# Tecnologías de alto impacto para la defensa en el entorno operativo 2035

MINISTERIO DE DEFENSA

# Tecnologías de alto impacto para la defensa en el entorno operativo 2035

MINISTERIO DE DEFENSA

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

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

Diseño de cubierta: Irene Paloma Medina Jurado

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Paseo de la Castellana 109, 28046 Madrid



NIPO 083-23-251-8 (impresión bajo demanda)
ISBN 978-84-9091-833-3 (impresión bajo demanda)

NIPO 083-23-252-3 (edición en línea)

Depósito legal M 33186-2023
Fecha de edición: febrero de 2024
Maqueta e imprime: Imprenta Ministerio de Defensa



publicaciones.defensa.gob.es
cpage.mpr.gob.es

# ÍNDICE


Página

**Introducción** ..... 9
*Luis Alberto Hernández García*

1. Objeto ..... 9
2. Introducción ..... 9
3. Tecnologías innovadoras, emergentes y disruptivas ..... 12
4. Estructura ..... 14
5. Agradecimientos ..... 20

**Capítulo 1**

**Estado actual de las comunicaciones militares por satélite: GEO *vs.* LEO** ..... 21
*Jaime Luis Sánchez Mayorga*

1. Introducción ..... 23
2. La capacidad SATCOM para Defensa: renovación en marcha ..... 27
3. La descripción de la necesidad: MILSATCOM, GOVSATCOM y COMSATCOM ..... 28
4. Estado de la cuestión SATCOM para los NGEO ..... 28
   - 4.1. Comparación entre GEO y NGEO (LEO/MEO) SATCOM ..... 29
   - 4.2. España: demanda de renovación desde el EMAD ..... 31
   - 4.3. Europa ..... 31
     - 4.3.1. La Evolución del Programa Espacial de la Unión Europea: componente GOVSATCOM ..... 31
     - 4.3.2. EDA: *pooling and sharing* ..... 35
   - 4.4. OTAN ..... 36
5. Capacidades para Defensa *vs.* mercado SATCOM ..... 38
   - 5.1. Comunicaciones seguras: evaluación del grado de incertidumbre ..... 38

Página

5.2. Vectores de MILSATCOM actuales ..... 39
5.3. Parámetros de mercado en SATCOM-LEO ..... 40
5.4. Resiliencia y protección en el entorno de amenazas actuales ..... 41
6. ¿Complementariedad o sustitución? El debate sobre el futuro de las comunicaciones por satélite ..... 43
7. Conclusiones del estudio ..... 44
8. Reflexiones para la hoja de ruta ..... 44
9. Bibliografía ..... 45

**Capítulo 2**

**Realidad y futuro de las redes móviles de nueva generación en el ámbito militar** ..... 49
*Montserrat Valdés Quintana*

1. Introducción ..... 51
2. Una vista al pasado y evolución de las comunicaciones móviles en el ámbito militar ..... 52
3. 5G, ¿en qué consiste y qué nos ofrece? ..... 53
4. Evolución futura del 5G ..... 60
5. Desarrollo nacional e internacional del 5G en el ámbito militar ..... 63
6. Conclusiones ..... 70
7. Bibliografía ..... 71

**Capítulo 3**

**Consideraciones sobre el potencial uso de *apps* en Defensa** ..... 73
*Ángel Gómez de Ágreda*

1. Introducción ..... 75
2. Ciclos de adquisición digital ..... 76
3. «Componentización» de aplicaciones *software* ..... 78
4. Definición de las características ..... 80
5. Creación de la *app* ..... 82
6. Propuesta de taxonomía ..... 83
7. Interacción hombre-máquina ..... 88
8. Sinergias e interoperabilidad ..... 88
9. Integración para mejorar la consciencia situacional ..... 91
10. Conclusiones ..... 92
11. Bibliografía ..... 94

## Capítulo 4

**Otras tecnologías y sistemas de alto impacto para las operaciones en el EO2035** ..... 97
*Enrique Martín Romero*

1. Introducción ..... 99
2. Técnicas novedosas de inteligencia artificial ..... 101
   2.1. *Deep Reinforcement Learning (Deep* RL) ..... 103
   2.2. AI Generativa (GenAI) ..... 104
   2.3. Causal AI ..... 109
3. Sistemas autónomos ..... 111
4. Técnicas para el incremento de las capacidades cognitivas ..... 114
5. Blockchain ..... 118
6. Hiperautomatización ..... 119
7. Sumario, conclusiones y reflexión final ..... 122
8. Bibliografía ..... 124

**Composición del grupo de trabajo** ..... 127

# Introducción

*Luis Alberto Hernández García*

## 1. Objeto

El presente documento se enmarca en el Plan Anual de Investigación (PAI) del Centro Conjunto de Desarrollo de Conceptos (CCDC)[1] para el año 2023. Tiene por objeto poner de manifiesto el potencial impacto para las cuestiones de defensa que poseen determinadas tecnologías. Dada la amplia gama de opciones tecnológicas en este tiempo de desarrollo acelerado, se han seleccionado un número limitado, sin que esta circunstancia descarte otras disponibles, teniendo en cuenta sus posibilidades de desarrollo y aplicación, así como su capacidad de influencia en el entorno operativo presente y futuro, con un horizonte temporal situado en 2035.

## 2. Introducción

El exponencial avance tecnológico constituye uno de los principales motores de cambio en todas las disciplinas del conocimiento, sectores de actividad y organizaciones, sin que la Seguridad y la Defensa puedan considerarse una excepción. De hecho, aunque la naturaleza del conflicto —que es política, social, violenta e impredecible— persista, cuando se analiza la evolución de su carácter, el impulso tecnológico es uno de los elementos invariables que contribuyen a marcar la diferencia con el anterior. Si esta dinámica es cierta a lo largo de la Historia, lo es mucho más hoy en día, cuando el ritmo de incorporación al conflicto de las diferentes tecnologías se acelera y la superioridad tecnológica puede ser decisiva en su resolución.

Es paradigmático, en este sentido, el conflicto en Ucrania de 2022-2023, el cual ha devuelto a escena un tipo de guerra en cierta medida clásica, en

[1] Perteneciente a la División de Desarrollo de la Fuerza (DIVDEF) del Estado Mayor Conjunto (EMACON).

la que dos actores estatales se disputan un territorio, enfrentándose en un combate de alta intensidad, en el que emplean medios, reeditan tácticas y procedimientos, muchas veces propios del pasado siglo. Sin embargo, se da al mismo tiempo una circunstancia que denota novedad, pues lo adaptan al tiempo actual, dando protagonismo a la tecnología, lo que, definitivamente, influye sobre su carácter.

En efecto, multitud de observaciones iniciales contenidas en los más variados análisis e informes estratégicos y operacionales militares dejan constancia del empleo de los drones en misiones diversas, desde la Inteligencia, al ataque; de la importancia de las redes terrestres y satelitales de comunicaciones y vigilancia; de la sensorización extrema del campo de batalla; del afán por el dominio del espectro electromagnético; de la profusión de los ciberataques, en paralelo o integrados con las operaciones físicas; de la potencialidad de la híper-velocidad aplicada a municiones; del uso de la Inteligencia Artificial (IA); de la importancia concedida a la influencia cognitiva para dominar el entorno informativo; del desarrollo de las aplicaciones móviles (*apps)* adaptadas al combate, etc.

En este conflicto, además, la tecnología ha sido un elemento ciertamente decisivo no solo como factor ofensivo, sino también en el plano defensivo, para fortalecer, por ejemplo, la resiliencia social, la cual soporta en gran medida la capacidad de combate ucraniana frente a un enemigo *a priori* superior en capacidades militares. El aseguramiento de la conectividad, así como las comunicaciones a través del empleo de redes satelitales, el refuerzo de internet y la telefonía, o el extendido uso de redes sociales y *apps,* han sido determinantes en este sentido. Todas ellas han abierto grandes posibilidades a la conexión internacional, a la propia seguridad, bienestar y supervivencia del ciudadano, así como a su colaboración en tiempo real en labores de Inteligencia o defensa de la nación, hasta hace poco reservadas a las fuerzas combatientes. En este último caso, es destacable, por ejemplo, el papel de la *IT Army of Ukraine*, organización aparecida al principio del conflicto, mediante la que voluntarios de la comunidad cíber ucraniana defienden su ciberespacio frente a la agresión rusa.

La tecnología juega un papel preponderante en el conflicto. Su incorporación al campo de batalla potencia las capacidades militares existentes e impulsa el desarrollo de otras nuevas. Su expansión en todos los órdenes de la vida, extendido potencial para el doble uso y accesibilidad, la sitúan al alcance de cualquier actor, estatal o no, que pretenda utilizarla, sea con fines defensivos u ofensivos. Además, las sociedades avanzadas confían cada vez más en la tecnología para el funcionamiento de sus sistemas, procesos, infraestructuras y servicios críticos, lo que, en caso de conflicto, abre nuevas vulnerabilidades. Todo esto propicia que, en el marco de una extrema competición internacional, la tecnología alcance una alta cuota de

protagonismo, también en el ya *cuasi* permanente enfrentamiento entre potencias y sus *proxies* por debajo del umbral del conflicto armado que se desarrolla en la zona gris[2].

El uso de medios de Inteligencia, Vigilancia y Reconocimiento (ISR-*Intelligence, Surveillance and Reconnaissance*) para potenciar la recopilación de información sobre adversarios y competidores; la carrera por la posesión de capacidades espaciales para uso civil y militar; o la recurrencia a ciberataques contra intereses empresariales y nacionales son una constante en el juego internacional, sin que este empleo se produzca necesariamente en el combate abierto.

A esta pugna en la zona gris sirven también en lugar destacado tecnologías como el *big data,* la inteligencia artificial o las tecnologías de la información y las comunicaciones, incluyendo internet y las redes sociales, empleadas, entre otras, para la desinformación, propaganda e influencia, propiciando efectos exponenciales, gracias a su capacidad de multiplicar alcances, velocidades y volúmenes de datos e información. En este sentido, no hay que olvidar que las narrativas son el principal elemento de cohesión para orquestar los esfuerzos de los diferentes instrumentos de poder del adversario, empleados para dar forma a lo que se conocen como estrategias o amenazas híbridas, elemento intrínseco al enfrentamiento en la zona gris.

Junto a las anteriores, los avances en otras tecnologías como son la biotecnología y la mejora de capacidades humanas (BHET-Bio and Human Enhancement Technologies o Biotechnologies), la computación cuántica, el *Blockchain*, los desarrollos de nuevos materiales, las armas de energía dirigida (DEW-*Directed Energy Weapons*), el electromagnetismo, las nuevas fuentes de energía y propulsión… se incluyen cada vez más frecuentemente en investigaciones, análisis y planes de desarrollo de capacidades relacionados con la Seguridad y Defensa a nivel global.

De esta manera se puede afirmar que, hoy en día, las nuevas tecnologías se encuentran ineludiblemente presentes en todo el espectro del conflicto, desde el enfrentamiento en la zona gris, por debajo del umbral de guerra, al combate armado de alta intensidad, sin olvidar otros tipos de conflictos que mantienen su vigencia, como los relacionados con la gestión de crisis o la lucha contra el terrorismo.

El espacio, el ciberespacio y el ámbito de operación cognitivo ocupan un lugar distinguido en este escenario. En efecto, estos tres espacios de operación, que pueden considerarse desde un punto de vista temporal como

[2] Según se recoge en la PDC-01(A) de JEMAD, «la zona del espectro de los conflictos donde predominan las actuaciones situadas al margen del principio de buena fe entre estados *(bona fide*) que pese a alterar notablemente la paz no cruzan los umbrales que permitirían o exigirían una respuesta armada».

las tres últimas extensiones del campo de batalla, son, a su vez, los que incorporan una mayor presencia tecnológica avanzada. No obstante, también se da en los tres ámbitos de operación físicos tradicionales: terrestre, marítimo y aéreo, pues de igual modo se incorpora a las capacidades en ellos empleadas.

Continuando con la referencia al conflicto en Ucrania, el profuso uso de drones aéreos o navales ha supuesto, por ejemplo, un punto de inflexión en la manera en que se empleaban medios y tácticas, tanto terrestres como navales o aéreas, hasta el momento de su aparición. Carros de combate y buques han de contar en su maniobra con la amenaza de esta ágil, sorpresiva y letal amenaza que, a su vez, acapara algunas de las misiones antes reservadas a aeronaves pilotadas.

Por su parte, la complejidad del campo de batalla y el extendido uso de la tecnología por todas las partes contendientes requiere una mayor integración de apoyos, sensores y efectores. La rápida y progresiva sensorización del campo de batalla demanda e impulsa a la vez la creación de un verdadero «Internet de las cosas militares» (IoMT–*Internet of Military Things* o IoBT–*Internet of Battlefield Things*), para asegurar la consciencia situacional (*SA–Situational Awareness*), la Inteligencia y el *Targeting* en un entorno con un alto componente híbrido, muy marcado por la ambigüedad de actores, medios, actuaciones, objetivos e intenciones, en el que, además, la toma de decisiones ha de acelerarse.

El IoMT o IoBT no es sino una adaptación del internet de uso civil, configurado para servir a las operaciones militares, en el que confluyen la gran mayoría de las tecnologías tratadas en los diferentes capítulos del presente documento. Aunque su principal funcionalidad reside en su capacidad para conectar todos los ámbitos de operación, impulsando el multidominio[3], se encuentra muy presente sobre todo en el ámbito terrestre, en especial en áreas urbanas, en las que se concentra gran parte de la población y capacidades, al tiempo que permiten, normalmente, una mayor conectividad.

## 3. Tecnologías innovadoras, emergentes y disruptivas

A estas alturas, ya se puede observar que la apuesta por la tecnología introduce un alto nivel de innovación en los asuntos de Defensa, a una velocidad y en una gama de aplicaciones nunca vista, optando así a un puesto

[3] La doctrina militar conjunta nacional define las operaciones multidominio (MDO-*Multi-Domain Operations*) como: «Aquellas operaciones realizadas por la Fuerza Conjunta que, por su agilidad y complejidad, necesitan de una adecuada interoperabilidad y conectividad que posibiliten un control distribuido de los medios para permitir la integración de todas sus capacidades y así poder producir efectos en y desde cualquiera de los ámbitos de operación».

destacado en la estrategia militar que, para adaptarse a la nueva situación, habrá de ganar en agilidad con respecto a tiempos pasados. Junto a lo anterior, la incorporación de la tecnología a las capacidades de defensa requerirá también de un importante esfuerzo para la cohesión continua y flexible de la organización militar, de sus estructuras, de su personal y, en general, de su cultura organizativa.

De hecho, el documento del EMAD «Entorno Operativo 2035. Primera revisión», de 2022, tras evaluar a lo largo de sus páginas las tendencias, los retos, los contextos de empleo, los desafíos y las oportunidades que se abren en los próximos años, concluye que una de las principales áreas de potenciales cambios que se avecinan en las FAS tiene que ver con la apuesta por la superioridad tecnológica ante el adversario, que garantice la hegemonía en el enfrentamiento. En este sentido, será, junto al personal, uno de los pilares sobre los que se asientan la transformación digital y la interoperabilidad plena desde el prisma del multidominio.

En el marco aliado, el término genérico más extendido para referirse con propiedad a lo que se entiende por «nuevas tecnologías», es el de tecnologías emergentes y disruptivas (EDT–*Emerging and Disruptive Technologies*). Las EDT incluyen en general a todas aquellas tecnologías o descubrimientos científicos que se encuentran en un estado de desarrollo embrionario y cuya aplicación no es aún una realidad (emergentes); así como a las que suponen o van a suponer un cambio rompedor con lo existente, una vez aplicadas en cuestiones, en este caso, de seguridad y defensa (disruptivas). A estas se añaden, por defecto, otras tantas, catalogables como «innovadoras» pues, a pesar de suponer avance o novedad, no se pueden incluir técnicamente en ninguna de las dos categorías descritas.

La mayoría de ellas poseen la característica de que han sido desarrolladas con base en necesidades propias del ámbito civil, bien sea por el impulso de los mercados, de empresas en busca de una mayor productividad o ventaja competitiva, o de regulaciones nacionales e internacionales. Algunas, como las relacionadas con los satélites, han recibido también un cierto impulso de la parte militar, pero lo que en general se puede afirmar es que prácticamente ninguna de ellas, a pesar de su innegable doble uso en la mayoría de las ocasiones, ha surgido y se ha desarrollado motivada por una necesidad estrictamente militar, como ocurría hace solo unas décadas, cuando las guerras eran el principal motor del desarrollo tecnológico, que transferían *a posteriori* al ámbito civil.

Otra peculiaridad de las EDT en el ámbito de la Seguridad y Defensa reside en su marcado carácter sinérgico, pues no es raro ver cómo de la aplicación de dos o más tecnologías de forma convergente pueden obtenerse planteamientos, resultados o efectos sorpresivos y ciertamente disruptivos

en relación con conflictos anteriores. Uno de los casos más patentes es, por ejemplo, el empleo de drones, en cuanto a la incorporación de robótica o sistemas de visión avanzada, con alto nivel de autonomía, impulsada además por técnicas de inteligencia artificial.

Las EDT presentan dos desafíos de gran calado en lo que se refiere al desarrollo de capacidades militares:

– Por un lado, no todas las EDT han de derivar necesariamente en el desarrollo de sistemas, equipos y medios técnicos novedosos. También ha de contemplarse su aplicación a capacidades existentes tipo *legacy*[4], sobre todo en lo referente a las grandes plataformas, que poseen ciclos de vida extensibles a lo largo de varias décadas, para poder mejorar progresivamente sus prestaciones, de acuerdo con el avance tecnológico de cada momento.

– El personal es un aspecto fundamental en la incorporación de las EDT a las capacidades militares y a la Seguridad y Defensa en general, pues la implantación tecnológica ha de ir acompasada con las regulaciones, conceptos y doctrinas de empleo, así como con el conocimiento tecnológico y grado de aceptación por parte de las personas, todo ello, para no crear un efecto de inoperancia. La concienciación y la formación, a todos los niveles, así como la gestión del talento propio y ajeno, han de ser esfuerzos principales de la organización y sus líderes en este proceso, que debe contemplar también la adaptación de estructuras y regulaciones.

## 4. Estructura

En este contexto, el grupo de trabajo que ha desarrollado el presente documento de investigación ha optado por seleccionar algunas de las EDT más relevantes, tomando como principales criterios el impacto que su uso puede tener en las operaciones militares, así como su accesibilidad, posibilidades de desarrollo y proyección de futuro en el entorno operativo que se avecina.

A lo largo de cuatro capítulos, los autores desgranan el «estado del arte», así como su visión sobre cada una de ellas, resaltando los aspectos que consideran más relevantes en la forma en la que afectan y afectarán a las diferentes actividades y operaciones militares, en particular, así como de Seguridad y Defensa, en general.

[4] Un ejemplo paradigmático, que además incorpora la «componentización» ***software,*** tratada en el capítulo 3 de este PAI, es la modernización de la aviónica del U2 que, junto con otras mejoras, ha facilitado la extensión de su ciclo de vida más allá de los setenta años.

En el capítulo primero, bajo el título «Estado actual de las comunicaciones militares por satélite: GEO *vs*. LEO», el coronel del Ejército del Aire y del Espacio Jaime Sánchez Mayorga aborda el importante dilema que afecta al futuro de las comunicaciones satélite militares, en un entorno de desarrollo global de las capacidades espaciales, cada vez más relevantes en la competición internacional.

El coronel plantea la disyuntiva que se presenta, de cara al empleo militar de los satélites, entre utilizar capacidades específicas de Defensa o recurrir a soluciones de mercado, en un sector en el que crece la colaboración público-privada y evolucionan los modelos de obtención y provisión de capacidades espaciales.

Para ello, el autor aborda las principales ventajas y desventajas que diferencian los satélites de órbita geoestacionaria (GEO) y no geoestacionaria (NGEO). Los primeros, más estables en sus prestaciones, parecen más aptos para las operaciones militares. Los NGEO, menos costosos son, sin embargo, más vulnerables a interferencias o ciberataques, lo cual, en cierta medida, los cuestiona, en materia de seguridad, para aplicaciones militares.

Expone, además, las iniciativas en marcha en la UE y en la OTAN, así como sus diferentes aproximaciones a la posesión y utilización de satélites de ambos tipos, si bien, apunta, coinciden en su preocupación por la seguridad. Finaliza su artículo el coronel Sánchez Mayorga planteando el futuro de las comunicaciones satelitales en una doble vertiente de desarrollo: satélites NGEO, como complemento a los GEO, o reemplazo de estos últimos por los primeros, eso sí, fortaleciendo sus actuales puntos débiles, debido al impulso que reciben desde el sector privado y a su creciente demanda.

El segundo capítulo tiene que ver con la conectividad, el auténtico «pegamento» de todo el entramado tecnológico, también cuando se trata de su aplicación a las operaciones militares. La Personal Civil Funcionaria (PCF) del Ministerio de Defensa, Monserrat Valdés Quintana lo desarrolla bajo el título «Realidad y futuro de las redes móviles de nueva generación en el ámbito militar».

La autora resalta la importancia de las nuevas generaciones de tecnologías de las telecomunicaciones, como es el caso de las de quinta generación (5G) y posteriores (6G, 7G), que ofrecen velocidades de transmisión, niveles de eficiencia y aplicaciones crecientes, al tiempo que contribuyen decisivamente a la transformación del modo en que las fuerzas militares operan y se comunican.

Tras un repaso por cuestiones técnicas relativas a la tecnología 5G, Valdés plantea diversas posibilidades de aplicación que poseen, a su juicio, un alto potencial para mejorar las capacidades militares en casos de uso como son

las comunicaciones, los vehículos no tripulados, la realidad virtual y aumentada, las redes de sensores, la ciberseguridad, la telemetría y el control de misiones, la telemedicina, etc.

La autora continúa explorando las posibilidades de empleo de esta tecnología, mirando al futuro, a las redes 6G y 7G, esta última en fase meramente conceptual, para finalizar con una detallada exposición de los diferentes proyectos y desarrollos en la materia, tanto a nivel nacional como internacional.

El tercer capítulo, más que a una tecnología, se refiere a un concepto que aprovecha las sinergias de varias EDT. Con el artículo «Consideraciones sobre el potencial uso de *apps* en Defensa», el coronel del Ejército del Aire y del Espacio Ángel Gómez de Ágreda se adentra en una temática ciertamente novedosa: el desarrollo y empleo de *apps* para fines militares como las que a diario manejamos en nuestros dispositivos inteligentes tipo *smartphone* o *tablet*. Se trata este de un fenómeno que, como se apuntó antes, se ha observado con cierta frecuencia en Ucrania, aunque aún queda mucho por investigar, desarrollar y, sobre todo, afirma el autor, conceptualizar sobre el asunto, pues tener clara la idea de por qué, para qué y cómo afrontar la incorporación de las *apps* es el primer y más importante de los pasos a emprender.

El coronel Gómez de Ágreda plantea la incorporación del uso de *apps* en el ámbito militar como un esfuerzo de cambio organizativo y cultural, más que individual, pues reconoce la familiarización de gran parte del personal militar con este tipo de tecnología, cuya aplicación al ámbito de la Defensa no es en esencia diferente del ámbito civil. Eso sí, con las precauciones y salvaguardas aplicables al entorno militar.

Considera el autor que la modularidad o diseño basado en componentes («componentización») es una característica básica para el desarrollo *software* que requieren las *apps*, el cual comienza con un claro entendimiento del desafío o problema a solventar, así como con la elección correcta de las características y posibilidades en cuanto a diseño y empleo. Frente a los sistemas monolíticos, la modularidad tiene un impacto significativo en las operaciones en cuanto al dinamismo y evolución continua de la capacidad individual de cada componente. La superioridad tecnológica, afirma, requiere de *apps* avanzadas, de rápido despliegue y de un diseño por componentes.

Tras proponer una taxonomía de posibles utilidades de las *apps,* según las diferentes áreas funcionales de un Estado Mayor, el coronel resalta la importancia de tener en cuenta las interacciones hombre-máquina y su potencial para ocasionar efectos no deseados, que habrá que prever, según advierte. A esto añade la necesaria interoperabilidad y capacidad

de adaptación a la situación de cualquier *app* y, para concluir, propone la inclusión de los condicionantes de seguridad desde la fase de diseño, adoptando el proceso *Development-Security-Operations* (Dev-Sec-Ops*)*, a fin de dotar al producto final de la adecuada resiliencia.

Finaliza este trabajo de investigación con el capítulo cuatro, en el que Enrique Martín Romero, ingeniero aeronáutico, bajo el título «Otras tecnologías y sistemas de alto impacto para las operaciones en el Entorno Operativo (EO) 2035» se adentra en la exploración, a modo de miscelánea, de diversas EDT adicionales a las anteriores que, si bien están siendo maduradas inicialmente en el mercado civil, son de alta aplicabilidad para el desarrollo de nuevas capacidades de Defensa.

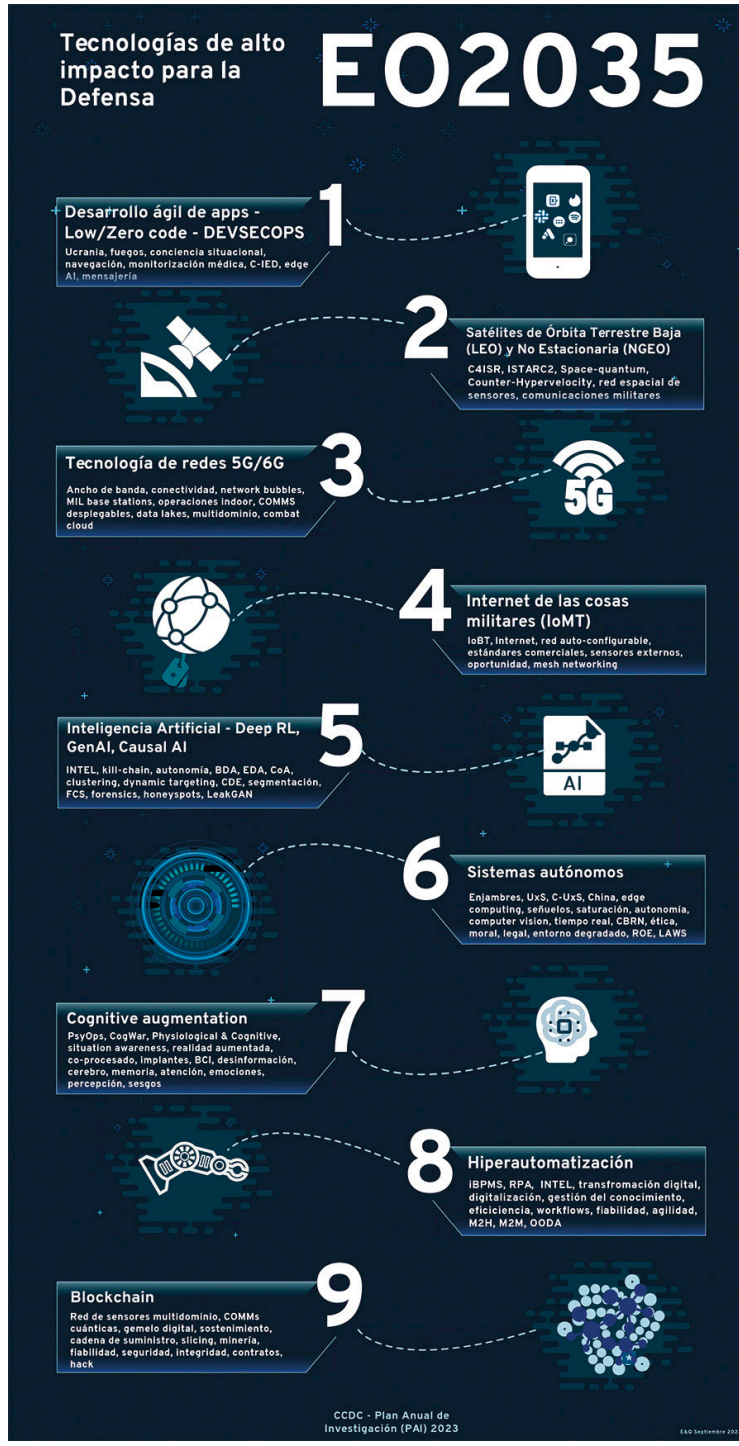
Martín sostiene que los productos y servicios civiles conocidos como *Commercial Off-The-Shelf* (COTS) han llegado a la Seguridad y Defensa para quedarse. No obstante, previene de que, a pesar de ser de fácil acceso en los mercados globales, su mera disposición no supone *per se* superioridad en cualquiera de los tipos de enfrentamiento. Para conseguir esta última, la clave reside en su correcta modificación y adaptación a las necesidades militares.

Comienza entonces el autor a tratar una serie de capacidades provenientes del ámbito civil que considera de especial interés por su impacto operativo, descartando las tratadas en capítulos anteriores, pues han sido ya ampliamente cubiertas. Inicia su repaso con las técnicas de inteligencia artificial, término genérico cuya definición aún requiere de matices importantes, refiriéndose al aprendizaje profundo reforzado *(Deep RL),* a la generativa (IA Generativa) o a la que permitirá identificar relaciones causa-efecto (*Causal AI*).

Continúa con otras tecnologías para las que la inteligencia artificial posee un carácter habilitante, como es la «autonomía», para la que explora múltiples posibilidades de cara a 2035, incluida la formación de equipos con humanos y la actuación en entornos degradados. Se abre entonces paso el apartado dedicado a las «técnicas para el incremento de capacidades cognitivas», imprescindibles en la «guerra cognitiva» y de la información, en la que atisba grandes avances que se sumarán a las aplicaciones actuales.

Aunque el *Blockchain* es un terreno no muy desarrollado en el ámbito militar, dada la seguridad, fiabilidad e incorruptibilidad de esta tecnología, el autor señala su potencial para todo lo relativo a la protección de la información en las adquisiciones militares y soporte del ciclo de vida de los productos en la próxima década. Finaliza su exposición con una referencia a la «híper-automatización» conjugando la inteligencia artificial con la extensión de los automatismos de gestores de procesos inteligentes (iBPMS) y los robóticos (RPA), de especial relevancia en un área clave como es el Mando y Control (C2) multidominio.

A modo de resumen visual del contenido de la presente obra, antes de dar entrada a los diferentes capítulos, se expone a continuación una figura que aglutina las principales tecnologías y sistemas considerados a lo largo del texto. Junto a cada tecnología, la imagen despliega algunas palabras clave en relación con las capacidades operativas y los entornos de aplicación más relevantes.


Tecnologías de alto impacto para la Defensa
EO2035
1
Desarrollo ágil de apps - Low/Zero code - DEVSECOPS
Ucrania, fuegos, conciencia situacional, navegación, monitorización médica, C-IED, edge AI, mensajería
2
Satélites de Órbita Terrestre Baja (LEO) y No Estacionaria (NGEO)
C4ISR, ISTARC2, Space-quantum, Counter-Hypervelocity, red espacial de sensores, comunicaciones militares
3
Tecnología de redes 5G/6G
Ancho de banda, conectividad, network bubbles, MIL base stations, operaciones indoor, COMMS desplegables, data lakes, multidominio, combat cloud
5G
4
Internet de las cosas militares (IoMT)
IoBT, Internet, red auto-configurable, estándares comerciales, sensores externos, oportunidad, mesh networking
5
Inteligencia Artificial - Deep RL, GenAI, Causal AI
INTEL, kill-chain, autonomía, BDA, EDA, CoA, clustering, dynamic targeting, CDE, segmentación, FCS, forensics, honeyspots, LeakGAN
AI
6
Sistemas autónomos
Enjambres, UxS, C-UxS, China, edge computing, señuelos, saturación, autonomía, computer vision, tiempo real, CBRN, ética, moral, legal, entorno degradado, ROE, LAWS
7
Cognitive augmentation
PsyOps, CogWar, Physiological & Cognitive, situation awareness, realidad aumentada, co-procesado, implantes, BCI, desinformación, cerebro, memoria, atención, emociones, percepción, sesgos
8
Hiperautomatización
iBPMS, RPA, INTEL, transfromación digital, digitalización, gestión del conocimiento, eficiciencia, workflows, fiabilidad, agilidad, M2H, M2M, OODA
9
Blockchain
Red de sensores multidominio, COMMs cuánticas, gemelo digital, sostenimiento, cadena de suministro, slicing, minería, fiabilidad, seguridad, integridad, contratos, hack
CCDC - Plan Anual de Investigación (PAI) 2023
EAG Septiembre 2023

## 5. Agradecimientos

Para despedir esta introducción, quisiera agradecer, en primer lugar, el gran trabajo realizado por los autores de los diferentes capítulos. Su extenso conocimiento sobre los aspectos tecnológicos tratados, experiencia y, sobre todo, dedicación durante os meses precedentes, constituyen un elemento clave para el éxito de la obra. Con ella, contribuyen decisivamente a impulsar el conocimiento y la comprensión tecnológica, uno de los fundamentos de la Transformación de las Fuerzas Armadas, para afrontar con garantías el entorno operativo venidero.

Mención especial merece el teniente coronel (IM) Ignacio Martínez de Galinsoga Alarcón, secretario del grupo de trabajo, que con su constancia y dedicación ha sabido impulsar con acierto las necesarias tareas de coordinación y administrativas del equipo, conducentes a la publicación que tiene ante usted.

Muchas gracias finalmente al lector, pues sin él la obra no tendría ningún sentido, quedando todos los integrantes del grupo de trabajo a la espera de que sea de su agrado y pueda servir a sus expectativas y necesidades.

Capítulo 1

# Estado actual de las comunicaciones militares por satélite: GEO *vs.* LEO

*Jaime Luis Sánchez Mayorga*

**Resumen**

En el mundo de las comunicaciones militares, se desata un debate crucial entre el uso de satélites en órbita geoestacionaria (GEO) y los satélites de órbita no geoestacionaria (NGEO), en medio de una renovación global de las capacidades SATCOM para defensa.

La necesidad de comunicaciones por satélite se divide en tres categorías: MILSATCOM para uso militar, GOVSATCOM para uso gubernamental y COMSATCOM para aplicaciones comerciales.

En el contexto europeo, la Agencia Espacial Europea (ESA), la Agencia Europea de Defensa (EDA), el Programa Espacial de la Unión Europea y las capacidades SATCOM de la OTAN son pilares fundamentales a tener en cuenta en la planificación y ejecución de estas.

La disyuntiva es clara: ¿se deben utilizar capacidades específicas de defensa o recurrir a soluciones de mercado?, buscando la complementariedad o sustitución entre GEO y NGEO. Los satélites GEO enfrentan crecientes amenazas espaciales, mientras que los NGEO ofrecen mayor versatilidad y resistencia.

