculo.es/>.
5. COIT-PÁGINA WEB. <https://www.coit.es/>.
6. IIE-PÁGINA-WEB. <https://www.iies.es/>.
7. IPTC-PÁGINA WEB. <https://www.upm.es/recursosidi/map/centro-de-idi-en-procesado-de-la-informacion-y-telecomunicaciones/>.
8. Pérez Martínez, Félix. Las tecnologías de la información y las comunicaciones en la seguridad y la defensa nacional. Boletín de Información del CESEDEN nº 275, Ed. Ministerio de Defensa, Madrid, 2002. https://publicaciones.defensa.gob.es/media/downloadable/files/links/b/o/boletin_ceseden_275.pdf.
9. Pérez Martínez, Félix. El papel de las TIC en los sistemas para la seguridad y la defensa. Revista BIT, nº 154. Ed. COIT-AEIT. Madrid, 2006.

³⁵ De la Fuente, 2022

³⁶ Pérez, 2020

- <https://www.coit.es/sites/default/files/archivobit/pdf/felixperez.pdf>.
10. THE ENTERPRISERS PROJECT. *What is digital transformation?* 2016.
<https://enterprisersproject.com/what-is-digital-transformation>
 11. Pérez Martínez, Jorge. “Las tecnologías de la información y las comunicaciones en la sociedad global de la información”. Tecnología y sociedad en el nuevo siglo, II Foro sobre Tendencias Sociales. Ed. Sistema, Madrid, 1998.
 12. Ortega Castro, Vicente et al. “Relaciones entre las innovaciones tecnológicas y la defensa”. Cuadernos Cátedra ISDEFE-UPM, nº 1. Ed. FUNDETEL, 2007.
 13. Intel 4004_WIKIPEDIA. https://es.wikipedia.org/wiki/Intel_4004.
 14. Alamo, Jesús del. “Al 50º aniversario de la ley de Moore, la nanoelectrónica en una encrucijada”. Discurso del acto de Investidura como Doctor Honoris Causa. Universidad Politécnica de Madrid, 2015.
https://www.etsit.upm.es/fileadmin/documentos/laescuela/la_escuela/conoce_la_escuela/Honoris_causa/Al_50o_aniversario_de_la_Ley_de_Moore-2_PDF_MARCA_DE_AGUA_.pdf.
 15. Martí Sempere, Carlos y Granda Coterillo, José María. “¿Qué se entiende por Revolución de los Asuntos Militares (RMA)? Ponencia presentada al Seminario La RMA y España. Ed. Fundación para el Análisis y los Estudios Sociales. 2000.
[http://www.gees.org/articulos/que-se-entiende-por-revolucion-de-los-asuntos-militares-rma#:~:text=d\)%20Una%20RMA%20es%20un,o%20formas%20en%20la%20guerra](http://www.gees.org/articulos/que-se-entiende-por-revolucion-de-los-asuntos-militares-rma#:~:text=d)%20Una%20RMA%20es%20un,o%20formas%20en%20la%20guerra).
 16. Esteve Domingo, Manuel. “La superioridad operacional como concepto multidominio”. Discurso pronunciado de ingreso como Académico de Número en la Academia de las Ciencias y las Artes Militares. 2022.
<https://www.acami.es/wp-content/uploads/2022/07/2022-06-22-Discurso-Esteve-Domingo-web.pdf>.
 17. García Servert, Ruben y Calvo Albero, José Luis. “El dominio cognitivo en las operaciones multidominio: concepto y problemática”. ANALES ACAMI, 2020.
<https://www.acami.es/wp-content/uploads/2022/05/dominio-cognitivo-operaciones-multidominio-web.pdf>.
 18. Millán Martínez, José María. “Transformación digital en el Ministerio de Defensa. El viaje inaplazable”. Revista Española de Defensa, 2022.
<https://www.defensa.gob.es/Galerias/gabinete/red/2022/01/p-36-38-red-390-digital.pdf>

