REAL ACADEMIA DE DOCTORES
DE ESPAÑA

DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL EN LOS FUTUROS ESCENARIOS DE CONFLICTO: HACIA UNA DEFENSA INTELIGENTE

DISCURSO
PRONUNCIADO POR EL

EXCMO. SR. DR. D. FÉLIX PÉREZ MARTÍNEZ

EN EL ACTO DE SU TOMA DE POSESIÓN
COMO ACADÉMICO DE NÚMERO
EL DÍA 12 DE JUNIO DE 2024

Y CONTESTACIÓN DEL

EXCMO. SR. DR. D. JOSÉ RAMÓN CASAR CORREDERA

MADRID
MMXXIV

REAL ACADEMIA DE DOCTORES
DE ESPAÑA

DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL EN LOS FUTUROS ESCENARIOS DE CONFLICTO: HACIA UNA DEFENSA INTELIGENTE

DISCURSO
PRONUNCIADO POR EL

EXCMO. SR. DR. D. FÉLIX PÉREZ MARTÍNEZ

EN EL ACTO DE SU TOMA DE POSESIÓN
COMO ACADÉMICO DE NÚMERO
EL DÍA 12 DE JUNIO DE 2024

Y CONTESTACIÓN DEL

EXCMO. SR. DR. D. JOSÉ RAMÓN CASAR CORREDERA

MADRID
MMXXIV

DISCURSO
DEL EXCMO. SR.
DR. D. FÉLIX PÉREZ MARTÍNEZ

"A Lalines,
compañera infatigable en un viaje lleno de satisfacciones,
a Paloma y Ana,
por darnos todo lo que esperábamos y mucho más,
a Nacho, Javier y Juan,
porque son el futuro

DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL EN LOS FUTUROS ESCENARIOS DE CONFLICTO: HACIA UNA DEFENSA INTELIGENTE

Félix Pérez Martínez

ÍNDICE

SALUTACIONES Y EXPRESIONES DE GRATITUD

Excelentísimo señor presidente,

Excelentísimos y excelentísimas señores y señoras académicos de la Real Academia de Doctores de España,

Señoras, señores, amigos,

Permítanme iniciar este discurso de ingreso en la Real Academia de Doctores de España expresando el profundo honor que representa para un Doctor Ingeniero de Telecomunicación ser admitido en esta prestigiosa institución, cuyos miembros, distinguidos investigadores, profesores, creadores y líderes de opinión, desempeñan un papel fundamental en el desarrollo de las Ciencias, las Letras y las Artes, así como en la promoción de la Cultura, según lo establecen los estatutos que rigen esta corporación y se hace realidad en su diaria actividad.

Ser acogido en una Real Academia cuya esencia es la interdisciplinaridad me brindará la oportunidad de colaborar con destacados profesionales en diversos campos científicos y tecnológicos. Este hecho culminará una trayectoria de más de cuarenta años dedicados a la investigación, la enseñanza y la difusión de tecnologías relacionadas con la defensa y seguridad, las cuales compartiré con ustedes en los próximos minutos.

Los siguientes párrafos no deben interpretarse como un mero protocolo de cortesía; por el contrario, expresan mi sincero agradecimien-

to y reconocimiento a las personas y entidades que me han acompañado a lo largo de estos años, haciendo posible que hoy comparta desde este estrado el contenido de mi discurso con todos ustedes.

Quisiera empezar expresando mi agradecimiento a la Real Academia de Doctores de España, a todos sus miembros, por admitirme como Académico de Número. En particular, deseo mostrar mi reconocimiento al Dr. Bascones Martínez, quien la preside con habilidad, logrando equilibrar con acierto la rica historia de tradiciones que deben preservarse y la necesidad de adaptar objetivos y procedimientos a las cambiantes exigencias de una sociedad en constante evolución. Muchas gracias Señor Presidente, le garantizo que no defraudaré la confianza depositada en este Doctor y me comprometo a contribuir con esfuerzo y dedicación al prestigio de esta institución en nuestra sociedad. Muchas gracias porque, como como dice el refrán que Sancho reivindica en El Quijote, "júntate a los buenos y serás uno dellos".

Y no será fácil suceder en el desempeño de la medalla nº 8 de la Sección de Ingeniería de esta Real Academia a los doctores Darío Maravall Casesnoves, José María Martínez-Val Peñalosa y Aníbal Figueiras Vidal, todos ellos insignes catedráticos de universidad con trayectorias profesionales reconocidas con numerosos honores y premios. Permítanme un sentido recuerdo para el Dr. Anibal Figueiras, que presidió la Real Academia de Ingeniería, Académico Electo de la nuestra que desgraciadamente nos dejó antes de tomar posesión de la medalla. Compartí con él durante muchos años numerosas actividades en la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universidad Politécnica de Madrid, en adelante ETSIT-UPM, y en otras entidades y foros. Le reconozco como uno de mis maestros. Además de ser uno de los principales introductores del procesado digital de la señal en nuestro país, también desde diferentes responsabilidades, contribuyó al desarrollo y difusión de las tecnologías de la información y comunicaciones, en adelante TIC. Sin duda fue uno de mis colegas más respetados.

Unas palabras también sobre el Dr. Dario Maravall Casesnoves, insigne matemático e ingeniero, que dejó su impronta en esta institución a la que perteneció durante casi 36 años. Como lo hizo en muchas otras, en la Real Academia de Ciencias Exactas, Físicas y Naturales, en la UPM o en los Colegios Oficiales de Ingenieros Agrónomos de España que le nombraron Colegiado de Honor, por citar solo algunas. Oí hablar de él a principios de los años ochenta en boca de su hijo, el Dr. Ingeniero de Telecomunicación Darío Maravall Allende, con quien compartí, además de mis primeros años de trayectoria profesional en la ETSIT-UPM, la participación en las actividades de nuestro colegio profesional y un interés por ir más allá de las puras labores de ingeniería. Recuerdo que "don Darío" era un referente en nuestro sistema universitario, que trabajaba en escenarios matemáticos de frontera, con una envidiable productividad científica en campos tan diferentes y a la vez tan sinérgicos como la filosofía, la física, las matemáticas o la ingeniería. Como no recordar su obra "Grandes Problemas de la Filosofía Científica", una reflexión metacientífica sobre estas disciplinas con la que realizó importantes aportaciones en el campo de la filosofía y de la teoría de la ciencia.

Es difícil no sentirse abrumado por la responsabilidad de continuar la labor de estos insignes académicos pero, con la ayuda de todos ustedes, confío en tener éxitos en las labores que se me encomienden desde esta institución.

Retornando a los agradecimientos, uno imprescindible al apoyo de la Sección de Ingeniería y a los académicos que avalaron mi candidatura, doctores José Javier Etayo Gordejuela, de la Sección de Ciencias Experimentales, José Manuel Ramírez Sebastián, de la Sección de Medicina, y un reconocimiento muy especial al Dr. José Ramón Casar Corredera, presidente de la Sección de Ingeniería que, además de promocionar y avalar mi candidatura, ha aceptado contestar a este discurso. Experto internacionalmente reconocido en el ámbito la ciencia y la ingeniería de datos, en particular en las técnicas asociadas a los procesos de decisión, con el Dr. Casar he com-

partido cuatro décadas de actividad docente e investigadora en el ámbito de las TIC, en la UPM. En mi etapa de Director de la ETSIT, juntos promovimos el Centro de I+D+i de Procesado de la información y las Telecomunicaciones (IPTC), el mayor por número de investigadores de nuestra Universidad, que con acierto dirige desde su creación. Su labor en esta Real Academia es de todos conocida y no necesita mayor elucidación, muchas gracias José Ramón. Gratitud que quiero extender a todos los miembros de la UPM que siempre han apoyado mis actividades docentes, investigadoras, de transferencia de tecnología y de gestión, tanto en el ámbito civil como en el de la defensa y seguridad.

No puedo dejar de mencionar a la Fundación Círculo de Tecnologías para la Defensa y Seguridad que me ha dado la oportunidad de compartir con centenares de personas del sector nuestro cariño y admiración por la labor de nuestras Fuerzas Armadas y Fuerzas y Cuerpos de Seguridad del Estado y la posibilidad de colaborar a que exista una base tecnológica e industrial en nuestro país que les ayude a cumplir sus transcendentes misiones. A la Academia de las Ciencias y de las Artes Militares (ACAMI) en la que, primero como Académico Correspondiente y ahora como Académico de Número he conocido a compañeros académicos interesados por estos temas con los que he compartido trabajos y reflexiones de enorme interés. También al Colegio Oficial, a la Asociación Española de Ingenieros de Telecomunicación (COIT-AEIT), y al Instituto de la Ingeniería de España, (IIE) que siempre me apoyaron en estos objetivos. Tampoco quiero olvidar a mis compañeros del grupo de investigación Microondas y Radar, uno de los grupos de investigación de nuestro país que más ha trabajado en la I+D+i para la Defensa.

Por último, pero los primeros en mi corazón, a mi familia que en todo momento me han acompañado y apoyado en mi trayectoria profesional: a mi compañera de este viaje, Lalines, a mis hijas Pa-

loma y Ana; y a mi hermano, el Profesor Jorge Pérez, con el que he compartido una buena parte de esta aventura en la UPM.

Muchas gracias a todos los que lo han hecho posible y mi agradecimiento a todos ustedes por su presencia aquí, compartiendo conmigo este acto, en el que, siguiendo los consejos del Dr. Casar, utilicé para mi exposición unos 45 minutos. En mi discurso en el Paraninfo de la Universidad Complutense de Madrid, muchas cosas se quedaron en el tintero pero todas se podrán recuperar en el libro impreso que tiene entre sus manos.

I. EXORDIO

Tu trabajo va a llenar gran parte de tu vida, y la única forma de estar realmente satisfecho es hacer lo que crees que es un gran trabajo. Steve Jobs. Discurso de graduación en la Universidad de Stanford en junio de 2005.

El título seleccionado para mi discurso, "Digitalización e inteligencia artificial en los futuros escenarios de conflicto: hacia una defensa inteligente*"* resume diversos artículos y conferencias de mi autoría, a lo largo de veinte años, complementados con reflexiones personales derivadas de mis interacciones con individuos vinculados al sector de la Defensa en las instituciones y entidades previamente mencionadas. El eje central de mi discurso versará sobre las causas y repercusiones que las TIC tienen en los actuales y futuros teatros de operaciones para el mantenimiento de la paz y, desgraciadamente en demasiadas ocasiones, para combatir en los campos de batalla.

La casualidad hizo que iniciase mis labores docentes e investigadoras en el área de las microondas y los radares, unas tecnologías que nacieron y se desarrollaron para aplicaciones militares jugando un papel esencial durante la Guerra Fría. Ello me condujo inevitablemente a entrar en contacto con nuestras Fuerzas Armadas y con sus necesidades en estos ámbitos a mediados de los años ochenta del pasado siglo.

Por otro lado, eran los años donde las TIC, cuyo potencial transformador había quedado demostrado tras la segunda Guerra Mundial, empezaban a digitalizarse. Tuve la suerte de participar en la ET-

SIT-UPM en este proceso de gran impacto en los ámbitos de la docencia y la investigación. Los finales de los 80 y los años 90, también fueron los de la gran transformación de nuestro país. Entramos en las instituciones europeas, se estabilizaron nuestros sistemas político, económico y judicial, se transformaron radicalmente nuestras Fuerzas Armadas. La digitalización de nuestras infraestructuras fue el germen de un incremento de actividad en todos los sectores, especialmente en el sector TIC. Se apostó por la industria nacional, se pusieron en marcha planes y programas nacionales y europeos que implicaban el desarrollo y empleo de tecnologías propias. Se desarrolló un sector industrial de la defensa que incorporaba las tecnologías digitales y, no sin esfuerzo, incidía en paradigmas doctrinales fuertemente asentados en nuestras Fuerzas Armada. Como espectador privilegiado de este proceso, no es extraño que, durante la realización del Curso de Defensa Nacional, impartido en el Centro Superior de Estudios de la Defensa Nacional (CESEDEN), escogiese como trabajo fin de curso uno titulado "Las TIC en la Seguridad y Defensa Nacional", que fue publicado en el Boletín de Información de dicha institución en el año 2002[(1)]. Posteriormente, un resumen actualizado se difundió en la revista BIT del COIT-AEIT en 2006[(2)], consolidándose como un área constante de estudio en paralelo a mi actividad principal como diseñador de sistemas radar y de radiofrecuencia.

En nuestro país, las actividades asociadas a la Defensa y Seguridad han sido tradicionalmente percibidos por la Academia con cierto distanciamiento, cuando no con una oposición frontal. En el año 2002 tuve ocasión de participar en un debate promovido por la Fundación para el conocimiento MadridI+D titulado "¿Contribuye la

---

(1) PÉREZ MARTÍNEZ, F. *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

(2) PÉREZ MARTÍNEZ, F. *El papel de las TIC en los sistemas para la seguridad y la defensa.* Revista BIT, nº 154. Ed. COIT-AEIT. Madrid, 2006.
https://www.coit.es/sites/default/files/archivobit/pdf/felixperez.pdf

investigación militar al desarrollo del sistema español de I+D?"[3]. No es objeto de esta alocución este debate en el que manifesté unas opiniones, que en buena medida sigo manteniendo y en las que no se contraponen la investigación militar y civil, y que tuvieron alguna transcendencia. Concretamente, en un debate similar en la Cortes de Aragón, la diputada socialista Mihi Tenedor, tal como recoge el diario de sesiones, expreso lo siguiente:

...me ha gustado, me ha parecido que era un artículo que aportaba bastantes cosas, el de Félix Pérez Martínez. Creo que es muy interesante ver también una posición de alguien que está defendiendo desde otros parámetros también el que se pueda investigar, es decir, que no le parece mal la investigación militar, sobre todo porque, entre otras cuestiones, plantea -y podemos coincidir- que no es incompatible una investigación con otra y que a todos, efectivamente, nos gustaría vivir en ese mundo ideal sin conflictos, y, además, hace una serie de consideraciones, que yo creo que todos debemos de ponernos de acuerdo, porque la paz la construiremos entre todos...[4].

Estoy convencido que muchos de los investigadores y políticos que participaron en esos debates hoy matizarían algunas de sus posiciones y se acercarían más a las que en aquel momento expuse y que resumo y actualizo en las siguientes afirmaciones:

- El bienestar de la ciudadanía, objeto último de nuestras actividades como académicos, es incompatible con una sociedad no segura.

- Nuestro país no ha sufrido una invasión por ejércitos extranjeros desde hace más de doscientos años, lo que explica que se considere una posibilidad muy remota a la que cuesta dedicar recursos siempre necesarios en otros ámbitos.

---

(3) https://www.madrimasd.org/cienciaysociedad/debates-actualidad/historico/default.asp?idforo=GlobalIDI-6

(4) DIARIO DE SESIONES DE LAS CORTES DE ARAGÓN Nº 056 SERIE A (VI LEGISLATURA)
https://www.cortesaragon.es/bases/disca2.nsf/(DiscaID)/44CE8102A974A67CC1256FA40030DCF4?OpenDocument

- La Guerra de Ucrania ha demostrado, y esta vez en nuestra puerta, que los países, o al menos sus dirigentes, no renuncian a sus intereses particulares y para defenderlos están dispuestos a utilizar los medios militares si es preciso.

- Los países deben de disponer de unas fuerzas armadas suficientes, preparadas y dotadas de medios adecuados para poder, mediante la disuasión, evitar situaciones similares.

- Unas fuerzas armadas y unas fuerzas y cuerpos de seguridad del estado eficaces necesitan una base tecnológica y una industria de defensa que asegure la soberanía tecnológica y la autonomía estratégica de un país y sus aliados(5).

- La actividad de I+D e industrial que de lo anterior se deriva es complementaria de la civil, aporta bienestar y crea riqueza a los países que intentan alcanzar el reto que ello supone. En el contexto actual, como muy bien expresa nuestro compañero académico, Dr. Gonzalo León:

Disponer de una gobernanza tecnológica inteligente en un contexto geopolítico inestable y de confrontación es un factor esencial para asegurar su correcto desarrollo y uso, y proteger al ciudadano en un mundo con crecientes interdependencias. La gobernanza tecnológica está relacionada con el concepto de "soberanía tecnológica" ligado a conseguir la máxima capacidad de decisión industrial, comercial y militar en determinadas tecnologías sin depender (excesivamente) de otros países(6).

---

(5) MINISTERIO DE DEFENSA. *Estrategia Industrial de Defensa 2023.* https://publicaciones.defensa.gob.es/media/downloadable/files/links/e/s/estrategia_industrial_de_defensa_2023.pdf

(6) LEÓN SERRANO, G. *Soberanía e interdependencias tecnológicas en el contexto geopolítico: hacia una gobernanza tecnológica inteligente.* Discurso pronunciado por el Dr. D. Gonzalo León Serrano en su Toma de Posesión como Académico Correspondiente de la Real Academia de Doctores de España el día 30-11-2022.
https://www.rade.es/imageslib/PUBLICACIONES/ARTICULOS/V8N2%20-%2013%20-%20TPC%20-%20LE%C3%93N_gobernanza%20tecnol%C3%B3gica.pdf

A tal efecto y con humildad, en los siguientes minutos intentaré describir las claves tecnológicas que caracterizarán los futuros conflictos y que condicionarán en buena medida su resolución. No son sino desafíos, en muchos casos similares a los de otras áreas de actividad, que deben superar con talento y recursos los científicos, ingenieros y tecnólogos.

II. EL CIRCULO VIRTUOSO ENTRE LOS DESARROLLOS TECNOLÓGICOS Y LOS "ASUNTOS MILITARES"

La guerra, el arte militar, la defensa, etc., de cualquier modo que se denomine, forma parte de nuestra civilización y el desarrollo de la técnica y de la ingeniería han estado siempre vinculados a la guerra… la ingeniería militar fue precursora de la ingeniería civil. Profesor Dr. Vicente Ortega. "Ingeniería y Civilización", conferencia pronunciada en el XXV Aniversario del Centro Politécnico Superior de la Universidad de Zaragoza.

Admitamos o no esta afirmación de otro de mis maestros, lo cierto es que el uso de una tecnología más avanzada que la del adversario ha sido en muchos casos uno de los elementos determinantes del desenlace de los conflictos. Por eso, a lo largo de la historia, los ejércitos se han ido dotando de medios cada vez más sofisticados aprovechando los progresos científicos y tecnológicos disponibles en cada momento en el mundo civil y, a su vez, han propiciado e impulsado tecnologías no existentes, necesarias para sus fines, que posteriormente han sido empleadas en aplicaciones civiles.

Inicialmente las tecnologías utilizadas para generar artefactos, ingenios y fortificaciones defensivas más eficientes estaban basadas en la fuerza muscular de hombres y animales. Posteriormente el uso de la pólvora incrementó substancialmente la eficacia de las armas y tecnificó los conflictos. Hasta entonces, las innovaciones se producían por intuición, destreza, incluso casualidad, consecuencia de la innata capacidad humana de buscar soluciones. Todo cambia a partir del siglo XVIII con la introducción del método científico

y llegada de la Primera y la Segunda Revolución Industrial[7]. Las nuevas tecnologías en materiales y propulsión, entre otras, propiciarán la aparición de nuevas plataformas y municiones que supondrán una mejora exponencial en la eficacia del armamento y las defensas que, a la postre, se traducirá en nuevas maneras de combatir y en la extensión de una nueva forma de imperialismo basado en las brechas tecnológicas con los países donde la intensidad de las citadas revoluciones industriales era muy escasa. Imperialismos con intereses contrapuestos que inevitablemente acabaron enfrentándose en la Primera y Segunda Guerra Mundial, poniendo de manifiesto el potencial destructor que las tecnologías industriales hacían posible. Más adelante cobrarán protagonismo las tecnologías con base en la electrónica y la microelectrónica[8].

