



Observatorio de Defensa y Seguridad
Nodo de Sistemas de Defensa y Seguridad
Informe de Prospectiva 2024



RED HORIZONTES ISDEFE
Madrid, 4 de diciembre de 2024

TABLA DE CONTENIDOS

1. INTRODUCCIÓN	1
1.1. Objetivo del informe	1
1.2. Contexto	1
2. FACTORES DE INFLUENCIA	7
3. IDENTIFICACIÓN DE TENDENCIAS	9
3.1. Tendencias actuales	9
3.1.1. Inteligencia artificial	9
3.1.2. Gemelo digital	13
3.1.3. Realidad Aumentada	13
3.1.4. Materiales para el combatiente (blindaje, tejidos)	14
3.1.5. Detectores de explosivos, drogas, etc.	14
3.1.6. NRBQ	15
3.1.7. Pilas de combustible: Power-producing Technologies	15
3.1.8. Fabricación aditiva	16
3.1.9. Unmanned systems	18
3.1.10. Sistemas anti-dron	20
3.1.11. Sensores ISTAR: IA y big-data	22
3.1.12. Sistemas AESA, C-RAM y radares pasivos	23
3.1.13. Procesado de señales acústicas	23
3.1.14. Identificación de emisiones con IA	23
3.1.15. Robots	24
3.1.16. Sistemas de potenciación de capacidades humanas	26
3.2. Tendencias emergentes	27
3.2.1. Armas hipersónicas	27
3.2.2. Tecnologías cuánticas	29
3.2.3. Receptores fotónicos	33
3.2.4. Metamateriales	33
3.2.5. Nube de combate	33
3.2.6. 6G	34
4. ESCENARIOS FUTUROS	36
4.1. Escenario #1 – Ataques masivos con drones	36
4.1.1. Análisis del escenario #1	36
4.1.2. Probabilidad del escenario #1	36
4.1.3. Riesgos, oportunidades y medidas de mitigación del escenario #1	37
4.2. Escenario #2 – Fuerte desarrollo de la IA en el entorno regulatorio europeo	37

4.2.1.	Análisis del escenario #2.....	37
4.2.2.	Probabilidad del escenario #2.....	38
4.2.3.	Riesgos, oportunidades y medidas de mitigación del escenario #2.....	38
4.3.	Escenario #3 – Mayor uso de misiles hipersónicos en conflictos bélicos.....	38
4.3.1.	Análisis del escenario #3.....	38
4.3.2.	Probabilidad del escenario #3.....	39
4.3.3.	Riesgos, oportunidades y medidas de mitigación del escenario #3.....	39
4.4.	Escenario #4 – Desarrollo de sistemas de computación cuántica operativos.....	40
4.4.1.	Análisis del escenario #4.....	40
4.4.2.	Probabilidad del escenario #4.....	40
4.4.3.	Riesgos, oportunidades y medidas de mitigación del escenario #4.....	40
4.5.	Escenario #5 – Desarrollo de tecnologías 6G para aplicaciones militares.....	41
4.5.1.	Análisis del escenario #5.....	41
4.5.2.	Probabilidad del escenario #5.....	41
4.5.3.	Riesgos, oportunidades y medidas de mitigación del escenario #5.....	42
5.	PROPUESTA DE ACCIONES	43
5.1.	Acciones recomendadas.....	43
5.2.	Plan de seguimiento.....	43
6.	CONCLUSIONES	44
7.	ANEXOS	45
7.1.	Referencias	45
7.2.	Acrónimos.....	48

FIGURAS

Figura 1. Parámetros del estudio bibliométrico ASSETS+.....	2
Figura 2. Mapa de peso-relación de diferentes keywords en el estudio bibliométrico de ASSETS+.....	3
Figura 3. Matriz de relevancia tecnología-misión.....	3
Figura 4. Mapa de calor de las tecnologías estudiadas.....	6
Figura 5. Prospectiva de mercado de la IA en los próximos años [Statista Market Insights].....	9
Figura 6. Ventajas y retos actuales de la OSINT [9].....	10
Figura 7. Principales hitos de la IA generativa tras ChatGPT [10].....	10
Figura 8. Estimación de las capacidades de la tecnología para emular las capacidades de nivel humano en los próximos años [10].....	11
Figura 9. Posible alternativa al reto de aplicar IA en entornos de escasez de datos suficientes para el entrenamiento [16].....	13
Figura 10. Soldado portando un prototipo de Integrated Visual Augmentation System (IVAS).....	14
Figura 11. Ejemplo de una pila de combustible PEM [22].....	16
Figura 12. Principales tendencias actuales de evolución de la fabricación aditiva [StartUs insights].....	17
Figura 13. Concepto del futuro caza europeo FCAS [Airbus].....	18
Figura 14. Taxonomía de la navegación autónoma de UAVs por aplicaciones y tipo de información de base [26].....	20
Figura 15. Sistema de energía dirigida Ranets-E, de fabricación rusa [online].....	21
Figura 16. Dron alimentado mediante un láser [Northwestern Polytechnical University].....	22
Figura 17. Firma microdoppler de distintos drones [31].....	22
Figura 18. Esquema de aprendizaje supervisado para la clasificación de señales radar [35].....	24
Figura 19. Prototipos de robots humanoides en desarrollo [IEEE Spectrum, enero 2024].....	25
Figura 20. Fase de aumento de capacidades humanas [37].....	26
Figura 21. Perfiles de trayectorias de armas hipersónicas frente a balísticas.....	27
Figura 22. (a) HTV-2 Vehículo glider hipersónico experimental, DARPA Falcon Project. (b) Vehículo hipersónico DF-ZF (c) vehículo ruso Avangard HGV.....	29
Figura 23. Escenario futuro de conflicto con fuerte presencia de tecnologías cuánticas [39].....	29
Figura 24. Fuentes de fotones de microondas entrelazados [41].....	30
Figura 25. Roadmap de computación cuántica de IBM [IBM Quantum].....	32
Figura 26. Principio básico de invisibilidad óptica, consistente en la desviación de los rayos de luz.....	33
Figura 27. Concepto de nube de combate del FCAS [AIRBUS].....	34
Figura 28. 6G: hacia un mundo totalmente digital y conectado.....	35