El futuro de las comunicaciones militares por satélite se encuentra en la búsqueda de un equilibrio entre GEO y NGEO, asegurando la seguridad y eficiencia en un entorno cada vez más desafiante. La resolución de esta disyuntiva tendrá un impacto determinante en las operaciones militares y la seguridad nacional.

**Palabras clave**

Dilema, Satélite, Geoestacionaria, Órbita Baja, Mercado, Medio Propio, Comunicaciones Militares, Resiliencia, Seguridad.

## *Current state of military satellite communications: GEO vs. LEO*


### *Abstract*

*In the realm of military communications, a pivotal debate rages on between the use of geostationary (GEO) and non-geostationary (NGEO) satellites, amidst a global overhaul of SATCOM capabilities for defence.*

*Satellite communications requirements are categorized into three segments: MILSATCOM for military use, GOVSATCOM for governmental purposes, and COMSATCOM for commercial applications.*

*In the European context, the European Space Agency (ESA), the European Defence Agency (EDA), the European Union Space Programme, and NATO's SATCOM capabilities stand as crucial pillars to consider in the planning and execution of these capabilities.*

*The dilemma is crystal clear: should specific defence capabilities be employed or should market solutions be sought, aiming for complementarity or substitution between GEO and NGEO? GEO satellites face increasing space threats, while NGEO satellites offer greater versatility and resilience.*

*The future of military satellite communications lies in striking a balance between GEO and NGEO, ensuring security and efficiency in an increasingly challenging environment. The resolution of this dilemma will have a decisive impact on military operations and national security.*



### *Keywords*

*Dilemma, Satellite, Geostationary, Low Earth Orbit, Market, In-house, Military Communications, Resilience, Security.*

## 1. Introducción

La era de las comunicaciones por satélite comenzó poco después de la Segunda Guerra Mundial cuando Arthur C. Clarke sugirió la idea de colocar repetidores de telecomunicaciones en órbita alrededor de la Tierra. Su visión estableció los principios para lo que hoy conocemos como comunicaciones por satélite.

Aunque el primer intento de comunicación espacial fue el radiofaro en el Sputnik ruso, en 1957, los Estados Unidos llevaron a cabo experimentos de comunicación espacial en 1951 y 1955. Estos experimentos sentaron las bases para las comunicaciones por satélite y el seguimiento de las misiones Apolo.

La actividad comercial en el espacio comenzó con la *Comsat Corporation,* en 1962, cuando lanzaron el Telstar-1, el primer repetidor activo en órbita. Le siguió el Telstar-2 y los satélites Relay-1 y 2, que permitieron compartir transmisiones de televisión entre Estados Unidos, Nigeria y Brasil, marcando un hito en las comunicaciones trasatlánticas. En ese momento, las comunicaciones por satélite eran principalmente en órbita baja, antes de la era de los satélites geoestacionarios (GEO).

En 1963, se lanzó el Syncom-2, el primer satélite geoestacionario, aunque tenía una inclinación de 28 grados, lo que limitaba su cobertura. Fue seguido por el Syncom-3, que se convirtió en el primer satélite geoestacionario en el anillo ecuatorial a 36.000 km de la Tierra. Este satélite permitió la transmisión en vivo de los Juegos Olímpicos de 1964, en Japón.

Desde entonces, a pesar de que exista una similitud de diseño en términos generales (figura 1), ha habido una carrera para aumentar el número de satélites y, por lo tanto, la cobertura, adaptando el despliegue a las necesidades de cada país. En esta evolución, surgieron dos corrientes principales de las comunicaciones por satélite (SATCOM): las comunicaciones comerciales por satélite (COMSATCOM) y las comunicaciones militares por satélite (MILSATCOM).

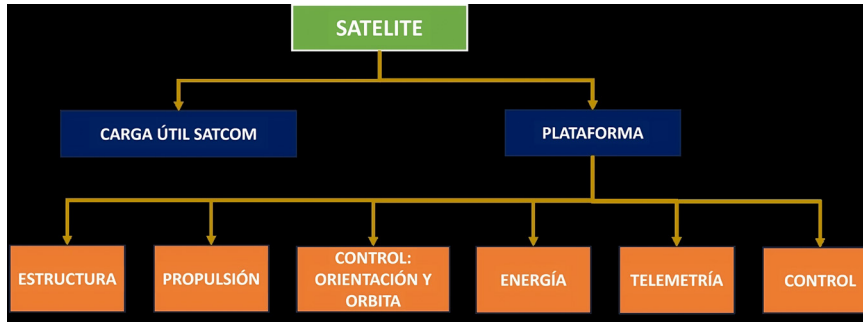



**Figura 1. Estructura genérica de un satélite**

La evolución de los modelos de negocio también es importante. Al principio, las soluciones de mercado satisfacían la demanda gubernamental, incluso para las Fuerzas Armadas, a pesar del uso de bandas no militares. Luego, surgieron acuerdos de alto nivel para garantizar la seguridad de las comunicaciones militares.

En los años ochenta, los satélites de órbita no geoestacionaria (NGEO) comenzaron a cambiar el panorama. Estos satélites se organizan en constelaciones y no están en órbita geoestacionaria. Su despliegue masivo marcó una diferencia notable. Debido a su elevado número, la gestión y el mantenimiento de estos sistemas de satélites es más compleja que en el caso de los GEO.

Los altos estándares empleados y la metodología de obtención en GEO, se refleja en la necesidad de obtener la certificación de determinados procesos, que podemos listar del siguiente modo:

– Alto grado de estabilidad en la posición y actitud del satélite.

– Precisión en el apuntamiento de las antenas.

– Larga vida útil en la posición orbital (>15 años).

– Suministro de energía eléctrica de alta fiabilidad.

– Control térmico de componentes expuestos.

– Funcionamiento continuado a pesar de eclipses solares.

– Lanzador capaz de efectuar la inserción en la órbita geoestacionaria.

Cuando nos referimos a satélites NGEO, en particular de órbita terrestre baja (LEO), no estamos solo frente a un cambio de paradigma en la provisión o explotación de servicios SATCOM, sino también en los procesos de fabricación y lanzamiento asociados.

Las constelaciones de satélites son grupos de satélites organizados en planos orbitales. Los satélites NGEO de un mismo plano orbital siguen la misma trayectoria orbital, uno tras otro, suelen estar uniformemente espaciados alrededor de la órbita (figura 2).

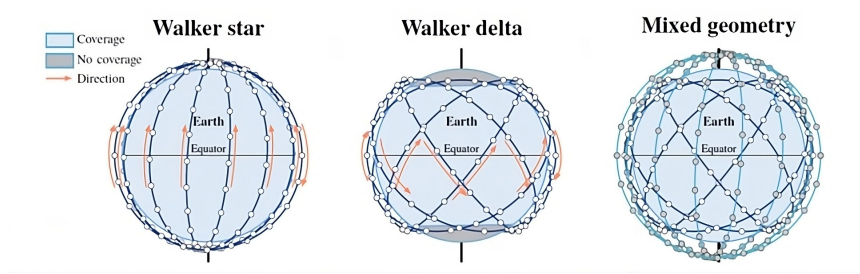



**Figura 2. Diagrama de geometrías Walker, Walker-Delta y mixta, en NGEO**

Para hacer una primera aproximación paramétrica, de lo que pueden significar las cifras de estos despliegues NGEO, podemos emplear la siguiente tabla:

| **Parámetro** | **Constelación** | | | | | | |
|---|---|---|---|---|---|---|---|
| | Starlink | | | | | OneWeb | Kepler |
| **Tipo** | Mixto | | | | | Walker star | Walker star |
| **Número de satélites** | 1.584 | 1.584 | 720 | 348 | 172 | 648 | 140 |
| **Número de planos orbitales** | 72 | 72 | 36 | 6 | 4 | 18 | 7 |
| **Altitud (km)** | 550 | 540 | 570 | 560 | 560 | 1.200 | 575 |
| **inclinación δ°** | 53,0 | 53.2 | 70,0 | 97.6 | 97.6 | 86.4 | 98.6 |
| **Servicio previsto** | Broadband | | | | | | IoT |

**Tabla 1. Comparativa de referencia entre constelaciones**

Para algunos autores (Barroso y Feijoo, 2010: 487-495), este momento está sobrepasando las actuaciones de las instituciones y el sector de las telecomunicaciones ha experimentado una transformación sin precedentes en la década anterior (figura 3), afectando a tres ejes principales del mismo: las infraestructuras involucradas en la provisión de capacidad SATCOM, la innovación como acelerador de las actuaciones en la industria espacial de las telecomunicaciones y la descentralización o reordenamiento de las decisiones.

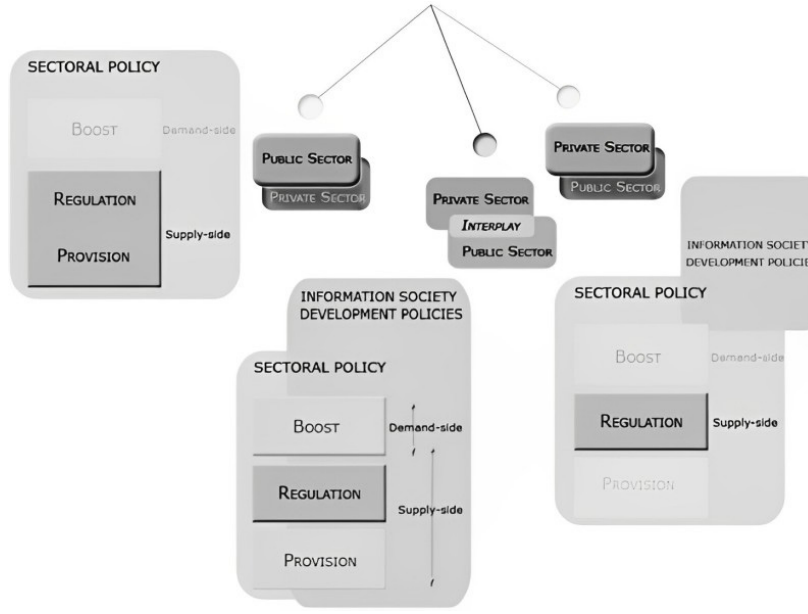



**Figura 3. Evolución de la actividad pública en el sector de las telecomunicaciones. Barroso y Feijoo, 2010**

Actualmente, el sector de las SATCOM se ve influido por varios factores clave, tales como: la apertura de mercados (Khodeli *et al.*, 2020: 70-109), la convergencia de ideologías, económicas y políticas, avances tecnológicos acelerados, la descentralización de decisiones, políticas, académicas e industriales, la inestabilidad, económica y geopolítica, y el cambio hacia una sociedad de la información.

Estos factores, que no son nuevos, están siendo aplicados de manera diferente en el ámbito espacial, en especial en los nuevos modos de entender las telecomunicaciones por satélite. La sociedad de la información busca un despliegue global de capacidades de conectividad y la participación de todos en esta revolución (Stock *et al.*, 2022). El sector público está interesado en fomentar esta transformación, ya sea incentivando la demanda o respaldando el crecimiento industrial y tecnológico del sector.

Estos cambios están llevando a una revisión en los modelos de relación entre los actores públicos y privados (Vernile, 2018) en el ámbito de las comunicaciones satelitales. También están influyendo en los modelos de negocio y en la prestación de servicios de las grandes operadoras, especialmente en lo que respecta a compartir riesgos en un ecosistema público-privado.

En este sentido, uno de los parámetros que marcan más la diferencia entre los modelos existentes de provisión de capacidades de comunicaciones espaciales y los modelos actuales, es el rol relevante del sector privado, más en concreto, el subsector de la inversión privada, en apoyo de iniciativas de alto riesgo, pero que implican una reducción proporcional de costes.

La colaboración público-privada (CPP) se ha vuelto fundamental en el sector espacial actual. La distribución de riesgos entre las partes pública y privada se ha reevaluado. Las operadoras tradicionales y los nuevos actores adoptan modelos mixtos para satisfacer la creciente demanda de SATCOM (Sánchez Mayorga, 2021).

La llegada de nuevos actores privados, como *Silicon Valley* y las grandes empresas tecnológicas (GAFA), ha transformado aún más el sector, aportando innovación y tecnología y abriendo nuevos horizontes en el espacio.

En resumen, el sector de las comunicaciones por satélite ha experimentado una transformación significativa con el surgimiento de las megaconstelaciones NGEO y la participación de nuevos actores privados (Del Portillo, Cameron y Crawley, 2019: 123-135). Esto ha llevado a una mayor colaboración público-privada y a un cambio en los modelos de obtención y provisión de capacidades espaciales, en un sector que se divide en dos corrientes principales: una enfocada en satisfacer las necesidades gubernamentales y garantizar la independencia tecnológica, otra que sigue principalmente las reglas del mercado (Höfner, Vahl y Stoll, 2018: 1-6), pero busca oportunidades para colaborar con el sector público.

## 2. La capacidad SATCOM para Defensa: renovación en marcha

Desde 1987, se iniciaron dos vías para mejorar las capacidades de comunicación satelital de nuestras Fuerzas Armadas. Se decidió equipar un satélite de la operadora comercial HISPASAT, el HISPASAT 1A, con una carga de pago gubernamental y formalizar un acuerdo con la operadora para utilizar posiciones orbitales y frecuencias exclusivas de la banda X. Esto permitiría brindar comunicaciones a las Fuerzas Armadas en zonas de operaciones donde el Sistema de Telecomunicaciones Militares no llegaba. Era el comienzo del Programa SATCOM.

Consecuencia de ello, se creó el Sistema Español de Comunicaciones por Satélite (SECOMSAT) para gestionar las señales asignadas a las unidades desplegadas y extender el Sistema Conjunto de Telecomunicaciones Militares (SCTM) a las Zonas de Operaciones. Este programa colaboró con el Programa SATCOM para obtener la capacidad necesaria para las FAS.

Con el tiempo, SECOMSAT se adaptó a las demandas cambiantes y la capacidad SATCOM, utilizando satélites Spainsat y XtarEur en bandas X y Ka militar. Ahora se prepara para la renovación, que se espera para 2024 con el lanzamiento de Spainsat NG 1, lo que implica un aumento significativo en la capacidad y una mayor complejidad operativa.

El Ministerio de Defensa optó por satélites SATCOM GEO como Spainsat NG 1 y 2, lo que proporciona una capacidad permanente y propia de las Fuerzas Armadas, gestionada a través de un modelo de colaboración con HISDESAT (figura 4).

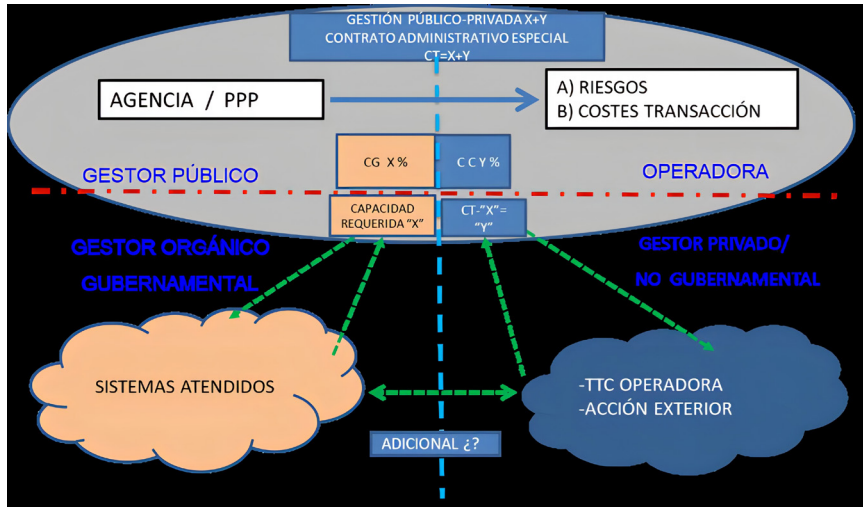



**Figura 4. Balance de una CPP en capacidades espaciales**

Cabría en este punto preguntarse: ¿qué hay sobre capacidades NGEO protegidas y seguras? (Townsend, 2017), ¿podemos estar en la antesala del impulso de capacidades complementarias a la renovación SATCOM, de origen COM o GOV?, en el caso de que se trate de un complemento comercial, de naturaleza dual, de interés para la Defensa, ¿qué papel puede jugar la nueva Agencia Espacial española en este contexto? (Mayorga, 2021).

## 3. La descripción de la necesidad: MILSATCOM, GOVSATCOM y COMSATCOM

Antes de abordar la respuesta a estas cuestiones, resulta interesante comprender las diferencias entre las diferentes categorías SATCOM y los factores que influyen en su definición. En primer lugar, reconocidas como categorías de referencia, tanto COMSATCOM como MILSATCOM, es importante entender el origen y el significado actual del término «GOVSATCOM», un tema de gran interés en la comunidad de Defensa, junto con la distinción entre GEO y NGEO, especialmente actual en Europa, en estos momentos.

Antes de la aparición del concepto de GOVSATCOM, los países con capacidades MILSATCOM solían firmar acuerdos con otros países para ofrecer su capacidad excedente, tanto para Fuerzas Armadas como para entidades gubernamentales que lo demandasen. España, como uno de los países pioneros en Europa en este aspecto, también seguía esta práctica.

Hasta ese momento, la inversión se destinaba principalmente a MILSATCOM o COMSATCOM. El primero se caracteriza por ser una inversión pública que no se rige por la competencia de los precios de mercado (€/Mb o €/MHz). Esto se debe a que las comunicaciones MILSATCOM requieren medidas adicionales y tienen una mayor complejidad, lo que se traduce en un aumento de los costos totales de prestación de este tipo de capacidad SATCOM.

Por otro lado, el COMSATCOM ha evolucionado para satisfacer la demanda del mercado SATCOM (Judice, Livin, y Venusamy, 2022: 1140-1143) en diversas aplicaciones, como la radiodifusión y las comunicaciones. En la actualidad, existe una amplia gama de servicios disponibles en este sector, como se analizará en el siguiente punto, está estrechamente relacionado con la demanda actual en términos de características y casos de uso.

## 4. Estado de la cuestión SATCOM para los NGEO

Es importante examinar detenidamente algunos datos y conceptos clave que ayudarán a arrojar luz sobre el actual debate entre GEO y NGEO

(órbita no geoestacionaria, incluyendo LEO, MEO y HEO[1]) en el contexto de GOVSATCOM. Tras considerar las ventajas, oportunidades, riesgos y vulnerabilidades de cada enfoque, surge la pregunta de cómo se encuentran nuestras capacidades en esta área y si las iniciativas duales de la Unión Europea resolverán la demanda de SATCOM NGEO para las Fuerzas Armadas.

### 4.1. Comparación entre GEO y NGEO (LEO/MEO) SATCOM

Si se abordase la comparativa en términos generales, nos podemos encontrar muy diversas fuentes, de distintas corrientes de opinión, no exentas de propuestas orientadas a los intereses concretos de cada autor. De este modo, el resultado se basaría en los parámetros más empleados en la literatura escrita hasta la fecha y su posible resultado nos enmarcaría esta disyuntiva en una tabla similar a la de la figura 5.

Analizaremos esta comparativa, en primer lugar, en términos de prestación de servicios. El sector comercial suscribirá contratos que darán lugar a acuerdos de nivel de servicio (SLA-*Service Level Agreement*) (Guerster *et al.)* que se adaptarán a parámetros cambiantes a lo largo del tiempo. Esto contrasta con el cálculo del coste para capacidades gubernamentales destinadas a la Defensa, que se basan en el desarrollo, fabricación, lanzamiento y operación de la capacidad. En el contexto de los satélites GEO, que ofrecen una estabilidad en la prestación, es posible establecer un SLA genérico al inicio.

Sin embargo, en el caso de NGEO, especialmente cuando las empresas del *New Space* están involucradas, los SLA adaptables son más complejos debido a la flexibilidad de los precios. Estos ajustes se basan en la adaptación del gasto a la demanda exacta del servicio, en un momento concreto de la prestación.

Debemos comprender que los satélites GEO se construyen bajo estándares rigurosos de diseño, certificación, pruebas de vuelo, pruebas medioambientales y condiciones de vuelo en el espacio, lo que garantiza su funcionalidad. Este enfoque ha llevado a un aumento en la construcción y lanzamiento de satélites GEO de mayor capacidad en respuesta a la creciente demanda.

Sin embargo, la dinámica cambió con la aparición de los satélites NGEO, en órbitas donde la exposición a la radiación es menor, lo que reduce los costes de industrialización y fabricación, así como de las pruebas de

[1] Órbita Terrestre Mediana (MEO) y Órbita Terrestre Baja (LEO) y Órbita Altamente Elíptica (HEO).

resistencia a la radiación, pero aumenta los riesgos de interferencias intencionadas, ataques contra su ciberseguridad y riesgos derivados de la superpoblación creciente.

| | GEO (36,000km) | MEO (5,000-20,000km) | LEO (500-1,200km) |
|---|---|---|---|
| Altitude latency[1] | High | Low | Very low |
| Earth coverage | Very large | Large | Small |
| Satellites required | Three | Six | Hundreds |
| Data gateways | Few fixed | Regional flexible | Local numerous |
| Antenna speed | Stationary | 1-hour slow tracking | 10-minute fast tracking |
| Advantages | High throughput (HTS) technologies enable basic broadband internet applications | Proven low latency comparable to terrestrial networks, offers fibre-equivalent performance | Claims support for high-frequency trading, virtual gaming, and high-performance computing applications |
| | Fewer satellites over very large fixed geographical areas | Simple equatorial orbit covers 96% of global population | Smaller, lower power satellites batch-launched more cheaply than GEO |
| Disadvantages | High altitude and distant ground networking impacts latency-sensitive applications | Dual tracking antennas required to maintain continuous connectivity | Very complex tracking and ground network, plus complete constellation must be in place before service starts |
| | Signal power losses require larger satellites and antennas | Inclined plane orbits needed to cover high latitudes | Unproven business model, risky technology, and space debris risk |

[1]*Total end-to-end network latency is dependent on ground infrastructure*

**Figura 5. Tabla comparativa de referencia. Fuente: abiertas**

Estos factores son beneficiosos para sistemas SATCOM NGEO, que requieren un gran número de satélites para una cobertura global y pueden aprovechar economías de escala para reducir costes.

Desde el punto de vista industrial, esto permite una mayor disponibilidad de componentes y una reducción en los costes unitarios de los satélites. Sin embargo, desde una perspectiva tecnológica, existe el riesgo de que la industria se acomode a modelos de producción de menor complejidad, lo que podría tener un impacto negativo en la alta cualificación del sector espacial.

En resumen, el debate entre GEO y NGEO en el contexto de GOVSATCOM es un tema de gran relevancia que implica consideraciones técnicas, comerciales y estratégicas. La Unión Europea está trabajando en regulaciones para abordar este cambio en el panorama de las comunicaciones por satélite y mantener su posición en el mercado espacial global.

### 4.2. España: demanda de renovación desde el EMAD

Se ha señalado, ya que, desde hace cinco años, la decisión respecto de la renovación de la capacidad SATCOM tuvo como consecuencia, la fabricación de dos satélites GEO de altísimas prestaciones, que son último «estado del arte» en el contexto de países que desarrollan capacidades SATCOM para sus Fuerzas Armadas.

Nuestras Fuerzas Armadas disponen de esta capacidad como medio propio y exclusivo, a pesar de la titularidad de los satélites bajo propiedad de una operadora de servicios estratégicos, fruto de una colaboración público-privada entre el Ministerio de Defensa y dicha operadora, de la alta fiabilidad y eficiencia del modelo (Mayorga, 2021).

En este punto, se analizará la necesidad de disponer, además de la capacidad SATCOM actual, una cierta capacidad NGEO (MEO y/o LEO) de utilidad para las Fuerzas Armadas y, sobre todo, cómo ha evolucionado su presencia en el marco europeo de las FAS, de resultas de su incuestionable utilidad en conflictos reales, como ha sido el caso en la invasión de Rusia a Ucrania.

### 4.3. Europa

Para entender el estado actual de la disyuntiva en Europa, es fundamental adentrarnos en cómo se experimenta esta dicotomía en los contextos más influyentes del ámbito europeo.

Estos son: la Comisión Europea y su destacado Programa Espacial, la Agencia Espacial Europea (aunque no sea parte de la Unión Europea), que se está volviendo relevante en el lanzamiento de un nuevo proyecto emblemático en respuesta a la categoría emergente de GOVSATCOM, la Agencia Europea de Defensa (EDA), que ha servido como escenario de demostración para examinar minuciosamente los pros y contras de esta evolución en el concepto de SATCOM para las Fuerzas Armadas.

#### 4.3.1. La Evolución del Programa Espacial de la Unión Europea: componente GOVSATCOM

En el emocionante panorama espacial, la Unión Europea ha delineado un ambicioso plan para el periodo 2021-2027 a través del reglamento (UE) 2021/696. Este reglamento da vida al Programa Espacial de la Unión Europea y establece la creación de la Agencia de la Unión Europea para el Programa Espacial (EUSPA). El objetivo claro de esta empresa es asegurar el liderazgo europeo en el espacio, fomentar la competitividad en la economía espacial emergente y abordar desafíos críticos, como el cambio climático y la promoción de la innovación tecnológica.

Dentro de esta iniciativa, un componente crucial es GOVSATCOM, una propuesta lanzada por la Comisión Europea como parte del Programa Espacial de la UE.

La misión de GOVSATCOM es garantizar la disponibilidad a largo plazo de servicios gubernamentales de comunicaciones por satélite, que sean robustos, seguros y eficientes. Estos están destinados a las autoridades nacionales y de la UE que son responsables de misiones e infraestructuras críticas para la seguridad.

Desde el lanzamiento de los Comités del Programa Espacial de la Unión Europea, en particular en el Comité de configuración GOVSATCOM, se hizo evidente la incertidumbre sobre la definición del alcance de esta iniciativa. Tanto la Dirección General de Industria y Defensa (DG DEFIS) como los Estados miembros se encontraban en terreno desconocido.

A diferencia de programas como Galileo y Copérnico, donde la Comisión Europea ejercía su capacidad de establecer normas y regulaciones sin menoscabar la soberanía de los Estados miembros, GOVSATCOM emergió desde un origen distinto y peculiar.

En sus albores, la Comisión carecía de medios propios SATCOM, lo que la llevó a buscar una solución a medio y largo plazo, aprovechando los recursos disponibles en los Estados miembros. Este planteamiento generó una ventana de oportunidad que podría haber posicionado a España como uno de los proveedores clave de capacidades en este sector en crecimiento.

Sin embargo, para entender la complejidad y los desafíos que rodearon a GOVSATCOM y su posterior evolución hacia la constelación IRIS2, conocida también como «la constelación Bretón», es esencial sumergirse en las discusiones y tensiones que dieron forma a este innovador aspecto de las comunicaciones por satélite en Europa (figura 6).

<table>
<tr><th></th><th>MILSATCOM</th><th>GOVSATCOM</th><th>COMSATCOM</th></tr>
<tr><td rowspan="2">GEO</td><td>MILSATCOM Y/O CAPACIDADES ESTRATÉGICAS</td><td>CAPACIDADES ESTRATÉGICAS GUBERNAMENTALES</td><td>OPERADORAS ESTRATÉGICAS</td></tr>
<tr><td>MEDIOS ESPECÍFICOS</td><td>COMUNICACIONES SEGURA</td><td>CAPACIDADES DE OPERADORAS COMERCIALES</td></tr>
<tr><td rowspan="2">NGEO</td><td rowspan="2">NO MIL</td><td>CONECTIVIDAD SEGURA</td><td>NEW SPACE</td></tr>
<tr><td>IRIS²</td><td>IRIS²</td></tr>
</table>

**Figura 6. Matriz de casos disponibles**

En las primeras conversaciones, dentro del Comité de Programa Espacial en configuración GOVSATCOM, quedó en evidencia una notable incertidumbre respecto a la definición del alcance y los objetivos de esta iniciativa. Tanto la Dirección General de Industria y Defensa (DG DEFIS) como los Estados miembros se encontraban en territorio desconocido, ante un desafío que iba más allá de las dinámicas conocidas de programas como Galileo y Copérnico.

Una de las razones detrás de esta incertidumbre se hallaba en la procedencia del personal que lideró los primeros pasos de la Agencia de la Unión Europea para el Programa Espacial (EUSPA). Este equipo de expertos provenía del Programa Galileo y estaba familiarizado con un modelo de provisión de servicios y capacidades de navegación por satélite (PNT) que distaba considerablemente de los requerimientos de GOVSATCOM.

Los programas Galileo y Copérnico constituían activos de la Unión Europea en sí, lo que permitía a la Comisión Europea establecer regulaciones y normativas sin vulnerar la soberanía de los Estados miembros. No obstante, GOVSATCOM presentaba una dinámica original y distinta en su origen y ejecución.

En el año 2021, aunque la Comisión aún no poseía medios SATCOM propios, ya había diseñado planes concretos para adquirirlos en el futuro cercano. Esta perspectiva redujo el periodo de disponibilidad de capacidades nacionales excedentes de los Estados miembros para beneficio de toda la Unión Europea.

La Comisión comprendió que GOVSATCOM, a pesar de formar parte del Programa Espacial destinado a contribuir a la independencia y soberanía de la Unión Europea, dependía, en gran medida, de las contribuciones de los Estados miembros, una dinámica que contrastaba con la gobernanza de Galileo y Copérnico.

Asimismo, el sector SATCOM se encontraba inmerso en una competencia global con los emergentes modelos del *New Space* (Quintana, 2017: 88-109), a pesar de los discursos que abogaban por una Política Espacial Europea que impulsara soluciones de carácter europeo. Esto condujo a una campaña desde dentro de la Comisión para primero promover las virtudes del *New Space* y luego presentar la opción NGEO como la mejor alternativa, enmarcada en el concepto de «Conectividad Segura».

Sin embargo, el presupuesto asignado a GOVSATCOM en el Programa Espacial se percibía insuficiente para una empresa de esta envergadura. Una parte limitada de los fondos se destinó a GOVSATCOM después de dividirlos entre los programas comunitarios Galileo y Copérnico, así como entre GOVSATCOM y SSA/SST.

A pesar de las limitaciones presupuestarias, la Comisión optó por hacer una llamada a todas las Direcciones Generales de la Comisión y se inició un proceso liderado por DG CONNECT, con el fin de crear un tercer buque insignia destinado a proporcionar conectividad segura a toda la sociedad de la Unión Europea.

Dentro de los comités del programa, GOVSATCOM se fragmentó en dos, con la aparición del programa *Secure Connectivity*. A pesar de que los reglamentos eran similares y este último era impulsado por DG CONNECT, la Comisión decidió gestionar ambos programas en el mismo comité de programa.

La constelación «Bretón» surgió como respuesta a la regulación de *Secure Connectivity* y esto tuvo un impacto inmediato: la envolvente tradicional de GOVSATCOM se redujo, lo que afectó las contribuciones de los Estados miembros y abrió la puerta a la presencia de NGEO (IRIS2), que se encontraba más cerca del mercado y tenía un enfoque comercial, a pesar de presentarse como una solución gubernamental.

Es relevante subrayar que, aunque se pretenda considerar a IRIS2 como parte de la solución para GOVSATCOM, esta constelación no es completamente compatible, comparable con las capacidades MILSATCOM ni cumple con los estrictos requisitos de seguridad de las Fuerzas Armadas. En lugar de ello, debería ser contemplada como un suplemento temporal en situaciones donde las capacidades estratégicas actuales muestren limitaciones.

Desde una perspectiva más amplia, aquellos Estados miembros que cuentan con capacidades propias podrían experimentar una reducción en los retornos esperados de la inversión realizada en la modernización de las capacidades SATCOM actuales, debido al nuevo rumbo de esta iniciativa.

Resulta esencial considerar factores como los despliegues terrestres requeridos para estas constelaciones, el efecto *Doppler* (Borek, Woźnica y Malawski, 2021), que pueden impactar en la continuidad del servicio y las restricciones asociadas a la movilidad de los terminales. La utilización de frecuencias no exclusivamente militares también introduce la posibilidad de interferencias, tanto intencionales como accidentales.

No obstante, a pesar de estas consideraciones, los beneficios de una baja latencia y una alta capacidad de comunicación resultan atractivos para una amplia variedad de usuarios SATCOM. Estos atributos son especialmente cruciales en situaciones donde la conectividad debe ser rápida y robusta, como en entornos hostiles.

Además, la complejidad geopolítica, la necesidad de salvaguardar tecnologías críticas para la independencia y autonomía tecnológica de la Unión Europea plantean desafíos adicionales. La UE debe equilibrar

cuidadosamente sus aspiraciones con las realidades técnicas, financieras y geopolíticas que afronta en su búsqueda de una conectividad segura y eficiente en el espacio. En este proceso, las decisiones que tome serán cruciales para determinar el rumbo de Europa en el ámbito espacial.

La Unión Europea se encuentra en una encrucijada, ya que la tendencia hacia la corriente de SATCOM LEO está ganando terreno dentro del concepto GOVSATCOM, lo que reduce la demanda de capacidades estratégicas en favor de soluciones NGEO, aunque estas últimas no están exentas de incertidumbres, especialmente en cuanto a su seguridad y su aplicabilidad en el ámbito militar.

En resumen, NGEO se presenta como una opción eficaz en circunstancias específicas, pero plantea desafíos en términos de resiliencia y sostenibilidad financiera a largo plazo.

### 4.3.2. EDA: *pooling and sharing*

Aunque cabría pensar que este asunto debería haber sido abordado antes del Programa Espacial, su inclusión intencionada en este punto del artículo nos permite extraer conclusiones que refuerzan lo ya expuesto al respecto.

– ¿Qué está ocurriendo en la EDA con respecto a SATCOM?

España, a través del Ministerio de Defensa y su compromiso con la iniciativa GOVSATCOM, tiene la capacidad y oportunidad de participar, en apoyo de ciertas operaciones de Política Común de Seguridad y Defensa (PCSD) de la UE, proporcionando capacidad SATCOM del excedente de su MILSATCOM. Esto es posible a través del proyecto de demostración de provisión SATCOM, que se enmarca en la EDA y ha sido liderado por España desde su inicio en 2015 hasta nuestros días.

Esta demostración resulta muy interesante para comprender el papel real de nuestras capacidades excedentes en un contexto de provisión estratégica de capacidades disponibles, que es el objetivo original del componente GOVSATCOM de la UE en lo que respecta a la contribución de los Estados miembros y sus medios gubernamentales/militares.