---

(7) En este discurso se utiliza la tipología más clásica para clasificar los cambios tecnológicos y sociales de la era contemporánea como revoluciones industriales:
- Primera Revolución Industrial. Desarrollada originariamente en Inglaterra durante el periodo 1760-1840, caracterizada por el uso extensivo del carbón, la máquina de vapor y la aparición de las fábricas.
- Segunda Revolución Industrial. Comprendida entre 1870 y 1910, caracterizada por la aparición de nuevos materiales, la electrificación, el motor de combustión interna, las diferentes tecnologías de telecomunicación (telégrafo, teléfono y radio) y la producción masiva.
- Tercera Revolución Industrial. También conocida como Revolución Digital, empieza en los años 50-60 del siglo pasado y está basada en las tecnologías microelectrónicas.
- Cuarta Revolución Industrial. Ha comenzado en algún momento del presente siglo y se basará en tecnologías tales como la inteligencia artificial, la robótica, la nanotecnología, la biotecnología…
Es una tipología muy empleada y útil a los efectos de esta disertación, pero también muy cuestionada. Ver, por ejemplo, Aibar, Eduard. "Revoluciones industriales: un concepto espurio". OIKONOMICS. Nº 12, 2019
https://oikonomics.uoc.edu/divulgacio/oikonomics/es/numero12/dossier/eaibar.html

(8) Una descripción detallada de estas tecnologías y su evolución puede encontrarse en MARTÍ SEMPERE, C. *Tecnología de la Defensa. Análisis de la situación española*. Instituto Universitario "General Gutiérrez Mellado". 2006.
https://es.scribd.com/document/373724137/16-TECNOLOGIA-DE-LA-DEFENSA-pdf

Por otro lado, la relación entre las tecnologías civiles y militares y la dualidad de muchas de ellas siempre ha sido una realidad, pero es durante la Segunda Guerra Mundial y la Guerra Fría cuándo con más intensidad se manifiesta[9]. De hecho, no es exagerado hablar de una militarización de la tecnología durante este periodo. Más adelante, la caída del Muro de Berlín en 1989 se interpretó como el fin de una época y prometía un nuevo periodo para la humanidad donde los conflictos se resolvieran por medios pacíficos. Las inversiones en Defensa cayeron drásticamente y las empresas del sector de la Defensa, en un claro ejercicio de supervivencia, reclamaron la dualidad como elemento esencial de sus tecnologías. El espejismo ha durado apenas unas décadas. Los últimos conflictos, especialmente el de Ucrania, han disparado las inversiones en Defensa y los países occidentales están sometidos a una dramática metanoia que nos devuelve a los casi olvidados bloques en un entorno geopolítico complejo e incierto. No les extrañará si les digo que ahora son las empresas del mundo civil las que aseguran que sus tecnologías son duales con objeto de acceder a un mercado en clara expansión… y tienen razón. Como se expondrá más adelante, la nueva situación geopolítica ha generado la necesidad de nuevos productos y servicios basados en innovaciones que se realizarán en el ámbito civil y garantizarán la soberanía tecnológica también en el militar[10].

---

(9) Ortega Castro, V. et al. *Relaciones entre las innovaciones tecnológicas y la defensa.* Cuadernos Cátedra ISDEFE-UPM, nº 1. Ed. FUNDETEL, 2007.

(10) LEÓN SERRANO, G. *Relevancia geopolítica de las tecnologías duales: consecuencias y oportunidades para reforzar la soberanía de la Unión Europea.* Colección Institucional. UPM Press, Madrid. 2023.
https://oa.upm.es/76650/

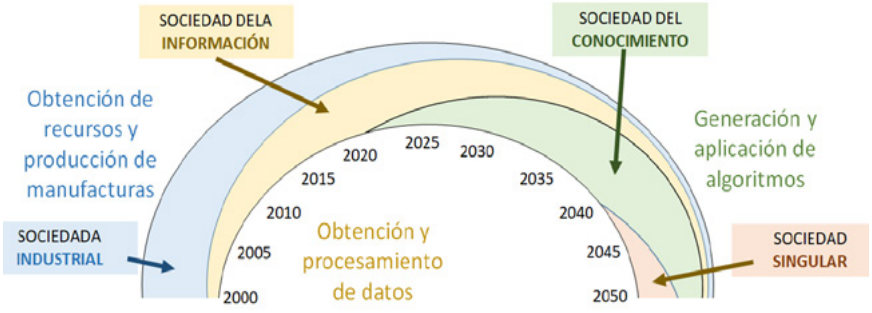

Figura 1. Evolución de las sociedades humanas

En todo caso, lo cierto es que los desarrollos tecnológicos son factores de cambio social cada día más importantes y están transformando radicalmente la sociedad a un ritmo creciente. Tal como se indica en la figura 1, con el cambio de siglo pasamos de una sociedad industrial, impulsada por la obtención de materias primas y producción de manufacturas, a una sociedad de la información impulsada por la obtención y procesamiento de datos. Estas dos sociedades coexisten hoy y lo harán durante años en un proceso de sustitución progresiva de una por la otra.

Lentamente y desde hace unos años, se ha iniciado una nueva transición hacia la llamada sociedad del conocimiento. Esta nueva ola está impulsada por la obtención masiva de datos en tiempo real y la generación y uso de algoritmos de inteligencia artificial (IA) integrados en todo tipo de aplicaciones. La transición de la sociedad de la información a la sociedad del conocimiento tampoco será inmediata, pero si inevitable. Más adelante en el horizonte, también se prevé el surgimiento de una sociedad singular, "singular" en la acepción de la Real Academia de La Lengua de "extraordinaria",

"rara", aunque quizá no nos equivoquemos mucho si empezamos a denominar cognitiva a esta sociedad que advendrá en dos o tres decenas de años[11].

En definitiva, la fluida integración de varias tecnologías digitales disponibles hoy en día, como big data (la captura, generación y análisis de datos masivos), Internet de las cosas, vehículos autónomos, nube, sistemas de información avanzados, ciberseguridad integrada y las comunicaciones móviles 5G y 6G, entre otros, están impulsado el despliegue de "sistemas inteligentes" impulsados por la convergencia de tecnologías en sectores como el hogar, las ciudades, el transporte, la salud, la educación, la agricultura y también en defensa y seguridad.

En paralelo y quizá a un ritmo algo inferior, estas mismas tecnologías están transformando los escenarios de conflicto.

Los escenarios de conflicto, los campos de batalla en situaciones de guerra, han evolucionado desde unos teatros de operaciones que denominaremos cinéticos, característicos del siglo pasado, a los digitales característicos de los conflictos modernos. Los primeros estaban basados en armas de efectos cinéticos y se libraban en los dominios físicos - tierra, mar, aire y en las últimas décadas en el espacio-, en ellos la superioridad de la fuerza y las maniobras era la garantía del éxito. Por el contrario, en los campos de batalla digitales de nuestros días, la superioridad de la información es condición necesaria para el éxito porque es requisito para obtener la ventaja en los dominios físicos. Por supuesto que durante muchos años han coexistido

---

(11) Esta descripción de la evolución paralela de las sociedades humanas y los campos de batalla fue presentada por primera vez por el autor de estas páginas en el IV FORO 2E+I, EL COMBATE INTELIGENTE celebrado en Toledo el 4 y 5 de octubre de 2023 en una ponencia titulada *Las tecnologías digitales y el futuro campo de batalla inteligente.*
https://foroejercito.es/

y coexistirán elementos del campo de batalla cinético en los escenarios de conflicto contemporáneos, como está acaeciendo en la guerra de ocupación que se dilucida en Ucrania.

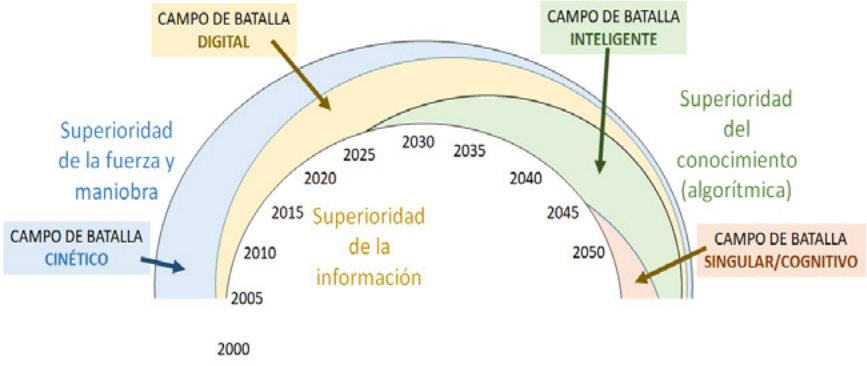

Figura 2. Evolución de los campos de batalla

Además, como en el ámbito civil, se está iniciando un proceso de transformación hacia unos escenarios de conflicto y campos de batalla que también denominamos inteligentes en los que la clave del éxito no es la superioridad de la información, sino la superioridad del conocimiento. En esta docta audiencia no es necesario explicitar la diferencia entre información y conocimiento, por eso todos ustedes ya han adivinado de que la diferencia esencial entre los escenarios de conflicto actuales y los de dentro de una o dos décadas es que el conocimiento, y por tanto las tomas de decisión asociadas a este, ya no se generarán mayoritariamente en los cerebros de los hombres, lo harán algoritmos contenidos en creaciones humanas que progresivamente asumirán unas funciones que creíamos exclusivas de nuestra condición.

El reto en los próximos años, tanto en el mundo civil como en los asuntos militares, es la asimilación de esta nueva revolución tecnológica con los menores daños posibles, porque efectos negativos y brechas entre sectores de la sociedad va a haber. Ya ocurrió en la

revolución industrial y está ocurriendo en la revolución digital. Por otro lado, nada permanece, la revolución de la inteligencia artificial, también será el precedente de una nueva revolución tecnológica a mediados de este siglo que ya se adivina y que nos llevará a escenarios de conflicto singulares/cognitivos de los que nada sabemos y en los que es muy difícil hacer conjeturas más allá de especular sobre la convergencia de unas tecnologías disruptivas, incipientes en la actualidad, pero que alcanzarán su madurez en ese momento.

Dedicaré la mayor parte de mi exposición al actual campo de batalla digital y su evolución al próximo campo de batalla inteligente, limitándome a formular algunas reflexiones complementarias dedicadas a su antecedente, el campo de batalla cinético, y su futuro a largo plazo, el campo de batalla singular.

III. EL CAMPO DE BATALLA CINÉTICO

No tengo nada más que ofrecer que sangre, esfuerzo, lágrimas y sudor. Winston Churchill. Discurso ante la Cámara de los Comunes del Reino Unido el 13 de mayo de 1940.

Lo que aquí se denomina campo de batalla cinético es el que se configura a partir de la revolución industrial y alcanza su madurez en la Primera y Segunda Guerra Mundial. Las fuerzas combatientes disponen de una gran potencia de fuego y movimiento con la que tratan de ocupar los dominios físicos, denominados tradicionalmente como tierra, mar, aire y espacio. La superioridad de la fuerza y la maniobra son las que permiten vencer al adversario en las batallas, aunque de ello no siempre se derive la victoria en el conflicto. Son numerosos los conflictos posteriores a la Segunda Guerra Mundial cuyo desarrollo y resolución avalan esta afirmación.

Obviamente este campo de batalla ha ido evolucionando con la introducción y desarrollo de nuevas tecnologías que han permitido incrementar la proyección, protección y movilidad de las fuerzas, dotándolas de unas capacidades crecientes de conocimiento del entorno gracias al desarrollo acelerado de los sistemas de comunicaciones y sensorización. En las últimas etapas de este campo de batalla cinético destacan tres tecnologías: la tecnología nuclear, de extraordinaria relevancia en el entorno geopolítico pero de escasa transcendencia en los escenarios de conflicto no globales, las TIC que, incluso antes de su digitalización, ya jugaron un papel esen-

cial en la resolución de los conflictos y modificaron las doctrinas y tácticas de las operaciones militares y, por último, las tecnologías espaciales que habilitan un escenario de conflicto que inicialmente estaba reservado a EEUU y Rusia pero que

...en estos momentos, con el abaratamiento y disponibilidad de tecnologías -al alcance de muchas más instituciones, organizaciones y empresas-, el control que de numerosas actividades humanas se puede hacer desde el espacio exterior y el valor económico de las numerosas aplicaciones y servicios que pueden desplegarse desde allí, le han convertido en el ámbito de futuros conflictos y enfrentamientos entre múltiples agentes. Un enfrentamiento donde la tecnología será el factor decisivo[(12)].

En las postrimerías de los escenarios de conflicto cinéticos, el espectro electromagnético ya se convierte en un elemento más del combate. Su uso, tanto para implementar sensores como para difundir la información obtenida, permite alejar a los combatientes entre sí y coordinar los combates en los diferentes dominios físicos. La superioridad aérea es imprescindible para asegurar la victoria en los dominios terrestre y naval pero solo puede habilitarse con el empleo de ondas electromagnéticas.

Lo cierto es que, a partir de la primera revolución industrial, y sobre todo a partir de la segunda, con el desarrollo de la electricidad, los motores de combustión interna y la telefonía, las innovaciones y el desarrollo de nuevos productos y servicios crecen exponencialmente en el ámbito civil con un impacto social y económico que minimiza las innovaciones en el ámbito militar. Estas solo toman protagonismo en los momentos de crisis. Es el caso de la Segunda

---

(12) Presentación del curso de verano de la UPM: *El espacio exterior: tecnologías y sistemas para un nuevo escenario de conflictos*, celebrado el 30 de junio y 1 de julio de 2021 en el CESEDEN y coordinado por el GB. Francisco Dacoba y el autor de este texto.
https://blogs.upm.es/catedra-ceseden-upm/wp-content/uploads/sites/580/2021/07/Programa-curso-de-verano-Espacio-Exterior_1-de-julio.pdf

Guerra Mundial y la Guerra Fría. La energía nuclear, el radar, las tecnologías de RF, el GPS o internet, son los ejemplos que siempre se ponen de innovaciones surgidas directamente en el ámbito militar de gran impacto en el ámbito civil. Sin embargo, en la tercera revolución industrial, la de la información, la innovación en el ámbito civil se ha impuesto definitivamente a la militar.

IV. EL CAMPO DE BATALLA DIGITAL

¡Muy delicado! ¡Realmente delicado! No existe lugar donde no se use el espionaje. Sun Tzu. "El arte de la Guerra". Siglo V o IV a.c.

A continuación, intentaré describir el origen y principales características de lo que en numerosos foros se denomina el campo de batalla digital que no es sino una forma de especificar el formidable impacto que tienen las tecnologías digitales en las actuales operaciones militares.

a) La digitalización y su potencial transformador[13] [14]

Electrónica, telecomunicaciones e informática, las TIC, son tres tecnologías con orígenes y desarrollos diferentes pero que en los

(13) Las ideas expuestas en este apartado han sido fruto de una reflexión de muchos años y de la participación del autor en la impartición de asignaturas de carácter transversal en la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universidad Politécnica de Madrid. Mi agradecimiento a los profesores Vicente Ortega Castro y Jorge Pérez Martínez que desplegaron y desarrollaron este tipo de conocimientos en un entorno académico nada favorable.

(14) La primera formulación estructurada de estas ideas fue desarrollada por el autor en la conferencia *El Futuro de los sistemas de mando y control* impartida durante el IV International Symposium on Security and Defense (SISEDE 2018), celebrado el Lima (Perú) en agosto del 2018. Una versión más extensa puede encontrase en el capítulo *Los sistemas autónomos y la Transformación Digital del Campo de Batalla* del libro "Sistemas Autónomos y Robótica Inteligente en Defensa" de la colección de la Academia de las Ciencias y las Artes Militares.
http://isbn.bnp.gob.pe/catalogo.php?mode=detalle&nt=104461
https://www.fundcami.org/producto/sistemasautonomosyroboticainteligentededefensa/

últimos cincuenta años han estado sometidas a un proceso de convergencia que las ha convertido en factores multiplicativos de las actividades humanas con un formidable potencial transformador(15). La clave de su convergencia ha sido la digitalización de la información introducida en las últimas décadas del pasado siglo. Es a lo largo de los años 70 cuando, con el desarrollo de la tecnología microelectrónica, se generaliza el uso de la circuitería digital para la generación, almacenamiento, transmisión y procesamiento de datos digitalizados, y se aplica a numerosas actividades: cálculo, gestión, sensorización, comunicaciones… Muy pronto comenzó el proceso de convergencia antes mencionado que se ha traducido en que ahora las denominemos a todas ellas tecnologías digitales.

La "digitalización" de la información aumentó la calidad y fidelidad de la misma (al posibilitar el uso de técnicas de corrección de errores); flexibilizó su tratamiento; permitió operaciones tan complejas como la compresión de la información (eliminación de la información redundante), el cifrado (acceso restringido a la misma) y la ecualización (corrección de los errores introducidos en su transmisión), optimizó su almacenamiento y presentación y, posteriormente, ya en este siglo, independizó el procesamiento, la transmisión, el almacenamiento y la presentación de la información de la fuente que la generaba. Todo lo cual desembocó en lo que se conoce como la tercera revolución industrial, cuya materia prima fue un intangible:

---

(15) PÉREZ MARTÍNEZ, J. *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. https://fundacionsistema.com/producto/tecnologia-y-sociedad-en-el-nuevo-siglo-segundo-foro-sobre-tendencias-sociales/

la información[16]. Una transformación socioeconómica ya madura cuyos inicios cabe situarlos hace unos 50 años cuando se anuncia el primer microprocesador. La evolución de estas tecnologías se describe en los siguientes párrafos:

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.

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 informa-

---

(16) En este artículo se proporciona una visión general sobre la transformación que están sufriendo las actividades económicas relacionadas con las comunicaciones electrónicas en un entorno económico global y de frecuentes disrupciones tecnológicas: PEREZ MARTÍNEZ J et al. *Desafíos de la gobernanza de Internet.* Revista TELOS (Revista de Pensamiento, Sociedad y Tecnología). ED Fundación Telefónica. Febrero - Mayo 2015.
https://telos.fundaciontelefonica.com/archivo/numero100/desafios-de-la-gobernanza-de-internet/

ción 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…[17].

b) Sociedad de la información y economías digitales

Una de las características más destacables de la actual sociedad de la información es que en ella se desarrollan a un ritmo acelerado lo que denominamos economías digitales[18]. 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[19].

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

---

(17) PÉREZ MARTÍNEZ, F. *La transformación digital en los nuevos escenarios de conflicto: del campo de batalla digital al campo de batalla inteligente.* Discurso de toma de posesión como académico de número de la Academia de las Ciencias y las Artes Militares. 8 de febrero de 2023.
https://www.acami.es/wp-content/uploads/2023/02/Discurso-toma-posesion-Felix-Perez-Martinez.pdf

(18) CHAKRAVORTI, B. et al. Digital in the time of covid. *Trust in the digital economy and its evolution across 90 economies as the planet paused for a pandemic.* Digital Intelligence Index. Dec.2020.
https://www.ffms.pt/sites/default/files/2022-07/digital-intelligence-index.pdf

(19) https://economipedia.com/ranking/empresas-mas-grandes-del-mundo-2024.html

al resto de organizaciones públicas y privadas, entre ellas las fuerzas armadas y los cuerpos de seguridad del estado. La digitalización es sin duda el factor tecnológico de cambio social más importante en estos momentos y su rápido y eficiente desarrollo se ha realizado en el ámbito civil donde se ha dispuesto de recursos muy superiores a los empleados en la introducción de estas tecnologías el ámbito de la defensa y la seguridad.