19. Gómez Pardo, Jesús Carlos. "Desafíos de la digitalización en la ingeniería militar". Comunicaciones académicas. ANALES ACAMI, 2022, <https://www.acami.es/publicacion/desafios-de-la-digitalizacion-en-la-ingenieria-militar/>.
20. Casar Corredera, José Ramón. "Ciencia de datos, inteligencia artificial, comunicaciones disruptivas: El potencial transformador de lo intangible". Conferencia de Apertura del Curso Académico 2021-2022 de la Real Academia de Doctores de España. 2021. <https://www.radoctores.es/imageslib/doc/Conferencia%20apertura%202022%20Dr.%20Casar.pdf>.
21. Gartner. "Gartner Identifies Three Megatrends That Will Drive Digital Business Into the Next Decade". 2017. <https://www.gartner.com/en/newsroom/press-releases/2017-08-15-gartner-identifies-three-megatrends-that-will-drive-digital-business-into-the-next-decade>.
22. FUNDEU. <https://www.fundeu.es/recomendacion/candidatas-a-palabra-del-ano-2022-de-la-fundeurae/>
23. Gartner. <https://www.gartner.es/es/tecnologia-de-la-informacion/insights/principales-tendencias-tecnologicas>. 2022.
24. Heikkila, M and Heaven, W.D. "What's next for AI". MIT Technology Review. Diciembre 2022. <https://www.technologyreview.com/2022/12/23/1065852/whats-next-for-ai/>
25. OPENAI. <https://openai.com>.
26. JEMAD. "El campo de batalla digital: Retos tecnológicos para la transformación de las FAS. Conferencia organizada por la Fundación Círculo de Tecnologías para la Defensa y la Seguridad. Junio 2021. <https://emad.defensa.gob.es/prensa/noticias/2021/06/Listado/210603-jemad-fundacion-circulo.html>.
27. OTAN. "Science & Technology Trends 2020-2040. Exploring the S&T Edge". NATO Science & Technology Organization. 2020. https://www.nato.int/nato_static_f12014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf
28. FUNDÉURAE. <https://www.fundeu.es/recomendacion/datificacion-no-dataficacion/>.
29. Frías Sánchez, Carlos Javier. "Ucrania: la guerra de los teléfonos móviles". Documento de opinión del Instituto Español de Estudios Estratégicos, diciembre 2022. https://www.ieee.es/publicaciones-new/documentos-de-opinion/2022/DIEEEO112_2022_CARFRI_Ucrania.html.
30. Watson, David P. and Scheidt, David H., "Autonomous Systems". Johns Hopkins Applied Physics Laboratory, Technical Digest, vol. 26, no. 4, 2005.

- <https://media.gradebuddy.com./documents/308016/50c4b270-5562-40d5-8e9d-5c3e29fde4bc.pdf>.
31. Haga W. and Crosby C. "AI's Power to Transform Command and Control". National Defense, 2020.
<https://www.nationaldefensemagazine.org/articles/2022/8/26/sustainable-aviation-market-takes-global-stage>.
 32. OTAN. "Emerging and disruptive technologies". Diciembre, 2022
https://www.nato.int/cps/en/natohq/topics_184303.htm?selectedLocale=en.
 33. OTAN. "Summary of the NATO Artificial Intelligence Strategy". Octubre, 2021
https://www.nato.int/cps/en/natohq/official_texts_187617.htm.
 34. OTAN. "Summary of NATO's Data Exploitation Framework Policy". Diciembre, 2022.
https://www.nato.int/cps/en/natohq/official_texts_210002.htm.
 35. De la Fuente Chacón, José Carlos (editor). "Sistemas autónomos y robótica inteligente en Defensa". Capítulo: "Los sistemas autónomos y la transformación digital del campo de batalla"; Pérez Martínez, Félix. ACAMI. Ediciones El Crítico. 2022.
<https://www.acami.es/noticia/sistemas-autonomos-y-robotica-inteligente-en-defensa/>.
 36. Pérez Martínez, Félix. "Defensa inteligente en un mundo inteligente". Comunicaciones académicas. Academia de las Ciencias y las Artes Militares, 2020.
<https://www.acami.es/publicacion/defensa-inteligente-en-un-mundo-inteligente/>.