– Factores clave en el GOVSATCOM de la EDA

En la medida en que hemos expuesto a lo largo de este artículo la verdadera naturaleza de la categoría GOVSATCOM, conviene recordar que no existía antes de 2015, cuando se comenzó a considerar una solución para proporcionar SATCOM a entidades gubernamentales de la UE. En su creación, surgieron numerosas discusiones sobre el nivel de los requisitos de esta nueva categoría, que se situaría entre dos categorías existentes (Klein

J.J., 2019), cada una con sus propios modelos de obtención. Entre los factores clave a considerar destacaron:

- La posición intermedia de GOVSATCOM entre las categorías existentes (categoría 1 para MILSATCOM y 3 para COMSATCOM), que debía cumplir con especificaciones de cierto grado de protección, resiliencia y seguridad, sin llegar a los estándares de MILSATCOM, sin ser tan abiertos como los empleados para las soluciones comerciales.
- Las discusiones en torno a la definición de ese «cierto grado de seguridad», que son fundamentales para las soluciones SATCOM estratégicas de los Estados miembros, máxime cuando estamos considerando comunicaciones seguras para las FAS.
- Y la pregunta de si GOVSATCOM, ocupando un lugar entre dos corrientes diferentes, compite en el mercado o se basa en desarrollos estratégicos específicos, elemento clave para comprender los esfuerzos necesarios para disponer de ello.

Estos factores continúan siendo objeto de debate y las decisiones tienen un impacto significativo en el costo, las prestaciones y la accesibilidad de esta nueva categoría SATCOM.

¿Se trata de una fragmentación del mercado (Guerster *et al.*), en favor de su tratamiento como un segmento del mercado, de mayor coste y prestaciones que el resto del mercado SATCOM?, o si, por el contrario, en similitud con la categoría MILSATCOM, ¿se trata de un modelo de obtención ajeno al mercado y para el cual el balance no se obtiene de la relación entre la oferta y la demanda, sino entre las altas prestaciones y la disponibilidad presupuestaria?

En resumen, la iniciativa en curso en la EDA, que España lidera en estos momentos, nos permite identificar aquellos factores que deben mejorarse y discutir antes de firmar acuerdos entre la Comisión y los Estados miembros con capacidades, especialmente con miras a la provisión de servicios iniciales en 2024.

### 4.4. OTAN

En sus primeras décadas, se encargó de satisfacer sus necesidades de SATCOM mediante medios propios, desde 1970 hasta el 2000. Sin embargo, desde entonces, ha optado por un enfoque diferente, similar al adoptado por la EDA, renunciando a disponer medios propios.

Este cambio se basa en una prestación de capacidades que deben cumplir unos requisitos extremadamente rigurosos, por lo que se diferencian del enfoque de la Unión Europea (UE), en este sentido, con el objetivo de

garantizar la máxima protección y estabilidad en la provisión de capacidades SATCOM para las operaciones militares de la Alianza.

Estos requisitos han influido en la especificación, diseño y fabricación de los sistemas nacionales actuales, un aspecto que cobra máxima relevancia en el actual momento en que nos encontramos.

En este contexto, es importante destacar que la OTAN no se centra en GEO como su objetivo principal, sino en las capacidades necesarias. Esto abre la puerta a la incorporación de modelos de nueva generación (NGEO), aunque deben cumplir con los estándares más elevados en términos de seguridad (Tonkin *y* De Vries, 2018), protección, resiliencia, ciberseguridad (Manulis *et al.*, 2021: 287-311) y sostenibilidad.

En cuanto al valor de las soluciones cooperativas, la OTAN emplea el enfoque de capacidades disponibles, muy próximo al concepto de *pooling and sharing* de la EDA. En este caso, las capacidades requeridas se obtienen mediante la firma de un Memorando de Entendimiento (MoU) en el que un consorcio de naciones se compromete a poner a disposición de la Alianza capacidades predeterminadas y que deben cumplir con los rigurosos requisitos establecidos por la OTAN.

En este contexto, no se debate sobre el precio, ya que este ha sido previamente calculado y discutido dentro de la OTAN, a través de la *NATO Communications and Information Agency (NCIA)* y el Comité de Infraestructura de la Alianza, que proporciona el presupuesto necesario y define el techo de gasto de la capacidad.

España ha contribuido en el pasado proporcionando capacidades a la OTAN, a través de acuerdos específicos para escenarios concretos. Actualmente, aspira a ser parte de este consorcio de naciones proveedoras, ya que la futura capacidad de los SATCOM Spainsat NG se considera una de las más avanzadas entre los países miembros de la OTAN.

Sin embargo, a pesar de que las referencias actuales se basan en sistemas GEO, considerando el crecimiento de las constelaciones NGEO y teniendo en cuenta los resultados obtenidos recientemente, es probable que la Alianza busque colaborar con actores NGEO para complementar sus capacidades actuales.

Y en este escenario será aún más crítico evaluar si los parámetros de latencia, capacidad y resiliencia compensan los desafíos y desventajas previamente mencionados en relación con el uso de constelaciones comerciales NGEO.

En cualquier caso, la metodología de obtención de la OTAN requerirá que las capacidades basadas en sistemas NGEO cumplan con los mismos estándares de seguridad exigidos para los sistemas GEO actuales, un desafío que las constelaciones comerciales aún no han superado en la actualidad.

## 5. Capacidades para Defensa *vs.* mercado SATCOM

En la presente exposición, examinaremos la situación actual y los factores clave que influyen en la evolución y disyuntiva entre los modelos de GEO tradicionales y las tendencias emergentes de NGEO (Al-Hraishawi, H. *et al.* 2022). Nuestro objetivo es identificar los elementos que caracterizan las diversas posturas en esta cuestión.

Para lograrlo, evaluaremos la relación entre el empleo de sistemas GEO convencionales y las soluciones NGEO, así como las soluciones de mercado asociadas a estas tecnologías. Utilizaremos los factores previamente discutidos en este documento para analizar ambas corrientes desde la perspectiva de su aplicabilidad en las Fuerzas Armadas.

Quizá se deba reconsiderar la viabilidad de las soluciones en los próximos años, independientemente del proceso de renovación en curso de la capacidad GEO.

Para ello, se ha elaborado una tabla o matriz que permita analizar los casos propuestos en la figura 5, respecto de una serie de factores que permitan orientar la decisión (figura 7), a la vista de los resultados que se obtengan en cada uno de los aspectos siguientes:

– Comunicaciones seguras: evaluación del grado de incertidumbre.

– Análisis de los actuales vectores de MILSATCOM.

– Evaluación de los parámetros de mercado en el ámbito de SATCOM-LEO.

– Valoración de la resiliencia y protección ante amenazas actuales en el entorno de las comunicaciones.

### 5.1. Comunicaciones seguras: evaluación del grado de incertidumbre

A lo largo de este documento, hemos identificado uno de los factores clave para determinar la dirección que tomarán los próximos documentos de necesidad en cuanto a sistemas SATCOM: la seguridad de las futuras opciones SATCOM.

En el contexto de los sistemas GEO, existen especificaciones y estándares rigurosos que garantizan su utilización en operaciones militares que cumplen con los requisitos de las Fuerzas Armadas. Esto se aplica tanto a misiones nacionales como a las operaciones de cooperación internacional, en las que España participa como Estado Miembro o aliado.

Para asegurar la interoperabilidad necesaria para afrontar nuestros compromisos, elemento especialmente sensible en el marco de GOVSATCOM, sería esencial que la Unión Europea, en ausencia de una entidad que

certifique el cumplimiento de estándares adecuados, reconozca los estándares de la OTAN como una referencia con las debidas garantías.

| | GEO | | | NGEO | | |
|---|---|---|---|---|---|---|
| CATEGORÍA/FACTORES DE SEGURIDAD | MIL | GOV | COM | MIL | GOV | COM |
| COMUNICACIONES SEGURAS | SOLUCION NACIONAL → | GOVSAT E.U. | OPERADOR ESTRATÉGICO | ¿? | IRIS2 → | OPERADOR COMERCIAL |
| | OTAN | ¿ESTANDAR?->NO | NO ESTANDAR | | | |
| VECTORES MILSATCOM | REQUISITOS MIL 100% | GOVSATCOM Y% MIL+Z% COM | NO REQ. MIL | NO | • RESILIENCIA<br>• BAJA LATENCIA<br>• ALTA CAPACIDAD → | GOVSATCOM NO MIL+Z% COM |
| | | | | ¿? ← | • ¿SEGURIDAD? → | OPERADOR COMERCIAL |
| MERCADO EN SATCOM-LEO | CAPACIDAD/ PRESUPUESTO | MERCADO vs CAPACIDAD/ PRESUPUESTO | ¿MERCADO? ← | NO | COM + SEGURIDAD<br>IRIS2-EUSPA | EUSPA:GOVSAT+IRIS2 |
| RESILIENCIA | X% | ¿? | X% | NO | SI | SI |
| PROTECCIÓN FRENTE AMENAZAS | SI | ¿? | NO | NO | ¿?-> NO | NO |

**Figura 7. Matriz de análisis de los casos de uso**

Esto requeriría de un proceso de armonización de estándares dentro de la UE, o la creación de una entidad de estandarización en materia de seguridad SATCOM. De lo contrario, la seguridad de nivel necesario (Tedeschi, Sciancalepore, y Di Pietro, 2022) no se cumpliría, lo que relegaría estas soluciones a niveles de protección similares a las ofertas comerciales, impidiendo su empleo en los casos de uso de Defensa que lo requiera.

En el caso de los sistemas NGEO, en particular, LEO SATCOM (órbitas baja o media), la situación con respecto a GOVSATCOM es similar a la de GEO, aunque es crucial definir el nivel de seguridad «objetivo» que busca la Comisión Europea.

Este tema sigue siendo un asunto pendiente y las medidas de seguridad para la información en LEO aún están en desarrollo. Se están considerando soluciones de criptografía, incluyendo la distribución de claves cuánticas en constelaciones LEO, dónde la baja latencia mejore las condiciones para garantizar un nivel adecuado de seguridad en estas soluciones SATCOM (Means, y Meganathan, 2023: 1479-1484).

## 5.2. Vectores de MILSATCOM actuales

Para caracterizar la demanda actual de SATCOM para las Fuerzas Armadas con altos estándares de exigencia, podríamos tomar como referencia las especificaciones previstas para la capacidad de los nuevos satélites Spainsat NG que renovarán la capacidad actual.

Los aspectos más relevantes para categorizar a los sistemas MILSATCOM incluyen: el número y tipo de bandas utilizadas, las antenas con doble

polarización, el uso de antenas activas, la gestión de la potencia asignada, la reutilización de frecuencias, la geolocalización de interferencias, la mitigación de interferencias, el control de ganancia automático por canal, el procesamiento digital a bordo, la conectividad entre bandas a bordo, la formación de haces, el salto de haces con reutilización de frecuencias (*Beam hopping*), la protección contra impactos en altura, la vigilancia del entorno, el cifrado de la telemedida y el telecomando, la gestión de la capacidad disponible en satélites de alto rendimiento (HTS-*High Throughput Satellite*), la cobertura máxima o las bandas militares, entre otros.

En sistemas GEO, las grandes plataformas están diseñadas para alojar cargas de pago de gran volumen y cumplen con altos estándares de flexibilidad, capacidad, optimización de energía, adaptabilidad y seguridad.

Sin embargo, estos estándares no son aplicables directamente a sistemas LEO, que se asemejan más a la electrónica de consumo en términos tecnológicos.

Esto plantea desafíos tecnológicos significativos para adaptar los sistemas LEO a las necesidades de defensa, especialmente cuando se despliegan en menor escala que las constelaciones comerciales NGEO.

### 5.3. Parámetros de mercado en SATCOM-LEO

A diferencia de lo anterior, el mercado de sistemas NGEO está desafiando a los operadores tradicionales de SATCOM GEO, ganando terreno en casos de uso específicos, no solo dentro del sector comercial, sino colaborando con el sector gubernamental y apoyando con éxito al sector militar, como es el caso de la guerra de Ucrania.

Los modelos de gestión de los impulsores del *New Space* son fruto de una serie de factores que, en realidad, no difieren significativamente de los parámetros de mercado más destacados del sector SATCOM tradicional, aunque haya que prestar atención a los matices.

Cuando analizamos la posición del *New Space* en el mercado (Voicu, Bhattacharya y Petrova, 2021), encontramos que existe una alta demanda, donde se busca personalizar la prestación de servicios al máximo, ampliar la cobertura de la solución global, mejorar los parámetros específicos de cada caso de uso y reducir tarifas mediante economías de escala. Estos mismos principios se aplican a los operadores GEO, aunque con enfoques operativos diferentes según el régimen desde el que proporcionan la capacidad.

A pesar de las similitudes en los principios de mercado, los operadores NGEO se benefician (y enfrentan a desafíos) debido a sus enfoques operativos únicos. Basta con hacer un recorrido por los parámetros tipo que

caracterizan una demanda, tanto para GEO como para NGEO (capacidad, frecuencias, latencias, anchos de banda, resiliencia...), para reconocer el valor de la intensidad de la irrupción del *New Space* en el sector SATCOM.

### 5.4. Resiliencia y protección en el entorno de amenazas actuales

Quizá de todos los parámetros referidos, sea la resiliencia uno de los que hoy día más se emplean para resolver esta comparativa, esta disyuntiva entre GEO y NGEO.

Le resiliencia se refiere a «la capacidad de un sistema para resistir perturbaciones y recuperarse rápidamente, retornando a su estado inicial». Esto incluye la prevención, la robustez, la reconstitución y la recuperación, se ha convertido en un criterio fundamental para evaluar sistemas espaciales alternativos, incluidas las constelaciones, independientemente de su tamaño.

Para el contexto del presente artículo sobre las capacidades espaciales SATCOM, vamos a considerar cuatro parámetros principales para analizar la resiliencia de un sistema: evitar eventos adversos, robustez de los sistemas, reconstitución de sistemas dañados o degradados y recuperación a la situación inicial.

– Evitar eventos adversos: este primer nivel de resiliencia implica la capacidad de prevenir y anticipar eventos que puedan afectar negativamente al sistema. Esto incluye la detección temprana de amenazas, como la radiación espacial o la interferencia intencionada, y la implementación de medidas preventivas.

– Robustez de los sistemas: se refiere a la capacidad de los sistemas para resistir y soportar eventos adversos sin sufrir daños significativos. Esto implica el diseño de componentes y sistemas capaces de soportar condiciones extremas, como las radiaciones espaciales y las variaciones en la temperatura.

– Reconstitución de sistemas dañados o degradados: incluso con medidas preventivas y una robustez adecuada, los sistemas pueden enfrentar situaciones en las que se dañen o degraden. La capacidad de reconstituir estos sistemas de manera eficiente y rápida es esencial. Esto incluye la redundancia de componentes críticos y procedimientos de recuperación y, en caso extremo, la reposición de un nuevo satélite y retirada del dañado.

– Recuperación a la situación inicial: la resiliencia completa implica la capacidad de volver al estado normal después de una interrupción. Esto implica la restauración de servicios sin problemas y la minimización del tiempo de inactividad.

La resiliencia en los sistemas de comunicaciones por satélite no solo garantiza la continuidad de las operaciones, sino que también es esencial para respaldar aplicaciones críticas, como la comunicación en situaciones de emergencia y la seguridad nacional. El diseño y la implementación efectiva de estos cuatro parámetros son esenciales para mantener la integridad y la eficacia de los sistemas satelitales en un entorno cada vez más complejo y desafiante.

En 2012, se emitieron recomendaciones basadas en entrevistas a actores clave del sector SATCOM de cara a determinar el impacto de la resiliencia en la decisión de la corriente a seguir (figura 8). A pesar de tesis posteriores (Turner, 2014) para determinar una metodología para el cálculo de la resiliencia en sistemas SATCOM, el reto es emprender un estudio específico que incline la balanza a favor de sistemas GEO o NGEO.

La resiliencia en sistemas satelitales NGEO, como los que operan en órbitas bajas de la Tierra, es fundamental para garantizar la continuidad de las comunicaciones y servicios críticos en situaciones adversas. Es uno de los argumentos principales en los análisis comparativos entre ambas corrientes.

Ya se ha comentado que, en esa comparativa, hay factores que son a favor de los sistemas NGEO, tales como su capacidad de resistir ante la radiación espacial, si bien tiene una mayor exposición a colisiones con desechos espaciales y ataques cibernéticos, sus componentes mayoritariamente *Commercial On the Shell* (COTS) (Rawlins, Baker y Martinovic, 2022) no parecen mejorar su capacidad de recuperarse rápidamente de posibles interrupciones en la señal.

| Interview Findings |
|---|
| 1. There is either a lack of consensus on the definition of the term 'resilience' or unfamiliarity with the term. |
| 2. A successful program will require an education and training component. |
| 3. Participation in resilience depends directly on costs versus benefits and a demonstrated return on investment. |
| 4. Optimally, resilience should be initiated in the design process and considered throughout the entire building lifecycle. |
| 5. Definitions of resilience tend to vary by industry. For example, the insurance sector strongly ties resilience to 'risk' and 'risk management,' while planners expressed the need for 'recovery' and 'continuity of operations' after an event or disaster. |
| 6. Building resilience extends beyond maintaining the building envelope and includes dependence upon the infrastructure required to operate the business conducted in the building. |
| 7. Interviewees mentioned that a public-private sector partnership model is important to the success of the program. |

**Figura 8. Tabla de resultado de entrevistas. Jennings et al., 2012**

La resiliencia en los sistemas NGEO implica el uso de tecnologías avanzadas de detección y corrección de errores, así como la redundancia en componentes clave. Estos factores, sumados a la supuesta rápida reposición de satélites dañados o degradados, aseguran que esta corriente va a seguir siendo una parte vital de nuestras infraestructuras de comunicación global.

Para profundizar sobre factores concretos a considerar en cuanto a resiliencia en sistemas NGEO, se recomienda acudir a los estudios sobre el uso de cadenas de Márkov[2] y enfoques analíticos, también son relevantes para evaluar la resiliencia de estos sistemas que trascienden del concepto tradicional de constelación para pasar a formar parte de un concepto más avanzado y plenamente relevante en el empleo del espacio para sistema de Defensa, tales como la componente SATCOM de una nube de combate.

## 6. ¿Complementariedad o sustitución? El debate sobre el futuro de las comunicaciones por satélite

En el sector de las comunicaciones por satélite, ya hemos identificado y caracterizado las dos corrientes que dan respuesta a las necesidades de hiperconectividad que requieren los diferentes casos de uso, en este momento del tiempo.

Dos son las teorías divergentes que están en pleno debate: la complementariedad de los sistemas NGEO con los sistemas GEO frente a la sustitución de estos últimos por los sistemas LEO.

Hemos visto que hay factores que apoyan la teoría de la complementariedad, la cual argumenta que los sistemas NGEO, no solo pueden coexistir, sino también mejorar las soluciones que utilicen capacidades SATCOM, sobre la base de los sistemas GEO existentes.

Estos satélites NGEO, situados en órbitas más bajas, que pese a algunas limitaciones, ya referidas en apartados anteriores, ofrecen ventajas como la menor latencia o la mayor velocidad y capacidad en la transmisión de datos, están ocupando un papel relevante en aplicaciones como Internet de las cosas y comunicaciones móviles, que sin duda complementan al portfolio de aplicaciones previstas por los satélites GEO, ideales para usos con necesidad de mayor cobertura y gran estabilidad en el apuntamiento de sus antenas. Esto permitiría una mayor flexibilidad y calidad en los servicios de comunicación.

[2] Las series de Markov permiten producir cadenas para analizar un número elevado de sucesos asociados, con el objetivo de obtener un resultado que defina la mejor respuesta a un evento, para producir el adecuado nivel de resiliencia.

Por otro lado, la teoría de la sustitución, principalmente alimentada por condicionantes de mercado y la intensidad del empuje de los actores privados del *New Space*, defiende que los satélites LEO son el futuro y deberían reemplazar gradualmente a los sistemas GEO.

La órbita baja ofrece una latencia significativamente menor, lo que mejora la experiencia del usuario en aplicaciones sensibles al retraso, como las videoconferencias. Además, la menor altitud en la que operan, si bien debe ser tenida en cuenta por parte de los sistemas de vigilancia espacial de cara al aumento de la densidad de sistemas operativos, facilita la eliminación de desechos espaciales y reduce los costos de lanzamiento.

## 7. Conclusiones del estudio

Considerando las diferentes perspectivas sobre modelos de gobernanza, corrientes de decisión en niveles nacionales e internacionales y el dinámico desarrollo de las telecomunicaciones por satélite, surge una pregunta crucial en torno a la estrategia y economía de la industria espacial y las empresas de telecomunicaciones, ¿es prudente continuar invirtiendo en la modernización de los sistemas GEO mientras los sistemas NGEO avanzan o deberíamos enfocarnos en una transición hacia sistemas LEO más avanzados para mantener la relevancia?

La respuesta dependerá de cómo se resuelven en el tiempo las incógnitas que han surgido al analizar los diversos factores planteados en el presente artículo, es decir, cómo se resuelven en el tiempo, las incógnitas presentadas en la matriz de hipótesis de la figura 7.

Para ello, se deberá prestar especial atención a los factores más destacables de cuantos se han empleado en la referida matriz, tales como la seguridad, estandarización, modelos de gobernanza, resiliencia, protección ante amenazas y la complementariedad con los sistemas SATCOM existentes, como si de indicadores de la evolución de esta disyuntiva se tratase.

## 8. Reflexiones para la hoja de ruta

Finalmente, una vez analizado el estado de cada una de las dos corrientes y sus posibles modelos de relación, podemos mantener que, en el actual escenario de las comunicaciones satelitales, especialmente en aplicaciones militares y de seguridad, se vislumbran dos enfoques fundamentales.

Por un lado, en situaciones que exigen un rendimiento excepcional, rigurosos estándares y una perfecta interoperabilidad, se perfilan nuevos desarrollos específicos que dependerán de la disponibilidad presupuestaria, tecnológica e industrial.

Por otro lado, en entornos más versátiles y disruptivos donde se permite un uso dual sin poner en riesgo la seguridad operativa, entran en juego factores más amplios como la demanda del mercado, inversiones en investigación y desarrollo y la colaboración a nivel internacional.

La resolución de este debate es de suma importancia, ya que marcará el rumbo de las comunicaciones satelitales en las próximas décadas. Las visiones de complementariedad y/o sustitución que se han expuesto, representan dos perspectivas distintas del futuro, en medio de la reestructuración del sector. A pesar de la intensidad de la irrupción de los nuevos actores, parece prematuro asegurar el modelo que prevalecerá en la era de la conectividad global y la habitabilidad del espacio.

Indudablemente, esta disyuntiva debe ser abordada en los actuales desarrollos de los sistemas de armas del futuro, en cuyo concepto se requiera disponer de una «nube de combate», respaldada por comunicaciones satelitales de máxima conectividad.

Todavía es temprano para determinar si esta «nube de combate» será una parte integral de la solución global para la hiperconectividad necesaria en los planes de exploración hacia la Luna o Marte, o si, por el contrario, se configurarán como escenarios independientes debido a las diferencias en los factores más restrictivos desde la perspectiva de su uso en las Fuerzas Armadas.

Lo que sí se puede afirmar es que, una vez iniciada la renovación de la actual capacidad GEO SATCOM, parece que el ciclo de decisión respecto del empleo, complementario o sustitutivo, de activos NGEO para las FAS, con las reservas oportunas, debería ser mucho más reducido y sincronizar con los movimientos que se inicien a nivel internacional, en los diferentes contextos de seguridad y defensa en que se requiera de nuestros esfuerzos.

## 9. Bibliografía

Al-Hraishawi, H. *et al.* (2022). *A survey on non-geostationary satellite systems: The communication perspective*. IEEE Communications Surveys & Tutorials.

Borek, R., Woźnica, J. y Malawski, M. (2021). *The satellite constellations in the respond to the governmental and military technological requirements of the current space communication trends.*

Del Portillo, I., Cameron, B. G. y Crawley, E. F. (2019). *A technical comparison of three low earth orbit satellite constellation systems to provide global broadband.* Acta astronáutica. 159, pp. 123-135

Gómez-Barroso, J. L. y Feijóo, C. (2010). *A conceptual framework for public-private interplay in the telecommunications sector*. Telecommunications Policy. 34(9), pp. 487-495.

Guerster, M. *et al.* (2023). *Contract Structures for SatCom: How will Competition from LEO Mega Constellations Change How Communications Services Are Purchased?* Disponible en: https://www.liebertpub.com/doi/abs/10.1089/space.2022.0020

Höfner, K., Vahl, A. y Stoll, E. (2018). Cost-efficient satellite constellation design by network reliability analysis. *Annual Reliability and Maintainability Symposium (RAMS)*. IEEE, pp. 1-6.

Judice, A., Livin, J. y Venusamy, K. (2022). Research trends, challenges, future prospects of Satellite Communications. *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*. IEEE, pp. 1140-1143.

Klein, J. J. (2019). *Rethinking Requirements and Risk in the New Space Age.* Center for New American Media.

Kodheli, O. *et al.* (2020). *Satellite communications in the new space era: A survey and future challenges*. IEEE Communications Surveys & Tutorials. 23(1), pp.70-109

Manulis, M. *et al.* (2021). Cyber security in new space: analysis of threats, key enabling technologies and challenges. *International Journal of Information Security*. 20, pp. 287-311.

Means, R. y Meganathan, R. (2023). Blockchain and QKD Protocol-based Security Mechanism for Satellite Networks. *2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS).* IEEE, pp. 1479-1484.

Quintana, E. (2017). The new space age: Questions for defence and security. *The RUSI Journal*. 162(3), pp. 88-109.

Rawlins, F., Baker, R. y Martinovic, I. (2022). *Death By A Thousand COTS: Disrupting Satellite Communications using Low Earth Orbit Constellations.* Disponible en: https://doi.org/10.48550/arXiv.2204.13514

Sánchez Mayorga, J. L. (2021). *La colaboración público-privada en la obtención de capacidades espaciales: evaluación a través de la metodología MAPS y optimización bajo entornos de agencia* [tesis doctoral]. Jorge Rosell Martínez. Zaragoza, Universidad de Zaragoza.

Stock, G. *et al.* (2022). *On the Automation, Optimization, and In-Orbit Validation of Intelligent Satellite Constellation Operations.* Disponible en: https://doi.org/10.48550/arXiv.2210.11171

Tedeschi, P., Sciancalepore, S. y Di Pietro, R. (2022). *Satellite-based communications security: A survey of threats, solutions, and research challenges.* Computer Networks. 109246.

Tonkin, S. y De Vries, J. P. (2018). *New Space spectrum sharing: Assessing interference risk and mitigations for new satellite constellations.* TPRC.

Townsend, B. R. (2017). *A small revolution in space: An analysis of the challenges to US military adoption of small satellite constellations.* School Of Advanced Air And Space Studies Air University Maxwell Afb.

Turner, J. (2014). *A Methodology For Measuring Resilience in a Satellite-Based Communication Network* [tesis]**.** Air Force Institute of Technology. Department of Air Force. Air Force University.

Vernile, A. (2018). The rise of private actors in the Space Sector. Springer, Cham.

Voicu, A. M., Bhattacharya, A. y Petrova, M. (2021). *Towards global and limitless connectivity: The role of private NGSO satellite constellations for future space-terrestrial networks.* Disponible en: https://doi.org/10.48550/arXiv.2107.10811

Capítulo 2

# Realidad y futuro de las redes móviles de nueva generación en el ámbito militar

*Montserrat Valdés Quintana*

**Resumen**

Este artículo trata de profundizar en la revolución que suponen las redes de nueva generación, especialmente en el ámbito militar. Se anticipa que el 5G, siendo una tecnología disruptiva, traerá consigo innovaciones significativas, pero también despierta interrogantes sobre sus posibles limitaciones. Es crucial seguir de cerca los proyectos 5G en el Ministerio de Defensa, pues definirán cómo se integrará esta red en el ecosistema militar. A nivel global, se realiza un análisis de las principales iniciativas y proyectos en el ámbito OTAN y de la Agencia Europea de Defensa (EDA), entre otros. Además, el artículo vislumbra el futuro de las redes, especulando sobre tecnologías futuras como el 6G y 7G, aún en etapas tempranas de conceptualización. En esencia, el 5G promete ser un catalizador de cambio en diversos sectores y es imperativo entender sus beneficios y desafíos.

**Palabras claves**

Disruptivo, 5G, IoT, IA, Latencia, *Open* RAN, *Non-Stand Alone* (NSA), *Stand Alone* (SA), *Edge Computing*, *Network Slicing*, Ciberseguridad.

## *Reality and future of new generation mobile networks in the military field*


### *Abstract*

*The purpose of this article is to explore the revolution that next-generation networks will bring, particularly in the military domain. As a disruptive technology, 5G is expected to bring significant innovation, but it also raises questions about its potential limitations. It is vital to closely monitor 5G projects within the Ministry of Defense, as they will determine how this network will be integrated into the military ecosystem. Globally, an analysis is conducted on the main initiatives and projects within NATO and the European Defense Agency (EDA), among others. Furthermore, the article provides a glimpse into the future of networks, speculating on upcoming technologies like 6G and 7G, which are still in the early stages of conceptualization. In essence, 5G promises to be a catalyst for change across multiple sectors, and it is imperative to understand its benefits and challenges.*



### *Keywords*

*Disruptive, 5G, IoT, AI, Latency, Open RAN, Non-Stand Alone (NSA), Stand Alone (SA), Edge Computing, Network Slicing, Cybersecurity.*

## 1. Introducción

En los últimos años el desarrollo de las redes de nueva generación ha sido un tema de gran relevancia en diversos sectores, incluido el ámbito militar. En este contexto, el despliegue del 5G ha marcado un hito significativo en el campo de las comunicaciones y ha abierto un amplio abanico de posibilidades, en términos de conectividad, velocidad y capacidades tecnológicas. En el marco de las tecnologías emergentes y disruptivas (EDT) el 5G se ha postulado como una tecnología de interés y con gran impacto futuro, además de abrir la visión y seguimiento de su evolución futura a la tecnología 6G; incluso se empieza a postular la futura evolución y uso del 7G.

En la era de la digitalización y la conectividad global, las redes de telecomunicaciones han experimentado una evolución sin precedentes. Desde las primeras señales de radio hasta la actualidad, hemos presenciado el nacimiento y desarrollo de tecnologías que han transformado nuestra forma de comunicarnos y de interactuar con el mundo. En este contexto, la quinta generación de tecnologías de telecomunicaciones, conocida como 5G, ha surgido como un hito revolucionario, prometiendo velocidades de conexión ultrarrápidas, muy baja latencia y una capacidad de red masiva.

Desde la mejora de la conectividad en áreas rurales hasta la habilitación de ciudades inteligentes y la Internet de las Cosas (IoT), las redes de nueva generación tienen el potencial de remodelar nuestra sociedad y economía. En el campo de batalla moderno, la información y la comunicación son tan vitales como las armas y la estrategia. Con la llegada de las redes de nueva generación, como el 5G, las Fuerzas Armadas de todo el mundo están experimentando una transformación radical en la forma en que operan y se comunican. En particular las Fuerzas Armadas españolas, reconocidas por su compromiso con la innovación y la modernización, están liderando el camino en la adopción de estas tecnologías emergentes. Pero ¿qué implicaciones tiene esta evolución para el futuro del combate y la defensa?

Este artículo explora la evolución de las redes de nueva generación, con un enfoque particular centrado en el 5G y sus futuras evoluciones, focalizando en su aplicación para las Fuerzas Armadas. Analizaremos cómo el 5G y las tecnologías futuras están cambiando las comunicaciones actuales y la cara de la guerra moderna, desde la mejora de la comunicación en el campo de batalla hasta la habilitación de sistemas de armas autónomos y la inteligencia en tiempo real. Para ello, deberemos abordar algunas de las principales características técnicas del 5G y sus cambios respecto a tecnologías anteriores como el 4G.

Además, examinaremos los desafíos y las oportunidades que estas tecnologías presentan, tanto desde un punto de vista operativo como de seguridad. A medida que nos adentramos en la era del 6G y más allá, las

implicaciones para la seguridad nacional y la defensa global son enormes. Todo ello, abordando también la perspectiva, proyectos e iniciativas a nivel OTAN, EDA y Ministerio de Defensa, así como de la Unión Europea y España.

## 2. Una vista al pasado y evolución de las comunicaciones móviles en el ámbito militar

La evolución de las comunicaciones en el ámbito militar ha sido un factor determinante en la forma en que las Fuerzas Armadas operan, coordinan y toman decisiones estratégicas. A lo largo de la historia, desde la comunicación visual y el uso de mensajeros hasta las tecnologías de última generación, las comunicaciones militares han avanzado de manera significativa para adaptarse a las necesidades cambiantes del combate y la seguridad nacional. En este artículo, exploraremos la evolución de las comunicaciones militares a lo largo del tiempo, desde los primeros sistemas hasta las redes de comunicaciones modernas y futuras.

El desarrollo de las comunicaciones militares se remonta a la antigüedad, cuando los ejércitos confiaban en señales visuales y sonoras para transmitir mensajes. Sin embargo, estas formas de comunicación tenían limitaciones en términos de alcance y velocidad, lo que dificultaba la coordinación en el campo de batalla. Con el avance de la tecnología, surgieron sistemas más sofisticados para las comunicaciones militares. Durante la Primera y Segunda Guerra Mundial, las Fuerzas Armadas utilizaron sistemas de telegrafía y teléfonos de campo para transmitir mensajes de manera más rápida y segura. Estos avances permitieron una mejor coordinación y control de las operaciones militares, en comparación con los métodos anteriores.

El siguiente hito importante en la evolución de las comunicaciones militares fue el desarrollo de las radios. La introducción de la radiotelegrafía y la radiotelefonía permitió la comunicación inalámbrica a larga distancia, lo que revolucionó las operaciones militares. Las radios portátiles y los sistemas de radio en vehículos y aeronaves proporcionaron una comunicación rápida y eficiente en tiempo real, lo que posibilitó una toma de decisiones más ágil y una mayor flexibilidad en el campo de batalla.

A medida que las tecnologías de comunicación avanzaban, los militares también se dieron cuenta de la necesidad de proteger sus comunicaciones de las interferencias y el espionaje. Surgieron técnicas de codificación y cifrado para garantizar la seguridad de los mensajes transmitidos. El desarrollo de sistemas de cifrado cada vez más sofisticados y la aplicación de protocolos de seguridad se convirtieron en una parte integral de las comunicaciones militares.

Con la llegada de la era digital las comunicaciones militares se han vuelto aún más complejas y avanzadas. Las redes de área amplia (WAN) y las redes de área local (LAN) se han utilizado para interconectar unidades y bases militares, permitiendo una comunicación rápida y segura entre diferentes puntos geográficos. Los sistemas de satélites han proporcionado una conectividad global, permitiendo una comunicación continua en cualquier parte del mundo. Además, el desarrollo de tecnologías móviles ha permitido a los ejércitos comunicarse de manera efectiva, incluso en movimiento.