Las tecnologías digitales han sido tecnologías disruptivas y han generado "cambios profundos", pero su velocidad de implantación ha sido relativamente lenta. 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. La transformación digital de las organizaciones humanas comenzó con la llegada de los primeros sistemas digitales de proceso de la información el siglo pasado. Una revolución que ahora percibimos como silenciosa pero que ha estado afectando a las personas y generado sucesivas brechas digitales desde que la microelectrónica entró en nuestras casas y lugares de trabajo, transformando nuestro modo de vida, e incluso, nuestra forma de pensar.

c) La microelectrónica: base de la revolución digital

Dedicaré ahora unos minutos a comentar algunos aspectos del nacimiento y evolución de las técnicas microelectrónicas responsables últimas de la revolución digital y del nacimiento de la sociedad de la información. Concretamente a aquellos aspectos que tienen que ver con el papel que las necesidades militares tuvieron en su desarrollo.

La tecnología microelectrónica nació para sustituir a los tubos electrónicos de vacío en dos aplicaciones concretas que intentaban resolver dos necesidades perentorias muy diferentes. La primera en el ámbito militar: la necesidad de realizar cálculos cada vez más complejos en el menor tiempo posible requeridos durante la Guerra Fría por la carrera espacial, el procesado de señal en los radares y la

encriptación de la información para las comunicaciones seguras. La segunda en el ámbito civil: la optimización de las centrales telefónicas de conmutación automática que debían interconectar un número de líneas de abonado en crecimiento exponencial.

Será en los Laboratorios Bell de la compañía telefónica AT&T, Inc. (American Telephone & Telegraph), donde se obtendrá la primera patente del transistor, el dispositivo semiconductor base de la microelectrónica[20] [21].

Era una invención totalmente civil derivada de las necesidades del sector de las telecomunicaciones y sin embargo, ya en 1952, el Departamento de Defensa de EEUU, en adelante DoD, estableció un Subpanel de Dispositivos Semiconductores para estudiar los nuevos dispositivos y sus aplicaciones. Los tres ejércitos de EEUU apoyaron los procesos de ingeniería de producción y otorgaron contratos de I+D cuyo valor se estima en 50 millones de euros entre 1952 y 1964[22]. El Gobierno de EEUU no sólo financiaba la I+D de los semiconductores, sino que aseguraba a su vez compras importantes de unos dispositivos y equipos electrónicos cuya fiabilidad todavía era discutida. En definitiva, fueron las necesidades militares las que aceleraron el desarrollo de la electrónica de estado sólido hasta 1970. Posteriormente con la invención

---

(20) MARTÍN PEREDA J. A. *Historia de las telecomunicaciones.* Ed. Guadalmazán. 2022
https://www.amazon.es/Historia-las-telecomunicaciones-Divulgaci%C3%B3n-Cient%C3%ADfica/dp/8417547576

(21) US 2524035, BARDEEN et al.: *Three-electrode circuit element utilizing semiconductive materials.* oldest priority 1948-02-26.
https://worldwide.espacenet.com/patent/search/family/026682082/publication/US2524035A?q=pn%3DUS2524035

(22) BRAUN E. y MACDONALD S. *Revolución en miniatura: La historia y el impacto de la electrónica del semiconduntor".* Fundesco/Tecnos, S.A. Madrid. 1984.
https://ingenio.upm.es/primo-explore/fulldisplay/34UPM_ALMA2145024530004212/34UPM_VU1

de los circuitos integrados, conocidos también como "chips", y los microprocesadores, serán las aplicaciones civiles las que desarrollarán el mercado con un crecimiento exponencial que se mantiene hasta nuestros días[23].

Desde entonces, han surgido sucesivas generaciones de "chips" (caracterizada por la anchura, cada vez más pequeña, del canal de los transistores[24]) con mejores prestaciones en su capacidad de cálculo, reduciendo sus tiempos de proceso de la información en uno o varios ordenes de magnitud, así como su consumo y precio. Se están fabricando dispositivos con anchuras de algunos nanómetros, de hecho la última generación de terminales móviles de Apple, el iPhone 15, incluye chips con una anchura de canal de 1,6 nm. Por otro lado, a partir de ahora será muy difícil reducir las anchuras de los canales, y será necesario emplear nuevos materiales, como el grafeno y el nitruro de galio, y apilar los circuitos verticalmente, implementando lo que se conoce como "chip-3D", para seguir incrementando las capacidades de los microprocesadores[25]. En definitiva, parece que la famosa Ley de Moore de la microelectrónica y sus consecuencias tecnológicas y sociales se seguirán manteniendo en los próximos

---

(23) RIORDAN, M. *From Bell Labs to Silicon Valley: A Saga of Semiconductor Technology Transfer,* 1955-61. The Electrochemical Society Interface. Fall 2007.
https://www.electrochem.org/dl/interface/fal/fal07/fall07_p36-41.pdf

(24) El canal de un transistor es la zona comprendida entre dos terminales que recorre el flujo de electrones que se quiere controlar. Cuanto más pequeña sea esta dimensión, más rápidamente será posible conmutar al dispositivo y más pequeño será. La anchura del canal, que actualmente se mide en nanómetros, está limitada por la tecnología empleada en el proceso de fabricación.

(25) 14. DEL ALAMO, J. *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

años hasta que las tecnologías cuánticas y las derivadas de la biotecnología estén disponibles y protagonicen una nueva revolución tecnológica[26].

Otro aspecto que merece resaltarse es que la capacidad de proceso se puede incrementar exponencialmente 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*).

En definitiva, es innegable que el ordenador personal, internet y el terminal móvil inteligente que disfrutamos hubiese llegado a nuestras manos tarde o temprano, pero fueron las aplicaciones militares y la apuesta del DoD por el desarrollo de la tecnología microelectrónica las que aceleraron los procesos y permitieron que la digitalización fuese una realidad en unas décadas. En la dualidad de esta tecnología estuvo la clave de su desarrollo exponencial de una tecnología que transformó nuestras vidas[27].

---

(26) A modo de ejemplo, la GPU H100 que comercializa NVIDIA desde el año 2022 dispone 80.000 millones de transistores y se presentaba como un chip con una capacidad de proceso "sin precedentes" orientado a aplicaciones de IA. Solo dos años después se anuncia el nuevo chip de esta empresa, la GPU B200, con 208.000 millones de transistores, que pondrá en el mercado NVIDIA en unos meses junto al superchip GB200. Con estos dispositivos, basados en la nueva arquitectura Blackwell, la potencia de cálculo en operaciones FP4 alcanza los 40 petaFLOPS con una reducción de un orden de magnitud en el consumo. Aunque comparar capacidades de cálculo de humanos y maquinas es muy complicado, Algunas estimaciones sugieren que el cerebro humano puede realizar entre 0,1 y 10 petaFLOTS.
https://www.larazon.es/tecnologia/nvidia-presenta-nuevo-superchip-40-petaflops-potencia_2024031965f99cb59e2a440001bfebf4.html

(27) Una descripción detallada de este proceso puede encontrarse en: PÉREZ MARTÍNEZ F., *Desarrollo de las tecnologías microelectrónicas Los programas militares que desarrollaron la tecnología del silicio en la segunda mitad del siglo XX.* Aportaciones militares a la sociedad civil. Fundación de las Ciencias y las Artes Militares. Mayo 2023.
https://www.fundcami.org/desarrollo-de-las-tecnologias-microelectronicas/#:~:text=Los%20programas%20militares%20que%20desarrollaron,o%20del%20nacimiento%20de%20Internet

d) La digitalización del campo de batalla: las operaciones multidominio, híbridas y en zona gris.

Los últimos conflictos en que se han involucrado los países con mayor capacidad militar se han caracterizado por su gran complejidad y por la aparición de nuevas formas de enfrentamiento como son las contiendas asimétricas, con adversarios muy desequilibrados en términos de recursos y tecnologías disponibles, y los híbridos[28], donde los combates se libran simultáneamente en los ámbitos militar y civil. Además, muchos de ellos se desarrollan en "zona gris"[29], es decir con unos niveles de enfrentamiento en los que no es posible una declaración formal del conflicto.

La necesidad de renovar los conceptos operativos para adaptarlos a los nuevos escenarios geopolíticos y tecnológicos fue puesta de manifiesto con claridad por el Departamento de Defensa de EEUU (DoD) a finales del siglo pasado en lo que definió como la Revolución de los Asuntos Militares (Revolution in Military Affairs o RMA)[30]. Los nuevos elementos doctrinales se basaban en principios similares a los que han generado la sociedad de la información en el ámbito civil, es el caso del concepto "Network Enabled Capability" (NEC) desarrollado por la OTAN que incluye la definición de una Infraestructura de Información y Comunicaciones (IIC) que, integrando sensores, redes de comunicaciones y sistemas de infor-

---

(28) CULLEN, P. y REICHBORN, E. *Understanding hybrid warfare.* MCDC Countering Hybrid Warfare Project. 2017.
https://bit.ly/38ohRIc

(29) JORDAN, J. *El conflicto en la zona gris: antagonismo por debajo del umbral de la guerra.* Global Strategy. 2021.
https://global-strategy.org/conflicto-zona-gris-estrategias-hibridas/

(30) MARTÍ SEMPERE, C. y GRANDA COTERILLO, J.M. *¿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

mación permite dotar a las organizaciones militares de la necesaria superioridad de la información[31] [32]. Esta superioridad se consigue haciendo que la información necesaria, y en la medida de lo posible solo esta, esté disponible en cualquier nivel de decisión, con independencia del lugar en que se encuentren y con las garantías de seguridad adecuadas, lo que modifica radicalmente las doctrinas del mando y control[33]. Nótese su similitud en cuanto objetivos de este combate en red con los requerimientos de los actuales sistemas de información y comunicaciones civiles, en particular, con Internet.

El concepto NEC era, y todavía es, un desiderátum para incorporar los avances de las TIC a los sistemas de defensa y seguridad, del mismo modo que la prevista "transformación" de las Fuerzas Armadas de EEUU y del resto de países se realizó a un ritmo mucho más lento del previsto. Hasta el año 2014 no se vuelve a impulsar "la Transformación Militar" en EEUU cuando con la invasión de Crimea por las fuerzas rusas y el conflicto del Dombás, se pone de manifiesto la progresiva erosión de la superioridad militar de las fuerzas armadas occidentales. En España la transformación digital de nuestras fuerzas armadas ha empezado hace sólo unos años[34].

---

(31) *Network Centric Warfare. Network Enable Capability.* Monografías del Sistema de Observación y prospectiva Tecnológica (SEOP) del Ministerio de Defensa. Catálogo General de Publicaciones Oficiales, 2009.
https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografias_del_sopt_n_3_network_centric_warfare.pdf

(32) *Network Enabled Capability Handbook.* Journal of Defence Science. UK Ministry of Defence. Vol 8, nº 3, 2003
http://www.dodccrp.org/files/journal_defence_science_web.pdf

(33) Alberts, D.S. et al. NATO NEC C2 Maturity Model. CCRP Publication Series. Feb. 2010
http://www.dodccrp.org/files/N2C2M2_web_optimized.pdf

(34) MILLÁN MARTÍNEZ, J. M. *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

Sin embargo, esta ralentización en los procesos de digitalización en el ámbito militar respecto del civil no ha impedido que, a lo largo de estos años, las tecnologías digitales se hayan introducido masivamente en los sistemas de defensa y seguridad aumentando la variedad y eficacia de las capacidades militares disponibles[35]. Desde el punto de vista operativo, quizá los cambios más significativos son:

- La aparición del concepto de multidominio en el que los dominios físicos, (tierra, mar y aire) se gestionan como un todo por una "Fuerza Conjunta" que aprovecha sus sinergias y se integra con las de los otros dominios –espacio ultraterrestre, ciberespacio y cognitivo- gracias a la conectividad disponible[36]. Todavía no es una realidad pues en todos los países perviven diferencias, tanto conceptuales como prácticas, entre los diferentes ejércitos y armadas de sus fuerzas armadas.

- La aparición de dos nuevos dominios, el ciberespacio y el dominio cognitivo. A diferencia de los anteriores son dominios no cinéticos, en ellos las acciones no son siempre observables y atribuibles al trabajar con un intangible: la información. Lo que modifica sensiblemente las "reglas de la guerra" tradicionales.

El ciberespacio siempre se ha asociado a los sistemas de información que tradicionalmente han estado constituidos por redes de ordenadores convencionales (redes de área local) con gran capacidad de computación que se conectaban entre sí mediante enlaces dedicados

---

(35) FOJÓN, E. *Desarrollos tecnológicos militares frente a nuevos conceptos operativos.* Real Instituto Elcano. Julio 2019.
https://www.realinstitutoelcano.org/analisis/desarrollos-tecnologicos-militares-frente-a-nuevos-conceptos-operativos/

(36) PERKINS, D.G. *La batalla multidominio. Impulsando el cambio para ganar en el futuro.* Military Rewiew. Primer trimestre 2018.
https://www.armyupress.army.mil/Journals/Edicion-Hispanoamericana/Archivos/Primer-Trimestre-2018/La-batalla-por-el-multidominio-Impulsando-el-cambio-para-ganar-en-el-futuro/

muy seguros[37]. Las amenazas se introducían por puertas externas e internas asociadas a las vulnerabilidades del software. De este modo, las acciones de ciberdefensa estaban alejadas de la guerra electrónica tradicional cuyo fin era determinar, explotar, reducir o prevenir el uso hostil del espectro electromagnético por el enemigo y a mantener su utilización por las fuerzas propias. La evolución de los escenarios de conflicto y la de las TIC no permiten mantener esta situación[38]. Actualmente se habla de conflictos ciberelectromagnéticos en los que las operaciones afectan simultáneamente a los sistemas de información y a las redes de comunicaciones lo que implica importantes cambios en aspectos doctrinales, organizativos y operativos[39].

En todo caso, el ciberespacio, tras veinte años de desarrollo y consolidación es sin duda el quinto área del ámbito bélico, "un terreno propicio para actos de espionaje, sabotaje y desestabilización entre Estados contendientes"[40].

Por otro lado, la dimensión psicológica está y ha estado siempre presente en todos los conflictos con el objetivo de influir sobre la mente de amigos y enemigos. En las operaciones militares, tradicionalmente estas actividades se han dividen entre lo que se conoce

---

(37) DOD. *National military strategy for cyberspace operations (NMS-CO).* 2006 https://gssd.mit.edu/search-gssd/site/national-military-strategy-cyberspace-60365-sun-06-16-2013-1531

(38) HEADQUARTERS DEPARTMENT OF THE ARMY. *Cyber electromagnetic activities.* FM 3-38. 2014. https://publicintelligence.net/us-army-cema/

(39) PÉREZ MARTÍNEZ, F. *Los futuros sistemas de guerra electrónica en el nuevo entorno del ciberespacio* conferencia impartida durante el V International Symposium on Security and Defense (SISEDE 2019), celebrado el Lima (Perú) en agosto del 2019.
https://www.losdelfineshotel.com/blog/v-international-symposium-on-security-and-defense-2019

(40) FERNÁNDEZ APARICIO, J. *Panorama geopolítico de los conflictos 2022. Capítulo undécimo: Ciberguerra y cibercrimen global, cuando lo virtual transciende a lo real.* Instituto Español de Estudios Estratégicos. Ministerio de Defensa. 2022.
https://publicaciones.defensa.gob.es/panorama-geopolitico-de-los-conflictos-2022-revistas-pdf.html

como “operaciones sicológicas” (PSYOPS) dirigidas a las fuerzas enemigas y a su población e “información pública” cuyo destinatario son las poblaciones propias o neutrales.

A partir de los años 90, la digitalización suministra nuevas herramientas que incrementa la importancia de estas operaciones de información y aparece el concepto de “desinformación” y las “batallas de las narrativas”. Algo, como se ha indicado, que siempre ha estado presente en los conflictos, pero cuya intensidad y efectos se han incrementado exponencialmente a lo largo de este siglo con el advenimiento de la sociedad de la información(41).

En las actuales operaciones multidominio, la superioridad en estos dos dominios, ciberespacio y cognitivo, es imprescindible para asegurar el éxito en los conflictos. La actual Guerra en Ucrania, lamentablemente, lo está poniendo de manifiesto.

e) Algunas características del campo de batalla digital: la superioridad de la información

Para finalizar esta parte de mi exposición, permítanme que resuma los aspectos tecnológicos que caracterizan el campo de batalla digital en el que se desarrollarán los conflictos en los próximos años. Permítanme también que lo haga mediante algunas palabras clave que definen funcionalidades de base tecnológica presentes en los actuales campos de batalla:

Sensorización

Los sensores constituyen los “ojos” y los “oídos” de los sistemas de seguridad y defensa por su capacidad para detectar, localizar, carac-

---

(41) GARCÍA SERVERT, R. y CALVO ALBERO, J. L. *El dominio cognitivo en las operaciones multidominio: concepto y problemática.* ANALES de la Academia de las Ciencias y las Artes Militares (ACAMI), 2020. https://www.acami.es/wp-content/uploads/2022/05/dominio-cognitivo-operaciones-multidominio-web.pdf.

terizar y/o identificar señales y objetos. Se emplean masivamente para suministrar los datos que permiten la operación de los actuales sistemas de mando y control, sistemas de armas, inteligencia, guerra electrónica y un largo etc. Especialmente importantes en las aplicaciones de defensa y seguridad son los sensores electromagnéticos, aquellos diseñados para extraer información a distancia mediante las propiedades de las ondas electromagnéticas: emisivilidad, reflectividad y propagación en un medio físico, generalmente la atmósfera terrestre. Se pueden clasificar en dos grandes grupos, los que trabajan en las bandas de radiofrecuencia, microondas y milimétricas, que se caracterizan por ser, en la mayor parte de los casos, "todo tiempo" y los que trabajan en las bandas electroópticas cuya característica más relevante son su precisión y su facilidad para formar imágenes, aunque las condiciones del medio atmosférico les pueden afectar muy significativamente[42]. La utilización conjunta de ambos sensores ha convertido a los teatros de operaciones en escenarios donde es muy difícil ocultar nada.

Entre los primeros destacan los radares[43] y los receptores, elementos que, aunque fueron ideados y desarrollados inicialmente en entornos científicos e ingenieriles del ámbito civil, lo cierto es que los vectores de desarrollo de las tecnologías que los soportan han sido las necesidades militares, entre las aplicaciones civiles cabe citar como más significativas las relacionadas con el transporte (control del tráfico aéreo, seguridad marítima, coche autónomo…) y el medio ambiente (obteniendo imágenes multiespectrales desde plataformas aéreas tripuladas o no tripuladas y satélites).