En la actualidad, las Fuerzas Armadas están adoptando tecnologías de vanguardia, como el 5G, para mejorar aún más sus capacidades de comunicación. El 5G ofrece velocidades de transmisión de datos mucho más rápidas y una menor latencia, lo que permite una comunicación en tiempo real y el uso de aplicaciones y dispositivos más avanzados en las operaciones militares. Además, con el impulso de organizaciones internacionales como la EDA y OTAN, se están explorando y desarrollando tecnologías futuras, como el 6G que prometen una mayor velocidad, eficiencia y capacidades de comunicación.

## 3. 5G, ¿en qué consiste y qué nos ofrece?

El avance tecnológico ha llevado a la creación de redes de comunicación cada vez más rápidas y eficientes. El 5G, la quinta generación de tecnología inalámbrica, ha emergido como un hito significativo en el ámbito de las comunicaciones. En este artículo exploraremos qué es el 5G, sus avances respecto a tecnologías anteriores, al igual que las posibilidades inmediatas y futuras que ofrece.

Esta quinta generación de tecnología inalámbrica representa un salto significativo respecto a sus predecesoras. Se caracteriza por ofrecer una mayor velocidad de transmisión de datos, menor latencia y mayor capacidad de conexión en comparación con el 4G y otras tecnologías anteriores. Estas mejoras permiten una comunicación más rápida y eficiente, impulsando el desarrollo de nuevas aplicaciones y servicios.

Ha superado las limitaciones de sus predecesoras en varios aspectos. En términos de velocidad, el 5G ofrece velocidades de descarga y carga mucho más rápidas (hasta 10 Gbps), lo que permite transmitir grandes cantidades de datos en cuestión de segundos. La baja latencia del 5G reduce significativamente el tiempo de respuesta entre dispositivos, bajando de los doscientos milisegundos que permitía el 4G a un milisegundo; lo que es crucial para aplicaciones que requieren una interacción en tiempo real, como los vehículos autónomos o la telemedicina. Además, el 5G permite una mayor capacidad de conexión simultánea, lo que facilita la conexión de una gran cantidad de dispositivos en un área determinada.

El futuro del 5G es prometedor, ya que ofrece un amplio abanico de posibilidades en diversas áreas. En términos de aplicaciones móviles, el 5G permitirá una experiencia de usuario mejorada, con descargas más rápidas, transmisión de video de alta calidad y juegos en línea sin problemas. Además, impulsará el desarrollo de otras EDT, como el Internet de las Cosas (IoT), la Inteligencia Artificial (IA) y la Realidad Virtual (RV), al proporcionar la conectividad necesaria para que estas tecnologías funcionen de manera eficiente.

En el sector industrial, impulsará la automatización y la digitalización de los procesos de fabricación, lo que llevará a la creación de fábricas inteligentes y sistemas de logística más eficientes, algo que interacciona directamente con el ámbito militar (como veremos más adelante en un proyecto actual del Ministerio de Defensa-MDEF). Tendrá un impacto significativo en sectores como el transporte, la salud, la energía y la agricultura, al permitir una mayor conectividad y eficiencia en estas áreas.

En cuanto a las posibilidades inmediatas del 5G, se está llevando a cabo su despliegue por todo el mundo. Las redes 5G comerciales están siendo implementadas en áreas urbanas y se espera que se expandan rápidamente a nivel global. Con la expansión en curso y las posibilidades inmediatas que ofrece, promete cambiar la forma en que nos comunicamos, trabajamos y vivimos en un futuro cercano. Estamos al borde de una nueva era de conectividad que transformará nuestra sociedad y abrirá la puerta a innumerables oportunidades tecnológicas.

Podríamos destacar entre las necesidades de uso futuro y sus aplicaciones las siguientes:

– Soporte a comunicaciones con baja latencia y alta fiabilidad en comunicaciones centradas en personas: respuesta instantánea, aplicaciones sanitarias o juegos en línea.

– Soporte a comunicaciones con baja latencia y alta fiabilidad en comunicaciones centradas en máquinas: *machine to machine* (M2M) con necesidades de tiempo real.

– Soporte a altas densidades de tráfico: aglomeraciones de público (estadios, centros comerciales...).

– Mantener alta calidad con alta movilidad: ofrecer alta calidad de experiencia en vehículo de alta velocidad (coches, trenes).

Por otra parte, una vez expuestos los avances y posibilidades que habilita esta tecnología, cabe abordar su análisis desde una perspectiva más técnica. El 5G ha supuesto un cambio de paradigma en muchos sentidos, para ello, abordaremos de manera breve algunos de sus rasgos más característicos.

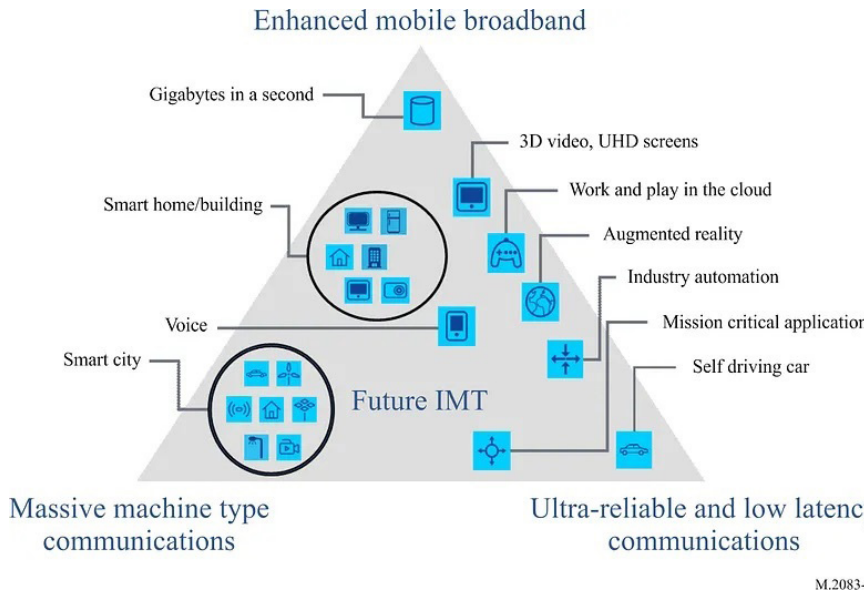



**Figura 1. Aplicaciones del 5G en torno a sus características más relevantes. Fuente: ETRI graphic, de ITU-R IMT 2020 requirements**

En primer lugar, a nivel europeo se identificaron tres bandas de frecuencia para el despliegue inicial de la tecnología; la banda de 700 MHz, la de 3,4 a 3,8 GHz y la de 26 GHz. Siendo la banda intermedia la seleccionada principalmente por las operadoras para los despliegues iniciales de la tecnología aquí en España, en la que se ha tenido que trabajar en una reorganización y realizar las subastas de espectro pertinentes. Por lo que realizando un breve resumen respecto al espectro de frecuencia destacaríamos los siguientes conceptos:

– Ondas milimétricas (mmWave): esta modalidad opera en bandas de frecuencia extremadamente altas (generalmente en el rango de 24 a 100 GHz), lo que permite velocidades de datos inigualables, a menudo superando 1 Gbps. Sin embargo, las ondas milimétricas tienen una desventaja significativa, su alcance es muy limitado y tienen dificultades para penetrar edificios o incluso la lluvia. Este tipo de 5G es ideal para áreas urbanas densas y lugares con alta demanda de datos, como estadios o centros de conferencias.

– Espectro de banda media: este espectro ofrece un equilibrio entre velocidad y cobertura, operando en el rango de 2,4 a 4,2 GHz. Aunque sus velocidades de datos son inferiores a las de las ondas milimétricas, supera ampliamente a las redes 4G actuales y puede cubrir áreas más grandes, haciendo de este un enfoque útil para las áreas metropolitanas.

– Espectro de banda baja: funcionando en el rango de 600 a 700 MHz, esta modalidad proporciona la mayor cobertura, pero con velocidades de datos más bajas. Sin embargo, estas velocidades aún podrían ser superiores a las de la 4G actual, el alcance mejorado es esencial para brindar cobertura 5G a áreas rurales y suburbanas.

Estos tres casos de uso ilustran la versatilidad de la tecnología 5G y las mejoras significativas que aportará en comparación con las generaciones anteriores de tecnología de comunicación inalámbrica.

Entre las principales modalidades de 5G vamos a señalar las siguientes:

– eMBB (*Enhanced Mobile Broadband*): se enfoca en proporcionar comunicaciones de banda ancha con velocidades de pico de 1 Gbit/s, mejorando significativamente la capacidad y la eficiencia de la red inalámbrica. Esta modalidad de 5G permite velocidades de descarga y carga mucho más rápidas en comparación con las generaciones anteriores de redes móviles como el 4G. Es ideal para aplicaciones que requieren un ancho de banda elevado, como *streaming* de video en alta definición, Realidad Virtual (VR), Realidad Aumentada (AR), juegos en línea y descarga rápida de archivos.

– uRLLC (*Ultra-Reliable and Low Latency Communications*): se centra en ofrecer servicios con una fiabilidad superior al 99,999 % y con una latencia extremadamente baja, inferior a 1 ms. Esta modalidad se utiliza en aplicaciones que requieren una conexión instantánea y sin demoras, donde la confiabilidad es fundamental. Ejemplos de aplicaciones que se benefician de uRLLC son los servicios de emergencia, el control remoto de maquinaria industrial, los vehículos autónomos, la telecirugía y las redes de energía inteligentes.

– mMTC (*Massive Machine Type Communications*): se dirige a la comunicación masiva entre máquinas (M2M) y dispositivos IoT. Esta modalidad permite la conexión simultánea de una gran cantidad de dispositivos con requisitos de ancho de banda más bajos, pero con una mayor eficiencia en términos de consumo de energía y cobertura de red. Es utilizado en aplicaciones como ciudades inteligentes, monitoreo ambiental, seguimiento de activos, gestión de tráfico y agricultura de precisión.

Otro aspecto relevante que comentar respecto a la tecnología de acceso radio es el concepto de *Open* RAN (Red de Acceso de Radio Abierta). Se refiere a una arquitectura de red de acceso de radio (RAN) que está basada en estándares y especificaciones abiertas. Esto permite que diferentes componentes de la RAN, como el *hardware* y el *software*, sean interoperables, independientemente del fabricante. Entre los beneficios de esta tecnología destacan:

– Flexibilidad: las operadoras pueden mezclar y combinar diferentes componentes de diferentes proveedores.

– Innovación: al ser una arquitectura abierta, fomenta la innovación y permite que nuevos actores entren en el mercado.

– Reducción de costos: puede llevar a una reducción de costes al permitir una mayor competencia entre proveedores y evitar el bloqueo entre ellos.

Este modelo de arquitectura resulta muy interesante en el despliegue de 5G, precisamente por proporcionar una infraestructura de red más flexible y adaptable.

Si seguimos avanzando en términos relevantes respecto al despliegue de esta tecnología, en el desarrollo inicial de 5G, la 3GPP (Sultan, 2022) hizo una propuesta de transición a 5G en dos fases; con los modos *Non-Stand Alone* (NSA) y *Stand Alone* (SA). La inicial fue desarrollada en la *Release* 15 3GPP con el despliegue del modo no autónomo, el NSA, que se basa en el aprovechamiento y reutilización de parte de la infraestructura 4G. La segunda fase, *Release* 16 o 5G SA (5G completo), requiere de la utilización de nuevos elementos *hardware*.

El modo NSA en 5G es una configuración en la que la red 5G se implementa en combinación con la infraestructura 4G existente. En otras palabras, 5G NSA utiliza la red 4G para algunas funciones, mientras que la interfaz de aire 5G NR se utiliza para otras. Técnicamente cabe destacar:

– Dependencia del núcleo 4G: en NSA la red 5G se apoya en el núcleo 4G (*Evolved Packet Core*, EPC) para ciertas operaciones, como la gestión de la conectividad y la señalización.

– Doble conectividad: los dispositivos en una red NSA pueden estar conectados simultáneamente a las redes 4G y 5G, lo que permite una transición más suave entre las tecnologías.

Sus beneficios en contraposición al despliegue de SA serían:

– Implementación rápida: al aprovechar la infraestructura 4G existente, los operadores pueden lanzar servicios 5G más rápidamente sin tener que construir una red 5G completa desde cero.

– Costo-eficiencia: NSA permite a los operadores ofrecer 5G con una inversión inicial menor, ya que pueden utilizar parte de su infraestructura existente.

– Cobertura amplia: al combinar 4G y 5G, NSA puede ofrecer una cobertura más amplia, especialmente en áreas donde la infraestructura 5G aún no está completamente implementada.

El modo SA en 5G se refiere a una configuración donde la red 5G opera completamente independiente de las redes anteriores, especialmente de la infraestructura 4G. Se trata de una red 5G «pura». Entre sus características técnicas destacan:

– Núcleo 5G (5GC): SA utiliza el núcleo 5G para todas las operaciones de la red. Este núcleo es una arquitectura completamente nueva diseñada para maximizar las capacidades de la tecnología 5G.

– Nuevo radio (NR): SA utiliza la interfaz de aire NR, que es la nueva interfaz de radio estándar para 5G, sin depender de las redes LTE existentes.

Por otra parte, cabe destacar los beneficios que aporta su implementación:

– Latencia ultra baja: SA puede ofrecer latencias de milisegundos o incluso menos, lo que es esencial para algunas aplicaciones como hemos mencionado anteriormente.

– Eficiencia y flexibilidad: al operar con un núcleo 5G, SA puede aprovechar al máximo las capacidades de la tecnología 5G, como la segmentación de la red, que permite a los operadores personalizar la red según las necesidades de diferentes aplicaciones.

– Capacidad mejorada: SA está diseñado para soportar una gran cantidad de dispositivos conectados simultáneamente, lo que es crucial para el IoT.

Mientras que el modo NSA es una solución intermedia que permite a los operadores lanzar 5G rápidamente y con menos inversión inicial, el modo SA representa la verdadera visión de 5G, con todas sus capacidades y beneficios. A medida que la tecnología y la infraestructura evolucionan, se espera que más operadores migren de NSA a SA para aprovechar al máximo las ventajas de 5G. En última instancia, la elección entre SA y NSA dependerá de factores como la estrategia del operador, la inversión requerida, la demanda del mercado y la madurez de la tecnología en una región específica. Ambos modos tienen un papel crucial en la evolución global de 5G.

Por último, los siguientes conceptos son ampliamente utilizados y reflejan tecnologías clave para el desarrollo del 5G:

– *Software Defined Networking* (SDN): esta tecnología permite un control más flexible y eficiente de la red, ya que las decisiones de enrutamiento y gestión de la red se toman mediante *software* en lugar de *hardware*.

– *Network Function Virtualisation* (NFV): su implementación ha permitido que las funciones de la red se realicen en *software* y se ejecuten en servidores estándar, en lugar de requerir un *hardware* especializado. Esto permite una mayor flexibilidad y eficiencia en la gestión de la red.

– *Cloud-Radio Access Network* (C-RAN): es una arquitectura de red que centraliza el procesamiento y la gestión de la red, permitiendo una mayor eficiencia y flexibilidad.

– *Edge computing*: esta tecnología permite que los recursos de computación se ubiquen más cerca de los usuarios, lo que puede mejorar la latencia y la eficiencia de la red.

– *Network slicing*: este concepto permite una separación más clara y una gestión más eficiente del plano de control y del de usuario. El plano de control se encarga de la señalización y el control de la red, mientras que el de usuario se encarga de la transmisión de los datos de estos. El *network slicing* ofrece varios beneficios y posibilidades, pero también presenta algunos desafíos y riesgos. Por ejemplo, en términos de ciberseguridad, un atacante que tenga acceso a la arquitectura de servicio 5G podría explotar un fallo en el diseño de los estándares de *network slicing* para acceder a datos en «múltiples rebanadas». Por lo tanto, es crucial implementar medidas de seguridad adecuadas para proteger contra estas amenazas.

Habiendo analizado desde un punto de vista técnico la tecnología 5G, podemos terminar abordando en este apartado, los desafíos en términos de seguridad y resiliencia de este tipo de comunicaciones desde la perspectiva militar. Aunque *a priori* se podría afirmar que el despliegue de una red 5G privada sería el escenario de implementación que mejor se adapta a las necesidades de las Fuerzas Armadas, debido a requisitos técnicos y/o legislativos, no siempre será la mejor opción. Por lo tanto, es necesario realizar un análisis de seguridad de las redes 5G públicas y privadas, en qué casos de uso la implementación de cada tipo resulta más interesante y beneficiosa. Ya que no podemos dejar de lado, el hecho del gran potencial de 5G para cambiar y mejorar las operaciones y capacidades en el ámbito militar.

Por lo que detallando más específicamente capacidades y casos de uso, que se han mencionado a lo largo de este apartado, y que pueden tener implicaciones tanto en el ámbito civil como el militar, cabe destacar:

– Comunicaciones mejoradas: la mayor velocidad de transmisión de datos y la latencia reducida del 5G pueden permitir una comunicación más rápida y eficiente en operaciones militares, incluyendo videoconferencias en tiempo real y transferencia de información crítica durante misiones.

– Vehículos no tripulados: la baja latencia del 5G puede mejorar el control y la eficiencia de los vehículos no tripulados, como drones y vehículos terrestres no tripulados. Esto puede permitir misiones de reconocimiento más efectivas y seguras.

– Realidad aumentada y virtual: la mayor velocidad de datos puede permitir el uso más efectivo de la realidad aumentada y virtual en entrenamiento militar y en el campo de batalla. El personal de Fuerzas Armadas podría tener acceso a información en tiempo real superpuesta en su campo de visión, como mapas, información del objetivo y más.

– Redes de sensores: el 5G puede permitir el uso de redes de sensores, más grandes y efectivas, en el campo de batalla. Los sensores pueden recopilar información sobre el entorno, detectar movimientos enemigos y mejorar la conciencia situacional.

– Ciberseguridad: aunque el 5G puede presentar nuevos desafíos de ciberseguridad, también tiene el potencial de mejorar la seguridad de las comunicaciones militares, mediante el uso de técnicas avanzadas de cifrado y autenticación. Abordaremos este tema con mayor profundidad más adelante.

– Telemetría y control de misiones: la velocidad y la capacidad de la red 5G pueden permitir un mejor seguimiento y control de las misiones militares.

– Telemedicina: la baja latencia y la alta velocidad del 5G pueden permitir aplicaciones de telemedicina en el campo de batalla, permitiendo que los médicos traten a heridos en tiempo real, a pesar de las distancias.

Es importante tener en cuenta que, aunque el 5G tiene un gran potencial para estas y otras aplicaciones militares, también presenta desafíos, incluyendo la necesidad de construir la infraestructura necesaria, garantizar la seguridad de la red y mitigar las posibles vulnerabilidades de ciberseguridad.

## 4. Evolución futura del 5G

Aunque el presente y futuro inmediato de las redes de nueva generación está centrado en el despliegue definitivo e implantación del 5G, podemos centrar nuestro punto de mira en un futuro a medio plazo, donde diferentes grupos de trabajo ya están trazando la ruta a seguir.

La evolución directa y futura del 5G es la denominada sexta generación de comunicaciones móviles (6G). Actualmente, esta tecnología se encuentra en fase de desarrollo y definición de sus características y especificaciones. Desde la asociación 3GPP se convocó en abril de este año una cumbre que reunió a compañías de telecomunicaciones globales, reguladores, organismos industriales y la parte academia para discutir sobre las posibilidades de negocio y futuras políticas del 6G.

Se espera que su despliegue se haga efectivo en la próxima década y promete revolucionar, de nuevo, la forma en que interactuamos con el mundo

digital. No obstante, expertos señalan (Harsh *et al.,* 2021) que sus primeras aplicaciones podrían ver la luz a partir de 2026, dado el actual escenario de competencia en el sector donde potencias como Estados Unidos, China y Corea del Sur, realizan grandes avances; y el esfuerzo que desde Europa se está realizando.

Aunque aún estamos en las primeras etapas de su desarrollo y diseño, ya podemos vislumbrar los avances significativos que traerá en comparación con las tecnologías de red anteriores. En este contexto, es esencial discutir tanto los avances tecnológicos que implica como las implicaciones normativas que acompañarán a su implementación. Además, es crucial explorar los diversos casos de uso, incluyendo su potencial en el ámbito militar.

6G promete ser el epicentro de una revolución digital sin precedentes. Se espera que esta nueva generación de redes móviles ofrezca velocidades de transmisión de datos que superen ampliamente las capacidades actuales, alcanzando hasta un terabit por segundo (Tbps). Esta velocidad vertiginosa permitirá una conectividad casi instantánea, facilitando la transmisión de grandes volúmenes de datos en fracciones de segundo. Además, se prevé que tenga una latencia extremadamente baja, lo que mejorará significativamente la eficiencia de las comunicaciones, permitiendo una interacción en tiempo real entre dispositivos ubicados en diferentes partes del mundo. También promete una mayor fiabilidad y una cobertura más amplia, lo que permitirá una conectividad ininterrumpida incluso en áreas remotas. Además, se espera que facilite la implementación de redes de sensores masivos, que podrían utilizarse para monitorear y gestionar una amplia gama de aplicaciones, desde el medio ambiente hasta la infraestructura urbana.

Desde una perspectiva normativa, la implementación de la tecnología 6G requerirá una revisión profunda y meticulosa de las políticas y regulaciones actuales. Las autoridades gubernamentales y los organismos internacionales tendrán que trabajar juntos para establecer normas claras que garanticen la seguridad de los datos y la privacidad de los usuarios en esta nueva era digital.

Las regulaciones deberán abordar una serie de cuestiones críticas, incluyendo la asignación de espectro radioeléctrico, que será fundamental para evitar interferencias y garantizar una transmisión de datos fluida. Proveedores como Samsung (Niknam, 2022) ha propuesto considerar para su despliegue todas las bandas que estén disponibles por debajo de 1 GHz, la banda media entre 1 y 24 GHz y por último entre 24 y 300 GHz en banda alta. Aunque habrá que realizar un estudio exhaustivo y considerar las implicaciones en cada país.

Además, será necesario desarrollar estándares internacionales que faciliten la interoperabilidad entre diferentes redes y dispositivos, promoviendo así

una adopción más amplia de la tecnología 6G. Asimismo, las autoridades tendrán que establecer marcos regulatorios que promuevan la competencia justa y eviten la monopolización del mercado por parte de unas pocas empresas gigantes. Esto será crucial para garantizar que la tecnología 6G sea accesible para todos y no solo para unos pocos privilegiados.

En el ámbito civil, la tecnología 6G promete revolucionar una amplia gama de sectores. En el sector de la salud, facilitará la telemedicina y permitirá intervenciones médicas remotas en tiempo real, lo que podría transformar la forma en que se presta la atención médica. Además, en el sector del entretenimiento, se espera que ofrezca experiencias de realidad virtual y aumentada más inmersivas, llevando el entretenimiento a un nuevo nivel. Las ciudades inteligentes serán otro ámbito clave de aplicación, donde la infraestructura urbana podrá comunicarse y coordinarse de manera eficiente para mejorar la calidad de vida de los ciudadanos. Esto incluirá sistemas de transporte inteligente, gestión de residuos optimizada y redes eléctricas más eficientes.

Si nos focalizamos en las implicaciones de su implantación en el mundo militar, la tecnología 6G podría tener aplicaciones significativas, revolucionando la forma en que se llevan a cabo las operaciones militares. La comunicación ultrarrápida y de baja latencia permitirá una mejor coordinación entre diferentes unidades militares, facilitando operaciones más eficientes y seguras. Además, podría facilitar el desarrollo de sistemas de armas autónomas, que podrían operar con una mayor precisión y rapidez, cambiando radicalmente la naturaleza del combate moderno. También se prevé su utilización para mejorar los sistemas de vigilancia y reconocimiento, permitiendo una monitorización más eficaz del campo de batalla y una respuesta más rápida a las amenazas emergentes. Asimismo, se espera que facilite la implementación de redes de comunicaciones seguras, que serían inmunes a las interferencias y los intentos de espionaje, garantizando así la seguridad de las comunicaciones militares.

De hecho, un informe publicado en agosto del pasado año por el Instituto Internacional de Estudios Estratégicos (IISS) (Lee, Nouwens y Tay, 2022) se centraba en la competencia entre Estados Unidos y China por liderar el desarrollo de esta tecnología, desde un punto de vista militar. De este estudio cabe destacar el hecho de que China ha centrado su desarrollo en un modelo de mando centralizado en la aplicación del 6G militar y se afirma que también podrían apoyarse en esta tecnología, para su programa de armas hipersónicas. Por otra parte, la visión estratégica de Estados Unidos se ha focalizado en dotar a los niveles inferiores de mando y operadores de capacidades para tomar la iniciativa en la toma de decisiones críticas. Abordando, por tanto, la sinergia generada con la IA y las técnicas de aprendizaje automático con el 6G para facilitar esta toma de decisiones,

así como el Mando y Control. Además, EE. UU. considera a 6G como un elemento clave para mantener su ventaja militar.

Y aunque este artículo se centre en una visión a corto y medio plazo hasta el 2035, podemos abordar lo que se prevé que sería la evolución lógica de 6G, es decir, la tecnología 7G que aún está en una fase conceptual y no se ha definido completamente. Especularemos, por tanto, sobre las posibles características y oportunidades que podría traer, basándonos en la progresión natural de las tecnologías de red y las tendencias emergentes en el campo de las telecomunicaciones.

Expertos del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), vaticinan que 7G aportará estándares que serán impulsores de mejoras muy significativas para las capacidades de análisis de datos, computación cuántica o IA, entre otros. Podríamos estar hablando de redes no solo ultrarrápidas, sino que posibiliten una flexibilidad en cuanto a punto de conexión y conectividad ubicua, verdaderamente omnipresente. Seguramente se necesiten bandas de frecuencia en terahercios, suponiendo un nuevo reto regulatorio respecto al aumento de frecuencias y regulación de su uso.

Es importante tener en cuenta que estas son especulaciones, basadas en las tendencias actuales. Las características exactas y las capacidades de la tecnología 7G se definirán a medida que se acerque su desarrollo y despliegue. Esto que podría llevarse a cabo en más de dos décadas, según la tendencia actual.

## 5. Desarrollo nacional e internacional del 5G en el ámbito militar

Para abordar este punto, en primer lugar, plantearemos la situación actual de la tecnología a nivel nacional y los proyectos asociados a la misma en el ámbito del Ministerio de Defensa (MDEF). Posteriormente, abriremos este análisis a nivel internacional.

En septiembre de 2022 se firmó el Acuerdo Interdepartamental entre el Ministerio de Asuntos Económicos y Transformación Digital (Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales) y el Ministerio de Defensa (Secretaría de Estado de Defensa) para el desarrollo de proyectos 5G en el MDEF en el marco del programa «UNICO SECTORIAL 5G» y «UNICO 5G CIBERSEGURIDAD-MDEF».

En este acuerdo se señala que bajo el amparo de la Política de Sistemas y Tecnologías de Información y Comunicaciones del MDEF (CIS/TIC), la Arquitectura Global CIS/TIC y el Plan Estratégico de los Sistemas y Tecnologías de la Información y las Comunicaciones del MDEF (PECIS), el MDEF se encarga de hacer un seguimiento continuo de las EDT, centrándose en su aplicación y posibles beneficios para el desarrollo de las

misiones y cometidos del Ministerio. Entre estas tecnologías por supuesto, destaca el 5G, como un elemento facilitador para poder alcanzar estas nuevas misiones y permitir el progreso de las capacidades de la Infraestructura de Telecomunicaciones Inalámbricas de la I3D.

Así pues, mediante la Resolución 307/08135/21 se aprobó también la Estrategia 5G del MDEF que abarca las actuaciones e iniciativas que se llevarán a cabo en el marco del impulso de dicha tecnología, persiguiendo dotar a las Fuerzas Armadas de recursos más allá del ámbito de las comunicaciones móviles que mejoren la eficacia y eficiencia en sus actuaciones.

Bajo todo lo anterior y en el contexto de la situación mundial acontecida desde la crisis del COVID-19, se aprobó por parte de la Comisión Europea y el Consejo de Ministros, en junio de 2021, el Plan de Recuperación, Transformación y Resiliencia (PRTR), como instrumento para la modernización de la economía española, que se apoya en la transformación digital como área clave para la consecución de estos objetivos. La Agenda Digital Española «España Digital 2025», aprobada en julio de 2020, ya definía parte de la hoja de ruta a seguir, apoyada además por la Estrategia de impulso de la Tecnología 5G, aprobada en diciembre de ese mismo año.

La Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales (SETELECO) es la encargada de liderar el componente 15 del PRTR concerniente a la «Conectividad Digital, impulso de la ciberseguridad y despliegue del 5G», en el cual se enmarcan todos los proyectos 5G que se describirán a continuación y que el MDEF llevará a cabo en los próximos tres años.

Tal y como se señala en el Acuerdo para el Ministerio de Defensa, es fundamental contar con comunicaciones basadas en el 5G en el desarrollo de sus distintos ámbitos, haciendo hincapié en el ancho de banda ofrecido, fiabilidad, baja latencia, comunicaciones entre dispositivos y máquinas o los términos anteriormente mencionados como el *network slicing* o el *edge computing*.

Se establecieron, por tanto, dos subproyectos a financiar con los créditos provenientes del PRTR. En primer lugar, los del Programa «UNICO SECTORIAL 5G», que en inicio abordaría ocho proyectos relativos al «despliegue de 5G en actividades económicas clave y en servicios esenciales». Los cuales se describen a continuación:

– Ejército de Tierra

- Ámbito operativo: red 5G ad-hoc de alta capacidad aérea y nube táctica distribuida: FANECT (*Flying Ad-hoc 5G Network & Distributed Mobile Tactical Cloud*)
- Ámbito gestión logística: desarrollo de una red segura de alta velocidad y baja latencia 5G para su futura implantación en la Base Logística del ET (BLET).

- Transversal: acceso a laboratorio con infraestructura 5G y asistencia técnica para desarrollar prototipos que incorporen tecnología 5G para su empleo en las Fuerzas Armadas. Se trata de un proyecto de apoyo al resto de los propuestos.

– Armada:

- Ámbito operativo: establecimiento de comunicaciones de una Fuerza Naval, basada en tecnología 5G, comunicaciones buque/IoT. sensorización y robotización.
- Ámbito operativo: incorporación de comunicaciones de una Fuerza de Infantería de Marina basadas en tecnología 5G.
- Ámbito operativo: comunicaciones 5G en litoral/base Naval.

– Ejército del Aire y del Espacio:

- Ámbito gestión logística: proyecto 5G en apoyo al ámbito de la Logística del Ejército del Aire y del Espacio.

– Unidad Militar de Emergencias (UME):

- Ámbito gestión de emergencias: implementación de la tecnología de telecomunicaciones para el transporte de datos y vídeo que permita facilitar la resolución de emergencias.

De estos ocho subproyectos iniciales, seis fueron adjudicados tras su licitación, a excepción del proyecto transversal del Ejército de Tierra y el de la UME. Actualmente, se está trabajando en redefinir el alcance y costes de ambos, con el fin de publicar una nueva licitación antes de que finalice el año.

Por otra parte, en el subproyecto «UNICO 5G CIBERSEGURIDAD-MDEF» se publicó un único expediente a licitar, centrado en la protección y seguridad para las redes de comunicación del MDEF.

Dicho subproyecto pertenece al ámbito del Estado Mayor de la Defensa, en concreto, su ejecución tendrá lugar en el Mando Conjunto del Ciberespacio, donde se va a implantar un Centro de Desarrollo, Adiestramiento y Pruebas para Operaciones Militares de Ciberdefensa con tecnología 5G (CDAP 5G DEF), que permita reforzar las capacidades de ciberdefensa en sistemas 5G militares. La publicación de este expediente, en concreto de su pliego de prescripciones técnicas, ha sido categorizada como clasificado, no obstante, tal y como se describe en el pliego abierto de cláusulas administrativas del mismo, estará destinado a la:

> «[...] investigación y experimentación para el fortalecimiento y mejora de las capacidades de Ciberdefensa en sistemas que utilicen tecnologías 5G y fomentando el conocimiento sobre las amenazas y

> vulnerabilidades de aplicación en dicha tecnología, permitiendo así responder a las demandas y retos de Ciberdefensa en redes 5G».

Tratando este aspecto tan relevante de la ciberseguridad en el contexto de la tecnología 5G, ya en 2018 se publicó el «Plan Nacional 5G» que no solo busca promover el desarrollo y despliegue de redes 5G, sino que también enfatiza la necesidad de garantizar la seguridad de estas redes. Por ello, en marzo de 2022, España promulgó el Real Decreto de Ciberseguridad 5G (BOE-A-2022-4973)**,** una normativa que establece las bases para garantizar la seguridad de las redes 5G en el país. Este decreto subraya la necesidad de implementar medidas de seguridad específicas para prevenir y mitigar los riesgos asociados con la tecnología 5G, que también debe ser tenido en consideración por el MDEF.

Por otra parte, en septiembre de 2022, la Armada llevó a cabo el ejercicio REPMUS, donde contó con la participación de Telefónica y se demostraron parte de las capacidades de 5G previstas para este entorno.

El objetivo del ejercicio era generar un escenario de experimentación, para comprobar las capacidades de los vehículos no tripulados en el ámbito marítimo, de la mano de la industria y la universidad. Se recurrió a la tecnología 5G con un escenario de despliegue SA, como elemento para proporcionar capacidades operativas a estos vehículos, destacando las bajas latencias en los sistemas de control y las cargas de pago.

En septiembre de este año, también han participado en el ejercicio *DYNAMIC MESSENGER* de la Armada que perseguía realizar ejercicios y pruebas con vehículos no tripulados (UXV) marítimos y aéreos, apoyando al desarrollo de conceptos y capacidades de la OTAN. Se ha instalado un nodo 5G en el buque, creando la denominada burbuja táctica 5G, que ha posibilitado la integración de estos vehículos con el sistema de combate del buque (SCOMBA), habilitando el intercambio de información.

En el plano internacional, para OTAN, el desarrollo e implantación de las EDT es una piedra angular en el futuro de la organización. La quinta generación de comunicaciones móviles se postula como un habilitador para la transformación de la sociedad, tanto en su modo de vida como de trabajar.

En un informe publicado en julio de este año por el *Consultation, Command and Control Board*[1] (C3B) de la OTAN se resalta la importancia de la utilización del 5G en el ámbito militar, generando nuevas oportunidades y teniendo en cuenta la importancia de proteger estas comunicaciones y los servicios asociados a la misma, pero también se manifiesta la falta de

[1] AC/322-WP (2023)0028-REV1-AS1 (INV), NATO 5G / ***Next Generation Networks Vision and Strategy***, 24 de julio de 2023.