---

(42) PEREZ MARTÍNEZ, F. *Sensores electromagnéticos. los "sentidos" de los sistemas para la defensa y la seguridad.* Colección cuadernos Cátedra UPM-Isdefe, nº 9. Ed. FUNDETEL. 2011.
https://forohistorico.coit.es/index.php/biblioteca/libros-electronicos/item/sensores-electromagneticos-los-sentidos-de-los-sistemas-para-la-defensa-y-la-seguridad

(43) SKOLNIK, M. I. *Fifty Years of Radar.* Proceedings of the IEEE. Vol. 73. No. 2, February 1985. https://ieeexplore.ieee.org/document/1457400

Los sensores electroópticos también aparecieron por el interés científico e ingenieril de buscar aplicaciones de los efectos fotoeléctricos a la generación de energía (láseres) y detección de señales en las bandas infrarrojas, visible y ultravioleta, tal como explicó con detalle y acierto en este mismo paraninfo nuestro académico Dr. José Luis Ocaña[44]. Sin embargo, muy pronto las aplicaciones militares también fueron el vector principal de desarrollo de estas tecnologías, aportando ingentes recursos para financiar la realización de aplicaciones de vigilancia y guiado de precisión de diferentes sistemas de armas. También es cierto que el desarrollo de las comunicaciones ópticas, especialmente por fibra, y de las cámaras digitales en el ámbito civil a lo largo de este siglo obliga a matizar la afirmación anterior. De hecho, este es uno de los ámbitos en que las tecnologías son claramente duales con sinergias muy importantes entre las aplicaciones civiles y militares.

Conectividad

La superioridad de la información no solo requiere extraer los datos necesarios mediante sensores, también, y en muchas ocasiones es lo más difícil, se debe hacer llegar a cada combatiente la información que le es útil y sólo esa información. A tal efecto se requiere el uso de unas redes de comunicaciones capaces de conectar, de modo seguro, ágil y eficiente, los elementos del entorno táctico (personas, vehículos, sistemas, dispositivos…) entre sí y con los niveles estratégicos y operacionales que toman las decisiones de alto nivel. Se trata de una comunicación bidireccional que debe funcionar en un ambiente de acciones ciberelectromagnéticas.

---

(44) OCAÑA MORENO, J. L . *El LASER: paradigma de la física cuántica e instrumento clave para el desarrollo científico-tecnológico.* Discurso pronunciado en el acto de su toma de posesión como Académico de Número de la Real Academia de Doctores de España. 2019.
https://www.rade.es/imageslib/ACTIVIDADES/TEXTOS/OCANA%20MORENO,%20Jose%20Luis_discurso%20de%20ingreso.pdf

Las redes militares tradicionalmente han trabajado de forma federada por misión, es decir, interconectando un conjunto de nodos capaces de operar de forma conjunta. De la misma forma, se ha tendido a configurar redes con arquitecturas y tecnologías diferentes en función de su cometido, distinguiéndose entre redes troncales de transporte, desplegables, móviles, de satélites… una estructura segmentada cuya interconexión es jerarquizada. El problema es que en este tipo de redes no es posible incrementar fácilmente los anchos de banda (para aumentar la capacidad de transmisión de datos), ni flexibilizar el intercambio de información entre los nodos como exigen, tanto los avances en los sensores, como los conceptos operativos modernos.

La digitalización ha permitido avanzar hacia arquitecturas de redes globales de concepción horizontal, capaces de responder a unos requisitos de usuarios que demandan un alto volumen de intercambio, disponibilidad de la información con bajo retardo y aseguramiento de la conectividad(45). Para ello se necesita un diseño de arquitectura que permita la conectividad lo más directa posible entre cualquier par de nodos, con redundancia y con gran ancho de banda, así como el acceso a nubes con capacidad de almacenamiento y cálculo, es lo que se conoce como nubes tácticas de combate. En definitiva, exactamente lo mismo que se ha conseguido con los nuevos sistemas de comunicaciones civiles, en buena parte ya desplegados y con crecimientos exponenciales en términos de redes y terminales. La última generación de sistemas de comunicaciones móviles, bajo en estándar 5G, es el paradigma de lo anterior.

Lo cierto es que fueron las necesidades militares las que impulsaron el desarrollo, a lo largo de la segunda mitad del siglo pasado, de muchos de los conceptos y tecnologías clave que incorporan los actuales sistemas de telecomunicación más avanzados, como el 5G y

---

(45) VARIOS AUTORES. *Telecomunicaciones militares para el despliegue de fuerzas en misiones humanitarias y de mantenimiento de la paz.* Grupo de Trabajo de Defensa y Seguridad. Colegio Oficial de Ingenieros de Telecomunicación. 2013. https://www.coit.es/informes/telecomunicaciones-militares-para-el-despliegue-de-fuerzas-en-misiones-humanitarias-y-de-0

el WiFi 7, por ejemplo las técnicas de espectro ensanchado, las técnicas de proceso de señal, los arrays de antenas controladas electrónicamente, los protocolos de internet, y más recientemente, la radio definida por software (SDR) con la capacidad de cargar diferentes formas de onda y con diseños de componentes que permitan capacidades multicanal y multibanda. Sin embargo, también es cierto que las aplicaciones civiles de las telecomunicaciones digitales han asumido y desarrollado estas técnicas, las han de desplegado con gran velocidad e intensidad y han suministrado a sus miles de millones de usuarios todo tipo de prestaciones, consumiendo una cantidad de recursos financieros muy alejada de los disponibles para aplicaciones militares.

En consecuencia, aunque haya reticencias, como las asociadas a la seguridad de las redes y la información que se transmite, es inevitable que las nuevas redes de comunicaciones militares, no solo se basen en tecnologías civiles, sino que usen equipos y sistemas civiles con las necesarias modificaciones para su implementación segura. Incluso, será difícil que su gestión y control no recaiga en parte en operadoras civiles. Me atrevo a afirmar que el 5G de uso militar será un estándar de uso común en las comunicaciones militares en las fuerzas armadas occidentales. Como conseguir que todo ello funcione adecuadamente en el campo de batalla digital con un espectro electromagnético escaso y sometido a acciones de ciberdefensa, es un reto nada desdeñable.

Procesado distribuido y ágil de la información

Como ya se ha indicado, las actuales y futuras operaciones militares se caracterizan por la necesidad de creciente flexibilidad en su diseño e implementación para adaptarlas a unos entornos cambiantes acortando los tiempos de reacción. Por otro lado, los actuales escenarios geoestratégicos requieren la escalabilidad de las mismas pues las misiones pueden ser de grados de intensidad muy diferentes y deben realizarse en un contexto transnacional y en colaboración con aliados externos.

Esto sólo puede conseguirse con unos sistemas de información descentralizados que permitan un proceso de información distribuido, en algunos casos deslocalizado, de tal modo que esta fluya selectivamente entre los diferentes los combatientes y las plataformas, casi en tiempo real. Algo que ya es una realidad en muchos ámbitos civiles, como en el sector financiero.

En el ámbito militar una dificultad es el coste que esto implica, sin embargo, el principal problema para introducir estas técnicas no es de tipo tecnológico sino cultural y doctrinal.

Lo que está en cuestión es la toma de decisión centralizada y jerarquizada que ha caracterizado la actividad militar a lo largo de casi toda su historia. La digitalización del campo de batalla permite una distribución de decisión y derechos, patrones de interacción no restringidos y una amplia difusión de información para elevar el nivel de colaboración. Con ello se optimiza la eficacia de las operaciones pero se requiere superar algunos lastres culturales y doctrinales presentes en las fuerzas armadas de todos los países[46].

Automatización y autonomía con IA estrecha

En su discurso de ingreso en esta Academia[47], el Dr. González de Posada, basándose en la figura de Torres Quevedo, describió brillantemente los orígenes y desarrollo de lo que denominó "una ciencia nueva", concebida por este, la Automática, cuyas "hijas", la Compu-

---

(46) SOARE, S. R. Digitalisation of defence in nato and the eu: making european defence fit for the digital age. The International Institute for Strategic Studies (IISS). 2023
https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2023/08/digitalisation-of-defence-in-nato-and-the-eu-making-european-defence-fit-for-the-digital-age.pdf

(47) Gonzalez de Posada, Francisco. *Automática, una ciencia nueva concebida por Torres Quevedo: su historia.* Discurso pronunciado en el acto de su toma de posesión como Académico de Número de la Real Academia de Doctores de España. 2021.
https://www.rade.es/imageslib/ACTIVIDADES/TEXTOS/GONZALEZ%20DE%20POSADA,%20Francisco_discursoingreso.pdf

tación, la Robótica, la Inteligencia Artificial y la Informática juegan un papel esencial en la ciencia, la ingeniería y la cultura actual. Obviamente, añado yo, también en el ámbito de la defensa.

La utilización de sistemas automatizados y el empleo de robots es algo muy extendido, tanto en el ámbito civil, especialmente en el sector industrial, como en el militar. La novedad, ya muy generalizada en el campo civil y que empieza a incorporarse en el campo militar, es el paso de sistemas automatizados a sistemas autónomos, aunque, como trataré de explicar a continuación, todavía con algunas limitaciones.

La autonomía implica la capacidad de detectar su entorno y saber qué hacer cuando un sistema se enfrenta a situaciones desconocidas, respondiendo de manera dinámica a entornos complejos y cambiantes. La autonomía requiere dotar al sistema de un cierto nivel de inteligencia, o, lo que es lo mismo, utilizar técnicas de IA. Las limitaciones en la operación de los sistemas autónomos están definidas por las de sus sensores, sus actuadores y, sobretodo, por la IA incorporada.

En estos momentos la IA está en la etapa que se conoce como IA estrecha (*Artificial Narrow Intelligence)*, también denominada IA débil o ANI por sus siglas en inglés, se caracteriza porque solo realizar una tarea específica basada en un conjunto de datos definido[48]. Actualmente ya pueden entrenarse con un gran número de datos y tomar decisiones o realizar acciones en base a este entrenamiento. Se ha demostrado que un algoritmo ANI es capaz de igualar o superar a la inteligencia y eficiencia humana pero solo en el área específica en la que opera. Algunos de los ejemplos más conocidos de ANI son el reconocimiento facial (los terminales inteligentes incluyen

---

(48) En este artículo de carácter divulgativo, se describen las diferentes etapas de la IA, un tema, por lo demás, muy controvertido. SMINK, V. *Las 3 etapas de la Inteligencia Artificial: en cuál estamos y por qué muchos piensan que la tercera puede ser fatal.* BBC News Mundo. Mayo 2023.
https://www.bbc.com/mundo/noticias-65617676

numerosas aplicaciones que usan esta tecnología), jugar al ajedrez, la conducción coches autónomos, o el popular ChatGPT al que luego me referiré. También en poco tiempo su utilización será imprescindible para asesorar la toma de decisiones durante el combate (por ejemplo, en la toma de decisión sobre qué tipo de arma emplear ante una determinada amenaza), en logística predictiva, para el guiado de sistemas de armas, para optimizar la navegación de las diferentes plataformas, entre otras muchas aplicaciones.

En los próximos años, el campo de batalla digital se caracterizará por la sustitución masiva y rápida de actividades humanas por robots y sistemas de información automatizados con ANI. El impacto social que ha tenido la aparición de Chat-GPT y sus consecuencias sobre amplios sectores tecnológicos y financieros asegura que será en el ámbito de las aplicaciones civiles y de la mano del mundo empresarial donde se desarrolle esta tecnología. Una tecnología que evolucionará hacia la IA general (*Artificial General Intelligence*, AGI) que definirá un nuevo campo de batalla: el campo de batalla inteligente.

Estas claves tecnológicas, sensorización, conectividad, procesado distribuido y ágil de la información y automatización y autonomía con IA estrecha modificarán los futuros campos de batalla. Se combatirá a mucha mayor distancia y se requerirán menos recursos humanos operando infraestructuras, equipos y sistemas de gran complejidad y sofisticación. La logística –predictiva no reactiva- se convertirá en un elemento esencial para asegurar el éxito en el conflicto. Las tecnologías utilizadas se basarán en las ya desarrolladas y aplicadas en actividades civiles, siendo estas el motor de desarrollo de los campos de batalla digital.

¿Cuándo los campos de batalla digitales serán una realidad? La batalla digital ya es una realidad desde hace años, especialmente en los conflictos entre naciones con elevadas capacidades tecnológicas, en

muchos casos en zona gris y por tanto no declarados. El conflicto palestino-israelí, es un ejemplo evidente de campo de batalla digital asimétrico[49].

En el caso de la Guerra en Ucrania, las imágenes servidas por los medios de comunicación tienden a presentarla como un conflicto de alta intensidad que nos retrotrae a la Primera y Segunda Guerra Mundial. En mi opinión, y en la de varios autores[50], esto está muy lejos de la realidad y se debe, entre otras muchas cosas, a que los bits no se ven, es el caso de los importantes combates que se están dando en los dominios del ciberespacio y cognitivo, de hecho, la guerra en estos dominios empezó mucho antes de que las tropas rusas invadieran Ucrania en febrero del 2022[51]. Por otro lado, si bien es cierto que las cifras de bajas y la destrucción producida en este conflicto corresponden más a un campo de batalla cinético que a un campo de batalla digital, también lo es que han aparecido numerosos elementos nuevos en la forma de combatir que son atribuibles a la digitalización del conflicto. De hecho, algunos analistas han introducido el concepto de participación online, para definir la contribución

---

(49) Martí Sempere, C. *El papel de la tecnología en los recientes conflictos de Ucrania y Gaza. Una valoración inicial.* Real Instituto Elcano. Febrero 2024. https://www.realinstitutoelcano.org/analisis/el-papel-de-la-tecnologia-en-los-recientes-conflictos-de-ucrania-y-gaza-una-valoracion-inicial/

(50) FRIAS SÁNCHEZ, C.J. *Rusia, Ucrania y el campo de batalla «transparente».* Instituto Español de Estudios Estratégicos. Documento de Opinión. Febrero 2024. https://www.ieee.es/Galerias/fichero/docs_opinion/2024/DIEEEO18_2024_CARFRI_Rusia.pdf

(51) ESTEVE DOMINGO M. *El horizonte de las operaciones en el ciberespacio tras la guerra de Ucrania.* Comunicaciones académicas. Academia de las Artes y de las Ciencias Militares. Enero 2024. https://www.acami.es/publicacion/horizonte-operaciones-en-el-ciberespacio-tras-la-guerra-de-ucrania/

de Estados Unidos y Reino Unido a la Guerra en Ucrania[52] y otros defienden que una buena parte de las operaciones del ejército ucraniano, con el soporte occidental, son los primeros ejemplos prácticos de operaciones militares en red[53].

Este "combate a distancia en red" es uno de los elementos característicos del campo de batalla digital y requiere una sensorización, una conectividad, unos sistemas autónomos y un proceso distribuido de la información muy desarrolladas. Sin estos elementos el limitado ejercito ucraniano, no hubiese podido detener la invasión del ejército ruso[54].

---

(52) *Además, Estados Unidos y Gran Bretaña están poniendo en práctica un modelo de "participación online" que está noqueando al orgulloso Ejército ruso.* Este párrafo escrito por el coronel José Pardo de Santayana y Gómez de Olea, coordinador de investigación y analista principal del Instituto Español de Estudios Estratégicos en la publicación "Panorama geopolítico de los conflictos 2022. Capítulo primero: La Guerra de Ucrania", editado por el Instituto Español de Estudios Estratégicos del Ministerio de Defensa, pone de manifiesto la aparición de una nueva forma de hacer la guerra que sólo es posible para países con unas fuerzas armadas con un elevado nivel de digitalización.
https://www.ieee.es/publicaciones-new/panorama-geopolitico-de-los-conflictos/2022/PGC2022.html

(53) GOBERNA J.L., *La Guerra Centrada en la Red (NCW) desde las Fuerzas Armadas de Ucrania.* Infodefensa. Sept. 2023.
https://www.infodefensa.com/texto-diario/mostrar/4441291/guerra-centrada-red-ncw-desde-fuerzas-armadas-ucrania

(54) PARDO DE SANTALLANA, J. *De nuevo guerra en Europa (capítulo 2 de Panorama Estratégico 2023.)Instituto Español de Estudios Estratégicos*
https://www.ieee.es/Galerias/fichero/panoramas/PE2023/PE2023_Capitulo2.pdf

V. EL CAMPO DE BATALLA INTELIGENTE

No es lo mismo información que conocimiento… El conocimiento es reflexión sobre la información, es capacidad de discernimiento y de discriminación respecto a la información que se tiene, es capacidad de jerarquizar, de ordenar, de maximizar, etc., la información que se recibe…todo es información menos el conocimiento que nos permite aprovechar la información. Fernando Sabater. RAZÓN, FILOSOFÍA Y EDUCACIÓN [(55)].

Permítanme que ahora analice como el campo de batalla digital evolucionará en unos años hacia un campo de batalla inteligente donde las máquinas generarán la mayor parte del conocimiento utilizado en los escenarios de conflicto[(56)].

a) Un nuevo paradigma: la sociedad del conocimiento

Ya se ha indicado que la digitalización de los sistemas de información y comunicaciones ha derribado las barreras temporales y espa-

---

(55) https://fraynelson.com/biblioteca/filosofia/razon_educacion_filosofia.htm

(56) PEREZ MARTINEZ, *F. Inteligencia en el campo de batalla.* Anales de la Real Academia De Doctores de España. Vol 9, Nº 1-2ª etapa, pp 121-141. 2024.
https://www.rade.es/imageslib/PUBLICACIONES/ARTICULOS/V9N1%20-%2001%20-%20AO%20-%20PEREZMARTINEZ_inteligenciaenelcampodebatalla.pdf

ciales para el acceso generalizado a la información, dando lugar a una nueva dinámica en las relaciones humanas. A medida que las tecnologías digitales continúan evolucionando, la próxima generación de equipos y sistemas se caracterizará por su capacidad de adaptarse a las necesidades individuales de los usuarios y a las circunstancias específicas en cualquier momento. Aunque aún estamos a la espera de que la capacidad y la velocidad del procesamiento de datos lo hagan posible, podemos afirmar que este proceso nos llevará hacia una sociedad del conocimiento en la que los sistemas y técnicas serán inteligentes, y los datos se compartirán no solo entre seres humanos, sino también con objetos, en un entorno de hiperconectividad.

Esta nueva sociedad, tal como describió el Dr. José Ramón Casar Corredera en la Apertura del Curso Académico 21-22 de esta Real Academia, será fruto del desarrollo de cuatro desarrollos relevantes de las tecnologías digitales:

Pues bien, creo que la evolución transcurrirá en un espacio definido por cuatro ejes principales, a saber:

- el desarrollo, despliegue y expansión de la tecnología de 5G y de su próxima sucesora, la 6G, y el desarrollo asociado de las necesarias infraestructuras de comunicación fija (backhaul) y de las comunicaciones entre vehículos, y en movilidad en general.

- la computación ubicua, construida sobre el borde de la red (edge) y unas nuevas arquitecturas de nube (cloud y cloudlets) y de computación distribuida, impulsada por las aplicaciones de Internet de las Cosas y el propio 5G (y 6G).

- las aplicaciones, servicios y negocios basados en los datos, con las utilidades de inteligencia artificial como herramientas principales para su analítica y valorización.

- *las interfaces y los nuevos modos "inmersivos" de interacción* [57].

La conjunción de todo ello permitirá la creación de nuevos sistemas de información y nuevos sistemas ciberfísicos, conectados entre sí y conectados a un mundo virtual de la mano de las redes digitales cuyo objetivo principal es controlar e interactuar con los procesos, tanto del ciberespacio como del mundo físico, y adaptarse a la evolución de sus condiciones en tiempo real. Nos estamos refiriendo sistemas expertos y sistemas ciberfísicos varios ordenes de magnitud más eficientes para combatir el cambio climático, descubrir nuevas medicinas y técnicas para luchar contra enfermedades hoy incurables, asegurar la alimentación y la energía de la humanidad o predecir cataclismos, pero también para implementar sistemas de defensa y de combate autónomos, en la que los *terminators* constituyen una de nuestras peores pesadillas.

¿Cómo será este nuevo mundo digital inteligente, ¿cómo será esta sociedad del conocimiento? Permítanme contestar a esta pregunta después de hacer algunas consideraciones previas sobre la tecnología disruptiva que forjará estos cambios.

b) La irrupción de la inteligencia artificial

Durante casi un siglo, los seres humanos hemos estado dedicados a resolver problemas complejos a través de máquinas que imitan nuestra capacidad de razonamiento. Para lograrlo, se han utilizado algoritmos capaces de aprender, razonar y tomar decisiones de manera similar a nosotros. Sin embargo, emular el funcionamiento del cerebro humano no solo requiere una gran capacidad de cálculo, ve-

---

(57) CASAR CORREDERA, J. R. *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.rade.es/imageslib/doc/Conferencia%20apertura%202022%20Dr.%20Casar.pdf

locidad de procesamiento y almacenamiento de datos, sino también habilidades adicionales como la percepción y la interpretación del entorno, así como la comprensión del lenguaje natural.

Cien años de esfuerzos que ahora están dando sus frutos gracias a los formidables avances en la capacidad de cálculo de los ordenadores y la disponibilidad de grandes volúmenes de datos tras la implantación de Internet y el acceso universal a la información. Las ingentes cantidades de datos que se generan permiten aplicaciones sustitutivas de múltiples actividades humanas como el aprendizaje automático, el aprendizaje profundo, la visión artificial, el procesamiento del lenguaje natural, el razonamiento automatizado para la toma de decisiones, la robótica, los vehículos autónomos y un largo etc.

La evolución en los últimos años de la IA se puede observar en los prestigiosos informes de Gartner sobre tecnologías digitales. Son el resultado de la investigación exhaustiva y el análisis de expertos del panorama tecnológico y proporcionan información muy valorada por empresas y profesionales para tomar decisiones sobre estrategias tecnológicas en el sector de las TIC(58).

Hace unos años, uno de estos informes establecía como una de las tres "megatendencias" que definirían la economía digital en la siguiente década lo que definía como "La IA en todas las partes"(59). Posteriormente estas "megatendencias" pasaron a ser: "la automatización acelerada de la IA"(60), o sea la IA diseña IA. Más adelante apareció "la IA adaptativa"(61), capaz de cambiar sus modelos ante

(58) https://www.gartner.es/es/tecnologia-de-la-informacion/insights/principales-tendencias-tecnologicas

(59) https://raona.com/tendencias-principales-hype-cycle-gartner-tecnologias-emergentes-2017/

(60) https://communicationsplatformforbusiness.computerworld.es/tendencias/gartner-identifica-las-tecnologias-emergentes-que-ayudaran-a-la-transformacion-de-las-empresas

(61) https://www.gartner.es/es/articulos/por-que-la-ia-adaptativa-es-importante-para-tu-empresa

cambios de su entorno, y finalmente, hace algo más de un año, ha emergido y asombrado la "IA generativa"[62]. Lo sorprendente de esta concatenación de megatendencias con la IA como protagonista es que todo ha ocurrido en unos pocos años y que todo lo que se anunciaba se ha convertido en gran medida en una realidad. La IA está en todos los ámbitos, prácticamente no hay servicio, empresa, producto o actividad humana en la que no haya entrado o amenace con entrar. ¿Es sólo una moda?, claro que no, "La IA para todo"[63], y por tanto también en el ámbito de la defensa y seguridad[64], es lo que mejor define las circunstancias tecnológicas actuales, pero desde luego la IA también es una moda.

Unas inevitables consideraciones sobre la IA generativa y el fenómeno "ChatGPT"[65] [66]. Si ustedes le preguntan a ChatGPT que es la IA generativa les contestará:

La Inteligencia Artificial Generativa, o IAG, se refiere a un enfoque dentro del campo de la inteligencia artificial que se centra en la creación de sistemas capaces de generar contenido nuevo y original, como imágenes, música, texto o incluso videos, que imitan o se asemejan al estilo de datos de entrenamiento proporcionados.

---

(62) https://www.gartner.es/es/articulos/mas-alla-de-chatgpt-el-futuro-de-la-ia-generativa-para-empresas

(63) https://www.gartner.es/es/articulos/novedades-del-hype-cycle-de-gartner-para-la-inteligencia-artificial-2022

(64) PÉREZ MARTINEZ F. *Defensa inteligente en un mundo inteligente.* Comunicaciones académicas. Academia de las Ciencias y las Artes Militares. Octubre 2020. https://www.acami.es/wp-content/uploads/2022/05/Defensa-inteligente-en-un-mundo-inteligente-web.pdf

(65) CASAR CORREDERA J.R. *Inteligencia Artificial Generativa.* Anales de la Real Academia de Doctores, Vol. 8, Nº 3, 2023, págs. 475-489. 2023. https://www.rade.es/imageslib/PUBLICACIONES/ARTICULOS/V8N3%20-%2001%20-%20ED%20-%20CASAR.pdf

(66) ARNETT, S. *ChatGPT no surge de la nada: es el resultado de 30 años de prueba y error.* MIT Technology Review. Febrero 2023. https://www.technologyreview.es/s/15081/chatgpt-no-surge-de-la-nada-es-el-resultado-de-30-anos-de-prueba-y-error

Los modelos de IA generativa suelen basarse en redes neuronales artificiales, como las Redes Neuronales Convolucionales (CNN) o las Redes Neuronales Recurrentes (RNN), y pueden utilizar técnicas como las Redes Generativas Adversarias (GANs) o las Redes Neuronales Autoencodificadoras (Autoencoders) para generar datos realistas.

Estos sistemas pueden ser utilizados en una variedad de aplicaciones creativas, como la generación de arte digital, la síntesis de música, la creación de texto creativo e incluso en la producción de imágenes realistas de personas que no existen. Además, la IAG también puede ser aplicada en campos como el diseño asistido por computadora, la creación de contenido multimedia y la investigación científica [(67)].

En definitiva, se define a sí mismo como una tecnología que permite crear contenidos originales e innovadores de manera autónoma, con capacidad de generar imágenes, música, textos, programas, etc. a partir del aprendizaje de grandes cantidades de datos, combinando ideas existentes para producir algo completamente nuevo y original. Nótese la fuerza y consecuencias de esto último que es más que discutible y es uno de los elementos clave del debate que origina esta nueva herramienta.

Pero, ¿qué opinamos los humanos de ChatGPT, en general, de la IA generativa?. Permítanme que no entre en esta cuestión pero que aporte un dato significativo: en estos momentos, trece millones de españoles han usado ChatGPT en horario de trabajo y el dominio de la IA generativa es la habilidad más demandada y de las mejor remuneradas por las empresas tecnológicas en 2024[(68)].

Por supuesto que existe fuertes corrientes de rechazo a este tipo de herramientas y al uso que se pueda hacer de ellas, también es evidente que su despliegue implica enormes problemas que resolver,

(67) https://chatgpt.es/

(68) https://www.computerworld.es/tendencias/el-dominio-de-la-ia-generativa-la-habilidad-mas-demandada-por-los-empresas-para-2024

entre los que no son menores la protección de los derechos de propiedad intelectual, la protección de los datos personales o su impacto en la mayor parte de las actividades humanas. Así se puso de manifiesto en la jornada "Visiones y aplicaciones de la inteligencia artificial", organizada por la Real Academia de Doctores de España en colaboración con la Universidad Politécnica de Madrid el pasado mes de octubre en la Real Sociedad Económica Matritense de Amigos del País.

Cuando se están escribiendo estas líneas, en "El economista.es" se publica la noticia de que un programa de inteligencia artificial ha eliminado 4000 empleos de profesores que hasta ahora corregían un examen estatal en Texas:

Al parecer los afectados son 4.000 examinadores del STAAR, un examen estatal que los estudiantes menores de 18 años deben de tomar para medir los conocimientos de estos en materias como la escritura, lectura, ciencia y estudios sociales.

Cada año el estado de Texas contrata a 6.000 profesores durante varias semanas para que se encarguen de supervisar y corregir estos exámenes. Pues al parecer, este año el estado tan solo ha contratado a 2.000 examinadores y el resto de vacantes serán cubiertas por una IA… muchos han alzado su voz criticando esta decisión debido a que el examen no es un tipo test, sino que se trata de un examen con respuestas libres, las cuales la IA tendrá que analizar e interpretar las respuestas para validarlas y nadie sabe con qué parámetros o criterios lo hará…(Miguel Terán Haughey, 15/04/2024) [(69)].

Una noticia de estas características, especialmente dolorosa para nuestra Academia, nos permite vislumbrar un futuro incierto para

(69) https://www.eleconomista.es/tecnologia/noticias/12769621/04/24/el-futuro-ya-esta-aqui-texas-anuncia-el-reemplazo-de-4000-examinadores-por-una-inteligencia-artificial.html#:~:text=Cada%20a%C3%B1o%20el%20estado%20de,ser%C3%A1n%20cubiertas%20por%20una%20IA.

nuestras instituciones. En todo caso, la presencia diaria de la IA en los medios de comunicación, las reacciones y debates que suscita o su impacto directo sobre las actuales estrategias institucionales y empresariales indica que estamos ante una tecnología disruptiva que tendremos que asimilar. Una tecnología que desembocará en cambios sociales muy profundos(70).

Y esto es solo el principio, la IA nos dará sorpresas similares en los campos de la visión artificial, robótica, programación, predicción, producción etc. pero en todos ellos la IA necesitará mucha, pero mucha, "Inteligencia Humana", tanto para funcionar con eficiencia como para evitar desastres de todo tipo.

El proceso es imparable y caminamos hacia la sociedad del conocimiento. La IA habilita unas tomas de decisión mucho más eficientes que las del ser humano, al menos en términos de volumen y velocidad de respuestas ante incertidumbres y problemas. 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. Lo que nos produce rechazo, especialmente cuando las decisiones afectan a personas, porque los algoritmos no entienden ni comprenden las razones para tomarlas, a diferencia de los humanos que si lo hacemos porque asociamos las decisiones a nuestras experiencias y somos conscientes de nuestros actos.

En definitiva, hablamos de la sustitución de personas por máquinas en muchas actividades humanas, 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,

---

(70) MEIGE, A. et al. *Generative artificial intelligence: Toward a new civilization?*. Blue Shift Report. Ed Arthur D. Little. Reino Unido. https://www.adlittle.com/en/insights/report/generative-artificial-intelligence-toward-new-civilization

lo harán en actividades que considerábamos exclusivas del ser humano y afectará a todas las capas sociales, incluidas las más altas, y generando una nueva brecha social de consecuencias desconocidas.

El reto radica en cómo asegurar en este contexto los estándares éticos que exigen nuestras sociedades democráticas. La regulación y la autorregulación, como la reciente ley de IA de Comisión Europea[71], son herramientas que han funcionado en otros dilemas similares, como por ejemplo en el desarrollo de la energía nuclear o la biología molecular, y confiemos en que su aplicación ralentice y encauce una dinámica que en estos momentos es muy peligrosa.

¿Y en el ámbito de la defensa y seguridad?, Obviamente las fuerzas armadas de todos los países y en particular, las nuestras y las de nuestros aliados, son conscientes de estos cambios. Son conscientes de la necesidad de incorporar inteligencia a los sistemas militares, 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, hablamos de hogares inteligentes, ciudades inteligentes, salud inteligente, industria inteligente…

¿Cuáles serán las claves tecnológicas del campo de batalla inteligente?, hagamos un ejercicio intelectual similar al realizado para el actual campo de batalla.

c) Algunas características del campo de batalla inteligente: la superioridad del conocimiento

En mi opinión estas son algunas:

Datificación

La datificación de la realidad será un hecho al que contribuirán tanto las mejoras tecnológicas en los sensores como la amplia disponibi-

(71) https://artificialintelligenceact.eu/es/

lidad y uso que de ellos se hará. La capacidad de almacenamiento y acceso masivo a los datos convierte a lo que antes eran instantes efímeros que recordar en datos de utilidad. El potencial de sensorización y capacidad de distribución de datos obtenidos por los miles de millones de propietarios de teléfonos inteligentes y de usuarios de internet es difícil de imaginar. De hecho, la cantidad de información producida y distribuida por fuentes abiertas es enorme y disponible en un futuro es difícil de imaginar.

Por otro lado, el futuro despliegue de los dispositivos y sistemas bajo estándares IoT, Internet de las Cosas, implica la instalación en numerosos objetos y asentamientos de dispositivos que adquieren información de su entorno y la distribuyen coordinadamente sin control humano directo. En unos años la estandarización de la IoT se traducirá en un radical abaratamiento de la tecnología necesaria, lo que permitirá configurar centenares de miles de redes con millones de millones de conexiones fiables y seguras. Además, el abaratamiento de las tecnologías espaciales, tanto por la reducción de peso y volumen de las plataformas como por la reducción de coste de los lanzadores, asegura la disponibilidad de miles de satélites observando con gran detalle el escenario completo de un conflicto.

Ya se maneja el concepto de "campo de batalla transparente"[72] en el que es prácticamente imposible ocultar los medios desplegados para el combate. Son muchas las consecuencias que este hecho tiene sobre los modos de combatir, siendo la más evidente la separación de los frentes de batalla e incluso la dispersión o desaparición de los mismos. La "guerra de drones y misiles" en Oriente Medio y Ucrania o el masivo empleo de artillería de larga distancia en esta última están indicando la dirección de los futuros enfrentamientos.

---

(72) FRIAS SÁNCHEZ, C.J. *Rusia, Ucrania y el campo de batalla «transparente».* Instituto Español de Estudios Estratégicos. Documento de Opinión. Febrero 2024.
https://www.ieee.es/Galerias/fichero/docs_opinion/2024/DIEEEO18_2024_CARFRI_Rusia.pdf

Hiperconectividad

Este concepto define el intercambio masivo de datos entre entornos digitales y la interacción entre sistemas de información, datos y dispositivos, interconectados a través de redes digitales capaces de gestionar y procesar en tiempo real grandes cantidades de información.

La hiperconectividad asegurará que cada participante en el conflicto reciba, en tiempo real y desde distintas fuentes, la información que requiere después de un proceso de elaboración complejo para adaptarla a sus necesidades. las redes de comunicación serán inteligentes, es decir procesarán y difundirán la información mientras se transmite entre los diferentes nodos de forma flexible y adaptada a los acontecimientos en tiempo casi real. La aplicación masiva de técnicas de IA en todos los niveles físicos y lógicos de las redes de comunicación será imprescindible. Las ventajas y riesgos de la hiperconectividad en las operaciones militares las he descrito en una publicación reciente[73]. Los riegos son muy relevantes (incremento de la vulnerabilidad ante acciones de ciberdefensa, necesidad de operadores muy cualificados, nuevas patologías en los combatientes…) pero no limitarán su extensión.

Afortunadamente, los estándares utilizados en las últimas generaciones de comunicaciones móviles, 5G y 6G, ya se han diseñado con la capacidad de trabajar de este modo, manejando cantidades ingentes de datos, con bajas latencias permitiendo la computación en los nodos de la red y facilitando la incorporación de las nuevas técnicas y algoritmos que precisa la implantación de la IA.

Por otro lado, la hiperconectividad incrementa exponencialmente la mayor parte de las actividades humanas por lo que su rápida evolución tendrá como motor las aplicaciones civiles. Además, y dado que la condición necesaria para tener éxito en los futuros escenarios

---

(73) PÉREZ MARTINEZ F. *Hiperconectividad. El sistema nervioso de los futuros campos de batalla.* Comunicaciones académicas. Academia de las Ciencias y las Artes Militares. Abril 2024
https://www.acami.es/publicaciones/?cat=comunicaciones-academicas.

de conflicto es la superioridad en la toma de decisiones basada en la conectividad y la algorítmica desplegada, condicionará las arquitecturas y despliegues de los futuros sistemas de información y comunicación militares.

Procesado cognitivo

A diferencia del procesado de la información característico de los campos de batalla digitales en que las técnicas de computación en la nube, borde o niebla solo pretenden optimizar la interpretación de los datos presentados a los usuarios para que estos tomen las decisiones más adecuadas, por el contrario, el procesado cognitivo está orientado directamente a la emulación de los procesos cognitivos humanos para permitir a las máquinas razonar y decidir cómo nosotros. Ello requiere reproducir algorítmicamente funciones cognitivas como la orientación, las gnosias, la atención, la ejecución, las praxias, el lenguaje, las habilidades visoespaciales, etc, que se desarrollarán mediante sistemas cognitivos basados en la IA(74).

Algunas de las aplicaciones ya operativas están asociadas al procesado cognitivo de documentos, audios o videos para resumirlos, encontrar los temas que contiene, monitorear los sentimientos de los interlocutores sobre ellos, determinar riesgos y amenazas, etc., pero es solo el principio de una disrupción que se verá acelerada por los avances de la neurociencia y la neurotecnología, todavía emergentes.

Automatización y autonomía con IA general

A diferencia de la actual IA estrecha, en la futura IA general las máquinas y algoritmos trabajan en diferentes tareas a la vez, con datos no específicos, casi ilimitados, alcanzando capacidades cognitivas a nivel humano y realizando tareas intelectuales propias de las perso-

---

(74) Una descripción de estos proceso, de carácter divulgativo pero completa y detallada, puede encontrarse en:
https://neuroblogic.com/2023/09/29/funciones-cognitivas-explorando-el-fascinante-mundo-del-pensamiento-humano/

nas. Los algoritmos serán las nuevas herramientas del combate no solo por su capacidad de automatizar muchas tareas para realizarlas más eficientemente que los humanos, sino también por su capacidad de encontrar patrones desconocidos y crear nuevos, empleándose tanto en los dominios físicos como en el ciberespacio y el dominio cognitivo.

La incorporación de técnicas de IA general permitirá que la mayor parte de los equipos y sistemas presentes en los conflictos puedan trabajar de forma automática y autónoma, limitando los riesgos de sus operadores. El campo de batalla inteligente es el hábitat natural de los sistemas autónomos y en él, el combate algorítmico definirá el resultado de las operaciones. A modo de ejemplo, hace escasas semanas el régimen chino liderado por Xi Jinping ha decidido que los dos pilares sobre los que basará la mejora de sus capacidades estratégicas de combate serán la Inteligencia Artificial y los vehículos no tripulados(75).

Estas claves tecnológicas, datificación, hiperconectividad, procesamiento cognitivo y automatización y autonomía con IA general, experimentarán entre ellas intensas relaciones sinérgicas con realimentaciones cruzadas que acelerarán su desarrollo para transformar radicalmente los escenarios de conflicto. A modo de ejemplo, en la referencia citada, se describen las relaciones sinérgicas entre la hiperconectividad y la IA:

La aplicación de las técnicas de IA permitirá optimizar el rendimiento de las redes asignando los recursos de manera dinámica y en tiempo real en función de las demandas de tráfico y a las condiciones de la propia red. También se empleará en su gestión y mantenimiento pues los algoritmos de IA permitirán monitorear y diagnosticar predictivamente los potenciales problemas y fallos en las redes.

---

(75) XUANZUN, L. *Chinese military aims to boost strategic capabilities in emerging areas such as AI, unmanned tech.* Global Times. March 2024. https://www.globaltimes.cn/page/202403/1308558.shtml

El uso de IA para la automatización de prácticamente todos los procesos necesarios incrementará espectacularmente la eficiencia operativa las redes y reducirá sensiblemente sus costes. Además, la IA se utilizará para detectar y mitigar las amenazas de seguridad, por ejemplo, analizando grandes volúmenes de datos de tráfico para identificar patrones sospechosos.