Figura 2. Despliegue de antenas 5G para ejercicios REPMUS'22 (izquierda) y DYNAMIC MESSENGER'23 (derecha). Fuente: Telefónica

Figura 3. Vehículo no tripulado de superficie (USV) Sead 23, de SEADRONE. Integración completa del sistema para llevar el control y carga de pago por 5G. Fuente: Telefónica

perspectiva común. A pesar de la estandarización de la tecnología 5G, las naciones y la OTAN presentan diferentes prioridades en términos de implementación de estándares y especificaciones técnicas, dependiendo de los casos de uso que se desarrollen. Por lo tanto, es muy importante tratar de

fomentar esta visión común de los requisitos y casos de uso militares, al igual que presentarla a las organizaciones de estandarización para su posible inclusión en los estándares y especificaciones que se publiquen en los próximos años.

Actualmente, hay una serie de proyectos e iniciativas relevantes que se están ejecutando en el marco OTAN. Destaca el «Test Bed 5G» (Pernik, 2021), como un banco de pruebas centrado sobre todo en la tecnología *Open* RAN. Se está trabajando en implementar esta tecnología, orientada a la generación de casos de utilidad de interés militar y experimentando con funciones como el uso compartido dinámico del espectro (DSS). Se espera contar con los primeros resultados a inicios del próximo 2024.

Desde la *NATO Communications and Information Agency* (NCIA) (Bastos, Capela y Koprulu, 2020) participan también como asesores en el proyecto *Horizon Europe* 6G-NTN, centrado en la investigación sobre la evolución de las redes no terrestres (NTN). Donde actualmente el 5G-NTN está posibilitando la extensión de la red terrestre 5G por satélite, proporcionando capacidades de cobertura ubicuas, sin contar con limitaciones de terreno o infraestructura. La Agencia asesora al equipo del proyecto, trabaja en los casos de uso objetivo y requisitos para NTN 6G para su aplicación a escenarios militares, considerando que pueda estar disponible a partir de 2030.

Por otra parte, desde la iniciativa del Acelerador de Innovadores de Defensa para el Atlántico Norte (DIANA) se están desarrollando bancos de pruebas de concepto. La idea es desarrollar una red 5G federada, liderada por la OTAN, compuesta por bancos de pruebas nacionales conectados virtualmente; y ser capaces de proporcionar acuerdos ágiles para su uso. Para garantizar que las implementaciones 5G de la OTAN sean interoperables, se requerirá este enfoque común ya mencionado, aparte de la armonización de los casos de uso. Esto implicará colaborar con la industria, asociaciones comerciales y la participación directa en organizaciones de estándares (por ejemplo, el Instituto Europeo de Normas de Telecomunicaciones (ETSI), 3GPP y la Alianza O-RAN).

Respecto al 6G, el informe del C3B también resalta el proyecto 6G *Flagship,* finlandés, centrado en la tecnología 5G e investigaciones sobre tecnologías habilitadoras para 6G; y donde se da importancia a la participación de universidades y centros de investigación con OTAN y las naciones asociadas para el desarrollo de estas tecnologías. Aunque no existe un centro de excelencia CoE 5G como tal, el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE), dedicado a la cooperación en Ciberdefensa ha integrado el 5G en sus últimos ejercicios técnicos anuales, *Locked Shields.* Lleva a cabo proyectos de investigación de seguridad 5G en cooperación con las naciones de la OTAN.

Es imperativo que estas iniciativas continúen evolucionando para mantenerse al día con los desarrollos rápidos en el campo de la tecnología 5G. A medida que avanzamos, será esencial mantener un enfoque equilibrado que promueva la innovación y el desarrollo tecnológico, mientras se garantiza la seguridad y la protección de la infraestructura crítica y los datos sensibles de las naciones aliadas.

En el plano de la Unión Europea, se cuenta con la Empresa Común para las Redes y los Servicios Inteligentes (Empresa Común SNS)[2] como asociación público-privada que cuenta con una doble misión, tal y como describen literalmente «fomentar la soberanía tecnológica de Europa en la 6G e impulsar el despliegue de la 5G en Europa». Se encarga de financiar proyectos de investigación e innovación (I+i) con el objetico de situar al sector industrial europeo «en la cadena de valor mundial de las redes y servicios inteligentes». Fue establecida en noviembre de 2021 como una entidad legal y de financiamiento, liderada conjuntamente por la Comisión Europea y la Asociación de Industria de Redes y Servicios Inteligentes 6G (6G-IA), con un presupuesto de la UE de novecientos millones de euros para 2021-2027.

En enero de 2023, la SNS inauguró su primera serie de 35 proyectos de investigación, innovación y pruebas, marcando un hito significativo en el avance hacia las tecnologías de comunicación de próxima generación. Estos proyectos, financiados con aproximadamente 250.000.000 € a través del programa *Horizon Europe*, están diseñados para fomentar la investigación 6G en Europa y facilitar la evolución de la tecnología y los ecosistemas 5G.

La iniciativa se centra en desarrollar componentes de comunicación inteligente, sistemas y redes para 6G, explorando tanto rutas evolutivas a través de mejoras en la tecnología avanzada 5G como investigaciones revolucionarias sobre tecnologías prometedoras. Estos proyectos están divididos en varias corrientes, cada una centrada en diferentes aspectos de la investigación:

– Corriente A: se enfoca en la investigación sobre redes de radio eficientes en energía, *Open* RAN adaptativo, redes no terrestres 5G integradas, plataformas de borde basadas en IA y gestión de recursos inteligentes que garantizan seguridad, privacidad y confiabilidad.
– Corriente B: orientada a tecnologías novedosas que se espera sean adoptadas en redes comerciales a medio y largo plazo, investigando arquitecturas de sistemas 6G novedosas, comunicaciones inalámbricas y ópticas avanzadas.

[2] SNS Journal. (2023). *SNS OPS-Supporting the SNS JU Operations*. Comisión Europea.

– Corriente C: desarrolla plataformas de experimentación a nivel de la UE que pueden incorporar habitadores técnicos para el 6G, que puedan ser implementados a futuro.

– Corriente D: implementa pruebas y pilotos a gran escala, de alta importancia económica y social, explorando y demostrando tecnologías en el espectro 5G/6G, aplicaciones avanzadas y servicios en sectores como el IoT industrial, energía, automoción, procesos de fabricación, *eHealth*, cultura, agricultura y educación.

El éxito en 6G dependerá de la capacidad de las regiones para construir una infraestructura 5G sólida, sobre la cual se puedan realizar experimentos y despliegues de tecnología 6G. Por lo tanto, la construcción de ecosistemas 5G es crítica. La SNS encapsula esta lógica en su enfoque de dos pilares, coordinando la Agenda de Despliegue Estratégico 5G y fomentando proyectos de despliegue 5G, mientras promueve las capacidades tecnológicas e industriales de Europa en 6G.

Por su parte, la EDA cuenta con grupos asociados a capacidades tecnológicas. En el denominado *CapTech Cyber Research & Technology (Cyber)* donde se aborda todo lo concerniente a capacidades ciber militares. Actualmente se está llevando a cabo un estudio relevante para la seguridad de quinta generación (5G). El proyecto ha comenzado en febrero de este año, a cargo de GMV y GRADIANT, con un presupuesto de 73 K €. Deberá estar preparado en un año e identificar los retos y aspectos de seguridad más relevantes para la implantación de 5G en el ecosistema militar.

## 6. Conclusiones

A lo largo de este artículo hemos explorado el universo de la tecnología 5G, qué mejoras ha supuesto, cómo se está implantando e intentando dar luz, cómo se traduce su uso en nuestra vida diaria o su impacto sobre otras tecnologías.

No obstante, más allá de su aplicación en el ámbito civil, se ha intentado reflejar como se traslada su llegada al plano militar. La revolución en el mundo de las telecomunicaciones que ha supuesto su reciente despliegue también ha tenido y tendrá impacto en la forma en que las Fuerzas Armadas evolucionan de mano a las nuevas EDT. Así pues, se ha tratado de reflejar, tanto en el plano nacional como el internacional, sobre qué aplicaciones y casos de uso se está trabajando y volcando esfuerzos, para obtener el mejor rendimiento de esta tecnología.

Si miramos al futuro, cómo toda tecnología disruptiva se prevé que siga posibilitando grandes avances y mejoras, pero también suscitando dudas y haciéndonos reflexionar sobre sus límites y retos.

No hay que olvidar que debemos hacer un seguimiento exhaustivo en los próximos años de los proyectos 5G que se van a llevar a cabo en el Ministerio de Defensa, ya que sentarán los cimientos de la utilización de esta nueva red de comunicaciones en el ecosistema militar. Nos permitirán decidir donde volcar esfuerzos y entender el verdadero valor de su aplicación, así como facilitar el camino y la entrada, a sus evoluciones futuras.

## 7. Bibliografía

Alain Sultan. "5G System Overview". August 2022. https://www.3gpp.org/technologies/5g-system-overview

Harsh Tataria, Mansoor S Hafi, Andreas F. M Olisch, Mischa D Ohler, Henrik S Jöland , And F Redrik T Ufvesson. "6G Wireless Systems: Vision, Requirements, Challenges, Insights, and Opportunities". PROCEEDINGS OF THE IEEE, Vol. 109, No. 7, July 2021.

S. Niknam *et al*., "Intelligent O-RAN for Beyond 5G and 6G Wireless Networks," *2022 IEEE Globecom Workshops (GC Wkshps)*, Rio de Janeiro, Brazil, 2022, pp. 215-220, doi: 10.1109/GCWkshps56602.2022.10008676.

John Lee, Meia Nouwens and Kai Lin Tay. "Strategic Settings for 6G: Pathways for China and the US". The International Institute for Strategic Studies (IISS). August 2022.

AC/322-WP(2023)0028–REV1-AS1 (INV), NATO 5G / Next Generation Networks Vision and Strategy, 24 July 2023.

Piret Pernik, Taťána Jančárková, Kadri Kaska, Urmas Ruuto, Costel-Marius Gheorghevici and Henrik Beckvard. "Research Report.Supply Chain and Network Security for Military 5G Networks". Tallin 2021. NATO CCDCOE.

Luis Bastos, Germano Capela, Alper Koprulu. "Potential of 5G technologies for military application". Working paper, 15 Sep 2020, NCI Agency.

SNS Journal 2023. SNS OPS – Supporting the SNS JU Operations. Comision Europea.

Capítulo 3

# Consideraciones sobre el potencial uso de *apps* en Defensa

*Ángel Gómez de Ágreda*[1]

> «Esta falta de buenos análisis acerca del complejo entramado social en el que se inserta la tecnología (con dimensiones antropológicas, sociales, medioambientales, legales, éticas y políticas) es lo más preocupante de la actual situación. Parafraseando lo que Lichtenberg decía de la química, podríamos afirmar que quien solo sabe de tecnología ni siquiera sabe de tecnología».
>
> La histeria digital, *El País*, 5 agosto 2023. Daniel Innerarity[2]

**Resumen**

La agilidad con la que puede evolucionar el *software* de las aplicaciones móviles ofrece innumerables posibilidades que, a su vez, quedan obsoletas o superadas en cortos periodos de tiempo. Resulta fútil pretender elaborar una relación de funcionalidades que podría proporcionar una *app*, tanto por la caducidad que tendría la relación como por la falta de exhaustividad de la que adolecería. Por ello, se propone una metodología para facilitar la identificación de opciones y se apunta un criterio para su elaboración, a partir del diseño inicial. Además, se identifican condicionantes y debilidades inherentes a la corporeidad y ubicuidad de estas aplicaciones en la autonomía del componente humano del sistema.

**Palabras Clave**

*App*, Inteligencia Artificial, Movilidad, Agilidad, Interoperabilidad.

[1] El autor quiere agradecer al Sr. Enrique Martín, CEO de ***E&Q Engineering***, sus aportaciones y sugerencias en la elaboración de este capítulo.

[2] Disponible en: https://www.danielinnerarity.es/opini%C3%B3n-preblog-2023/la-histeria-digital/

## *Considerations on the potential use of apps in Defense*


### *Abstract*

*The agility with which mobile application software can evolve offers countless possibilities that, in turn, become obsolete or outdated in a short period of time. It is futile to try to draw up a list of functionalities that an application could provide, both because the list would soon become obsolete and because it would suffer from a lack of completeness. Therefore, a methodology is proposed to facilitate the identification of options, and a criterion for their elaboration from the initial design is pointed out. In addition, conditioning factors, and weaknesses inherent to the corporeality and ubiquity of these applications in the autonomy of the human component of the system are also identified.*



### *Keywords*

App, Artificial Intelligence, Mobility, Agility, Interoperability.

## 1. Introducción

El *software* ha pasado a ocupar la posición central en lo que a relevancia se refiere en la cadena de suministros y en la criticidad de componentes. Sus características, las de su generación y distribución, difieren, de forma significativa de las de los bienes físicos y, en lo que respecta a la defensa, del armamento convencional. Conviene, por lo tanto, partir de estas diferencias para entender las necesidades y las oportunidades distintivas que llevan asociadas.

Las Fuerzas Armadas, tanto las españolas como las de la práctica totalidad de los países, carecen de una estructura optimizada para la producción y explotación de este armamento digital. En primer lugar, porque no disponen de capacidad autónoma para la elaboración del código o para su integración en aplicaciones operativas[3]. En segundo lugar, porque la externalización de esta función se realiza de una forma muy similar a la del resto de los sistemas de armas: en ciclos muy largos y no iterativos que producen resultados ineficientes, tardíos, muchas veces no interoperables y rápidamente obsoletos. Finalmente, porque ni la arquitectura de personal ni los procedimientos que se siguen en combate o en la retaguardia responden a unos criterios lo suficientemente ágiles como para sacar partido a lo que el *software* puede ofrecer.

Por todo ello, antes que a la adopción de aplicaciones móviles (*apps*) para la resolución de problemas convencionales —para lo cual también son de utilidad—, es preciso atender al rediseño de los procesos de adquisición de capacidades y los procedimientos de empleo de estas en función de su dinamismo. De este modo, se estará en mejor disposición para generar un conjunto de capacidades coherente e interoperable.

Al igual que el *software*, las plataformas físicas están evolucionando hacia el concepto de enjambres de unidades de menor tamaño y poder, pero especialmente de una más reducida huella y coste. Los procesos ágiles de desarrollo y adquisición deberán aplicarse también a este armamento que, por otro lado, comparte numerosas interdependencias con las soluciones basadas en *software*.

Estos enjambres van a estar también relacionados muchas veces con sistemas híbridos hombre-máquina en los que el *software* vuelve a jugar un papel importante. Es muy probable que el concepto de *app*, vinculado ahora a los teléfonos móviles, sobreviva incluso a la eventual desaparición de estos en favor de otros dispositivos cuya interfaz sea más cómoda

[3] En el Ejército de Tierra de España, la Jefatura de Sistemas de Información, Telecomunicaciones y Asistencia Técnica (JCISAT) se ha dotado de una cierta capacidad para desarrollar estos programas.

y transparente. Será muy conveniente, por lo tanto, que estas aplicaciones puedan evolucionar de forma independiente de la plataforma que las contenga.

Los altos niveles de atrición de los últimos conflictos (Nagorno Karabaj, Ucrania) muestran la dificultad para sostener el esfuerzo bélico basado en grandes y sofisticados sistemas de armas como principal fuerza de combate. La capacidad de los sistemas más pequeños y ágiles para evolucionar, la rapidez con la que pueden ser puestos en servicio desde la fase de diseño y el coste marginal que suponen les permitirán siempre encontrar vulnerabilidades críticas en plataformas prácticamente irreemplazables.

Los sistemas de Mando y Control actuales, a todos los niveles, aspiran a integrar enormes cantidades de datos para ofrecer al comandante una representación intuitiva de las opciones disponibles. Para ello, también es imprescindible disponer de una red de sensores distribuida en múltiples plataformas. Estos sensores tienen que integrar los ciclos logísticos para garantizar la sostenibilidad del esfuerzo. Es decir, la sensorización se convierte en la piedra angular sobre la que se apoya la acción del mando en todos los escalones.

A partir de los datos obtenidos por estos sensores se podrá generar una imagen global de la situación de las Fuerzas Armadas, tanto en el frente como en sus labores logísticas o de entrenamiento.

Las *app*s permiten actuar como sensores y en funciones de distribución de la información e, incluso, de Mando y Control. La precisión de los vectores requiere de una exactitud no menor en la identificación y ubicación de los objetivos. En ese papel se están empleando ya numerosas aplicaciones en Ucrania.

Sin embargo, la sostenibilidad del esfuerzo requiere que esos mismos datos se recojan en la cadena de suministro y, en una situación óptima, también en el diseño de nuevos sistemas (en el espíritu mencionado de la agilidad que permite el *software*).

Se describen en el artículo algunos casos de uso de cada una de estas actividades, pero se pretende dejar suficientemente abierta la clasificación como para permitir una innovación de abajo arriba, desde el nivel del usuario.

## 2. Ciclos de adquisición digital

Las *app*s se llevan utilizando en la sociedad desde la última década del siglo pasado. Una parte muy significativa del personal en activo de las Fuerzas Armadas las ha manejado regularmente desde su infancia. No se trata de una tecnología novedosa que vaya a requerir un tiempo de adaptación de

los usuarios militares. Todo ello a pesar de que sí puedan ser recientes algunas de las técnicas empleadas en su elaboración y, evidentemente, algunas de las funcionalidades que ofrecen. Al contrario, es la madurez de la organización como tal —y no la de sus miembros individuales— la que está limitando su adopción.

Por eso mismo, no es preciso un entrenamiento genérico en su empleo ni generar una doctrina *ex novo*. Será suficiente con adaptar las pautas de empleo que ya existen en el ámbito civil, con las que ya están familiarizados los usuarios militares, pero con el añadido de las salvaguardas y particularidades del entorno militar.

Para ello, igual que ocurrió antes en otros ámbitos digitales, será preciso establecer, por un lado, una unidad orgánica capaz de desarrollar y/o centralizar/supervisar la generación de aplicaciones móviles. De forma paralela, será necesario hacer permear las dinámicas asociadas al *software* al resto de la organización en todo aquello que suponga una mejora en los resultados finales. Es decir, adecuar la organización al medio según viene determinado por la tecnología. Nada distinto a lo que se ha venido haciendo históricamente en circunstancias similares.

Para ello, se requerirá la adaptación de las estructuras, procesos, tácticas, técnicas y procedimientos a los ciclos ágiles que van asociados con el *software*.

Estos ciclos tienen mucho que ver con su:

– Carácter inmaterial.

– La facilidad con la que puede reconfigurarse.

– Su carácter abierto.

– Las oportunidades y vulnerabilidades que introduce el bajo umbral de acceso que presenta (la mal llamada «democratización» de su uso).

Aunque aquellas estructuras específicas que habrá que establecer para gestionar este ámbito concreto no requieren de grandes medios personales ni materiales, la dinámica de funcionamiento que impone el *software* demanda una adaptación del conjunto de las Fuerzas Armadas (igual que ha ocurrido en la sociedad en general).

La producción de aplicaciones —llevada a cabo según los procedimientos que se describirán someramente— resulta rápida y segura. Al mismo tiempo, encierra enseñanzas útiles en otros campos que solo parcialmente se están aplicando a otros procesos de adquisición de capacidades.

En cuanto a la necesidad de que la cultura asociada al *software* permee en el resto de las estructuras, es suficiente con observar el modo en el que ha

cambiado la sociedad con su empleo y la irreversibilidad de estos procesos. Ya no es imaginable la vida en nuestras ciudades sin acceso a aplicaciones de mensajería instantánea, de geolocalización, incluso de adquisición de bienes y servicios *online*.

Los ritmos de adopción de la tecnología se han acortado exponencialmente en el último siglo como consecuencia de la mayor agilidad en su evolución y en función de la interiorización del proceso por parte de los usuarios. En realidad, lo que penalizan los consumidores actuales es el estatismo, la falta de evolución constante y la necesidad de plazos de espera para el disfrute del producto.

Si eso sucede así en el entorno civil, tanto más cabe esperar de un escenario tan dinámico como es el bélico. De hecho, hemos observado este fenómeno en la guerra que provocó Rusia con la invasión de Ucrania. La población y los combatientes no solamente no rechazan la introducción de aplicaciones móviles de uso militar, sino que las adoptan de forma entusiasta con un elevado grado de competencia en su manejo, casi desde el principio.

Los elevados índices de atrición, el altísimo consumo de munición y la rápida evolución de la situación sobre el terreno demandan la traslación de esta aproximación ágil, desde la mentalidad digital a la analógica, como única respuesta posible para la obtención de la ventaja estratégica.

Por supuesto, las aplicaciones móviles asociadas a funciones de combate son las más llamativas y las que más interés acaparan. Sin embargo, como también se observa en Ucrania, diversas Fuerzas Armadas en todo el mundo han desarrollado o adaptado *apps* específicas para otras labores propias de la vida militar. En muchas ocasiones, estas aplicaciones tienen o podrían tener un uso dual y, frecuentemente, incluso proceden de diseños civiles. La razón estriba en que el carácter modular de las utilidades permite que se desarrollen aplicaciones a partir de componentes de otras cuyo objetivo final es muy diferente.

Esta deberá ser una característica básica del diseño de *apps*: la modularidad o diseño basado en componentes.

## 3. «Componentización» de aplicaciones *software*

Se podría definir como la fragmentación del *software* en piezas bien delimitadas, reutilizables y con un ciclo de vida independiente. La relevancia es mayúscula si se contempla en toda su extensión en cuanto supone un cambio de paradigma frente a los desarrollos de *software* monolíticos. El concepto implica granularidad, no solo en el producto, sino también en la propia fabricación, la cual se divide de manera que cada componente puede pertenecer a un desarrollador diferente. De este modo, el conjunto

verdaderamente opera en cada momento a su máxima capacidad, ya que sus integrantes individuales se pueden actualizar con la cadencia evolutiva que demanda su propia funcionalidad.

El concepto no está exento de desafíos. Al fin y al cabo es la gestión de un puzle que exige conocimiento profundo y detallado de sus piezas, o al menos de la función individual que se les exige.

Esta gestión puede involucrar a múltiples suministradores con cadenas de contratos que, si bien garantizan que el *software* disponga de las mejores prestaciones del momento, pueden llegar a incrementar la huella logística y demandar una agilidad contractual que es difícilmente compatible con los procedimientos directos en el ámbito de la administración.

Un segundo reto es la necesidad de que la suma incremente verdaderamente el valor de las partes, de tal manera que se justifique el esfuerzo, no solo por las prestaciones individuales. Para ello, la interoperabilidad de los componentes[4] debe garantizarse a pesar de la posible falta de sincronía entre los distintos desarrolladores. Esto, a su vez, implica compaginar diferentes arquitecturas (espacios) y adaptarse a momentos de despliegue de nuevas versiones (tiempos) que pueden no ocurrir simultáneamente.

La metodología para dividir en módulos funcionales un *software* requiere voluntad e intuición, pero también la profunda comprensión del problema a solventar. Como antes se mencionó, abordar proyectos de desarrollo que sigan este concepto puede llegar a ser rupturista, entrópico y alejado de la zona de confort de quien decide. Se sustenta en la cultura de la excelencia, de la obtención de lo más eficaz en cada momento, para que el puzle resultante de componentes ofrezca garantías de éxito en cumplimiento de su misión.

Desde la óptica del impacto en el ámbito de la Defensa, este concepto se ha estudiado con especial vigor, derivado de la necesidad de las nuevas nubes de combate donde se distribuyen los nodos o componentes del despliegue de la Fuerza. Las capacidades militares se concentran en orquestar la eficacia de sus elementos. En el campo del *software*, la combinación de técnicas como los contenedores[5], la hiperautomatización con tecnologías cuánticas y la IA facilitan una armonía impensable hace solo una década.

[4] Los componentes se interconectan con enlaces de intensidad variable (un enlace más débil no siempre deriva en equivalente interoperabilidad y uno más fuerte no siempre resulta más eficaz) y lo hacen normalmente siguiendo un modelo de interfaces que articula el conjunto en un todo funcional.

[5] Los contenedores ***software*** habilitan la adaptación de componentes de generaciones pretéritas (***legacy***) a las nuevas arquitecturas. De esta manera se reutilizan aquellas funcionalidades de probada eficacia y se extiende la vida útil de los sistemas y subsistemas con la consecuente disminución del coste de los ciclos de vida y el impacto sobre cadenas de desarrollo cada día más eficientes. De nuevo, un concepto altamente deseable también en el mundo del ***hardware***.

Sin la «componentización» de los sistemas solo queda el manejo de grandes *softwares* monolíticos cuya actualización se ha mostrado ineficaz en aplicaciones militares como el Mando y Control, los sistemas de armas o la explotación ISR (*Intelligence, Surveillance and Reconnaissance*). Su obsolescencia conlleva no solo mayores costes económicos para la actualización de los sistemas, sino un proceso mucho más prolongado en el tiempo que elimina o amortigua la ventaja obtenida con la actualización.

La «componentización» de aplicaciones *software* proporciona ventajas operativas indudables, entre otras:

– Se introduce industria especializada en campos concretos que no necesariamente han trabajado en el ámbito militar con anterioridad pero que producen capacidades y efectos disruptivos.

– Se reduce la dependencia tecnológica y los riesgos asociados a los tiempos de desarrollo y despliegue de capacidades.

– Se mejora la eficiencia por el reemplazo de pequeñas unidades en tiempos acotados.

– Se adapta el paradigma al del combate previsto para 2035 en múltiples nubes y dominios.

– Se incrementa la escalabilidad, reusabilidad y disponibilidad de los sistemas preservando la eficacia y la eficiencia en el combate.

## 4. Definición de las características

Para establecer los posibles usos de las *apps* es preciso conocer las características que deben reunir y las posibilidades que existen en relación con su diseño y empleo. Igualmente, conviene tener en cuenta las opciones disponibles para ajustar, en lo que fuera viable, las características de cada una a las necesidades que tiene que cubrir, lo que debería facilitar la optimización del esfuerzo dedicado a su creación (Seymour *et al*., 2014).

Una primera decisión que tomar es la necesidad de que la aplicación mantenga abierto un canal de comunicación en tiempo casi real con otro terminal. De este modo, podemos clasificar las *apps* como:

– Síncronas (SC).

– Asíncronas (AC).

Es evidente que para una aplicación que pretenda permitir la emulación de un *walkie-talkie*, o para una que cumpla funciones de traducción simultánea, la sincronía es una característica irrenunciable. Sin embargo, una

que nos facilite un manual de empleo de un equipo puede contener la información en el propio terminal y no requerir interacción alguna (salvo que se pretenda que exista un *call center* para resolver las dudas en tiempo real).

En línea con lo anterior, es preciso definir si la comunicación tiene que llevarse a cabo en ambos sentidos, si solo un sentido es suficiente o, incluso, si es preferible evitar que se pueda interactuar. De ese modo, serán:

– Unidireccionales (UD).

– Bidireccionales (BD).

De hecho, es conveniente considerar la necesidad de que la comunicación se lleve a cabo entre dos interlocutores únicamente o que tenga un alcance más amplio, para incluir a un grupo de agentes conectados:

– Individual (IN).

– Grupal (GR).

Estos agentes pueden, a su vez, requerir de una identificación que personalice a cada componente de la red. En otros casos, esta faceta no será necesaria, puede contravenir alguna normativa de privacidad o ser contraria a los intereses y a los fines perseguidos. En este caso, la clasificación resultante sería:

– Identificada (ID).

– Anónima (AN).

Finalmente, la posibilidad de geolocalización del terminal puede resultar crítica en *apps* relacionadas con actividades de combate o logísticas. Para algunas aplicaciones, como la emulación de un teodolito o la dirección de tiro artillero, se convertirá en una función clave. En otros casos, esta característica puede suponer un riesgo no asociado a un valor añadido y, por criterios de economía de medios y de seguridad de las operaciones, debe estar deshabilitada.

– Geolocalizada (GEO).

– No geolocalizada (NG).

Todas estas funcionalidades pueden estar contenidas en aplicaciones que pueden ser:

– Públicas (PUB).

– Privadas (PRV).

En interés de sacar el mayor partido posible a las ya disponibles en el mercado, que no requieran de mayores adaptaciones.

## 5. Creación de la *app*

Las técnicas actuales para la elaboración de aplicaciones móviles permiten y aconsejan una aproximación modular, como veremos. Desde el punto de vista del operador militar, el esfuerzo debe centrarse en la primera de las cuatro fases de la creación de la *app,* a saber: diseño, implementación, pruebas y publicación[6]. Se desarrolla el tema en detalle más abajo, una vez definidas las posibles utilidades.

En esa fase de diseño se debe establecer una aproximación inicial a la funcionalidad que se pretende que cubra la *app* y, basándose en los criterios expuestos anteriormente, las interacciones que debe ser capaz de crear. Sin embargo, el proceso Dev-Sec-Ops (*Development-Security-Operations*/ Desarrollo-Seguridad-Operación), que se define a continuación, establece la iteración constante. No es un ciclo único, sino un ciclo constante en el que se deja abierta la puerta a que el objetivo se pueda alcanzar con un producto o con unas características diferentes a las definidas, algo que vuelve a hacerse difícilmente compatible con los modelos actuales de contratación (pública).

En este sentido, la forma que adopte la interfaz puede ser clave en la obtención del resultado deseado. De poco sirve tener un gran poder de cálculo que reduzca a milésimas de segundo la obtención de *outputs* en combate si la introducción de los datos previos es lenta y farragosa, o si la interpretación de estos no resulta intuitiva y directamente accionable. Cada *app* requerirá, en función del escenario y de la plataforma sobre la que se vaya a utilizar, una forma distinta de interfaz.

Esta interfaz definirá la relación hombre-máquina que influirá, a su vez, grandemente en el equilibrio de funciones entre ambos actores (Diggelen *et al*., 2023). Cabe esperar que, a mayor nivel de integración y mayor transparencia en la relación, menor sea la capacidad crítica del operador humano en el análisis y tratamiento de los resultados ofrecidos por la máquina.

En la «soledad del Mando» y especialmente en las actividades táctica, cuando el asesoramiento procede de un algoritmo que no tiene que asumir responsabilidad alguna, la libertad real de elección del comandante o del combatiente para contradecir el criterio propuesto puede verse muy limitada.

[6] El Plan de Implementación de Modernización del ***software*** del Departamento de Defensa de Estados Unidos parte, desde su primer párrafo, de esa premisa cuando afirma que el objetivo es «simplificar la mecánica de entrega del ***software*** permitiendo que los equipos (de diseño) se centren en la creatividad» (*Department of Defense*, 2023).

Las llamadas de atención de los eticistas, previniendo frente a la antropomorfización de los robots y el exceso de verosimilitud en las presentaciones, apuntan a otro de los riesgos asociados a la introducción de agentes «inteligentes» artificiales. La realidad física y la virtual se entremezclan hasta hacerlas parecer equivalentes.

## 6. Propuesta de taxonomía

Estableceremos una propuesta de taxonomía de las diversas funcionalidades que se puede dar a las *apps* en el ámbito de la Defensa. El objetivo no es meramente académico, sino que pretende servir de inspiración para la identificación de nuevas posibilidades al establecer los «cajones» básicos sobre los que efectuar el diseño de estas. Queda abierto a las distintas unidades el camino de la innovación y la creatividad sobre esta base.

Una propuesta más ambiciosa implicaría clasificar las funcionalidades ya estandarizadas para permitir una rápida asociación de varias de ellas en el diseño de programas novedosos. Esto es, identificar funciones concretas contenidas en módulos estandarizados que sirvan de bloques de construcción de las aplicaciones.

Incluso en el caso en que existan escrúpulos morales o limitaciones legales para el empleo de determinadas aplicaciones, el conocimiento de las posibilidades que ofrece el *software* aplicado a dispositivos móviles es crucial para poder preparar una defensa adecuada frente a los usos ofensivos que podrían hacerse de estas tecnologías. Con independencia de la intención de emplear estas herramientas, su estudio sigue siendo irrenunciable para contrarrestar sus efectos.

Una forma de sistematizar las distintas funcionalidades que pueden acometer las *apps* sería vincularlas a las diferentes secciones de un Estado Mayor.

– En un primer grupo se integrarían, por lo tanto, aquellas que permiten acometer la gestión del personal. Dentro de ellas, a modo de ejemplo no exhaustivo, podemos diseñar aplicaciones dedicadas a los siguientes usos:

- Identificación segura del personal, que puede ir asociada a otras *apps* como forma general de acceso al sistema.
- Gestión de perfil de carrera y asesoramiento. Puede servir para mejorar las elecciones sobre la trayectoria profesional y para optimizar el acompañamiento por parte de la institución.
- Notificación de incidentes en una aplicación centralizada o distribuida en función de la orgánica, que permita reportes inmediatos sobre incidencias de las que deba tener conocimiento la organización.

- Plataforma contra el acoso laboral o sexual, ya existente en algunas Fuerzas Armadas en otros países,
- Apoyo paramédico y de primeros auxilios, físico y psicológico. Estas aplicaciones también se encuentran ya en servicio en algunos países aliados. Pueden incluir desde apoyo psicológico hasta una solución personal y desplegable de telemedicina,
- Provisión de servicios sociales y culturales (de un modo más accesible y ágil que a través de la página web correspondiente y siempre sobre modo seguro).
- Activación y participación de reservistas, con la posibilidad de incorporar un método ágil de comunicación entre la administración y los reservistas que permita una mayor inclusividad de estos.
- Servicios sociales a familiares y veteranos, en la misma línea de facilitar la integración y participación de estos en las actividades relacionadas con las Fuerzas Armadas.
- Acceso a noticias relativas a Defensa, en distintas posibles configuraciones de seguridad y como alternativa al uso de otras opciones de mensajería instantánea.

– En el segundo grupo tendrían cabida aquellas relacionadas con la gestión de inteligencia, incluyendo:

- Acceso seguro a bases de datos, a través, por ejemplo, de la aplicación de identificación segura.
- Procesamiento y análisis asistido centralizado, recopilando los datos aportados por los sensores distribuidos y utilizando la mayor capacidad de cómputo de la central para su conversión en inteligencia.
- Canales seguros de comunicación, etc.

– Ucrania ofrece múltiples ejemplos de la utilización de *apps* en operaciones. También la industria se ha volcado en la comercialización de otras aplicaciones que facilitan:

- La consciencia situacional, base de la capacidad para adoptar decisiones en el campo de batalla o en los distintos niveles de mando. Ya existen ejemplos concretos de aplicaciones comerciales que ofrecen estas funcionalidades, como ATAK[7].