Por último, pero no menos importante, permitirá la personalización de los servicios, en base al análisis del comportamiento de los usuarios, adaptándolos a las necesidades individuales en cada momento. Por ejemplo, decidiendo que una información que se transmite por la red es útil para alguna persona conectada y traduciendo en tiempo real los contenidos a su idioma para hacérsela llegar.

Por otro lado y en sentido contrario, las redes de telecomunicación son imprescindibles para el desarrollo y empleo eficaz de la IA. En primer lugar asegurando una conectividad global necesaria para la adquisición y distribución de las grandes cantidades de datos necesarias para el entrenamiento y optimización de los algoritmos y, por otro, permitiendo la computación distribuida para poder realizar los complejos algoritmos a veces requeridos. Así mismo, muchas aplicaciones de la IA trabajan en modo distribuido con despliegues en la nube y/o integración de dispositivos (IoT u otros sensores y actuadores), donde las redes son imprescindibles. [(76)]

En definitiva, la condición de para alcanzar la victoria en los futuros conflictos será la superioridad del conocimiento obtenida mediante la disponibilidad de mejores algoritmos en los artefactos y sistemas de información y comunicaciones utilizados[(77)].

---

(76) PÉREZ MARTINEZ F. *Hiperconectividad. El sistema nervioso de los futuros campos de batalla.* Comunicaciones académicas. Academia de las Ciencias y las Artes Militares. Abril 2024
https://www.acami.es/publicaciones/?cat=comunicaciones-academicas.

(77) Un análisis interesante sobre la contribución de la IA al planeamiento de las operaciones militares puede encontrarse en: GARAT GONZALEZ, J. M. *La inteligencia artificial como factor de transformación de las operaciones militares en el nivel operacional.* Documento de Opinión. Instituto Español de Estudios Estratégicos. Diciembre 2024. https://www.ieee.es/Galerias/fichero/docs_opinion/2024/DIEEEO12_2024_JUAGAR_Inteligencia.pdf

Solo podemos intuir algunos aspectos concretos de estos nuevos escenarios que se irán desplegando progresivamente a un ritmo que es objeto de controversia. Sobre lo que hay un consenso generalizado es que esta nueva revolución tecnológica, como la revolución digital, se producirá primero en el ámbito civil y, posteriormente y en buena medida con bases tecnológicas ya desarrolladas en este, en el ámbito de la defensa y seguridad [(78)].

Por supuesto que hay otras tecnologías no consideradas en los párrafos anteriores que jugarán un papel importante en la definición de los futuros escenarios. Existen numerosos informes de instituciones y organismos de carácter militar que catalogan y describen las posibles tecnologías que marcarán el devenir de los conflictos en las próximas décadas y en general coinciden en sus pronósticos[(79)]. Es el caso del reciente informe de la Agencia Europea de Defensa (EDA, European Defence Agency) titulado "Enhancing EU military capabilities beyond 2040" [(80)]. Todos incluyen las tecnologías digitales ya comentadas y añaden las hipersónicas y las espaciales, las biotecnologías, las tecnologías cuánticas, la nanotecnología o la impresión 3D entre otras. En todo caso, son las tecnologías digitales las que más preocupan en estos momentos, entre otras razones por velocidad de desarrollo y su fuerte dependencia del ámbito civil.

---

(78) CENTRO CONJUNTO DE DESARROLLO DE CONCEPTOS. *Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R).* Ministerio de Defensa.2020
https://publicaciones.defensa.gob.es/usos-militares-de-la-inteligencia-artificial-la-automatizacion-y-la-robotica-iaa-r-libros-ebook.html

(79) VARIOS AUTORES. *Emerging and disruptive technologies.* OTAN. Dec, 2022
https://www.nato.int/cps/en/natohq/topics_184303.htm?selectedLocale=en

(80) EUROPEAN DEFENCE AGENCY. *Enhancing EU military capabilities beyond 2040. Main findings from the 2023 Long-Term Assessment of the Capability Development Plan. 2023.*
https://eda.europa.eu/docs/default-source/eda-publications/enhancing-eu-military-capabilities-beyond-2040.pdf

d) Del campo de batalla digital al campo de batalla inteligente

¿Cómo será la transición desde unos escenarios de conflicto digitales a otros inteligentes? Por supuesto a la estela del desarrollo de esta nueva forma de sociedad que hemos denominado del conocimiento y, en mi opinión y como ya ocurrió con la revolución digital, será un cambio progresivo y sujeto a fuertes resistencias. La transición supondrá un enorme esfuerzo científico e ingenieril al que se opondrán algunos sectores en las fuerzas armadas que se sentirán amenazados, en algunos casos con razón, por cambios tan profundos. Las demoras vendrán de condicionantes de índole socioeconómico, así como del factor humano de resistencia al cambio.

Por otro lado, las características específicas de las aplicaciones militares aseguran que su introducción será más lenta que en la mayor parte de los sectores económicos civiles. Las razones son numerosas y van desde elevado ciclo de vida de los equipos y sistemas militares que dificulta su modernización, a las condiciones críticas en que trabajan y la tolerancia a los fallos casi cero que se exige lo que retrasa la incorporación de nuevas tecnologías. Además, las instituciones y organizaciones militares son muy conservadoras, nada proclives a los cambios, aunque debemos reconocerles su capacidad de implementarlos eficazmente cuando se asume su necesidad.

En todo caso ya estamos viendo a los primeros sistemas autónomos en los campos de batalla y su número y complejidad irá aumentado con el tiempo a un ritmo vertiginoso. Veremos, a corto plazo la introducción de sistemas inteligentes de asesoramiento en los sistemas de mando y control, que con el tiempo reducirán a la mera supervisión la mayor parte de las decisiones tomadas durante las operaciones. Los sistemas de ciberdefensa y guerra electrónica serán también de los primeros en incorporar masivamente la IA por la reducción de tiempos de respuesta que requieren este tipo de enfrentamientos. Luego lo harán sistemas de reconocimiento y vigilancia, los sistemas de transporte, los sistemas logísticos, etc.

Los sistemas de armas también serán inteligentes. Su objetivo final es la destrucción y, por tanto, son susceptibles de producir daños colaterales, por lo que la introducción de IA requerirá precauciones adicionales de índole ético, jurídico y humanitario que pueden limitar y retrasar la introducción de aquellas técnicas que supongan altos niveles de autonomía. Sin embargo, aunque personalmente lo rechace, veo inevitable que la aplicación de las tecnologías disponibles convierta en pocos años a los sistemas de armas en sistemas ciberfísicos, capaces de actuar simultáneamente en un mundo virtual y en el mundo real, con capacidades de detección y precisiones no imaginables y dotados de elevados niveles de autonomía por el uso masivo de técnicas de IA. Harán realidad el aforismo de que "todo lo que es detectado es destruido", lo que llevado a un campo de batalla transparente solo puede llevar a la conclusión de que los conflictos armados no serán posibles entre contendientes que dispongan de estas tecnologías o se resolverán con tácticas y reglas de enfrentamiento difíciles de imaginar en estos momentos… quizá el enfrentamiento electrónico sustituya en gran medida al combate cinético, limitando drásticamente el número de bajas.

El desarrollo de lo que se conoce como armas autónomas letales, en las que el arma detecta y selecciona el objeto a batir, ha sido y es objeto de intenso debate, especialmente ahora que estás armas empiezan a introducirse en los campos de batalla(81).

¿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

---

(81) Un estudio académico muy completo y detallado sobre las armas autónomas puede encontrarse en la tesis doctoral: WALKER, P.W. *War without oversight; challenges to the deployment of autonomous weapon systems.* The University of Buckingham. July 2019.
https://www.academia.edu/40066000/WAR_WITHOUT_OVERSIGHT_CHALLENGES_TO_THE_DEPLOYMENT_OF_AUTONOMOUS_WEAPON_SYSTEMS

eficiencia en las operaciones, cualidades esenciales en esta 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». La presencia del "hombre en el lazo" es lo que se propone como solución, lo que queda por ver es si es algo fácil de implementar[82].

Otro de los componentes esenciales en los futuros escenarios de conflicto es que una buena parte de las hostilidades se librará en el dominio cognitivo en un entorno de hipercomunicación con un uso masivo de algorítmica basada técnicas de IA. En estos enfrentamientos los algoritmos son armas tácticas y estratégicas invisibles capaces de cambiar las opiniones y comportamientos de los ciudadanos y alterar la realidad de grupos sociales e incluso países:

…. los algoritmos y sus capacidades analíticas especializadas son las nuevas herramientas del combate del siglo XXI, pues desde allí es posible encontrar patrones conocidos y crear nuevos, de tal forma que se posicione un mensaje en el imaginario de las personas… La propaganda política como estrategia tradicional utilizada en los conflictos regulares, en un escenario global e interconectado, adquiere una dimensión diferente, dado que no solamente podrá crear

(82) Un artículo muy interesante y actual sobre las implicaciones éticas y jurídicas del empleo de sistemas de armas autónomas letales puede encontrarse en MOLINER GONZÁLEZ, J.A. *Ética y control humano significativo en sistemas de armas autónomos letales regidos por la Inteligencia Artificial.* Comunicaciones académicas. Academia de las Ciencias y de las artes Militares. Marzoo 2024 https://www.acami.es/publicacion/etica-y-control-humano-significativo-salas-ia/

la inquietud y la duda entre las personas, sino que tendrá la capacidad de modificar la perspectiva de la acción humana y confundir la dinámica social basada en los fines de los adversarios…[83]

Es un tipo de combate, ya utilizado, radicalmente diferente al que se libra en los dominios físicos o cibernéticos. La novedad radicará en su utilización masiva. Así, en un reciente artículo se afirma que:

La batalla la ganará quien controle la generación y distribución interesada - gramsciana- de las etiquetas… quien denomine creyentes o gentiles, demócratas o fascistas, patriotas o traidores, puros o impuros, gente de orden o subversivos. El etiquetado contrario al mensaje propio puede convertirse en sinónimo de exclusión. Una máquina de deshumanizar bajo etiquetas dogmáticas, como facha o rojo. En regímenes democráticos, solo son una porción maleducada de la dialéctica política y social de cada sociedad. Sin embargo, su empleo sistemático para obtener ventaja política, económica, social o incluso deportiva, cambia ahora con la revolución de los medios de proceso del lenguaje, de su mecanización y del control de la algoritmia y sus efectos sistematizados y sistémicos[84].

---

(83) CANO, J. *Los conflictos híbridos y el poder de los algoritmos.* Revista SISTEMAS. 2021
https://sistemas.acis.org.co/index.php/sistemas/article/view/168

(84) VARIOS AUTORES. *Quién defiende a quién en la batalla de la verdad, de la mentira y de la memoria.* Comunicaciones académicas. Academia de las Ciencias y de las artes Militares. Enero 2024
https://www.acami.es/publicacion/batalla-de-la-verdad-la-mentira-la-memoria/

VI. EL CAMPO DE BATALLA SINGULAR

"El campo de operaciones se ampliará del dominio físico y el dominio de la información hasta el dominio de la conciencia, el cerebro humano se convertirá en el nuevo espacio de combate". General He Fuchu, vicepresidente de la Academia de Ciencias Militares de China

Especular sobre lo que ocurrirá dentro de un cuarto de siglo es un ejercicio de osadía cuando no de melancolía. Sin embargo, la historia de la humanidad nos demuestra que el filósofo griego Heráclito, si es que él fue de verdad su autor, acertó cuando aseguró que "todo fluye, todo cambia, nada permanece". Lo que es seguro es que la revolución de la inteligencia será solo el precedente de otra revolución tecnológica, como la revolución digital lo fue de ella. Lo que es seguro es que a mediados de este siglo la sociedad del conocimiento evolucionará hacia una sociedad nueva, singular, que algunos autores definen como cognitiva, asumiendo que el hecho de que las máquinas puedan razonar como nosotros y puedan comunicar directamente con el cerebro humano será una de sus características esenciales.

Personalmente no me atrevo a teorizar demasiado sobre lo que ocurrirá dentro de veinticinco años por eso prefiero denominarla sociedad singular, en la que lo único seguro es que será muy diferente a la actual, consecuencia del impacto de unos progresos científicos y tecnológicos que ya están entre nosotros.

En estos momentos se están desarrollando tecnologías que alcanzarán su madurez y por tanto su aplicación generalizada en unas décadas. En buena medida son tecnologías potenciadas por las digitales aquí descritas y a su vez ellas permitirán que las digitales se desarrollen aceleradamente. Son tecnologías convergentes que anuncian "una tormenta perfecta". Entre ellas es relevante citar, además de las ya consideradas en este discurso, las siguientes:

- Las tecnologías cuánticas a las que en estos momentos se les atribuye un impacto disruptivo en cuatro áreas de aplicación en el ámbito de la defensa[(85)]:

  - Los sensores cuánticos capaces de medir con extraordinaria precisión y sensibilidad variables físicas (tiempo, gravedad, campo magnético) cuya distorsión permite detectar y localizar blancos para conseguir, por ejemplo, que los océanos sean transparentes.

  - Las comunicaciones cuánticas mucho más seguras por su propiedad intrínseca de detectar sus escuchas indeseadas y ataques.

  - La computación cuántica que incrementará en varios ordenes de magnitud la velocidad de los cálculos, lo que incrementará exponencialmente las capacidades militares. La convergencia entre la computación cuántica y la IA puede ser el desencadenante de esta "revolución tecnológica singular"[(86)], de hecho, en Estados

(85) DARIAS, E. M. et al. *Las tecnologías cuánticas en la cuarta revolución industrial.* Documento de Opinión. Instituto Español de Estudios Estratégicos. Abril 2024.
https://www.ieee.es/publicaciones-new/documentos-de-opinion/2024/DIEEEO34_2024_VVAA_Tecnologias.html

(86) VARIOS AUTORES. Quantum Computing e Inteligencia Artificial: la revolución silenciosa. FUTURE TRENDS FORUM. Fundación Innovación Bankinter. Diciembre 2022.
https://www.fundacionbankinter.org/wp-content/uploads/2023/03/Informe-FTF-Tecnologias-cuanticas-y-IA-marzo23.pdf

Unidos, China, Europa, Japón, Canadá, Corea del Sur o Rusia se están dedicando muchos recursos al desarrollo de ordenadores cuánticos.

•La simulación cuántica que facilitará el desarrollo de nuevos materiales y medicamentos o el modelado de numerosos sistemas naturales y artificiales.

- Biotecnologías sobre las que el Dr. Costa comenta, *...Podríamos hacer clones de cualquier humano o desarrollar personas con cerebros mucho más grandes. Incluso podríamos llegar a revivir a un neandertal. Domesticamos microorganismos que pueden conseguir cosas tan sorprendentes como enriquecer uranio. Sin biotecnología no seríamos la especie que hoy somos, ni mucho menos la que seremos*[(87)].

- Tecnologías para la mejora de las capacidades humanas[(88)], como las anteriores intrínsecamente duales, son tecnologías, como la biomecánica, la neurotecnología, o la integración hombre máquina, entre otras muchas, todavía inmaduras para aplicaciones militares cuyo objetivo es conseguir una superioridad entre combatientes basado en un principio de "superioridad individualizada".

- Materiales y fabricación avanzados con numerosas aplicaciones que van desde nuevos metales y técnicas de producción hasta biología sintética, nanotecnología y diseños de materiales no detectables por los sensores electromagnéticos. Por otro lado, la fabricación aditiva *transformará la logística y las cadenas de*

---

(87) COSTAS, E. *Biotecnología el potencial insospechado para cambiar radicalmente nuestras vidas.* Revista BIT, Nº 228, especial "Disrupción tecnológica", pp.18-22. 2023.
https://bit.coit.es/el-potencial-insospechado-para-cambiar-radicalmente-nuestras-vidas/

(88) LEÓN SERRANO, G. *Tendencias de las tecnologías para el aumento de las capacidades humanas.* Colección ACAMI. Ediciones El Criticón. 2024.
https://www.fundcami.org/producto/tendencias-de-las-tecnologias-para-el-aumento-de-las-capacidades-humanas/

suministro al permitir la producción remota de piezas, componentes y suministros, incluidos repuestos para vehículos, armas, municiones y suministros médicos[(89)].

- Sistemas hipersónicos que aportarán nuevas prestaciones en términos de velocidad, maniobrabilidad y trayectoria, lo que forzará el desarrollo de nuevos sistemas de detección y contramedidas basados en conceptos y arquitecturas no utilizados hasta ahora. En un reciente trabajo se asegura que:

By 2042, conventional hypersonic strike weapons are expected to be widely proliferated throughout the world, with the continual development of new offensive and defensive capabilities providing a rich background for technology improvements in the areas of propulsion, materials, sensors, and autonomous operations of coordinating salvos of weapons. Although hypersonics will have widely proliferated, only the most advanced countries will have the ability to integrate offensive and defense capabilities at scale using the needed underlying capabilities of distributed intelligence, surveillance, reconnaissance, and targeting and distributed command and control driven by autonomous decision aids[(90)].

---

(89) EUROPEAN DEFENCE AGENCY. *Enhancing EU military capabilities beyond 2040. Main findings from the 2023 Long-Term Assessment of the Capability Development Plan. 2023.*
https://eda.europa.eu/docs/default-source/eda-publications/enhancing-eu-military-capabilities-beyond-2040.pdf

(90) VAN WIE, D. M. *Hypersonics: Past, Present, and Potential Future.* Johns Hopkins APL Technical Digest, Volume 35, Number 4. 2021.
https://secwww.jhuapl.edu/techdigest/Content/techdigest/pdf/V35-N04/35-04-Van%20Wie.pdf

- Armas de energía dirigida, actualmente en fase embrionaria pero que en la segunda mitad de este siglo pueden sustituir a buena parte de las actuales armas cinéticas[91].

Podemos seguir incluyendo algunas más, como las nuevas tecnologías espaciales, pero permítanme que desde este estrado me limite a llamar la atención sobre sus consecuencias. ¿somos capaces de imaginar los efectos, gracias a las tecnologías cuánticas, de una capacidad de computación casi infinita desde la perspectiva actual, con una IA camino de alcanzar la Superinteligencia Artificial (SAI, "Artificial Superintelligence"), aquella que supera al ser humano en casi todos los aspectos. Todo ello en un contexto en que sea posible interactuar directamente con el cerebro humano, consecuencia de los avances de la neurotecnología, y se estén desarrollando nuevos seres vivos y máquinas, quizá algunos híbridos y con características para nosotros extraordinarias, fruto de los avances de la biología molecular y la nanotecnología?.

A un mundo digital e inteligente le sucederá un mundo bio-cuántico que nuestros nietos percibirán también como amenaza y oportunidad. Confiemos en que tanto esta transición como la del mundo digital al mundo inteligente, contribuya al progreso y bienestar de la humanidad.

---

(91) VARIOS AUTORES. *Directed Energy Futures 2060.* Office of the U.S. Air Force's Chief Scientist for Directed Energy, Air Force Research Laboratory. 2021.
https://www.afrl.af.mil/Portals/90/Documents/RD/Directed_Energy_Futures_2060_Final29June21_with_clearance_number.pdf

VII. A MODO DE CONCLUSIÓN. HACIA UNA DEFENSA INTELIGENTE

I visualize a time when we will be to robots what dogs are to humans, and I'm rooting for the machine. Claude Shannon, "the father of information theory"

A la sombra de esta antigua y conocida aserción que pone de manifiesto la gravedad e importancia de todo lo que aquí se ha tratado, vuelvo al presente y voy concluyendo esta intervención.