[7] ATAK es un ejemplo de uso dual de las *apps*. En su versión civil es el acrónimo de *Android Team Awareness Kit*, en su versión militar se traduce como *Android Tactical Assault Kit*. En ambos casos es una aplicación que proporciona información geoespacial que permite la colaboración entre distintos individuos o equipos sobre el terreno. Sus utilidades, por lo tanto, pueden variar desde la gestión de equipos en

- La capacidad para la coordinación entre unidades, apoyándose en la compartición de la geolocalización y permitiendo la reducción de las comunicaciones entre ellas y una mayor sincronización de sus acciones.
- La precisión y coordinación de fuegos de artillería (*Ballistic Advanced, GIS Arta*[8]).
- Movimientos de unidades.
- La identificación y selección de blancos (*Assault Rifle Combat Application System* de *Elbit Systems*[9], *Smartshooter*[10]).
- La gestión y dirección de vehículos autónomos de reconocimiento (*Urban Reconnaissance through Supervised Autonomy* (URSA[11]), DARPA (Russell, 2018)) y de combate.

La mayor eficacia se obtiene de la integración de soluciones en una red de aplicaciones que extraiga el mayor partido posible de la sensorización del campo de batalla y de las aportaciones parciales de cada una de ellas en una *kill-web* (Holland Michel, 2023). Se vuelve sobre este concepto más abajo. Baste constatar aquí que los sensores son los proveedores de datos sobre los que calcula el sistema. Una ineficaz red de sensores puede ofrecer una visión solo parcial o, peor aún, distorsionada, del escenario a estudiar. Por otro lado, la capacidad de computación distribuida en los propios

---

el acometimiento de emergencias hasta la coordinación de actividades entre pequeñas unidades sin necesidad de comunicaciones indiscretas entre ellas. Disponible en: https://www.civtak.org/documentation/

[8] Disponible en: https://gisarta.org/en/#about. GIS Arta es un ejemplo de aplicación a fines militares de conceptos empleados en aplicaciones civiles. El algoritmo realiza una función similar a la de Über, vinculando objetivos con sistemas de armas en función de unos criterios preestablecidos y reduciendo el tiempo requerido para batir un objetivo de veinte minutos a uno.

[9] La empresa israelí ofrece un complemento para los fusiles de asalto con diferentes funcionalidades. Las ***apps*** no necesariamente tienen que ir asociadas al dispositivo móvil convencional, sino que pueden desarrollarse para cualquier dispositivo con capacidad de computación y comunicación digital. Véase en: https://elbitsystems.com/product/arcas/

[10] Disponible en: https://www.smart-shooter.com/products/. Las ***apps*** pueden proporcionar funcionalidades de control remoto a dispositivos sencillos acoplados a armamento convencional que multiplican sus capacidades. Aparentemente, este sistema se empleó para el asesinato de forma remota del científico nuclear iraní Mohsen Fahrizadeh en 2021. El fusil estaba instalado en el interior de un vehículo aparcado en una carretera por la que tenía que circular la víctima. La combinación de sensores con controles remotos permitió escapar al comando que ejecutó la acción.

[11] URSA pretende gestionar la información recibida desde diferentes sensores (normalmente sobre plataformas de guiado autónomo o remoto) para establecer una identificación positiva de los elementos que están presentes en el campo de batalla. Una vez más, es un intento de materialización de un escenario «tipo videojuego» en el que el soldado cuenta con información procesada sobre los distintos elementos presentes en su radio de acción.

terminales puede proporcionar una flexibilidad irrenunciable en función de la conectividad disponible.

La mayor parte de estas aplicaciones hacen uso de la geolocalización y la conectividad que proporcionan los terminales móviles para facilitar una visión más completa de la situación operativa (modo «máster», similar a los juegos de estrategia) que facilita la toma de decisiones a todos los niveles.

Aplicaciones simples como la de emular un teodolito para geolocalizar y referenciar blancos o unidades propias proporcionan una imagen operacional de mucha utilidad.

– El cuarto grupo, el de la logística, es quizás el que más sinergias presenta respecto de las aplicaciones del ámbito civil. Para conseguir un aprovechamiento máximo de las posibilidades que ofrece requeriría de una sensorización lo mayor posible del personal, material y entorno. Afortunadamente, este aspecto puede abordarse de un modo incremental e ir aprovechando las ventajas que ofrecen soluciones parciales para alcanzar objetivos concretos. Entre estos se encontrarían:

• Control de stocks en los distintos escalones logísticos.

• Optimización de transporte.

• Apoyos logísticos entre unidades.

• Disponibilidad de manuales de mantenimiento.

• Fabricación aditiva de piezas críticas.

– El área del planeamiento puede hacer un uso intensivo del *software* para apoyar la tarea de los analistas, desarrollar escenarios y simular opciones. Existen numerosas aplicaciones desarrolladas por países aliados que ya han mostrado las posibilidades que ofrece este campo. El planeamiento táctico también puede verse muy beneficiado con el uso de programas que optimicen las capacidades disponibles en función de la situación sobre el terreno.

– El entorno de las comunicaciones se puede beneficiar de numerosas *apps* comerciales disponibles como *Commercial Off-The-Shelf* (COTS). Los requisitos adicionales que cabría añadir a estas aplicaciones se limitarían, en muchos casos, a la incorporación de una capa de seguridad en función del nivel de clasificación requerido. Algunas de las más básicas utilidades que se pueden incorporar con relativa facilidad son:

• Comunicaciones en tiempo real con emulación *walkie-talkie* (Parmar, 2023).

• Servicio de traducción simultánea, bien basado en sistemas automatizados o a través de relé de comunicaciones con intérpretes humanos.

- Incorporación de una capa de ciberseguridad y encriptación para las propias comunicaciones y para otras aplicaciones.

– Las áreas de instrucción y adiestramiento son las que, probablemente, requieren de una menor inversión en innovación por parte de Defensa. Existen numerosas aplicaciones comerciales que permiten su traslación directa al ámbito militar. Otras apenas demandarían la introducción de los contenidos propios a difundir y, finalmente, unas pocas podrían necesitar de la adaptación de módulos ya disponibles para su personalización en función de la actividad concreta a entrenar. Entre ellas, están plenamente establecidas y difundidas:

- Aplicaciones de entrenamiento físico.
- Cursos de idiomas.
- Simulación (de operación de plataformas, de conducción de operaciones...).
- Difusión de cursos y formación en base a podcasts.
- Cursos y formación genérica sobre áreas de interés.

La personalización de las aplicaciones puede permitir también el seguimiento por parte del Mando del progreso en la consecución de objetivos de formación por parte del personal complementando así a los centros de formación presenciales y descargando a estos de trabajo.

A pesar de la aparente inocuidad de estas aplicaciones, es preciso tener en cuenta las vulnerabilidades que, potencialmente, introducen. Un caso muy conocido es el de la aplicación Strava[12], cuyo uso por parte de miembros de las Fuerzas Armadas de varios países delató la existencia de instalaciones y la presencia de fuerzas en ubicaciones secretas (Hern, 2018).

Los contenidos de algunos cursos también podrían tener un carácter clasificado o de difusión restringida a los miembros del Servicio. Por ambas razones, es imprescindible la supervisión en la adaptación de las aplicaciones al uso militar y, en su caso, su adaptación y «securitización».

– Las aplicaciones basadas en *software* se adaptan también de forma excelente a su empleo en acciones de comunicación pública, influencia y operaciones en el ámbito cognitivo, tanto de carácter ofensivo como defensivo. Además, permiten:

- Difusión de cultura de Defensa.
- Reclutamiento e información pública.

[12] Véase en: https://www.strava.com/mobile

## 7. Interacción hombre-máquina

La implantación de aplicaciones en dispositivos portátiles, como teléfonos, puede comportar efectos no deseados. El análisis algorítmico (desprovisto de emociones) induce sesgos y condicionamientos en el operador (que sí las tiene), tanto más intensos cuanto mayor sea la presión a la que esté sometido en el campo de batalla. Determinadas decisiones son más efectivas si se toman desde un puesto de mando, incluso si la información disponible es la misma.

La presión a que está sometido impide que el operador disfrute de condiciones óptimas para decidir con criterio, pero no le exime de la responsabilidad de esa decisión. La presión será particularmente intensa si la decisión contradice el consejo de la máquina, obligando al humano a justificar —ante sí mismo y, en su caso, ante sus superiores— haber optado por una línea de acción diferente.

Como vemos, también se intensifica en función del grado de integración de la información. Es decir, cuanto más trasparente sea la interfaz que une los sistemas cognitivos humano y artificial, menor será la capacidad para distinguir entre las apreciaciones personales, las indicaciones de la máquina y la realidad. La antropomorfización, la apariencia humana del dispositivo, puede crear empatías indeseables que faciliten la confusión de las prioridades en momentos de tensión.

## 8. Sinergias e interoperabilidad

Cualquiera que sea la aplicación concreta que se desarrolle, la tendencia actual de las operaciones apunta a una integración en la *kill-web* que se mencionaba más arriba. El diseño de todas ellas debe, por consiguiente, prever su convergencia con una red distribuida en nube basada en la confianza cero (*zero-trust*) que garantice su seguridad al tiempo que permite compartir datos, análisis y capacidad de cómputo. Dispositivos, datos, usuarios y todos los demás componentes requieren de una identificación positiva para acceder al sistema.

Es más, la misma funcionalidad de la *app* debería ser susceptible de adaptarse a la evolución de las circunstancias. A ser posible, las adaptaciones tendrían que ser transparentes para las acciones del usuario.

La técnica más recomendable para construir esta red se denomina Dev-Sec-Ops, un desarrollo realizado pensando en la operatividad del producto que incluye la seguridad en todas las fases de su diseño. Como se ve en la figura, se trata de un proceso iterativo que requiere de la participación de los usuarios en su evaluación y mejora.

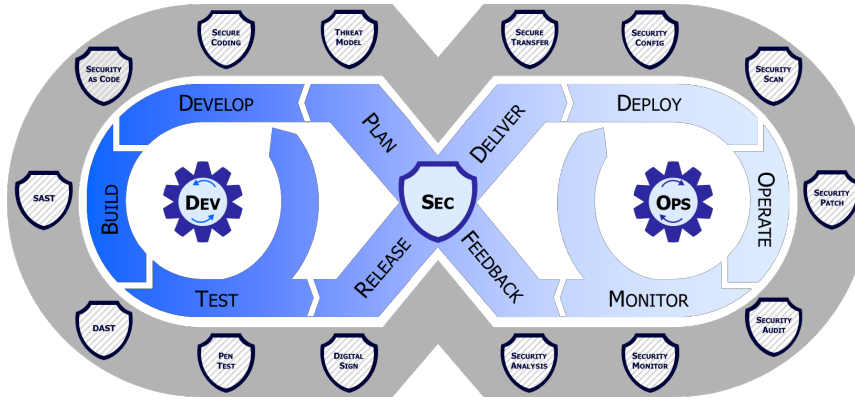



**Figura 1. DEV-SEC-OPS desarrollo de aplicaciones operativas integrando la seguridad en el diseño. Se trata de un proceso iterativo de mejora y comprobación constante**

Otras Fuerzas Armadas aliadas han desarrollado ya guías estratégicas para la implantación de este método de trabajo (DoD CIO, 2021), aplicable también con carácter general a otros procesos de adquisición de capacidades.

En los procesos tradicionales los equipos de desarrollo trabajan con los operadores para conseguir las funcionalidades requeridas y, posteriormente, se dota al producto de una capa de seguridad. Sin embargo, en Dev-Sec-Ops los equipos incluyen de partida a los responsables de la seguridad. De este modo se consigue un resultado con mayor resiliencia, ya que la supervivencia es un requisito en todas las fases de la generación. Según se constata, también se acortan los plazos de finalización del producto al llevar a cabo todas las funciones en paralelo, en lugar de en forma secuencial, además de evitar el rediseño de productos viables, pero sobre los que no es posible o práctico establecer una capa ulterior de seguridad.

La ciberseguridad es una pieza clave en el diseño de las *apps*. Ambos procesos de desarrollo tienen que ser compatibles y la mejor forma de lograrlo es llevarlos a cabo de forma simultánea.

Dev-Sec-Ops introduce también indicadores clave y métricas en todos los pasos del proceso, facilitando la evaluación constante de este, su futura acomodación a los avances aplicables o la eliminación de ineficiencias en su funcionamiento.

Es importante que los equipos de desarrollo, operación y seguridad trabajen no solamente de forma simultánea, sino también de manera integrada para evitar, en menor escala, las mismas ineficiencias que se producían con otros procedimientos.

Según el citado documento del DoD (Departamento de Defensa), los beneficios que se obtienen de la aplicación de esta técnica son:

– La reducción del tiempo medio de producción.
– El incremento de la frecuencia de entrada en servicio de versiones mejoradas de un producto.
– La disminución del tiempo de recuperación (identificación y resolución) de incidencias o ineficiencias.
– El descenso de los casos de introducción fallida de nuevos modelos.
– La completa automatización del proceso de gestión de riesgos.
– Ciberseguridad integrada, tanto en producción como en las actualizaciones y en el parcheo de vulnerabilidades.

La plasticidad del *software* y su necesidad constante de evolución para mantener las capacidades que ofrecía hacen de las aplicaciones basadas en código el referente inicial sobre el cual anclar la transformación del modelo de adquisiciones en su conjunto. Un liderazgo convencido y un equipo con capacidad para entender los distintos procesos implicados serán claves para esta transformación.

Esta transformación no es inmediata ni inminente. Requiere de un proceso gradual de entendimiento corporativo de la ciencia de datos y su aplicación a la inteligencia artificial. Scott y Michell, 2023, abordan este proceso y sus distintas fases de forma metódica.

En el presente artículo se describen los distintos pasos necesarios para alcanzar los diferentes grados de capacidad operativa aplicada, en este caso, a la mejora de la consciencia situacional —probablemente, el eje central de las aplicaciones basadas en datos— que se trata de forma separada más abajo.

Una de las grandes ventajas de este modelo de adquisición de capacidades es la posibilidad de dar entrada a pequeñas y medianas empresas a nivel nacional con suficiente experiencia en desarrollos civiles como para poder cooperar en la obtención de las funcionalidades requeridas.

La composición modular, la programación en código abierto y la disponibilidad comercial de esos componentes facilita soluciones en las que se minimiza la necesidad de elaborar código nuevo (*Low-code*), con la aspiración final de realizar un simple ensamblado de módulos prediseñados que no requieran programación adicional alguna (*Zero-code*)[13].

Con estas soluciones, el desarrollador no necesita escribir líneas de código y, por lo tanto, no necesita conocimientos profundos de programación, sino que emplea herramientas visuales con las que, selecciona componentes

[13] Disponible en: https://appmaster.io/blog/zero-code

ya diseñados previamente y los ensambla de un modo similar a como se podría configurar la carga de pago de un avión para las distintas misiones. Se parte de un «contenedor» y de distintos «contenidos» que se complementan para generar la función deseada.

A pesar de ello, las nuevas herramientas basadas en inteligencia artificial generativa (del estilo de GPT) permiten ahorros muy significativos de tiempo en las tareas de codificación en caso de que estas sigan requiriendo su elaboración *ex novo* (Deniz *et al*., 2023). Para las tareas más sencillas este ahorro puede suponer hasta el 50 % del tiempo en colaboración con un programador experto (lo cual refuerza la idea de disponer de equipos, internos o externalizados, especializados y permanentes).

El mismo hecho de emplear código abierto y una mentalidad ágil que permita modificar cada componente de la aplicación redunda en un lógico beneficio en lo que respecta a la interoperabilidad de la *app* en su conjunto. Al estar sus componentes ya diseñados pensando en su intercambiabilidad, también el conjunto resulta compatible por defecto con el resto de las aplicaciones.

La dirección centralizada de los diseños desde Defensa fomenta también el futuro empleo en red que se mencionaba más arriba, aprovechando funcionalidades de una *app* para alimentar a otras. Igualmente, minimiza las redundancias, si no entre aplicaciones, al menos en lo que respecta a los componentes o subprogramas. Es decir, una vez identificado el modo más adecuado de llevar a cabo una función, se puede replicar esta funcionalidad en distintas *apps* o aprovechar los vínculos entre aplicaciones para evitar tener que montarla en varias de ellas.

## 9. Integración para mejorar la consciencia situacional

También en las operaciones que se desarrollan en Ucrania encontramos ejemplos válidos de uso de las tecnologías digitales para la mejora de la función de Mando y Control en base a una mayor consciencia situacional. El sistema DELTA ucraniano, desarrollo basado en las operaciones basadas en la red (CNO), adopta muchos, si no todos, los principios que hemos enunciado hasta aquí: «como un entorno nativo en la nube, seguridad de confianza cero, operaciones multidominio, y orientaciones de arquitectura y soluciones de última generación, interoperables con soluciones similares a las utilizadas por otros países miembros de la Alianza» (Goberna Caride, 2023).

Las *apps*, popularizadas para los teléfonos móviles, no tienen necesariamente que limitarse a estos dispositivos. Ni tampoco el uso de los teléfonos requiere ir asociado a un usuario (en lo que se denomina «corporeización»,

o fusión a niveles prácticos de usuario y la plataforma que se convierte en extensión de sus capacidades). Hemos visto cómo estos aparatos pueden acoplarse a vectores o a vehículos para emplear sus funcionalidades embebidas en lugar de equipos que harían más pesada y voluminosa la carga de pago.

Un *smartphone* no es ya un teléfono al que se le han incorporado otras funciones, sino una plataforma que integra estas funciones con la capacidad de comunicación que proporcionan las redes 4G y 5G, o wifi. Por lo tanto, las *apps* tampoco limitan su alcance al uso tradicional de los teléfonos, sino que tienen que entenderse como mejoras de la plataforma a través del *software*. Algo muy similar a lo que ocurre con los sistemas aéreos sin tripulación (UAS), que han cedido la centralidad de su función de volar a la carga de pago en forma de sensores o transmisores.

Esta sensorización de las Fuerzas Armadas no está exenta de riesgos, ya que la protección de los datos obtenidos, tanto en los dispositivos y los servidores como en tránsito, se convierte en fundamental para no dar al adversario inteligencia precisa sobre nuestras unidades.

También será preciso calibrar con precisión la calidad de dichos datos y de su procesamiento para determinar a su vez la de la inteligencia que proporcionan. A pesar del avance que supone la capacidad de las redes 5G (Payne y Fowler, 2022)[14] y de los últimos procesadores y modelos de procesado distribuido, las valoraciones de las máquinas siguen distando mucho de la perfección o, incluso, de mejorar las de los humanos en algunos casos.

Una aproximación evolutiva parece ser la estrategia más eficiente. Para ello, se debe ir estableciendo la cultura del dato e ir incorporando aplicaciones según sus resultados vayan siendo lo suficientemente buenos. El combatiente tiene que conocer, en todo momento, qué puede obtener de sus *apps* y el grado de fiabilidad que ofrecen. De este modo, debería ser capaz de distanciarse de los extremos de la confianza ciega en la *app* y el temerario desdén por la utilidad de las funcionalidades que aporten.

## 10. Conclusiones

Los conflictos recientes y, muy en particular, la guerra en Ucrania, han mostrado la utilidad de las aplicaciones basadas en *software* para plataformas móviles en las operaciones de combate. No obstante, estos usos no deberían limitarse únicamente a la gestión de la información en el campo de

[14] Las mismas redes 5G, que sirven de soporte a las ***apps*** móviles, tienen su propia utilidad en el escenario bélico, como se describe en el informe del ***Cybersecurity & Information Systems Information Analysis Center*** del Departamento de Defensa de Estados Unidos.

batalla, sino que deberían extenderse a operaciones de retaguardia y rutinarias por varias razones:

– Las aplicaciones móviles se vienen empleando en el entorno civil con asiduidad para la gestión logística y otras funciones en las que han demostrado su utilidad.

– Buena parte de estas aplicaciones pueden tener un uso dual que apenas requeriría pequeñas modificaciones en su adaptación al ámbito militar. Con ello se facilitaría también la adquisición de estas herramientas *Commercial Off-The-Shelf* (COTS) y se abarataría su coste.

– El uso cotidiano de *apps* en el servicio sirve en concienciación y entrenamiento para el empleo de otras equivalentes en situaciones de mayor estrés y urgencia.

– No menos importante, los sensores y datos empleados en las *apps* de retaguardia aumentarían la eficacia de las de combate con un mayor número de parámetros a considerar.

– De esta manera se conseguiría generar una red más completa de aplicaciones y datos para dar lugar a una *kill-web* en la que cada plataforma se beneficiaría de lo aportado por todas las demás.

La identificación concreta de las aplicaciones que podrían ser de utilidad para Defensa es una labor continua y que dependerá de la evolución de las posibilidades tecnológicas y de la naturaleza de las funciones a llevar a cabo. En lugar de llevar a cabo un intento poco metódico de enumerarlas, se propone que su definición se divida tomando como referencia las funciones clásicas de un Estado Mayor, como una forma de agrupar funcionalidades afines y de enfocar la búsqueda en campos concretos.

De esta definición de la necesidad debería partir una fase de diseño que tendrá que estar liderada por una unidad específicamente creada para la elaboración de todas las *apps*, pero que deberá contar con la activa participación del proponente. Este último deberá estar implicado, además de en la definición del resultado deseado, en el diseño de la interfaz con que se presentará este.

Esta interfaz puede resultar clave en el funcionamiento de la *app*, no solo desde el punto de vista positivo de su operatividad, sino también desde el negativo en cuanto al grado de autonomía que permita al operador humano. El equipo de diseño deberá contemplar la ergonomía, pero también los factores psicológicos afectados.

Finalizado el diseño inicial, será preciso que el equipo técnico defina las características que debe cumplir, según la clasificación que se incluye en el texto. Factores como la seguridad, la agilidad, la interoperabilidad o el

coste influirán en el modelo concreto de *app* que se selecciona para cada caso. En todos ellos, la capacidad para formar parte de una red de *apps* debe ser una característica irrenunciable.

Las fases de implementación, pruebas y publicación son procesos estandarizados en los que el valor añadido del empleo de un equipo propio es bastante reducido más allá de la supervisión que se lleve a cabo.

Estos procesos, basados en la modularidad de las funcionalidades que se incluyen en las aplicaciones, suelen requerir una cantidad mínima o, incluso, nula, de redacción de nuevo código. Buena parte del trabajo consiste en identificar y acoplar piezas disponibles ya en el mercado o de dominio público.

Sin embargo, la metodología de trabajo seguida sí resulta de capital importancia. El método que se propone es Dev-Sec-Ops, seguido por la mayor parte de la industria puntera. En él, la seguridad se incorpora al mismo diseño como parte del proceso de desarrollo al mismo nivel que el cumplimiento de la función. Es un método iterativo que prevé la introducción de mejoras constantes que, en el mejor de los casos, deberían ser transparentes para el usuario y no afectar a la interoperabilidad con el resto de la red.

A pesar de que buena parte del personal en activo está familiarizada con el uso de las *apps* en su vida cotidiana, es deseable que su empleo en labores de servicio tenga lugar con carácter previo a la necesidad de utilizarlas en un conflicto. De este modo, su manejo resultará más intuitivo y se habrán podido identificar más necesidades adicionales.

## 11. Bibliografía

APP MASTER [en línea]. (2022). *Full Guide about Zero-Code*. Disponible en: https://appmaster.io/blog/zero-code

Bastos, L, Capela, G. y Koprulu, A. (2020). Potential of 5G technologies for military application. *Working paper*. NCI Agency.

Deniz, B. K. *et al.* (2023). *Unleashing developer productivity with generative AI*. Disponible en: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/unleashing-developer-productivity-with-generative-ai#/

Department of Defense. (2023). *Department of Defense Software Modernization Implementation Plan Summary*. Disponible en: https://dodcio.defense.gov/Portals/0/Documents/Library/SW-Mod-I-PlanExecutiveSummary.pdf

Diggelen, J. *et al.* (2023). Designing for Meaningful Human Control in Military Human-Machine Teams. En: *Research handbook on Meaningful Human Control of Artificial Intelligence Systems*, pp. 1-20.

DoD CIO. (2021). *DoD Enterprise DevSecOps Strategy Guide*. Disponible en: https://p1.dso.mil/resources/dsop

Goberna Caride, J. L. (2023). *La Guerra Centrada en la Red (NCW) desde las Fuerzas Armadas de Ucrania*. Academia de Las Ciencias y Las Artes Militares. Disponible en: https://www.acami.es/wp-content/uploads/2023/07/La-Guerra-Centrada-en-la-Red-FAS-Ucrania-web.pdf

Hern, A. (2018). Fitness tracking app Strava gives away location of secret US army bases. *The Guardian*. Disponible en: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Holland Michel, A. (2023). Inside the messy ethics of making war with machines. *MIT Technology Review*. Disponible en: https://www-technologyreview-com.cdn.ampproject.org/c/s/www.technologyreview.com/2023/08/16/1077386/war-machines/amp/

Lee, J., Nouwens, M. y Tay, K. L. (2022). *Strategic Settings for 6G: Pathways for China and the US*. The International Institute for Strategic Studies (IISS).

Niknam, S. *et al*. (2022). Intelligent O-RAN for Beyond 5G and 6G Wireless Networks. *2022 IEEE Globecom Workshops (GC Wkshps)*. Río de Janeiro, pp. 215-220. DOI: 10.1109/GCWkshps56602.2022.10008676.

Parmar, D. (2023). *10 Best Walkie Talkie Apps to Turn Your Phone Into a Walkie Talkie*. Geekflare. Disponible en: https://geekflare.com/best-walkie-talkie-apps/

Payne, P. y Fowler, R. (2022). *The State of 5G Technology and Applications to the DoD and Military*. Disponible en: https://csiac.org/wp-content/uploads/2022/07/TI-Snapshot-Report_5G-Technology.pdf

Pernik, P. et al. (2021). Research Report. Supply Chain and Network Security for Military 5G Networks. Tallin 2021. NATO CCDCOE. Disponible en:

https://ccdcoe.org/uploads/2021/10/Report_Supply_Chain_and_Network_Security_for_Military_5G_Networks.pdf

Russell, B. (2018). *Urban Reconnaissance through Supervised Autonomy (URSA)*. Disponible en: https://www.darpa.mil/program/urban-reconnaissance-through-supervised-autonomy

Scott, B. y Michell, A. (2023). El futuro de la comprensión situacional: la inteligencia artificial. *Military Review*. Disponible en: https://www.armyupress.army.mil/Journals/Edicion-Hispanoamericana/Archivo-de-articulos-exclusivos-en-linea/Hispanoamericana-On-line-2023/Scott-SPA-OLE-Jan-2023/

Seymour, T., Hussain, J. Z. y Reynolds, S. (2014). How To Create An App. *International Journal of Management & Information Systems (IJMIS)*. 18(2), p. 123. Disponible en: https://doi.org/10.19030/ijmis.v18i2.8494

STRAVA [en línea]. https://www.strava.com/mobile

Sultan, A. (2022). *5G System Overview*. Disponible en: https://www.3gpp.org/technologies/5g-system-overview.

Tataria, H. et al. (2021). *6G Wireless Systems: Vision, Requirements, Challenges, Insights, and Opportunities*. Proceedings of the IEEE. Vol. 109, n.º 7.

Capítulo 4

# Otras tecnologías y sistemas de alto impacto para las operaciones en el EO2035

*Enrique Martín Romero*

> «El siglo XX fue la quiebra de la utopía social; el XXI lo será de la tecnológica».
>
> Nassim N. Taleb

**Resumen**

Antes de la caída del muro de Berlín, en el siglo pasado, las tecnologías militares suponían el umbral de partida para muchas aplicaciones en el ámbito civil. La industria de la automoción, comunicación, transporte o la del ocio se aprovechaban de los materiales avanzados, los satélites, el radar, la criptografía y la digitalización global que supuso internet. El paradigma actual invierte este ciclo, dando protagonismo a los desarrollos que emanan de utilidades civiles para luego ser adaptados a necesidades militares específicas. Son los productos y servicios *Commercial-Off-The-Self* (COTS) cuya evolución es tremendamente rápida. Las tecnologías como la Inteligencia Artificial (IA) generativa, la hiperautomatización, los implantes que permiten superar discapacidades relacionadas con la movilidad y la comunicación, o el *Blockchain*, se han abierto paso al empleo militar desde su aplicación en las finanzas, las telecomunicaciones globales, la medicina y la logística. Los sistemas autónomos como los drones de pequeño tamaño son también ejemplos basados en COTS que se muestran a diario en los medios de comunicación como vectores de ataque en los diversos conflictos que asolan nuestro planeta. Toda esta panoplia de promesas y de realidades ocupará una parte sustancial del espacio de los recursos militares necesarios para combatir eficazmente en el entorno operativo de 2035.

**Palabras clave**

Tiempo real, Inteligencia artificial, Inteligencia Artificial Generativa (GenAI), Inteligencia artificial causal, Aprendizaje máquina, *Deep learning*, Ética, Modelos de lenguaje, LLM, *Deep* RL, COTS, Automatización, Autonomía, Sistema autónomo, Cognitivo, *Blockchain*, *Cognitive warfare*, RPA, *Unmanned*, Gestión de procesos (BPM), Fuegos, Mando y control, Logística, Sostenimiento.

## *Other high-impact technologies and systems for operations in EO2035*


### *Abstract*

*Before the Berlin Wall felt last century, military technologies were the starting point for many civilian applications. The automotive, communications, transport or leisure industries took advantage of advanced materials, satellites, radar, cryptography and the global digitalization entailed by internet. The current paradigm reverses such cycle by giving prominence to developments which emanate from civilian utilities and then be adapted to specific military needs. They are the Commercial-Off-The-Self (COTS) products and services whose evolution is extremely fast. Technologies such as generative artificial intelligence, hyper-automation, implants to overcome mobility and communication disabilities, or blockchain have found their way into the military from previous applications in finance, global telecommunications, medicine, and logistics. Autonomous systems, such as small drones, are also COTS-based examples shown daily in the media as attack vectors in the various conflicts of our planet. All of these promises and realities will play a significant role as part of the military capabilities to fight effectively in the operational environment of 2035.*



### *Keywords*

Real time, Artificial intelligence, Generative Artificial Intelligence (GenAI), Causal artificial intelligence, Machine learning, Deep learning, Ethics, Language models, LLM, Deep RL, COTS, Automation, Autonomy, Autonomous system, Cognitive, Blockchain, Cognitive warfare, RPA, Unmanned, Process Management (BPM), Fires, Command and control, Logistics, Sustainment.

## 1. Introducción

Poco antes de la Segunda Guerra Mundial, la aparición del radar proporcionó un nuevo uso de las señales de radiofrecuencia como parte de los sistemas de armas y de apoyo a la navegación aérea. En el último tercio del conflicto, la Fuerza Aérea inglesa (RAF) explotó esta novedad tecnológica en combinación con receptores de alertas y contramedidas en sus unidades de guerra electrónica a gran escala[1] y con gran eficacia. En paralelo, la utilización militar del radar derivó rápidamente en su empleo aeronáutico civil. Este arquetipo, que se repitió con cierta regularidad durante algo más de medio siglo en ausencia de un conflicto bélico a escala mundial[2], ocurre hoy día a la inversa, con desarrollos militares basados en novedades tecnológicas primeramente maduradas en el mercado civil.

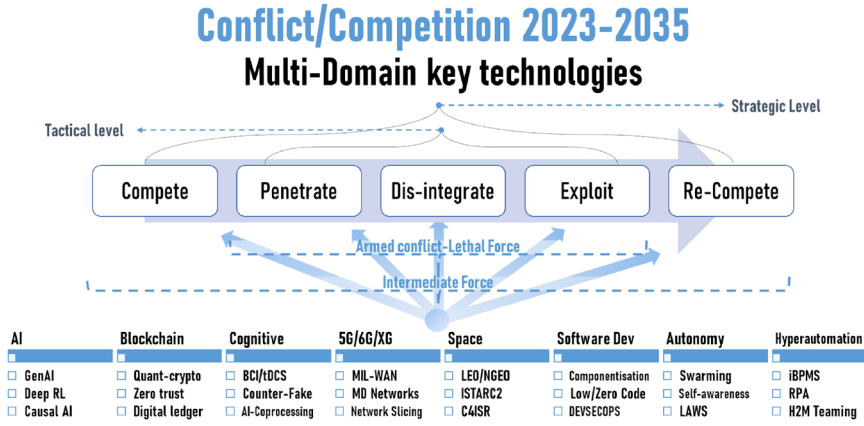



**Figura 1. Aplicabilidad de alguna de las tecnologías de mayor relevancia, no solo en las fases clásicas de cualquier conflicto armado, sino incluyendo todas aquellas previas a la escalada (compete) y la transición a la paz (conflict continuum). Fuente: E&Q Engineering.**

Numerosas razones justifican el notable incremento del nivel tecnológico de los sistemas civiles. Cabe citar, entre otras, la economía de escala y la deslocalización industrial que abaratan las tecnologías habilitantes; la existencia de grandes corporaciones tecnológicas que abarcan mercados globales y lideran la oferta en múltiples áreas de conocimiento; la aparición

[1] El término acuñado por la Armada norteamericana en 1940 es acrónimo de RAdio Detection And Ranging. La RAF británica fue quien desplegó más medios de guerra electrónica incluidos la detección y contramedidas radar de gran importancia para el devenir del conflicto.

[2] A pesar de no acaecer una guerra global de alta intensidad similar a las ocurridas en el siglo XX, sí que existe una pujanza por la superioridad tecnológica y armamentística en bloques bien diferenciados que se muestra en un conflicto velado y continuo *(conflict continuum)*.

del ciberespacio[3] y sus elementos, tanto físicos como virtuales, extendidos a todo tipo de sociedades y economías; y un mercado de bienes y servicios tecnificado y digitalizado hasta un nivel de ambición que inadvertidamente dirige al ciudadano en su vida diaria. Todo ello confiere un papel fundamental a los *Commercial Off-The-Shelf* (COTS)[4], anglicismo que denomina los servicios y productos de mercado, como parte esencial de las capacidades y de las adquisiciones de Defensa.

Aunque es solo un elemento más de las tácticas, técnicas y procedimientos que se despliegan para cumplir eficazmente la misión, las tecnologías son especialmente relevantes cuando proporcionan superioridad en el combate. Dado que la gran mayoría de COTS están disponibles (con mínimas restricciones) en el mercado global, por sí mismas, de manera aislada, carecen de ese efecto. Su modificación y adaptación a las necesidades militares serán los factores diferenciales para conseguirlo.

Otro aspecto por considerar es que las máquinas y su capacidad de proceso no son independientes del ritmo ni del área donde se desarrolla el combate y se pretende generar los efectos[5]. Los entornos operativos actuales, degradados y denegados, ya dificultan enormemente —cuando no impiden— que muchas de las funcionalidades COTS sean válidas, obligando a reconfigurar, entre otros aspectos, la propia operativa de las unidades militares. Un ejemplo es el escenario urbano, de gran complejidad y en el que los sistemas basados en tecnologías COTS tendrán que adaptarse adecuadamente para cumplir la legislación internacional y garantizar —hasta un nivel razonable— la seguridad de los no combatientes.

La lista de áreas de conocimiento y de capacidades que proceden del mercado civil y pueden ser de interés para la Defensa en el entorno 2035 es inabarcable en la extensión de esta publicación. Algunas como las espaciales, las de comunicaciones (5G/6G) o las de desarrollo de aplicaciones se han tratado en otros capítulos. Junto a ellas, las mencionadas a continuación, sin ánimo de ser una enumeración exhaustiva, completan un elenco

[3] Denominado quinto dominio para el combate, ha evolucionado sobre la base de una red global (www), que si bien tuvo sus orígenes en el ámbito militar, ha sido el civil en el que ha sustentado su gran desarrollo y formidable potencial.

[4] Aunque este artículo no es puramente técnico, se emplearán preferentemente aquellos anglicismos que definan mejor y de manera más precisa la materia a tratar. Tal es el caso de las tecnologías, técnicas o métodos científicos que, además de ser origen del vocablo, dotan de una mejor comprensión al lector. Algunos ejemplos serían *Machine Learning o knowledge-based* en el ámbito de la inteligencia artificial.

[5] La eficacia de las acciones de combate requiere contemplar múltiples dominios, incluyendo el ciberespacio. Estas operaciones multidominio se sustentan en conceptos actuales de matices aún por explorar. En 2035 alcanzarán la madurez necesaria como para analizar la validez y eficacia de las COTS del momento.

representativo que con toda seguridad será empleado con profusión por nuestras FAS más allá de la próxima década.

Las técnicas de Inteligencia Artificial (IA), muy diversas (más aún si se entiende por tales los innumerables tipos de redes neuronales, métodos estadísticos y sistemas expertos), no serán tratadas en toda su extensión. Se relaciona únicamente una muestra de las más prometedoras y relevantes para 2035. El bloque de IA se introduce al inicio, pues es habilitante de las tecnologías postreras, no solo para potenciar su capacidad, también forma parte de su núcleo, es decir, sin las cuales estas últimas podrían no tener sentido operativo. Un ejemplo son los sistemas autónomos, cuyo grado de autonomía depende enormemente de su capacidad de percepción y adaptación al entorno para tomar decisiones y cumplir la misión encomendada, tareas complicadas sin la contribución de lo que hoy se conoce como IA.

## 2. Técnicas novedosas de inteligencia artificial

«Crear un ser artificial ha sido el sueño del hombre desde que nació la ciencia».

*Inteligencia Artificial* (película de Steven Spielberg).

Acordar con precisión la definición de cualquier realidad es una circunstancia controvertida, especialmente cuando su observación directa e interpretación y entendimiento requiere de un nivel de conocimientos notable. Esa dificultad se incrementa cuando el término o vocablo que la determina no se refiere a la realidad concreta, sino a la propiedad común de un compendio de elementos o entidades; es este el caso de la denominada IA.

Definir la IA es un acto objetivamente controvertido, casi de rebeldía, por lo que comporta tal atrevimiento en ciertos foros. La demostración es el número de veces que diversos organismos internacionales han cambiado de parecer desde hace más de un lustro. La Comisión Europea[6], apoyada en una pléyade de estudios, encuestas y asesoramiento de los —llamados— expertos en la materia, tras otras iniciativas[7], lanzó en abril de 2021 su propuesta de reglamento sobre la IA denominado *Artificial Intelligence Act*, siendo votada positivamente en el parlamento en junio de 2023. La redacción final aún no se encuentra cerrada y uno de los temas abiertos

[6] Aunque quizá la Unión Europea no sea el contexto más relevante para la Defensa en la actualidad, si se considera la OTAN como referencia operativa. Quizá pueda llegar a tener un peso sustancial en 2035. Dicha orientación vendrá en gran medida determinada por los movimientos geoestratégicos en el Pacífico y el conflicto de Ucrania.

[7] Los pasos dados por la Comisión desde 2018 se encuentran muy bien detallados en este enlace: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.

continúa siendo la definición del propio sujeto del reglamento. Tal y como figura en la actualidad:

Artículo 3. «Sistema de inteligencia artificial (sistema de IA)»: el *software* que se desarrolla, empleando una o varias de las técnicas y estrategias que figuran en el anexo I[8], que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa.

Sin entrar en detalles, la propuesta de reglamento anteriormente expuesta sugiere la exclusión de los sistemas basados en IA de empleo militar[9] por lo que de momento su regulación en el contexto de la Defensa no tendrá ningún efecto limitativo adicional al ya existente sobre determinados sistemas de armas.

En los próximos párrafos se debe entender la IA como el conjunto de técnicas instaladas y procesadas en las máquinas con las características y capacidades tal y como se especifican y describen en cada apartado.

Hablar de la IA de manera absoluta, como un término que fácilmente se entiende desde la definición oficial o académica, puede aportar poca información, amén de lo intuitivo e, incluso en algún caso, mal informar.

La combinación de técnicas de IA con otras muchas, como las de visión avanzada (*Advanced Computer Vision),* facilitará enormemente la comprensión del entorno operativo y la conciencia situacional en combate, tanto a los operadores en conducción como a los mandos de planeamiento. Más adelante se citarán algunos ejemplos, pero la necesidad de estos sistemas parte de un oponente del mundo occidental muy capacitado tecnológicamente, como es China, al igual que la respuesta rápida que requieren los automatismos a los que nuestras FAS estarán expuestas en 2035. El contexto además involucra múltiples dominios al combate en los que observar y, en su caso, provocar los efectos requeridos para el cumplimiento de la misión. Esta tarea no es sencilla sin la participación de agentes virtuales y autómatas que procesen y aprovechen los datos disponibles[10], cuando lo

[8] El anexo I de la propuesta de reglamento menciona técnicas muy diversas, bien conocidas y maduras, como las estadísticas e inductivas, o los sistemas expertos y otros métodos *knowledge-based,* que sugieren una amplitud del término IA más allá del ***machine learning*** o cualquier otra técnica basada en aprendizaje.

[9] Los sistemas de IA desarrollados o utilizados exclusivamente con fines militares deben quedar excluidos del ámbito de aplicación del presente reglamento cuando su uso sea competencia exclusiva de la política exterior y de seguridad común regulada en el título V del Tratado de la Unión Europea (TUE).

[10] Se debe entender aquí por dato no solo el elemento básico sin procesar, estructurado o no estructurado, sino ya procesado en información e inteligencia. Esta

estén, ayudando a las unidades militares a comprender el entorno operativo de manera completa (*comprehensive understanding of the environment*).

Sin entrar en detalles técnicos, la IA es todo sistema no natural que involucra paradigmas de aprendizaje como el *Machine Learning* (ML) y otros simbólicos que comprenden sistemas expertos, métodos estadísticos y de optimización que con la capacidad de proceso actual se implementan con sencillez y proporcionan salidas en tiempos otrora impensables. Dicho de otro modo, las técnicas no son nuevas, sino que ahora son verdaderamente funcionales y operativas. En 1955, John McCarthy[11] acuñó un término que, quién sabe si voluntariamente, concedía a las máquinas un atributo de significado controvertido como es la inteligencia[12]. Dejémoslo ahí.

### 2.1. Deep Reinforcement Learning (Deep RL)

Como se ha mencionado anteriormente, los sistemas IA se basan en modelos que sin ser novedosos en lo teórico sí que lo son en su aplicación práctica. Uno de esos paradigmas es el de aprendizaje (*Learning AI*) dentro del cual se erige el destacado bloque de las técnicas de *Machine Learning* (ML), que son diversas a su vez, una de las cuales es el *Reinforcement Learning* (RL) que sobresale por su empleo en desarrollos como los vehículos autónomos o los enjambres de UAV. Para no entrar en entresijos matemáticos, RL es un tipo de aprendizaje natural que se basa en el retorno positivo (*reward*) o negativo (*punishment*) de la acción con uno (SARL) o varios agentes (MARL).

Este tipo de aprendizaje puede tener problemas de convergencia y, por tanto, errores en las decisiones de actuación que conllevan riesgos importantes para el propio actor y para el entorno. Los MARL añaden más incertidumbre debido, entre otros, a la interacción entre los diversos agentes (sistemas cooperativos).

última, tanto restringida (HUMINT, SIGINT, IMINT) como de fuente abierta (OSINT). Los asistentes virtuales en ocasiones son denominados directamente como IA.

[11] La búsqueda inicial del término inteligencia artificial parece que perseguía encontrar una denominación adecuada para las máquinas que piensan (***thinking machines)***. Un grupo de cuatro científicos e ingenieros alentados por la iniciativa de John McCarthy encontraron financiación para disertar acerca de este asunto. La inteligencia se asoció al hecho de que una máquina pudiese simular aprendizaje junto con otras características asociadas a la inteligencia humana, pero siempre sobre la base de modelos (es decir, un cierto nivel de abstracción) y, por tanto, sin tratar de imitar al humano en el modo de pensar, sino en el resultado mismo de aprender.

[12] Este estudio proporciona una reflexión atrevida sobre lo que se considera inteligencia humana y, por tanto, cuáles son las diferencias explícitas y medibles respecto a la de una máquina. Disponible en: https://arxiv.org/abs/0712.3329v1

Cuando se añaden redes profundas al RL se habla del *Deep* RL, cuya complejidad intrínseca se soslaya con algoritmos empaquetados de fuente abierta[13]. Estas redes profundas añaden elementos predictivos a los algoritmos, de manera que se ajusten a lo previsto, según las condiciones cambiantes del entorno en el que operan. Aunque no son una promesa, sino una realidad en proceso de investigación y de validación (no puede ser de otro modo al menos para sistemas críticos), se diría el *Deep* RL en 2035 formará parte del bucle de refinamiento de cualquier *chatbot* avanzado incorporado a tareas de interacción para el mando y control de todo sistema autónomo, incluyendo los de combate, que incorpore ayudas a la navegación y al cumplimiento de la misión; de los sistemas colaborativos para fabricación industrial[14] y a pequeña escala[15]; así como de sistemas de armas con sensores distribuidos que requieran de una combinación óptima, multidominio y eficacia en tiempos muy cortos, como son los de detección y seguimiento (incluido el espacial) contra amenazas híper-veloces.

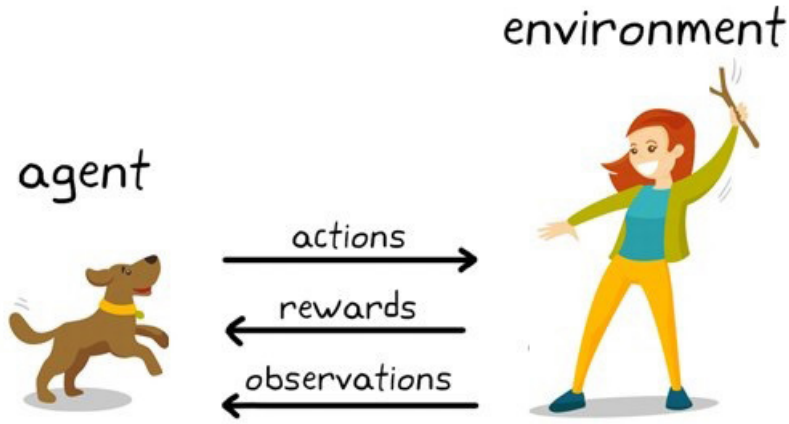



**Figura 2. Lógica del funcionamiento del aprendizaje por RL.**

## 2.2. AI Generativa (GenAI)

Diversos motivos justifican el interés suscitado por la GenAI. Hay mucha literatura reciente al respecto, como la creación de una unidad específica

[13] Los algoritmos DRL, basados en modelos, se emplean en el refinamiento de otras redes neuronales: *Dueling Deep Q-Network* (DQN), ***Deterministic Policy Gradient*** (DPG), etc.

[14] Se pasará del precedente actual entre hombre-máquina o *Human Robot Collaboration* (HRC) a reglas de colaboración entre máquinas o robots.

[15] Con máquinas especializadas, mediante ***Deep*** RL, se podrá realizar el mantenimiento en los primeros escalones utilizando, por ejemplo, fabricación aditiva, sin mediar el uso extensivo del factor humano en las tareas de control de calibración o de calidad.

por parte de DoD norteamericano[16] y la promesa de más de tres mil millones de dólares de negocio para la industria de Defensa en 2035[17]. Los métodos de la GenAI no responden a una disciplina científica nueva, sino que la novedad radica en sus sistemas aplicados.

La producción de contenido multimedia falso o modificado, con o sin intención de engañar, es portada de noticias y materia habitual en las redes sociales. Además de la legislación y los límites que impone, los principios éticos que sustentan las creaciones de un sistema GenAI y aquellos aspectos morales que pueden impactar sobre quien los usa o los recibe son motivo de debate transversal, sin limitarse a un sector.

La generación sintética de datos[18] es una disciplina bien conocida en el ámbito científico de la modelización y la simulación. Se puede definir como la generación deliberada y artificial de datos a partir de algoritmos para reproducir o simular los existentes, originados o que se puedan suscitar en eventos del «mundo real»[19]. Partiendo de un modelo o de unas reglas generales, la máquina es capaz de jugar a ser un artista, un ingeniero o un profesor, siendo más ambiciosa una factoría de datos que incrementa las posibilidades de aprendizaje de otras máquinas[20]. La utilidad directa es enorme en términos prácticos y económicos, al igual que los riesgos[21], derivados tanto del buen como del mal uso.

Durante el último año ha habido una explosión de soluciones abiertas al público que combinan las clásicas aplicaciones tipo *bots* conversacionales[22] o *chatbots* con modelos de aprendizaje basados en Procesamiento del Lenguaje

[16] La integración de LLM en las herramientas *software* actuales ha influido enormemente en la creación de AI Task Force: *DOD Announces Establishment of Generative AI Task Force*

[17] Disponible en: https://marketresearch.biz/report/generative-ai-in-defense-market/

[18] Los datos han de entenderse en sentido amplio, con todo tipo de formatos incluyendo el multimedia. Hay ejemplos de libre acceso como DALL-e, HeyGen, Ras AI para imagen y video o Polly para sonido.

[19] En este contexto se debe entender dato real o generado en el mundo real, en oposición al dato ficticio o simulado.

[20] La generación de conjuntos masivos de datos, de acuerdo con ciertos patrones, satisface el hambre de los sistemas de aprendizaje que carecen de dosis suficiente para que dicho aprendizaje sea completo.

[21] Este aspecto es de vital importancia en sectores como la medicina, la seguridad y la defensa o en el que los errores tienen consecuencias catastróficas. Los riesgos de la AI en Defensa, incluyendo la AI generativa, se han tratado en detalle en la jornada a tal efecto organizada por EMACON el 6 de julio de 2023 con la participación de las FAS y la asociación ODISEIA.

[22] Los ***chatbots*** en una década han pasado de intercambiar con el usuario mensajes de texto o voz sobre la base de fórmulas predeterminadas (***dumb***, ***word-spotting***) a combinar otras técnicas de aprendizaje y generación que dotan a las máquinas de una capacidad lingüística muy superior, asemejando la apariencia de la conversación que mantendrían los seres humanos.

Natural (PNL o NLP en inglés) como el GPT-3.5/4 de OpenAI, el FLAN T5 de Google o el LLaMA[23] de Meta AI (estos dos últimos *Open Source*). Representan muy bien el llamado «Nuevo Renacimiento» dirigido por la IA[24].

Estas combinaciones de técnicas computacionales proporcionan una capacidad que va más allá de la interacción simple con la máquina, generando una enorme cantidad de información, desde informes completos sobre una determinada materia hasta códigos informáticos. Estos modelos de generación avanzada, conocidos como los *Large Language Models* (LLM), más allá de su empleo generalista a través de internet, se pueden integrar en arquitecturas privadas[25], como las de Defensa, para servir de interfaces hombre-máquina en la elaboración de inteligencia, la propuesta de alternativas en planeamiento o en conducción de una operación, el apoyo a la resolución de un problema logístico, o formar parte de un ejercicio para instrucción y adiestramiento de las unidades.

Tales arquitecturas se componen de tres grandes bloques para una adaptación completa de los LLM a la utilidad y el problema militar específico:

– Un primer módulo incluye el modelo y motores de entrenamiento y refinado[26], junto con herramientas de desarrollo[27], para adaptar el LLM al negocio concreto[28], en este caso, al lenguaje doctrinal[29], siempre

[23] Este modelo cuenta en la actualidad con hasta 65 billones de parámetros (febrero 2023) lo cual indica su complejidad con independencia de los datos con los que sea entrenado.

[24] Así lo ha denominado Pilar Manchón, directora senior de Estrategia de Investigación en Google.

[25] La integración de LLM en *softwares* privados *(in-house LLM)* no es un campo tan intuitivo como lo es el empleo a través de internet de estas aplicaciones web, que habitualmente por subscripción, gratuita o de pago, responden a las demandas de información en campos como la ciencia, el periodismo, la empresa, el ocio o la legislación, en múltiples idiomas y con una calidad que ha sorprendido, incluso al público más especializado. Además del modelo, adaptado al dominio concreto, en estos aplicativos ***in-house*** la soberanía sobre el dato se convierte en un elemento a considerar para soslayar las limitaciones impuestas por el uso de datos de terceros (privacidad, imprecisiones, etc.)

[26] Este módulo del sistema dispone, típicamente, de redes neuronales supervisadas cuyo refinado, normalmente, requiere una intervención humana más intensiva.

[27] Son las herramientas que permiten realmente incorporar los modelos a una arquitectura privada. En Defensa se emplearían plantillas para las funciones de combate adaptadas a la doctrina nacional. Estas herramientas pueden ser las de mayor coste de adquisición y mayor dificultad en caso de desarrollo nacional.

[28] Los LLM definidos para un área de conocimiento o un sector concretos deben ser validados. Este es un proceso que permite garantizar la eficiencia y eficacia del modelo. En medicina, el Google Med-PaLM 2 es un LLM diez veces más reducido que GPT4, habiendo sido entrenado y validado específicamente con cuestiones y respuestas basadas en mementos de medicina.

[29] Con datos inapropiados y de poca calidad cualquier sistema de apoyo basado en LLM tendrá un aprovechamiento deficiente. Asimismo, el enfoque debe contem-

teniendo en cuenta que es un sirviente del ser humano, interactúa con él y debe ser entrenado con ese espíritu.

– Un segundo módulo son las aplicaciones de desarrollo que gestionan los contenidos, como, por ejemplo, los repositorios de información e inteligencia para las operaciones, el *targeting*, los fuegos y los datos de apoyo logístico. Sin este sustrato la aplicación basada en el GPT-X del momento no proporcionará más que vaguedades para un usuario especializado.

– Un tercer módulo englobaría los conectores a las bases de datos y el *software* de generación final de contenidos que busca e identifica los datos clave y elabora la respuesta de manera razonada a partir del LLM bien entrenado, refinado y validado[30].

La identificación de vulnerabilidades de toda la estructura anterior no es algo baladí, requiere una especialización concreta, no solo centrada en el desarrollo *software*, sino en los métodos de entrenamiento y de evaluación.

Todo lo mencionado muestra un buen ejemplo de IA generativa cuya esencia no está solo en el modelo LLM empleado, sino en su entrenamiento, que a su vez no está únicamente basado en los datos, sino en la manera que el ser humano los segmenta, anota y refina para que la interacción con la máquina sea apropiada, y en códigos de desarrollo de todo tipo (más allá del ML) que facilitan el cálculo y procesado, así como una extracción rápida y completa de las bases de datos. Es una maquinaria que bien engrasada capacita a cualquier puesto de mando, de un potencial sorprendente para dar respuesta y generar apoyos en tiempos que pueden llegar a ser nimios.

Existen muchos otros ejemplos de GenAI de aplicación en Defensa que no por conocidos y maduros dejarán de ser mejorados. Como se ha mencionado al comienzo de este epígrafe, la simulación es uno de los campos en los que más se ha empleado la generación de datos para instrucción y adiestramiento. Pero la simulación es mucho más. Los métodos no determinísticos permiten suponer casuísticas que no necesariamente siguen un patrón contrastado. De hecho, los sistemas de inferencia estocástica habilitan supuestos extremos, nada habituales y cuyo impacto conviene conocer en cuanto a riesgo operacional.

---

plar que la interacción con un ser humano, de momento, requiere de refinamiento posterior al entrenamiento. Y que este último no está exento de problemas legales cuando se emplea internet como fuente de información.

30 Se puede intuir que un sistema basado en LLM no produce ni genera nada más allá de lo que figura en los datos con los que ha sido entrenado. No es así, se dan fenómenos como la alucinación en los que las respuestas a ciertas demandas son o parecen inventadas y nada tienen que ver con los datos de partida.

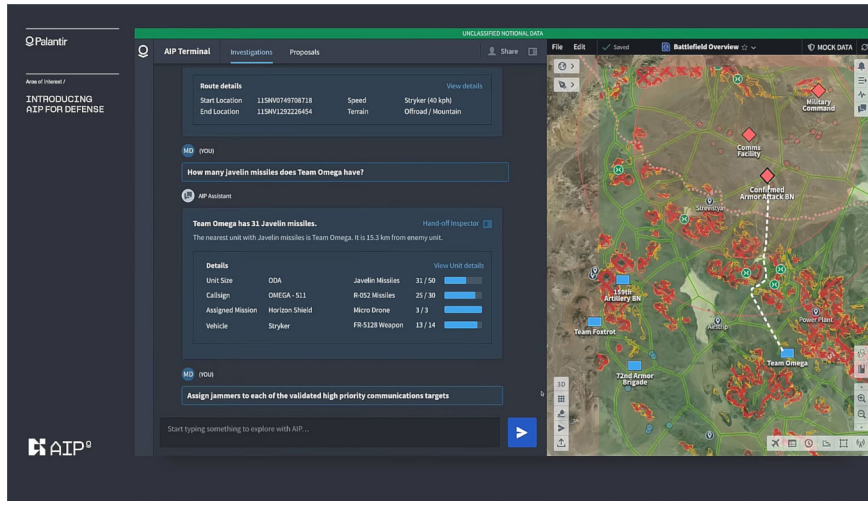



**Figura 3. Interfaz del nuevo chatbot de Palantir, basado en LLM para interactuar con el operador humano. Fuente: Palantir.**

Las finanzas, la meteorología y la generación de energía son campos de aplicación de este tipo de simulación, pero también hay ejemplos en Defensa como el planteamiento de supuestos tácticos, donde se asesora sobre la maniobra, la configuración de los fuegos y la distribución óptima de los sistemas de comunicación. En todos estos casos la simulación típicamente plantea el reto con una amplia generación de parámetros, para posteriormente ser resuelto por un motor de cálculo a modo de sistema experto (*knowledge-based*). Preguntas y respuestas con tiempos de proceso compatibles con la operación y necesidad del momento, obviamente mayores en planeamiento que en ejecución.

En el 2035, casi todos los sistemas de Mando y Control operativo incorporarán funcionalidades habilitadas por GenAI, simulando en tiempos más rápidos que el real (*faster than real-time*).

En el dominio del ciberespacio la GenAI no es de menor utilidad y se tornará en breve, mucho antes de 2035, como una de las capacidades críticas y más diversificadas en todo tipo de sector. Concretamente, se puede emplear como parte de los sistemas defensivos para la detección de amenazas en las primeras fases de un ciberataque[31] con estrategias de alerta temprana y de engaño (*deception*) mediante redes neuronales no

[31] Existe un nutrido número de modelos de ciberataque entre los que se encuentra el propuesto por Lockheed Martin denominado *Cyber Kill Chain* (CKC). Es una cadena de fases o actividades operativas, donde establece como primera el reconocimiento, en ella se identifican los puntos vulnerables por parte del atacante. La segunda es la generación de vectores de ataque sobre las vulnerabilidades. En ambas la GenAI juega un papel muy relevante.

supervisadas basadas en aprendizaje profundo o *deep learning*. Algunos ejemplos podrían ser los siguientes:

– La detección de patrones asociados a un comportamiento anómalo o propio de un ataque se puede llevar a cabo mediante redes adversarias no supervisadas o *Generative Adversarial Networks* (GAN), que confrontan el comportamiento normal de la red con su incipiente alteración.

– El empleo de ciber-señuelos generados como falsos usuarios (*honeyspots*) mediante *autoencoders*, en redes ficticias y vulnerables que atraen a los ciberdelincuentes, facilitando su identificación.

– LeakGAN o la conjunción de las GAN con LLM para la detección de *phishing* (Zahra Qachfar, Verma y Mukherjee, 2022)[32] y otras amenazas como las *synthetic media threats*[33] (*deep fakes)*. Ejemplos significativos son los programas del DARPA, *Media Forensics* (MediFor) y *Semantic Forensics* (SemaFor)[34].

Tal y como ocurre en campos como la medicina a la hora de proponer un diagnóstico, la IA generativa para Defensa no es ni será un sustituto del ser humano, sino una herramienta que puede asistir a sus usuarios para estimar o predecir, instruir acerca de un tema y apoyar la decisión con un razonamiento lógico y bien sustentado —casi— en tiempo real.

### 2.3. Causal AI

Este es un concepto, más allá de la marea de intenciones que puede haber por los que acuñan estos términos, cuyo desarrollo está orientado a identificar las relaciones causa-efecto, dando un paso más en las correlaciones de variables. Siendo esto posible, en hipótesis, la eficacia del asesoramiento de las máquinas se incrementa enormemente debido a su mayor fiabilidad en las predicciones, sus prescripciones a otras máquinas o el asesoramiento en temas concretos.

La correlación existente en las relaciones causales tiene un valor sustancialmente diferente que la de la propia causalidad. Dicho de otro modo, las correlaciones no siempre explican u obedecen a una causa. Steven D. Levitt ya trató hace casi veinte años este asunto en *Freakonomics* cuando

[32] La GenAI en este caso facilita pistas mediante la generación de instancias que tras su clasificación concede un balance adecuado amenaza/falsa amenaza.
[33] Las imágenes manipuladas no solo proceden de la GenAI, sino que se emplean otras técnicas de eficacia contrastada como las *Shallow/Cheap Fakes.*
[34] Estos programas detectan sobre la base de algoritmos generativos. Aunque existen un mayor número de herramientas estas dos fueron las pioneras. El DARPA realizó una descripción extensa de sus modelos en 2019. Disponible en: https://www.darpa.mil/attachments/SemanticForensics-IndustryDay-2019-08-12a.pdf

hablaba de las existentes entre los maestros de escuela y los luchadores de sumo. En este ejemplo la ausencia de lógica no admite una explicación directa e intuitiva, la correlación estadística no infiere una causa evidente.

La motivación causal y el razonamiento elemental convencen de lo apropiado y persuaden sobre el peligro y el riesgo de un modo más convincente para el humano. Asimismo, los algoritmos que procesen la información de tal manera que su lógica no se ciña únicamente a lo puramente matemático (manteniendo un enfoque científico, pero no solo centrado en mostrar la correlación), están dando un paso más hacia la inteligencia artificial generalista (*Artificial General Intelligence*, AGI).

El interés de Defensa por ese tipo de técnicas es creciente, como por ejemplo el empleo de sistemas en combate para el esclarecimiento causal de un daño físico, la primera fase de un *Battle Damage Assessment* (BDA). La OTAN ya pulsó su utilidad militar en los retos del Hackathon de 2021 justamente para evaluar los resultados de posible impacto a partir del análisis de imagen[35].


**Figura 4. Resultados de la aplicación de los algoritmos de análisis de daño por imagen mediante el sistema CADET durante el Hackathon de ACT 2021. Fuente: E&Q Engineering.**

Cuantiosas publicaciones en redes y fuentes abiertas presentan aplicaciones que aluden a esta técnica. Su capacidad, de momento, está alejada de la AGI. Incorporan un *knowledge-based* similar a los sistemas expertos, donde la causa es parte de las tripas del programa o, en el caso de sistemas de aprendizaje, está presente en los datos introducidos en el

[35] La capacidad causal se centra en dirimir si el BDA realizado tiene sentido como consecuencia de un ataque aéreo o, por el contrario, sin fuentes de información adicionales, ya que el análisis lo debe efectuar la máquina de manera autónoma, es alguna otra causa, como por ejemplo un incendio. En la imagen se observa finalmente que la posibilidad de que los daños físicos procedan de un impacto (***strike***) no son muy elevados. En cualquiera de los casos, se trataba también de evaluar automáticamente el daño cualitativo mediante algoritmos de visión avanzados (***change detection***) y técnicas de *Deep Learning* (DL).

entrenamiento. No hay ninguna inferencia adicional a la correlación causa-efecto ya preprogramada.

Estas técnicas parten de la premisa de la persistencia del posible error o de la alucinación que se mencionaba en la GenAI. Dicho error puede conllevar riesgos diversos. En algunos, como los asistentes virtuales, no tendrá mayor consecuencia que el propio fallo en la correlación, una opción equivocada. En otros, como los sistemas autónomos, que toman decisiones basadas en criterios de causalidad para generar efectos en una fase terminal sí pueden ser trascendentes.

Los sistemas que den un paso más hacia la AGI se acercarán al cumplimiento correcto de la misión tal y como conoce el humano, pues las decisiones tomadas por la máquina no se fundamentarán en simples hechos estadísticos, sino que responderán a la causa que los motiva.

## 3. Sistemas autónomos

> «Nunca confíes en un ordenador que no puedas lanzar por la ventana». Steve Wosniak.

Al igual que en la IA, las definiciones de autonomía y de sistema autónomo (Proud et al., 2003; Clough, 2002; ALFUS, NIST 2008; etc.)[36] son controvertidas por lo que conviene contextualizar mediante algunos casos ilustrativos para comprender qué consecuencias se derivan de tal discrepancia. Estos sistemas forman parte del imaginario popular, de tal forma que la ficción se convierte en un problema explícito: las máquinas autónomas atentan contra la esencia del ser humano y contra su libertad[37], pudiendo terminar con sus derechos y, en último caso, con su existencia. De momento las máquinas completamente autónomas, en toda la extensión del término, no existen. Y así acontecerá en 2035. La interacción de la máquina con el humano es imprescindible, no necesariamente durante el planeamiento o la ejecución de la operación, sino previamente, en el desarrollo, en su entrenamiento. Esa subordinación *ex ante* determinará, en muchos casos,

[36] Andrew Williams, en su documento a ACT sobre este asunto, argumentó la conveniencia de cambiar el término de sistema autónomo a sistema con funciones autónomas. La noción de autonomía de un sistema se puede entender en el contexto de sus relaciones con el ser humano o de una manera intrínseca referida únicamente a sus capacidades para interactuar con el entorno. La necesidad o no de la intervención humana se puede contemplar en un plano independiente, sean unas u otras esas capacidades. Existen múltiples modelos que permiten categorizar el nivel de autosuficiencia de un sistema, siendo el nivel más alto aquel en el que la máquina observa, orienta, decide y actúa sin la intervención humana.

[37] Tal y como se entiende la libertad —si se me permite— desde una perspectiva occidental.

la eficacia, el riesgo y también los posibles problemas éticos, morales y legales derivados.

**Figura 5. 1500 drones en el Countdown Gwangalli M Drone Show. Fuente: ntoday, 06-01-2023**

La capacidad operativa de los sistemas aéreos no tripulados comerciales actuales es sorprendente. Sobre la base de un gran mercado civil, liderado por la oferta china de bajo coste[38], estos sistemas ostentan una asombrosa estabilidad en vuelo, gracias a dispositivos de control y guiado muy simples y refinados. Integran sistemas de visión formidables y exhiben una capacidad increíble para operar con garantías cuando no se dispone de comunicación con el operador.

En 2035 los sistemas autónomos de múltiples plataformas, en configuración de enjambre o de equipo[39], dotarán de nuevas capacidades defensivas y ofensivas, cuyo concepto de operaciones se encuentra en fase de experimentación. Estos sistemas combinan técnicas de visión y de comunicaciones, junto a otras mencionadas anteriormente como el *Deep* RL, que les confieren una gran capacidad de adaptación, sin necesidad de intervención humana, salvo que las reglas de enfrentamiento así lo sugieran.

[38] Entiéndase comparativamente con los precios típicos de los sistemas militares. La inmensa demanda de drones para el conflicto de Ucrania ha promovido una fabricación simple y de mínima huella logística.

[39] Empleando la aproximación de Ben Clough (AFRL), la diferencia entre enjambre y equipo es que el segundo no requiere la colaboración activa entre sus miembros que determine su comportamiento o sus reacciones.

El nivel de autonomía de los sistemas no tripulados ha sido incremental en la última década, aunque no en términos exponenciales, como reflejaban algunos vaticinios. Los protocolos que habilitaron las operaciones remotas de estas plataformas (individuales, en equipo con formación tipo líder-esclavo o *leader-follower* y en redes como nodos, siguiendo un patrón orquestadas desde una estación central[40]) han evolucionado hacia otros más avanzados que no requieren modelos con elementos de control dependientes[41]. Cuando se recurra a esas tácticas de empleo con esquemas predeterminados será por preferencia y oportunidad, no por necesidad. Que la intervención humana sea o no posible lo determinará la situación, pero no será la consigna para el cumplimiento de la misión.

En 2035 las máquinas formarán equipos con los humanos, tendrán instrucciones y actuarán según la doctrina y los procedimientos, en caso de tener que tomar decisiones en entornos degradados. El mayor nivel de autonomía posible será de gran utilidad en misiones críticas, donde la velocidad de decisión requerida sea muy elevada, en entornos extremadamente hostiles o en aquellas situaciones que impiden la presencia o el acceso de cualquier mortal. El riesgo de fallo en todos estos casos se asume y balancea de forma positiva el despliegue y operación de máquinas completamente autónomas, contribuyendo a la mejora de la conciencia situacional sin sobrecargar las funciones de los combatientes, al apoyo del planeamiento de la maniobra y a la toma de decisiones, al incremento de la letalidad sin exponer vidas humanas y a la dispersión de nodos de combate heterogéneos que permitirán cumplir la misión en escenarios multidominio y entornos degradados.

Uno de los ejemplos de actualidad es la incorporación a los arsenales de sistemas autónomos desechables de bajo coste de aplicación, entre otras, como señuelos en masa para cumplir misiones defensivas y ofensivas. En el horizonte de 2035, estos sistemas confrontarán adversarios de similar capacidad tecnológica, por lo que la superioridad militar la determinarán pequeños detalles derivados de la tecnología, pero no necesariamente sus prestaciones. Las limitaciones éticas y morales, los riesgos asumidos por los Mandos y las habilidades para inferir la evolución de la situación táctica,

[40] Los equipos de drones han sido escogidos como sustitutos de los espectáculos pirotécnicos. Esta tecnología COTS es directamente aplicable a situaciones tácticas militares, aunque en los próximos años el control no será orquestado de manera centralizada o en redes preconfiguradas, sino independientes y adaptativas.

[41] Para mantener cualquier enjambre se han de establecer reglas básicas de cohesión, distancias, alineamiento y evasión de obstáculos, con o sin líder. Para un mayor detalle del estado del arte en relación con los enjambres desde 2011 a la actualidad se sugiere consultar la tabla 1 del trabajo de Nikita Bhamu *et al* citado en las referencias.

adaptándose con anticipación al adversario serán algunas de las claves del combate simétrico con máquinas autónomas.