A modo de resumen, permítanme insistir en alguna de las ideas fuerza que incluyen las anteriores páginas:

- El avance imparable de las tecnologías y técnicas destinadas a mejorar la generación, transmisión, almacenamiento y procesamiento de datos está marcando el rumbo de las próximas décadas, con un crecimiento exponencial que parece no tener límites.

La llegada inevitable de la IA está llevando consigo una transformación social sin precedentes, una revolución tecnológica que nos está encaminando hacia una sociedad del conocimiento. En este nuevo paradigma, vemos cómo el razonamiento y la toma de decisiones, antes reservados principalmente a los humanos, están siendo cada vez más asumidos por algoritmos, relegándonos a un papel de supervisión.

El impulso de las economías digitales globales seguirá siendo el principal motor de desarrollo de las tecnologías digitales. Así mis-

mo, estas tecnologías duales están delineando un nuevo escenario donde el campo de batalla digital está evolucionando hacia un campo de batalla inteligente.

A corto plazo, en este nuevo campo de batalla, las tecnologías digitales desempeñarán un papel fundamental, especialmente en áreas como el manejo de datos, la conectividad y la IA, en conjunto con otros avances como las tecnologías hipersónicas o espaciales.

A medida que avanzamos, las tecnologías cuánticas, las biotecnologías y aquellas que amplían las capacidades humanas cobrarán una importancia aún mayor.

Simultáneamente, tecnologías transversales como las nanotecnologías, la impresión 3D, entre otras, seguirán madurando hasta converger en lo que podría describirse como "la tormenta perfecta" que descargará a mediados del presente siglo...

Señores y señoras académicos, amigos y amigas, permitidme finalizar con cuatro afirmaciones, dos deseos y una esperanza…

La innovación es innata al ser humano y ha sido y será fuente de progreso y bienestar. En particular las innovaciones científicas y tecnológicas han transformado las sociedades y, especialmente en los últimos siglos, son uno de los factores de cambio que más han definido su evolución, casi siempre hacia sociedades más prosperas con un incremento constante de la calidad de vida de sus ciudadanos.

Sin seguridad no es posible disfrutar de la prosperidad. Las necesidades de defenderse de posibles amenazas, cuando no la necesidad de mantener posiciones de dominio, han sido siempre uno de los principales motores de innovación. La innovación en el ámbito de la defensa y la seguridad, apoyándose en los desarrollos científicos y tecnológicos del ámbito civil o apoyando estos a los primeros, transforma los escenarios de conflicto en una dirección similar a la que orienta el devenir de la sociedad.

Las tecnologías digitales han transformado las operaciones militares convirtiendo a un intangible, como es la información, en un ele-

mento más del combate, de la misma manera que su evolución introduciendo la inteligencia, convertirá al conocimiento en la mejor munición para asegurar el éxito.

Las tecnologías implicadas son en buena medida las mismas en los ámbitos civiles y militares, ambos comparten amenazas y riesgos. Controlar los efectos de su despliegue y paliar las desigualdades y brechas que origina su aplicación es un reto inaplazable. Y debe hacerse desde todos los campos del conocimiento, porque afecta a todos y cada una de ellos. Es un error pensar que es un problema de los ingenieros o de ciertos ámbitos científicos, las soluciones solo pueden venir de visiones multidisciplinares, atrevidas, basadas en el conocimiento y con un fuerte contenido ético que salvaguarde los firmes valores que nos definen como seres humanos.

Mi primer deseo se dirige a todos ustedes, queridos compañeros académicos. Esta Academia, por su carácter multidisciplinar, por su independencia de los poderes públicos, por la experiencia que acumulan sus miembros y por muchas otras razones que todos compartimos, es el lugar adecuado para reflexionar, para cuestionar aseveraciones, para anticipar soluciones creativas, para orientar a aquellos de cuyas decisiones dependemos. Continuemos el camino emprendido con el excelente discurso de toma de posesión de nuestro académico Dr. Marchena sobre "Inteligencia artificial y Jurisdicción Penal"[92], o las recientes jornadas sobre IA organizadas por varias de nuestras secciones, concedamos a estos temas el esfuerzo y dedicación que merecen.

Mi segundo deseo está destinado a aquellos de los que dependemos, a nuestros dirigentes y líderes. En los próximos años se producirá una brecha digital en la IA entre los países que dispongan de una

---

(92) MARCHENA GÓMEZ, M. *Inteligencia artificial y Jurisdicción Penal.* Discurso pronunciado en el acto de su toma de posesión como Académico de Número de la Real Academia de Doctores de España. 2023. https://www.rade.es/imageslib/doc/MARCHENA%20GOMEZ,%20M_Discursoingreso.pdf

"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, en la futura sociedad del conocimiento.

Y la esperanza final de que todos los implicados en los procesos descritos en este discurso se guíen por el principio de "Primun non nocere", lo primero es no hacer daño, porque parafraseando lo que un buen amigo ha escrito[93], nadie sabe qué nos deparará el futuro, pero sin duda las disrupciones se convertirán en catástrofes si olvidamos este límite.

He dicho.

---

(93) COSTAS, E. *Biotecnología el potencial insospechado para cambiar radicalmente nuestras vidas.* Revista BIT, Nº 228, especial "Disrupción tecnológica", pp.18-22. 2023.
https://bit.coit.es/el-potencial-insospechado-para-cambiar-radicalmente-nuestras-vidas/

EPÍLOGO

Acabas de empezar tu turno de trabajo, has llegado en un coche eléctrico autónomo al que sólo le dices a donde quieres ir y te lleva. Tu misión es vigilar que no ocurre nada anormal, para ello utilizas unos artefactos de realidad virtual extendida muy cómodos que te permiten ver los escenarios como si estuvieses allí y, además, te aporta numerosas ayudas insertadas en ellos que facilitan tu labor, en especial la capacidad de controlarlo casi todo sólo con tus pensamientos. Lo manejas con facilidad porque es la misma tecnología que utilizas en casa cuando te conectas a un aula virtual para seguir las sesiones de gimnasia o disfrutar de tu ingente material audiovisual con tus hijos. Sabes que estás utilizando unos datos seleccionados para ti por unos algoritmos de inteligencia artificial a partir de un número casi infinito de datos recogidos por una enorme red de sensores, muchos de ellos en el espacio o embarcados en vehículos autónomos, conectados con unas redes de telecomunicaciones que han roto las barreras espaciales y temporales de la comunicación humana. Trabajas en un entorno multidominio y con compañeros de otros países cuyos idiomas no entiendes, pero no hay problema porque la red de comunicaciones que utilizas facilita la traducción simultánea en tiempo real. Tu trabajo te gusta, aunque es un poco estresante –como lo indican los datos del sistema que monitoriza tu cerebro- porque serás el responsable de generar una alerta que puede desencadenar el uso de unos sistemas de armas capaces de trabajar a centenares de Km, con una precisión de metros que al-

canzarán sus objetivos en algunos minutos, claro que tu asesor digital te lo pone muy fácil porque es capaz de analizar la situación mucho más eficientemente que tú y te propondrá lo que tienes que hacer, como ocurre en tu entorno privado donde asesores digitales también te aconsejan sobre tus dietas, tus finanzas o tus decisiones cotidianas. Confías en que los sistemas de ciberdefensa lo protejan todo y que se impongan es un combate algorítmico cada día más importante…. Peor lo tienen tus compañeros de los grupos de intervención sobre el terreno que, aunque disponen de numerosos robots inteligentes y sofisticados sensores y armas, al final tienen que ocupar las posIciones y desarrollar las operaciones cerca de la población civil…[(94)]

(94) PEREZ MARTÍNEZ, F. *Presente y futuro de las tecnologías de aplicación militar: duales, inteligentes y disruptivas.* Conferencia de apertura de la Jornada sobre Ciencia y Tecnología en Defensa celebrada el 6 de junio de 2023 en la E.T.S. de Ingenieros Industriales de la UPM.

DISCURSO DE CONTESTACIÓN
DEL EXCMO. SR.
DR. D. JOSÉ RAMÓN CASAR CORREDERA

Sr. Presidente,

Excmos. Señores Académicos y Señoras Académicas de la Real Academia de Doctores de España,

Señoras, señores, amigos:

Recibimos en esta sesión solemne al Dr. D. Félix Pérez Martínez, que contribuirá a partir de hoy a dar aún más autoridad a esta muy prestigiosa Real Academia, con su dedicación, su experiencia y su valioso conocimiento. Sucederá en la medalla número 8 a varios admirados compañeros. Incluso para tus muchas capacidades, igualarles en su desempeño te resultará un reto, que superarás, sin ninguna duda.

Permítanme que exprese que representa para mí un honor haber sido designado para contestar a este discurso de ingreso, y tener así la ocasión de reflexionar sobre el tema elegido por él tan oportunamente. Agradezco la confianza de la Junta de Gobierno, que espero no desmerecer demasiado en esta intervención, para la que he seleccionado algunos párrafos de la contestación escrita completa.

Para empezar, quiero presentar brevemente la trayectoria profesional de mi compañero y amigo. Es tarea muy complicada seleccionar unos cuantos méritos que resaltar hoy, de entre tantos que acumula. Voy a leerles apenas unas líneas:

- Ingeniero de Telecomunicación por la ETSI de Telecomunicación de la Universidad Politécnica de Madrid (UPM), con la calificación de sobresaliente.
- Doctor Ingeniero de Telecomunicación por la UPM en 1982.
- Catedrático desde 1989, lideró en los 80, y dirige actualmente, el Grupo de Microondas y Radar.
- Siempre con dedicación exclusiva a la Universidad y sirviendo a sus intereses, incluso en el periodo en el que, en servicios especiales, se dedicó a ejercer de director del departamento de acreditaciones de la ANECA.
- Director de Departamento de 2001 a 2007 y Director de la Escuela desde 2013 a 2021.
- Miembro de varias comisiones, que no hace al caso mencionar hoy. Quizás sólo recordar sus 12 años como miembro de la Comisión de Investigación y Doctorado de la UPM.
- Es también Diplomado en Altos Estudios Estratégicos por el CESEDEN.

Algunas de sus distinciones o reconocimientos:

- Premio Extraordinario de Doctorado. Curso 1981/82 de la ETSI de Telecomunicación de Madrid.
- Premio a la mejor Tesis Doctoral leída en las Universidades de Madrid. Otorgado por la Fundación Universidad-Empresa. 1983.
- Premio "Año Mundial de las Telecomunicaciones". Otorgado por Standard Eléctrica. 1982.
- Premio "General Fernández Chicarro 1997". Otorgado por el Ministerio de Defensa.
- Socio de Honor de la Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información.
- Premio Honorífico Cátedra UPM-CESEDEN, Ingeniero General D. Antonio Remón y Zarco del Valle. 2019.

- Colegiado de Honor del Colegio Oficial de Ingenieros de Telecomunicación. 2017.
- Académico de Número de la Academia de Ciencias y Artes Militares (ACAMI). 2022.
- Artillero de Honor. Reconocimiento de la Academia de Artillería del Ejército de Tierra. 2019.
- Cruz al Mérito Naval con distintivo blanco. 2008.
- Cruz al Mérito Militar con distintivo blanco. 2019.
- Ingeniero del Año del Colegio Oficial de Ingenieros de Telecomunicación. 2020.
- Ha dirigido más de 100 trabajos de fin de titulación.
- Ha participado en 30 proyectos de investigación competitiva y en más de 100 de cooperación con la industria.
- Autor o coautor de 200 artículos y de 20 libros.
- Miembro del Comité Editorial de las revistas más prestigiosas del área de conocimiento.
- Naturalmente, ha impartido numerosas conferencias invitadas, y participado en múltiples mesas redondas y en otras actividades relevantes de difusión y diseminación.
- Muy involucrado, desde la Universidad, en actividades del ámbito profesional de la Ingeniería de Telecomunicación, tanto en el entorno asociativo como en diversos sectores económicos. Fue Secretario del Colegio Oficial y de la Asociación Española de Ingenieros de Telecomunicación y miembro de los órganos de gobierno del Instituto de Ingeniería de España.
- En la actualidad es Director de las Cátedras Universidad-Empresa de la UPM con INDRA (desde 2006) y con el Ministerio de Defensa-CESEDEN (desde 2020).
- Es también Presidente de la Fundación Círculo de Tecnologías para la Defensa y la Seguridad, cuyo objetivo es promover

y desarrollar una base tecnológica y un sector industrial que soporte a nuestras FFAA y a nuestros Cuerpos de Seguridad del Estado, y en el que participan además de las empresas españolas más relevantes del sector, los ministerios de Defensa, Interior, Economía y Ciencia, además de varias Universidades y el CSIC.

Más allá de los números, los premios y los cargos, al Dr. Pérez Martínez le caben dos méritos incuantificables: haber contribuido decisivamente al desarrollo científico y tecnológico de las Telecomunicaciones en España, a principios de los 80, al desarrollo del sector de la radio en general y del radar en particular; y haber mantenido la presencia pública y profesional de la tecnología y de la universidad en el sector de las Telecomunicaciones, especialmente en el ámbito de la Defensa, pero no sólo.

Ha elegido el Dr. Pérez Martínez para su discurso el tema de la digitalización en los futuros escenarios de conflicto. Hace en él una revisión desde el campo de batalla cinético, al digital y al inteligente y al futuro singular, cuyas características, prudentemente, no se atreve a vaticinar. Diríamos que su tesis principal es que el campo de batalla será más inteligente que digital, que la reconocida superioridad de la información dará paso a la superioridad del razonamiento. Por eso habla también de Inteligencia Artificial. En el camino, ha reflexionado sobre algunos otros aspectos, como la dualidad de las tecnologías, los conflictos híbridos y el papel de determinadas tecnologías habilitadoras como la microelectrónica, las comunicaciones, los sensores, la computación, etc.

Esboza así, en unas líneas, desde lo histórico y lo prospectivo, un marco de evolución hacia lo que denomina Defensa Inteligente.

Yo les voy a distraer sólo unos minutos adicionales para comentar algunas de las ideas expuestas y alguna otra.

Parece que los conflictos actuales son meramente cinéticos y que lo digital es un simple instrumento para que lo cinético sea más eficaz. Pero el campo de batalla digital tiene otras facetas. Me voy a referir al ciberespacio y a la ciberdefensa, a algunas características de la

guerra híbrida y al papel de la Inteligencia Artificial en la Defensa en general; y en particular en el ámbito de la toma de decisiones y el mando y control, prestando finalmente una atención breve a la Inteligencia Artificial generativa.

Quiero empezar, no obstante, por referirme a ese concepto universal y actual de Transformación Digital al que no son ajenas las FFAA, ni en su organización ni en sus operaciones.

Nos recordaba nuestro compañero Gonzalo León, en un número reciente de los Anales de nuestra Academia, que la OTAN había adoptado su primera visión y su estrategia de implementación de transformación digital, que la Unión Europea había consolidado su plan de digitalización, como parte del cuarto pilar de la estrategia de la llama "Brújula Estratégica" (Strategic Compass), y que el Comité Militar de la UE ha venido desarrollando una agenda para la digitalización de la defensa desde hace algún tiempo.

Y también nos recordaba que el compromiso de llevar a cabo esta transformación digital se había reforzado en la cumbre de la OTAN de julio de 2023; prestando atención en su comunicado final a varios aspectos: desde la necesidad de una implicación mayor de la industria de defensa a una mayor preocupación por los asuntos relacionados con la ciberseguridad.

El Dr. Pérez Martínez no habla de eso estricta o exclusivamente, de esa tendencia común a la transformación digital en todas las organizaciones, sino que se refiere al campo de batalla, a las múltiples visiones del campo de batalla, en particular a las digitales.

Pues bien, una versión primordial del campo de batalla digital es el campo de batalla ciberespacial. Nos referimos con tal nombre a ese escenario de operaciones en el que las actuaciones se hacen con y contra las infraestructuras de telecomunicaciones e informáticas (al menos, aunque no sólo); espacio en el que no siempre es fácil distinguir entre cibercrimen, ciberterrorismo y ciberguerra, términos que se definen a sí mismos. Del cibercrimen nos dan

cuenta cotidianamente los medios, el ciberterrorismo usa los mismos instrumentos con fines pretendidamente políticos y la ciberguerra sería el último eslabón del conflicto político con armas informáticas.

Quizás uno de los primeros casos documentados de ciberconflicto sea el de Stuxnet, que comprometió los sistemas de control SCADA de casi mil centrifugadoras iraníes de enriquecimiento de uranio. Un ejemplo este, por cierto, de ataque al mundo físico.

Los casos de agresiones de organizaciones rusas a Estonia, Georgia y Ucrania son bien conocidos también.

Los ataques de denegación de servicio a servidores informáticos de Estonia tuvieron lugar en 2007 y procedían de *botnets* de todo el mundo. El objetivo, probablemente, era desestabilizar a la sociedad estonia.

En 2008, coincidiendo con la invasión de Ossetia, de nuevo unas operaciones de denegación de servicio atacaron a ministerios, bancos y otras infraestructuras y empresas en Georgia. Este es un caso singular, en el sentido de que se produce combinadamente con operaciones militares convencionales, al modo de lo que denominamos guerra híbrida.

En 2015, se produce un ataque a la red eléctrica de Ucrania, inhabilitándose remotamente varios centros de distribución de energía. Se dice que, coincidiendo con la anexión de Crimea, fue, como otras actuaciones, una respuesta a diversas iniciativas de nacionalización de compañías eléctricas por ambas partes.

Como pueden apreciar, los objetivos pueden abarcar desde una mera desestabilización psicológica y social de consecuencias limitadas, al apoyo a operaciones militares convencionales o a la inutilización de infraestructuras físicas civiles, muchas veces en combinación con otras medidas políticas, económicas o de información intoxicada.

Este, el ciberespacio, es el denominado quinto dominio, dentro del entorno de la Información (entendido como el conjunto de individuos, organizaciones y sistemas que recogen, procesan y difunden información). Se diferencia de los otros dominios (tierra,

mar, aire, espacio) en que los medios pueden estar, potencialmente, a disposición de toda la población y extender la zona de combate globalmente, con operaciones y tropas ubicuas y anónimas.

La cuestión que se plantean algunos es si estamos ante una verdadera revolución militar. Los conceptos de revolución militar técnica y la revolución en los asuntos militares (no sólo tecnológicos) tienen su origen en las reflexiones de varios teóricos como Michael Roberts y Geoffrey Parker.

Como nos recuerda Mark Williamson, según Knox y Murray, han sucedido cinco revoluciones militares en los últimos 400 años.

- El desarrollo de los estados nación, después de la paz de Westfalia en 1648, y la constitución de sus ejércitos.

- La revolución francesa y la implicación de la población civil en la defensa.

- La revolución industrial, y el consecuente desarrollo de armas y uso de infraestructuras industriales en el desarrollo de la guerra.

- La guerra de armas combinada, la llamada Blitzkrieg de las guerras mundiales.

- El desarrollo de armas nucleares y la guerra fría.

Estemos o no de acuerdo con esta periodificación en cinco etapas, la pregunta que nos podemos hacer es si hay una sexta, si podemos hablar de una revolución ciber-militar (llamémosla así), que consistiría no sólo en apoyar las operaciones militares tradicionales con medios electrónicos e informáticos sino también en atacar (o defender) los sistemas de información, la economía o las infraestructuras civiles con medios no cinéticos.