Las implicaciones legales derivadas del uso de un sistema completamente autónomo se conocen desde que existen autómatas en los sistemas de armas, es decir, los modos automáticos que gestionan los fuegos sin que intervenga el operador en la selección y la decisión de disparo o activación final. Un ejemplo en relación con la defensa antiaérea[42]: el operador decide el comienzo y el final del «éxtasis del arma», pero no participa activamente de la algazara intermedia.

Los principios clásicos del *arte de la guerra* y el concepto más actual de Mando orientado a la misión o *Mission Command* gobernarán las decisiones de cómo programar, activar o desactivar sistemas autónomos capaces de operar en dominios variados y de resolver, en caso de encontrarse aislados (ejemplo, en entornos degradados), las cuestiones de a qué objetivo, cómo, cuándo y hasta cuándo proyectar efectos de todo tipo.

## 4. Técnicas para el incremento de las capacidades cognitivas

> «Lo más importante en la comunicación es escuchar lo que no se dice». Peter Drucker

Una de las maravillas y a su vez de los misterios aún por descubrir es el funcionamiento detallado del cerebro humano. Ha habido avances indudables en materia neurocientífica, pero aún quedan por resolver muchas incógnitas. Al tiempo que se descubren nuevas estructuras cerebrales[43] que afectan al comportamiento cognitivo y al motor, se identifican nuevas ligaduras entre su anatomía y la actividad en ciertas áreas y se atisba el camino hacia la regeneración neuronal.

Aunque la apoptosis permanezca inevitable, los avances en la neurociencia indican la posibilidad de que nazcan nuevas neuronas haciendo un balance —al menos— neutro y, por tanto, manteniendo las capacidades cognitivas hasta el final. Como complemento a estos avances científicos, la tecnología y determinados métodos que se citarán a continuación[44] son capaces de

[42] El comandante de Artillería José María Lorenzo empleó el término «éxtasis» —que creo muy bien traído—durante la Jornada de Riesgos del uso de la IA en las FAS. CESEDEN, 6 de julio 2023.

[43] Un ejemplo es el descubrimiento del astrocito glutamatérgico, a medio camino entre las neuronas y las células gliales. Estas nuevas células parece que reproducen un comportamiento similar a la sinapsis en cuanto a liberación de sustancias y, por tanto, pueden tener un papel en el control neuronal e influencia en el desarrollo de tratamientos contra determinadas patologías.

[44] La mayoría de los desarrollos primigenios proceden, sobre todo, del ámbito civil, aunque tienen una indudable utilidad militar.

incrementar, temporal o permanentemente, la memoria de trabajo, la atención selectiva y otras funciones ejecutivas. Un resumen de estas tecnologías se muestra en la figura 6.

La estimulación cerebral es uno de los métodos más prometedores. Es capaz de mejorar las funciones cognitivas y de tratar diversas patologías[45]. Los estímulos pueden proceder de elementos exógenos como los dispositivos que operan a través de las interfaces cerebro-máquina (*Brain-Computer Interface*, BCI) y de sustancias neuroestimulantes (fármacos y otros). Estos últimos son eficaces durante cierto tiempo con dosis y efectos secundarios que en ocasiones desaconsejan su uso sostenido.

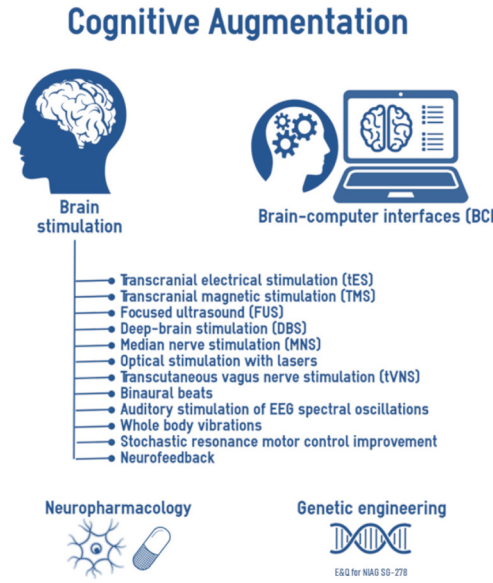



**Figura 6. Técnicas para incrementar la capacidad cognitiva mediante dispositivos de estimulación cerebral, interfaces con máquinas, fármacos e ingeniería genética. Fuente: E&Q Engineering.**

Los equipos de estimulación neuronal[46] como la eléctrica (tDCS/TACS) y la magnética (TMS) se pueden emplear en bucles abiertos (*open-loop stimulation*) para mejorar funciones cognitivas concretas, o enlazados con algún sistema adicional con el que operar (*closed-loop*) mediante la modulación de la estimulación con tecnologías de neuroimagen de extensa utilización en medicina.

[45] Algunas que cabe nombrar son: disfunciones cognitivas, visuales, auditivas, etc. causadas por daños cerebrales debido a traumatismos, alteración del sueño, problemas de conducta, cansancio y anomalías en el equilibrio.

[46] tDCS, véase en: https://caputron.com/collections/vendors?rb_vendor=Caputron; TMS, disponible en: https://www.magstim.com/row-en/product/lite/

Las aplicaciones más prometedoras para Defensa en el entorno de 2035 van desde la mejora en la percepción visual y la atención para misiones de búsqueda y vigilancia, la optimización del sueño o el control de efectores mediante la mente.

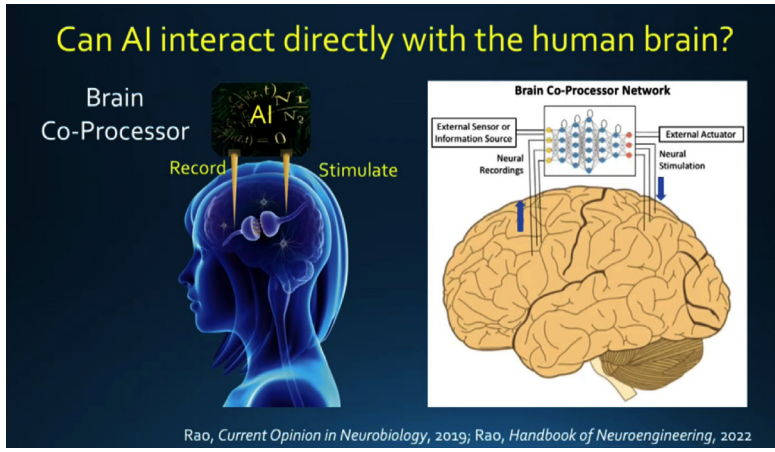



**Figura 7. Concepto de coprocesado de información mediante bucles cerrados con sistemas de IA. Fuente: Handbook of Neuroengineering, capítulo «Brain Co-processors: Using AI to Restore and Augment Brain Function».**

La combinación de la IA con el ejército neuronal de cada combatiente puede suponer un desarrollo extremo de funciones como la memoria y la capacidad de proceso. El coprocesado, mediante implantes (y quizá en un entorno más allá del 2035 con medios no invasivos), es una técnica que consiste en dotar al cerebro de estímulos en bucle para inducir plasticidad neuronal, inhibiendo la generación de químicos y aplacando las emociones de modo que los razonamientos no se filtren, se aumente la atención y las decisiones se produzcan sin pasión alguna. Los sistemas de IA[47], cuyo estado del arte se ha descrito en apartados anteriores, capturan y procesan las ondas cerebrales fomentando la rapidez de procesado para tomar decisiones, intensificando la memoria en todas sus fases[48] y valorando opciones basadas en una comprensión pormenorizada de la situación.

El coprocesado se realiza mediante aprendizaje profundo y como se desprende de la lectura del apartado de la IA, existen numerosos condicionantes a tener en cuenta. Este caso es un buen ejemplo de la implementación de los modelos LLM en una arquitectura privada, el refinamiento no es un entrenamiento sencillo, y el sistema de coprocesado implica sesgos y riesgos que no eximen al sujeto de responsabilidad en las acciones.

47 Un ejemplo es el *Neural Co-Processor, NCP, Network.*
48 Codificación, almacenamiento y recuperación.

La ingeniería genética[49], con serios condicionantes éticos, morales y legales, augura la posibilidad de engendrar filiaciones con inteligencias incrementadas. En el terreno militar esta potencial capacidad natural de las nuevas generaciones de combatientes originaría asimetrías difíciles de asimilar y de contrarrestar, tanto por aquellos que las desconozcan como por los que las descarten. Un nuevo damero de alcance estratégico cuyas reflexiones bien merecen un análisis en detalle.

Abordar el problema de combatir contra un oponente superior técnicamente, en cuanto a medios, requiere de información e inteligencia. Más aún para hacerlo contra humanos de capacidades cognitivas superiores. Pensar en un oponente que encuentra en estas técnicas un vasto campo de posibilidades de desarrollo, sin problemas ni éticos ni morales para su experimentación y posterior empleo, parece un relato o un cliché de la literatura de ficción. Nada más alejado de la realidad como lo demuestra el caso de China.

Uno de los vaticinios acerca de los conflictos del futuro concluye que el «gatillo» puede ser digital. Tanto en el concepto nacional como en el OTAN sobre *Cognitive Warfare* (CogWar) los humanos son los protagonistas sobre los que se centra el combate en el ámbito cognitivo. Individuos, grupos y sociedades enteras pueden ser empleadas como armas (*human weaponisation*), instigando revueltas y generando caos contra el objetivo señalado por el adversario. *De la guerra entre la gente a la guerra en la gente*[50]. La psicología de la masa social es la «base sobre la que se sostiene la acción en el ámbito cognitivo» (Calvo)[51], ese es el sustrato del combate en el que las técnicas de guerra psicológica, habitualmente más quirúrgicas, se quedan pequeñas ante el tamaño del objetivo. Esta circunstancia con matices de corrección parece que persistirá en 2035. En CogWar el proceso de *targeting* no requiere la localización precisa del objetivo en coordenadas y tiempo ni la estimación de daños colaterales derivados de la configuración del fuego o cualquier otro tipo de acción y efecto[52]. El objetivo a batir es un oponente no necesariamente militar y los efectos a neutralizar y, en su caso, mitigar se encuentran en el ámbito cognitivo, en el imaginario colectivo, transformando completamente las tácticas, técnicas y procedimientos aplicables a los dominios físicos.

---

[49] Las técnicas de edición genética junto a las de selección embrionaria, *Genetic Cognitive Enhancement* (GCE), pueden dar lugar a dilemas similares a los del pasado con la energía atómica.

[50] Parafraseando al coronel Gómez de Ágreda en Ministerio de la Paz, de Mundo Orwell (véase en referencias)

[51] Refiere la psicología como concepto general no aplicado necesariamente a un grupo de determinado tamaño.

[52] El tipo de ***targeting*** que se requiere vendrá derivado del concepto de operaciones *CogWar*, aún por definir.

## 5. Blockchain

> «Blockchain simboliza el desplazamiento del poder desde el centro a los nodos de las redes». William Mougayar.

Esta tecnología de bloques se hizo famosa hace unos años por su empleo en el campo financiero para la gestión de criptomonedas. Su funcionamiento y ventajas son conocidos.

Consiste básicamente en un tipo de base de datos distribuida[53], donde cada bloque se enlaza con el siguiente de manera unívoca y contiene una cadena de datos (*hash*) criptográfica[54]. Los contenidos de cada bloque se mantienen íntegros mediante dicha cadena, garantizando la seguridad del activo que protege. Estos pueden ser los términos de un contrato (legal), una pieza de un caza de combate, un elemento concreto de la cadena de suministro de componentes (físico), o un dispositivo virtual (electrónico). La red puede estar repartida geográficamente y tener nodos en diferentes contratistas e instituciones. Todos los participantes de la red poseen una copia idéntica que refleja casi instantáneamente cualquier alteración (segundos o minutos). Las reglas de la red son aceptadas por todos sus partícipes y solo puede ser actualizada por ellos mismos como instrumento esencial y concurrente de confianza. Como se advierte, esta tecnología aporta sinergias entre dichos mecanismos de confianza y consenso, la criptografía, que a buen seguro evolucionará en los próximos lustros con las tecnologías cuánticas y los sistemas distribuidos. Esto último hace que se contemple como opción para sistemas en red multidominio, soportados por nubes de combate jerarquizadas que intercambian información coherente entre nodos (incluyendo sensores y efectores) y puestos de mando distribuidos.

Las aplicaciones militares actuales que implementan *Blockchain* no son excesivas ni van más allá de la exploración de sus posibilidades[55]. La incorporación de esta tecnología será gradual y estará ligada a la evolución de los sistemas de encriptación cuántica. En el entorno de operaciones de 2035 las aplicaciones son diversas y cabe mencionar las siguientes: mensajería, comunicaciones robustas, sostenimiento de sistemas, control de las adquisiciones y la cadena de suministro y la gestión segura de las redes de sistemas de armas (enjambres y otras mallas desplegadas en las nubes de combate multidominio).

---

[53] ***Blockchain*** es una tecnología bajo el paraguas de las *Distributed Ledger Technology.*

[54] El algoritmo criptográfico que utiliza la conocida *Blockchain Bitcoin* se denomina SHA-256. Fue creado por la NSA norteamericana.

[55] Las desventajas de esta tecnología también pueden ser un impedimento para su desarrollo y despliegue. Una de ellas es la dificultad de incorporar todo tipo de activos y actores. Otra es la descentralización, que no siempre es aceptada en defensa, donde el paradigma tiende a cierta centralización.

La necesidad de esta tecnología se cuestiona en algunos casos al confiar en la seguridad de redes aisladas y de nubes de combate privadas sin interconexión a redes globales. Pero puestos a pensar en modo *Zero Trust*, el *hackeo* siempre puede ser una potencial causa de fallo en la misión (figura 8).

En todo caso, la naturaleza y ventajas del *Blockchain* invita a una prospección de soluciones para Defesa más activa en las próximas décadas.

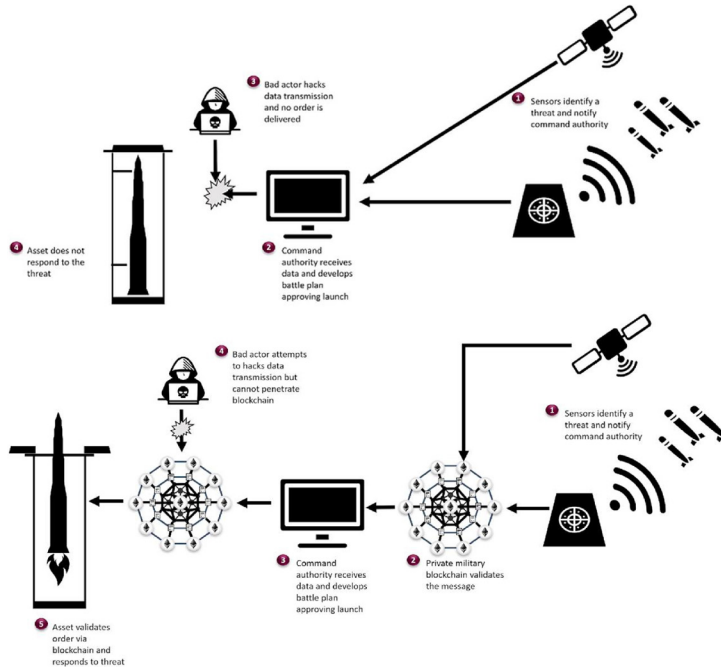



**Figura 8. Ejemplo de eficacia de Blockchain en una secuencia de fuegos a partir de la cadena de mando. La imagen de arriba muestra el hackeo antes del lanzamiento. Fuente: Blockchain Technology in the Asymmetric Warfare Study: Indonesian Perspective**[56]

## 6. Hiperautomatización

> «La mayoría de las eficiencias modernas son castigos diferidos». Taleb.

La hiperautomatización es una expansión del concepto de automatización[57], que incorpora a los clásicos autómatas algunas tecnologías habilita-

[56] Licencia *Creative Commons* (CC BY-NC-ND 4.0 DEED). Disponible en: http://dx.doi.org/10.33172/pa.v8i2.1435

[57] En OTAN los automatismos siempre han sido muy relevantes. Sirva como ejemplo curioso el siguiente informe de julio de 1969: IMSWM-226-69-the application of automatic data processing to the NATO military command and con-

doras[58] como el mencionado *Machine Learning*, los sistemas de gestión de procesos inteligentes (iBPMS) y los agentes *software* robóticos (RPA) para automatizar en la mayor extensión posible todo tipo de procesos.

Este concepto, acuñado por las grandes consultoras como uno de sus emblemas de negocio para la próxima década, pretende dotar de herramientas muy potentes a todos los organismos y a sus unidades. En Defensa será especialmente relevante su implantación en los Centros de Mando y Control (C2) donde se crean espacios inteligentes multidominio, en los que las personas y la tecnología interactúan, se conectan, analizan, monitorizan y coordinan.

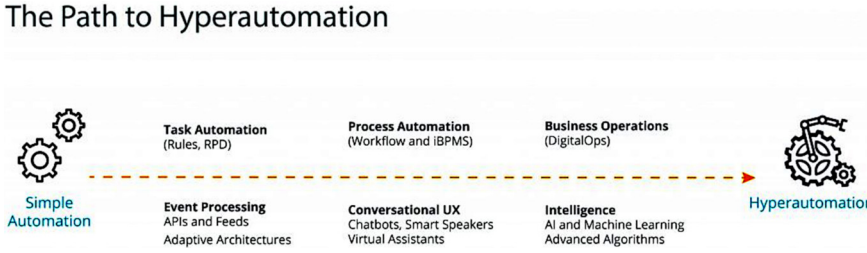



**Figura 9. Concepto evolutivo desde la automatización hasta la hiperautomatización mediante la combinación de diversas tecnologías como iBPMS y ML. Fuente: Gartner.**

Hablar de hiperautomatización en Defensa es tratar con el Mando y Control (C2). Obviamente, hay otras funciones del combate que le son relevantes, pues los procesos habitan en la sombra de todas ellas, alguna como el sostenimiento es una de las que incorpora mayor automatización. Debido a que el C2 es arte y es ciencia, los sistemas incorporan implícitamente una carga enorme de tareas que requieren la participación del ser humano.

La hiperautomatización impulsa el C2 a nivel estratégico, operacional y táctico, con la gestión digital de todos los procesos máquina-máquina (M2M) y máquina-humano (M2H) que sean de relevancia para alcanzar los objetivos establecidos y conseguir el éxito de la misión. Los indicadores de rendimiento y otras métricas ayudan a mejorar, de manera continua, mediante los procesos de lecciones aprendidas y la explotación de los conocimientos post-misión.

Dado que la ejecución demandará tiempos cada vez más cortos, la hiperautomatización será vital para facilitar procesos de C2 más eficientes,

trol and information system. Disponible en: https://archives.nato.int/uploads/r/nato-archives-online/1/1/9/11934c4d751612cd9bcb05cad1993885e31f3d3e65ab-5b3151ab8f43a2645500/IMSWM-226-69_ENG_PDP.pdf

[58] Al ser un término tan intuitivo no es de extrañar que integre nuevas técnicas a su colección de la mano de la industria 4.0.

confiables, regulares y rápidos, para lo cual se cuenta con tecnologías habilitantes como las anteriormente citadas IA y RPA.

Los RPA son fundamentalmente robots *software* que ejecutan tareas de soporte, a menudo burocráticas, como rellenar formularios, buscar y filtrar ficheros o seleccionar información. Generalmente, emulan al humano llevando a cabo las labores más repetitivas (procesos en sí mismos) que están ligadas a procedimientos de más alto nivel.

La hiperautomatización desempeñará un papel muy significativo en la generación de equipos híbridos conformados por máquinas y humanos (*human-machine-teaming*) con *chatbots* avanzados (basados en LLM) que integrarán órdenes en procesos con conectores a otros sistemas y RPA, acelerando enormemente los flujos de trabajo. Tendrán más importancia, si cabe, en el contexto multinacional, donde la jerarquía de los procesos requiere garantizar la interoperabilidad entre las FAS de los integrantes de cada coalición.

En 2035 se pronostica que los ciclos OODA[59] podrán estar verdaderamente interconectados por procesos digitales en los que los datos serán la *commodity*, el producto que se comercializará (entiéndase adecuadamente en este contexto) en el seno de los procesos de negocio. Estos estarán soportados por infoestructuras hiperautomatizadas capaces de proporcionar una granularidad extrema, llegando al nodo, allí donde los procedimientos y la información serán más críticos cuando se encuentren aislados. En ese caso, la toma de decisiones «nodal» vendrá matizada por el concepto de mando orientado a la Misión (*Mission Command*) lo cual no restará valor a los procesos y tareas que se deben automatizar en el propio nodo (*edge computing*)[60].

El paradigma de la intervención humana en 2035 sobre el C2 multidominio cambiará para centrarse en actividades de alto valor como la planificación y la asignación de tareas, así como la toma de decisiones de los nodos, en especial aquellos que integran sistemas de armas. El conjunto de subsistemas que articulan el concepto de hiperautomatización, los iBPMS, como motor de orquestación de procesos y de control de las tareas críticas, los RPA, como subsistema que reduce la carga de trabajo humana mediante la ejecución de instancias repetitivas, y la combinación con sistemas basados en LLM que dotan al proceso de una carga y procesado de información completa, disminuirán sobremanera la tasa de error humano y facultarán

[59] Observación, Orientación, Decisión, Acción.

[60] La capacidad de generación rápida de *software*, adaptable mediante actualización continua y con conectores que permitan enlazar con los procesos y tareas, será otra de las piezas claves de la hiperautomatización. Véase el capítulo de consideraciones sobre el potencial uso de apps en defensa.

un C2 multidominio de manera transparente a los nodos desplegados en cada operación.

Además del C2, la hiperautomatización habilitará flujos de inteligencia con accesos a grandes bloques de información, rastreará los nodos y trasladará decisiones relacionadas con la generación de efectos en diferentes dominios, repitiendo la ejecución del proceso —si fuera menester— con datos completamente actualizados. Asimismo, en el corto plazo, hay diversas iniciativas en OTAN para implantar este concepto, comenzando por el sostenimiento de los sistemas y la digitalización de los procesos referidos a sus ciclos de vida[61].

## 7. Sumario, conclusiones y reflexión final

Cada una de las tecnologías y sistemas anteriores revelan su estado de madurez a través de publicaciones científicas, publicidad empresarial, información abierta de organismos de I+D+i y otros medios de divulgación especializada. Mediante una consulta rápida se puede comprobar que la mayoría se encuentra en fase de desarrollo avanzada, su gradiente evolutivo es creciente y sin afán de profetizar parece lógico prever que su influencia será significativa en las operaciones de 2035.

Se han enumerado alguna de las técnicas de IA de mayor proyección. La GenAI, Causal AI y el aprendizaje reforzado profundo (*Deep* RL) proporcionarán nuevas capacidades de asesoramiento y apoyo a la decisión en el marco del C2 multidominio. Dotarán a la Fuerza de una capacidad de respuesta a las amenazas con una celeridad asombrosa (ej. hipervelocidad) y ayudarán a desenmascarar ligaduras causa-efecto mediante automatismos en las diversas fases del *Combat Assessment* (ejemplo, *Battle Damage Assessment*).

La explotación masiva de estas y otras variantes atribuidas al término IA, junto con automatismos (RPA) y gestores de procesos (iBPM), hará de la digitalización una herramienta que incrementará la agilidad de las cadenas de mando, la eficacia del enlace persona-efector y la sistematización del sostenimiento militar.

Los sistemas denominados autónomos o con capacidades autónomas serán desplegados en entornos degradados, donde la conectividad sea escasa, nula o intermitente. Estos sistemas son capaces de proyectar los

[61] STANREC 4808 ALP-10 NATO *Guidance for Integrated Life Cycle Support*. Aún en borrador para pasar a STANAG, esta publicación menciona la hiperautomatización como una de las tecnologías innovadoras que jugarán un papel relevante en la digitalización de los procesos en el marco del AAP-20-NATO *Programme Management Framework (NATO System Life Cycle Model)*.

efectos letales y no-letales sin mediar enlace o interacción humana, de manera aislada o de un modo coordinado. Adicionalmente, aquellos con el máximo nivel de autonomía estarán preparados para operar siguiendo reglas programadas, aprendizaje previo y procesado en tiempo real, basado en la percepción exhaustiva del entorno. Se enfatizará su empleo como señuelos para sesgar y, en su caso, saturar la actuación de las defensas. Los enjambres no dejan de ser redes cuya operación segura, desde el planeamiento hasta la ejecución, tiene vulnerabilidades cuya protección se puede incrementar con el empleo de *Blockchain*.

La capacidad cognitiva del ser humano está limitada por sucesos naturales y por acciones deliberadas de un adversario. Las técnicas de estimulación cerebral combinadas mediante interfaces cerebrales (BCI) con sistemas de coprocesado, basados en IA, son capaces de solventar alguna de estas limitaciones. La primera, la natural, mediante implantes, interfaces no invasivas y actuadores de todo tipo (voz, señales, movimiento, control de sistemas de armas...) que a su vez pueden dotar a una persona sana del incremento de capacidades cerebrales como la atención, la memoria y la resiliencia emocional. La segunda, mediante sistemas de alerta, lo más temprana posible, tratará de advertir sobre cualquier ataque y de prevenir el uso de las personas por parte del oponente como si fuesen armas contra sus propias FAS y su sociedad e instituciones (*human weaponisation*).

Son cuantiosos los ejemplos de publicidad engañosa en los medios de comunicación. No por conocidos dejan de multiplicarse. La exageración y el empleo de *buzzwords* o palabras «molonas»[62] no son algo ilícito en sí mismo, sino parte del surtido muestrario de mañas que realzan las capacidades de un servicio, de un sistema o de una tecnología. Por una parte, el exceso conlleva promesas inalcanzables y, por otra, la terminología de masas sugiere capacidades y funcionalidades que no son más que una vaga predicción basada en el deseo o la intuición del universo de «cientólogos»[63] que proliferan en los medios.

La necesidad de concreción, el nivel de especialización y el espíritu crítico debiera impregnar a la ciencia aplicada a la Defensa por la propia naturaleza del sector, un monopsonio, su impacto estratégico y, en ciertos, casos

[62] Las corrientes de opinión requieren de elementos simples e intuitivos que faciliten la interpretación del público, lo cual suele llevar a enormes imprecisiones en la terminología. Entre otras motivaciones está el propio negocio. Véase en: https://ichi.pro/es/como-la-acunacion-de-terminos-puede-impulsar-todo-su-negocio-a-nuevas-alturas-230097461452922

[63] En este contexto, entiéndase como la impostura que refiere a los científicos y tecnólogos que basan su —supuesto— conocimiento en la vigilancia de la novedad tecnológica y el abuso de términos vagos, habitualmente acuñados por corrientes de consultoría.

su carácter tractor. En este contexto, la correcta definición y adaptación de los términos procedentes del ámbito civil son de vital importancia para evitar predicciones vacías de contenido operativo y una errónea interpretación de las capacidades derivadas en los entornos futuros.

La amalgama de técnicas de IA[64] e hiperautomatización, los sistemas basados en *blockchain* y los denominados comúnmente como autónomos, así como las metodologías y medios capaces de incrementar las capacidades cognitivas, junto con el resto de tecnologías de esta publicación (LEO, 5G o 6G, IoMT, Dev-Sec-Ops, etc.) son algo más que un escaparate de tendencias[65]. En el entorno operativo de 2035 no serán conjuntos disjuntos, sino que se solaparán, proporcionando las funcionalidades necesarias para disuadir, evitar la escalada de conflictos, resolver situaciones de crisis, dominar el combate y reestablecer la situación a una paz sostenida.

Como medios materiales son un elemento de capacidad más. La aplicación práctica en sistemas militares exigirá una combinación eficiente y eficaz que no siempre coincidirá con el enfoque civil, aunque su procedencia y resorte de desarrollo sea ese mercado.

En el ámbito de la Defensa, el adversario condicionará los efectos a conseguir, es decir, el qué, cuánto, cómo, dónde y cuándo será posible y moralmente aceptable el empleo de todas estas tecnologías y sistemas. Con relación a este último aspecto, el moral, el adversario actual parece tener claro cuál es su posición. La nuestra, según no pocos foros, aún está por definir.

## 8. Bibliografía

Bhamu, N. *et al.* (2023). SmrtSwarm: A Novel Swarming Model for Real-World Environments. *Drones.* 7, 573. Disponible en. https://doi.org/10.3390/drones7090573

Calvo, J. L. (2020). *Conflicto, información e influencia*. Centro Conjunto de Desarrollo de Conceptos (CCDC). *Implicaciones del ámbito cognitivo en las Operaciones Militares*.

Centro Conjunto de Desarrollo de Conceptos (CCDC). (2020). *Usos militares de la inteligencia artificial, la automatización y la robótica (IAA&R)*.

[64] «La inteligencia artificial es el futuro, no solo de Rusia, sino de toda la humanidad. Quien se convierta en el líder en este ámbito se convertirá en el gobernante del mundo». Vladimir Putin, 2017. Traducido del inglés.

[65] Se podrían haber citado muchas otras como las de procesos y encriptación cuántica, los gemelos digitales, GitOps y una hornada adicional de técnicas IA (TRISM, *neuro-symbolic*, etc.).

CISA, FBI y NSA. (2023). *Contextualizing Deepfake Threats to Organizations*.

Comisión Europea. (2019). *High-Level Expert Group on Artificial Intelligence. A definition of AI: Main capabilities and scientific disciplines.* Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf

Comisión Europea (2020). *White paper on On Artificial Intelligence-A European approach to excellence and trust.* Disponible en: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

Comisión Europea. (2021). *Propuesta de Reglamento del parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la unión*. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52021PC0206

Estado Mayor de la Defensa. (2019). *Doctrina de targeting conjunto*. [PDC-3.9 (A)].

Gebhard, L. A. (1979). Evolution of Naval Radio-electronics and Contributions of the Naval Research Laboratory. Disponible en: apps.dtic.mil/sti/pdfs/ADA084225.pdf

Gómez de Ágreda, A. (2019). *Mundo Orwell. Manual de supervivencia en un mundo interconectado*.

Kendal, S. y Creen, M. (2007). *Types of Knowledge-Based Systems. In: An Introduction to Knowledge Engineering*. Springer. London.

Kwan, C. y Ayhan, B. (2019). Reinforcement Learning a Panacea for Solving All Contingencies in UAVs? *Robotics & Automation Engineering Journal*. Vol. 5(1).

Legg, S. y Hutter, M. (2007). *Universal Intelligence: A Definition of Machine Intelligence*.

Leys, N. (2018). Strategic Studies Quarterly: *Autonomous Weapon Systems and International Crises*.

Madiega, T. (2023). *Briefing on Artificial intelligence act*. EPRS. European Parliamentary Research Service. 2.ª edición. [PE 698.792]. Disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

Roorda, M. (2015). *NATO's targeting process: ensuring human control over (and lawful use of) 'autonomous' weapons*. University of Amsterdam.

McCarthy, J. *et al.* (1955). *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*. Disponible en: https://raysolomonoff.com/dartmouth/boxa/dart564props.pdf

NATO C2 COE. (2021). *Multi-Domain Command and Control. Providing a "working description" of the term Multi-Domain C2 (MDC2).* Disponible en: https://c2coe.org/2021/09/08/study-provide-a-working-description-of-the-term-multi-domain-c2-mdc2/

NATO NIAG SG-263. (2022). *Command and Control Capabilities in support of Multi Domain Operations (Multi Domain C2)*.

NATO NIAG SG-278. (2023). *Cognitive augmentation for military applications*. 2023

National Institute of Standards and Technology (NIST). 2004. *Autonomy Levels for Unmanned Systems (ALFUS) Framework*.

Neupane, S. *et al*. (2023). *Impacts and Risk of Generative AI Technology on Cyber Defense*. Mississippi State University. Dept. of Computer Science & Engineering. Disponible en: https://arxiv.org/abs/2306.13033

Platts, J. (2006). Autonomy in unmanned air vehicles. *The Aeronautical Journal, 110*(1104), 97-105.

Proud, Ryan & Hart, Jeremy & Mrozinski, Richard. (2003). *Methods for Determining the Level of Autonomy to Design into a Human Spaceflight Vehicle*.

PWC. (2020). *How blockchain can transform defence assets and give armed forces an advantage on the battlefield*.

Qachfar, F. Z., Verma, R. M. y Mukherjee, A. (2022). Leveraging synthetic data and pu learning for phishing email detection. Disponible en: https://dl.acm.org/doi/10.1145/3508398.3511524

Levitt, S. D. y Dubner, S. J. (2005). *Freakonomics*.

Kilcullen, D. y Pendleton, G. (2021). *Future urban conflict, technology, and the protection of civilians: Real-World Challenges for NATO and Coalition Missions.* The Stimson Center. Disponible en: https://www.stimson.org/2021/future-urban-conflict-technology-and-the-protection-of-civilians/

Wang, X. *et al*. (2023). *Model-based Multi-agent Reinforcement Learning: Recent Progress and Prospects.*

Wikipedia. *Commercial off-the-shelf* [en línea] (15-11-2023). Disponible en: https://en.wikipedia.org/wiki/Commercial_off-the-shelf

Williams, A. P. y Scharre, P. D. (2015). *Autonomous Systems. Issues for Defence Policymakers*. NATO SACT.

## Composición del grupo de trabajo

*Presidente:* **D. Luis Alberto Hernández García**
Coronel del Ejército del Aire y del Espacio.
Jefe de la Sección de Análisis y Prospectiva (EMACON/DIVDEF).

*Secretario:* **D. Ignacio Martínez de Galinsoga Alarcón**
Teniente coronel del Cuerpo de Infantería de Marina.
Joint Force Command Naples (JFCNP).

*Autores:* **D. Jaime Luis Sánchez Mayorga**
Coronel del Ejército del Aire y del Espacio.
Doctor en Economía y Organización.
Estado Mayor del Aire y del Espacio.

**Dña. Montserrat Valdés Quintana**
Personal civil funcionaria. Jefa de Unidad. MCCE-EMAD.
Directora técnica CDAP 5G DEF.

**D. Ángel Gómez de Ágreda**
Coronel del Ejército del Aire y del Espacio.
Doctor en Ingeniería de Organización Industrial.
Agregado militar en la República de Corea del Sur.

**D. Enrique Martín Romero**
Ingeniero aeronáutico.
Director *E&Q Engineering*.


PUBLICACIONES
Pd
DE DEFENSA

GOBIERNO
DE ESPAÑA

MINISTERIO
DE DEFENSA

SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

SUBDIRECCIÓN GENERAL
DE PUBLICACIONES
Y PATRIMONIO CULTURAL