Si la hay, si esta revolución existe, es probable que no le sea ajena la revolución tecno-social que la acompaña, en la que las armas son medios informáticos y de comunicación al alcance de toda la población. Es otra variedad del campo de batalla digital. Les podría poner algunos ejemplos de influencia de los ciber-medios sociales, o si lo prefieren, por simplificar, de las redes sociales, con su capacidad

de movilización y de influencia en la opinión de la población: desde la llamada primavera árabe con la caída de los regímenes de Túnez y Egipto a otros muchos acontecimientos, recientes y próximos.

De los muchos aspectos que tiene este nuevo dominio, hay uno sobre el que quisiera hacer una brevísima consideración. Es el de la disuasión. Son bien conocidos los casos, por ejemplo, de la disuasión de la Guerra Fría, de la disuasión espacial o los basados en la posesión de armas de destrucción masiva (por ejemplo, los casos de Irak o Libia y la conocida operación El Dorado).

La disuasión en el ciberespacio es un problema diferente por varios motivos (como nos sugiere Andrew P. Hansen). Uno de ellos es la dificultad de atribución de la autoría, la capacidad de identificar a los atacantes. Otro es que, no siendo el ciberespacio un dominio esencialmente militar, el concepto de desarme como tal es poco factible. Y un tercero, es que no es fácil determinar la efectividad y la proporcionalidad de la respuesta, sea esta de un tipo u otro, a un ataque de este tipo. Sin embargo no hay razón para creer que no se pueda desarrollar una teoría de la disuasión en este dominio.

Algunos califican la mayoría de estas acciones en el ciberespacio de ciberdelincuencia; y por tanto remiten el asunto a uno de cumplimiento de la ley, no de teoría de la guerra. La frontera entre un ámbito y otro es frecuentemente apenas distinguible y el umbral de discriminación es difuso (recuérdese el episodio de CAST LEAD entre Israel y Hamas o el del Grupo XP entre Israel y algunos Países Árabes)

En todo caso, sí podemos convenir en que aparece una nueva arma, como nueva fue la munición de precisión o el *stealth*, que habilita una guerra basada, al menos parcialmente, en la denegación, la explotación o la manipulación de la información. Una guerra de operaciones de información, habilitada por las tecnologías de la información y telecomunicaciones. Lo que me lleva naturalmente al concepto de guerra híbrida, como campo de batalla digital, como una perspectiva crítica del campo de batalla digital.

Según Frank G. Hoffman (citado por Hasan Aktas, en Beyond the Horizon), "la guerra híbrida incorpora una variedad de modos de guerra, que incluyen las capacidades convencionales, tácticas y formaciones irregulares, actos terroristas, incluyendo la violencia indiscriminada y actuaciones criminales".

Según Rasmussen (Secretario General de la OTAN entre 2009 y 2014) "la guerra híbrida es una combinación de acciones militares, operaciones encubiertas y un programa agresivo de desinformación". En buena medida, desde alguna perspectiva al menos, diríamos que es la aproximación tradicional a la guerra de los últimos siglos, pero soportada por tecnologías modernas.

En todo caso, tiene dos características frecuentes: la primera es que se pretende que el país objetivo no descubra fácilmente que está siendo agredido, que no pueda atribuir demostrablemente a un estado u organización los efectos de la agresión. La segunda es que las operaciones se dirigen a una o varias supuestas vulnerabilidades del país agredido; operaciones que pueden adoptar diversas formas, desde la propagación de noticias falsas a la financiación de grupos opositores o la organización de desórdenes urbanos.

De entre todos los aspectos que pueden componer la guerra híbrida, seguramente el de capturar, analizar, explotar y diseminar interesadamente la información y la desinformación es, probablemente, uno de los aspectos decisivos.

El campo de batalla híbrido, más allá de los instrumentos de ciberataque y ciberdefensa (*bots*, gusanos, troyanos, etc.), hace uso de las técnicas de analítica de datos, especialmente de los no estructurados, que representan más del 90% de los datos accesibles. Nos referimos con la denominación de datos no estructurados a aquellos a los que no se les puede dar fácilmente la organización formal de una base de datos tradicional y que incluyen, por ejemplo, el audio, el vídeo, el texto y los datos sociales, y en cuya interpretación reside una "inteligencia" específica para la guerra híbrida defensiva y ofensiva.

No puedo hoy revisar en detalle las técnicas de análisis de este tipo de datos, que incluyen, por ejemplo:

- la minería de textos (correos electrónicos, noticias o mensajes en redes sociales, etc.) para extraer eventos de interés e interpretar tendencias en las conductas de grupos sociales, y el uso de técnicas de análisis de sentimientos u opiniones para inferir preferencias o intenciones.

- la analítica de audio (de voz hablada) y reconocimiento de emociones y de acentos.

- la analítica de vídeo, para extraer, reconocer o identificar personas, grupos u objetos.

- la analítica de atributos estructurales de las redes sociales, que tiene que ver con la intensidad y carácter de las relaciones entre sus miembros.

Para ello, se utilizan técnicas en la frontera de la Inteligencia Artificial: correladores entre eventos, procesado de lenguaje natural, traductores automáticos, rastreadores web, técnicas numéricas y simbólicas de detección, reconocimiento, identificación y seguimiento de objetos, métodos de detección de anomalías o de análisis de conducta, herramientas de ciberanálisis, etc.

Se pueden preguntar qué tiene que ver esto con la guerra. Parecen operaciones de información, de espionaje, de inteligencia. Y lo son. Pero es que eso es la guerra híbrida: la combinación de determinadas operaciones cinéticas o encubiertas con el manejo de las operaciones de información.

Es lo que podríamos denominar el campo de batalla nativo digital. No meramente las tecnologías digitales aplicadas a las armas que una vez fueron convencionales para aumentar su eficacia, como la munición inteligente, la contramedida, el autoguiado de drones o el soldado conectado.

Y esto me lleva a la segunda parte de esta contestación; la que se refiere a la Inteligencia Artificial en Defensa.

No es este el momento apropiado para hacer ninguna consideración profunda sobre la Inteligencia Artificial, ni siquiera sobre la Inteligencia Artificial en Defensa. Consideraciones que, ciertamente, se pueden encontrar en multitud de documentos fácilmente accesibles.

Quizás podríamos quedarnos como definición de referencia para Inteligencia Artificial con una de las muchas propuestas, la de la Agencia Europea de Defensa: "Inteligencia Artificial es la capacidad de los algoritmos de seleccionar opciones óptimas o subóptimas, de entre un amplio espacio de posibilidades, para cumplir los objetivos pretendidos, aplicando diferentes estrategias, incluyendo la adaptación a las condiciones dinámicas del contexto y aprendiendo de la propia experiencia y de los datos suministrados o autogenerados".

Sepan que las posiciones de expertos y usuarios no son exactamente unánimes en cuanto a su papel, y que varían desde las más críticas, que sostienen que, en el corto plazo al menos, la Inteligencia Artificial tendrá un impacto mínimo, por problemas de seguridad de difícil resolución y de desconfianzas institucionales y personales, hasta las más entusiastas que predicen un impacto revolucionario, usada en combinación con otras tecnologías y nuevas doctrinas. Probablemente, la opinión de la mayoría de nosotros se encuentre en algún punto del justo medio, que predice un impacto notable y evolutivo, habilitando mejoras en la efectividad y el potencial de combate de los ejércitos, avanzando los actuales sistemas de armas y haciendo más eficientes los procesos; y también aprovechando la inmensidad de los datos disponibles para mejorar la interpretación de la información y los procesos de toma de decisiones.

En cualquier caso, la aplicación de estas técnicas es una realidad demostrable en algunas áreas de la Defensa, como, por ejemplo, siguiendo a Hoadley, y por mencionar sólo unos ejemplos:

- En la operación de vehículos semiautónomos y autónomos (vehículos aéreos, terrestres y navales), con tecnologías para percibir

el entorno, reconocer obstáculos, fusionar sensores, planificar la navegación, etc., incluyendo la gestión de enjambres de formaciones no tripuladas (*swarms* de drones), etc.

- En la gestión de los sistemas de armas autónomos.

- En las operaciones en el ciberespacio, en las que el uso de la Inteligencia Artificial será inevitable en el corto plazo, por puro volumen de actividad y transacciones.

- En las operaciones de ISR (Información, Vigilancia y Reconocimiento), para procesar conjuntos de datos de inteligencia (inmensos) difícilmente analizables por humanos (ej. vídeos de vehículos no tripulados, por ejemplo) o el reconocimiento y traducción automática multiidioma en entornos ruidosos.

- O en Operaciones de Información, propias de las actuaciones de la Guerra Híbrida.

Pero su papel principal en la transición hacia el campo de batalla inteligente (el papel crítico de la Inteligencia Artificial) estará en su aplicación en el Mando y Control (o en el denominado C4ISR), en los sistemas de Toma de Decisiones.

Entendamos por Mando y Control (C2), en este contexto, el conjunto de procesos y sistemas que habilitan la gestión de las actividades operacionales de una misión.

Y admitamos que los objetivos de cualquier sistema de apoyo al C2, en lo que nos interesa hoy al menos, es i) obtener una imagen, una escena que permita el diagnóstico de la situación y ii) proporcionar al comandante ayudas a la decisión que faciliten sus procesos de decisión y acción.

En cualquiera de los modelos propuestos (por ejemplo, JDL u ODDA), la arquitectura del C2 está formada por una etapa de medida, otra de fusión de datos, posiblemente heterogéneos, otra de interpretación de la situación y otra de valoración de alternativas de actuación. Es decir, se trata de, a partir de los datos capturados por los sensores, sean estos cuales fueren, y quizás de otra información

de inteligencia, interpretar la situación y sugerir posibles "cursos" de acción. También, con frecuencia, de gestionar las comunicaciones. En resumen, es la toma de decisiones basada en la información disponible; y la gestión de las operaciones. Y es precisamente en esos cometidos en los que la Inteligencia Artificial tendrá un papel prominente en el corto y medio plazo. Y ello por su propia naturaleza, por la esencia de la Inteligencia Artificial, que está hecha de métodos, de algoritmos de interpretación, evaluación y decisión.

Podríamos identificar las funcionalidades de la Inteligencia Artificial en los procesos de Toma de Decisiones, en general, como las de:

- Describir la situación. ¿Qué ha pasado o está pasando?

- Diagnosticar. ¿Por qué? ¿Cuáles son las causas de lo que se observa?

- Predecir qué es lo que va a suceder.

- Identificar alternativas y recomendar actuaciones, razonadamente.

- Automatizar decisiones, si es posible y conveniente, en un proceso de toma de decisiones automática o dar soporte cuantitativo para que un humano pueda elegir una opción.

Pues bien, la Inteligencia Artificial puede proveer esas funcionalidades en las cadenas de Mando y Control militar. Les pongo algunos ejemplos (apenas unos pocos de una larga lista):

- Aprendizaje automático para reconocimiento de contexto y entorno, analizando y procesando datos masivos de sensores y datos de inteligencia.

- O gestión de los sensores y las comunicaciones para afinar y refinar la llamada *Common Operational Picture*, que representa, digámoslo así, la escena dinámica actual del campo de batalla.

- O la detección y seguimiento automáticos de objetos de interés militar a partir de secuencias de imágenes tomadas en varias bandas de frecuencia por satélites, aeronaves o drones.

- O el análisis de fuentes de información no convencionales para entender la situación y valorar la amenaza, extrayendo información de inteligencia e interpretando textos o conversaciones o relaciones entre personas u objetos.

- O facilitando la comunicación natural con la máquina y el entorno, mediante realidad aumentada, lenguaje natural, reconocimiento de gestos o representaciones visuales avanzadas, adaptativas, contextuales.

- O el soporte a la toma de decisiones, mediante la evaluación de los efectos de las alternativas de decisión posible, los llamados "cursos" de acción.

Y así un largo etcétera, con técnicas que van desde las de los tradicionales sistemas expertos o las de razonamiento basado en casos hasta las actuales de aprendizaje automático y profundo sobre redes neuronales (sea supervisado, no supervisado o por refuerzo).

Y tengo que mencionar también ahora el concepto de campo de batalla digital, global, compartido, que hace referencia a las capacidades de comunicar en red para mejorar la calidad y relevancia de la información disponible y una evaluación de la situación más precisa, menos ambigua, más fiable.

De hecho, los objetivos formales que guían los principios de diseño de la OTAN para los sistemas C4ISR son:

- apoyar la consecución de la superioridad de la información en un entorno de información compartida en red.

- apoyar el uso efectivo y eficiente de los recursos de información en el desarrollo de las misiones de OTAN.

Es la tendencia hacia soluciones federadas, cooperativas, que tanto se está impulsando, críticamente dependientes del grado de interoperabilidad entre sistemas en todos los niveles.

Y en el marco del Mando y Control, federado o no, no puedo dejar de mencionar la importancia trascendente de las técnicas de simulación en los procesos de toma de decisiones para Mando y Control y cómo

la Inteligencia Artificial puede soportarlos. Apenas unos párrafos para mencionar tres metodologías, tres tecnologías, que he elegido de entre varias, de entre muchas posibles: la simulación orientada a *Wargaming*, los llamados Gemelos Digitales y los Agentes. *Wargaming* (juegos de guerra) es un paradigma con el que se simula un escenario de batalla en el que dos o más actores compiten por una ganancia, usando sus propias estrategias, sus propias doctrinas y su propia gestión de recursos. Como tal, es un instrumento de simulación insustituible para la formación, el entrenamiento y la valoración de actuaciones y tácticas (y estrategias), en cuanto que permite contrastar opciones frente a las posiciones de un posible competidor o enemigo inteligente. Un Gemelo Digital es una réplica software de un sistema físico, que actúa en paralelo con las mismas señales y la misma escala de tiempos que el sistema real y que, por tanto, permite valorar, sin interferir con el sistema real, qué sucede, predecir las consecuencias y anticipar el resultado de las acciones. Un Agente es un módulo software que representa la estructura y características, en términos de comportamiento e intención, de las unidades individuales de un sistema, para componer agregadamente un escenario global frente al que simular operaciones. Estos tres conceptos y otros varios pueden ser la base del soporte a la Toma de Decisiones por Simulación, un instrumento clave en el desarrollo de operaciones del actual y futuro campo de batalla inteligente, incluido el ámbito de la guerra híbrida.

En este hilo, hay al menos otro tema de interés (en el ámbito de la Defensa, pero no sólo en él); me refería a él en un reciente Editorial de los Anales de nuestra Academia (Editorial del número 3 del volumen 8 de 2023), en el ámbito médico. Es el de la explicabilidad y también el de responsabilidad, que se describen por su propia denominación. Escribía entonces y repito ahora casi literalmente, adaptándolo al dominio de la Defensa: "si un programa basado en inteligencia artificial diagnostica una situación, debería ser capaz de explicar o al menos visualizar las evidencias en las que se ha basado, lo que no siempre es posible con los modelos actuales de aprendizaje profundo de Inteligencia Artificial. Del mismo modo,

si sugiere una acción, debería poder justificarlo o quizás suministrar algunos datos de probabilidad de acierto (histórica). Y si la acción se toma pero no tiene éxito, se añade un tema, nada menor, de atribución de responsabilidad, como es sabido".

Y ya para ir terminando, tengo que aludir, inevitablemente, a la Inteligencia Artificial Generativa; al menos, por lo que nos concierne hoy, a sus aplicaciones para aumento de datos, producción de escenarios y comunicaciones con el operador. Usaré, casi literalmente, algunos párrafos del artículo Editorial de los Anales al que me refería antes.

Ya saben que nos referimos con el término de Inteligencia Artificial Generativa "a ese tipo de inteligencia artificial capaz de generar contenidos, emulando lo que produciría un creador humano, y que ha supuesto una revolución viral a finales de 2022 y, sobre todo, durante 2023."

"Para ello, esencialmente, las aplicaciones aprenden las características propias de los contenidos para las que han sido concebidas, a partir de una colección considerable de ejemplos reales, preferentemente de manera no supervisada, y terminan por ser capaces de producir nuevos contenidos con esas propiedades, con las instrucciones de generación que les pueda dar un usuario humano (instrucciones típicamente construidas en lenguaje natural o *prompts*). La reciente irrupción popular de ChatGPT o Bard han supuesto una revolución en la generación automática de contenidos."

"Las posibilidades que ofrecen estas aplicaciones para acelerar la producción de contenidos valiosos son potencialmente inmensas, bajo la tutela y valoración de un humano experimentado (o sin ellas). Y las capacidades reales de la Inteligencia Artificial Generativa trascienden a los objetivos de generar texto informativo, educativo o conversacional o imágenes artísticas o publicitarias. Pueden producir también música o código de software o fórmulas de medicamentos o argumentos legales o estrategias industriales."

“Esa capacidad de producir ejemplares es intrínseca al concepto de Inteligencia Artificial Generativa. Queda por asegurar que los que se generan son los ejemplares adecuados y no se propagan los sesgos, si los hubiera, de los modos de generación.”

Pues bien, esa Inteligencia Artificial Generativa aplicada a la toma de decisiones y al campo de batalla digital se podrá concretar, al menos, en herramientas de aumento de datos, de generación de escenarios y de gestión de las comunicaciones, como les decía.

El término “aumento de datos” se refiere a la producción de datos sintéticos con características equivalentes, indistinguibles de los datos reales disponibles y por tanto aptos para el entrenamiento, la valoración de la eficacia de estrategias y tácticas y el aprendizaje automático de técnicas específicas de Inteligencia Artificial. Y la “generación de escenarios” se refiere, en este contexto, a la producción de entornos sintéticos, de posibles iniciativas o reacciones del adversario a nuestras decisiones, con sus resultados y sus explicaciones, más allá de lo que es actualmente posible con aproximaciones de simulación clásica de Montecarlo y bases de datos de escenarios prediseñados.

Estas capacidades proporcionadas por la Inteligencia Artificial Generativa son especialmente valiosas en aquellos dominios en los que la disponibilidad de datos no es grande o no es variada o no es representativa de determinados casos relevantes, porque permite extender los espacios de simulación y el número de escenas disponibles para analizar y aprender.

Finalmente, la Inteligencia Artificial Generativa basada en los llamados modelos de lenguaje de gran tamaño será también de utilidad crítica en la gestión de la comunicación entre humanos y máquinas, entre máquinas y entre humanos (como hace la aplicación de Meta, SeamlessM4T, capaz de trabajar con cien lenguajes distintos y de traducir de texto a voz o a la inversa y de voz a voz o de texto a texto).

Pues bien, estos conceptos, junto con otras tecnologías habilitadoras y disruptivas, como la computación cooperativa o distribuida en la nube y en el borde, la realidad extendida, la neurotecnología o las tecnologías cuánticas nos irán llevando a nuevos modos de entender y conducir el conflicto (ese estúpido empeño recurrente que nos acompaña desde los orígenes de la Humanidad).

Nuestro nuevo Académico nos ha hablado de un futuro campo de batalla singular. Que esperamos que sea tan singular que no sea de batalla, que no sea tanto de atrición como de argumentación, ni tanto de enfrentamiento como de negociación. De momento, dada la historia documentada, debemos entender vigente el principio de disuasión "*si vis pacem para bellum"*; también "*si vis pacem para verbum"*, como nos sugería recientemente un ilustre compañero. Pero también, "*si vis pacem"* prepara el progreso, las tecnologías y las ideas.

Querido Félix, gracias por elegir este tema para tu discurso de ingreso y por haberlo desarrollado con tanto acierto. Esta Real Academia de Doctores de España te da la bienvenida y te confirma, en este acto, que sabe, con certeza, que tus reflexiones y trabajos contribuirán a mejorarla; a ella misma y a la sociedad a la que nos debemos.

He dicho.