TABLAS

Tabla 1. Tecnologías analizadas.....5
Tabla 2. Factores de influencia en el sector de la defensa y la seguridad.....8

1. INTRODUCCIÓN

1.1. OBJETIVO DEL INFORME

El objetivo del presente documento es analizar las líneas tecnológicas y tendencias a futuro con más relevancia y presencia en las actividades de I+D de la comunidad científica en el ámbito de la defensa y la seguridad, considerando un alcance temporal a medio plazo (entre 5 y 10 años).

El informe realizado analiza las tendencias tecnológicas y posibles escenarios en varios ámbitos temáticos clasificados en seis grandes grupos seleccionados en base a la relevancia a futuro en el sector de la defensa y la seguridad: (i) tecnologías de la información incluyendo tecnologías cuánticas e inteligencia artificial, (ii) materiales, (iii) plataformas autónomas incluyendo también los sistemas anti-dron, (iv) sensores, (v) robótica y (vi) tecnologías de comunicaciones. Este informe pretende ser más extensivo que intensivo, en el sentido de que no se profundiza excesivamente en cada línea de I+D, pero sí que pretende cubrir todas las que sean relevantes. Además, dada la existencia de cátedras específicas en la red horizontes centradas en los temas de ciberseguridad y segmento espacial, no se han considerado en este informe las líneas relacionadas.

Este informe de prospectiva forma parte de los trabajos realizados por el nodo de Sistemas de Defensa y Seguridad del observatorio de Defensa y Seguridad de la Red Horizontes Isdefe en 2024 articulado a través de la Cátedra Isdefe-UPM (Universidad Politécnica de Madrid).

1.2. CONTEXTO

Las líneas de I+D identificadas en este informe se han seleccionado en base a los siguientes criterios:

- Temáticas más abordadas en las ediciones recientes del congreso DESE I+D [1]
- Listado y contenidos de los Capability Technology Groups (CapTechs) de la Agencia Europea de Defensa [2]. La definición de los programas de trabajo 2023-2025 de los programas Horizon Europe de los clusters 3 (Civil Security for Society) [3] y 4 (Digital, Industry and Space) [4] y el programa de trabajo del Fondo Europeo de Defensa (EDF) 2024 [5].
- Las tecnologías abordadas en el estudio realizado por Estado Mayor Conjunto, y titulado “Tecnologías Emergentes Y Disruptivas (EDT) de Mayor Interés/Aplicación a Nivel Nacional (BITD)” con el objeto de estudiar e identificar aquellas tecnologías avanzadas, emergentes y que puedan tener un efecto disruptivo, de mayor interés y potencial aplicación para las Fuerzas Armadas, en las que la Base Industrial y Tecnológica de Defensa nacional se encuentre bien posicionada [6]
- Las tecnologías descritas en los años recientes del número de enero de la revista IEEE Spectrum, que presenta cada año en dicho mes una prospectiva de los avances tecnológicos esperados para el año [7]
- Resultado del proyecto ASSETS+: Alliance for Strategic Skills addressing Emerging Technologies in Defence [8], proyecto Erasmus+ cuyos resultados se harán públicos en un plazo de doce meses desde la finalización del mismo.
- Indicadores bibliométricos relativos al número de publicaciones encontradas en cada temática desde el año 2020.

En cada línea identificada se ha hecho un análisis de las ideas más relevantes en las que se está investigando actualmente y que se espera que marquen el desarrollo y aplicaciones futuras.

En el WP1 del proyecto ASSETS+ se realiza un estudio exhaustivo de las tecnologías más relevantes para el ámbito de la defensa, en base al tratamiento automático de más de 500.000 referencias bibliográficas, clasificando múltiples tecnologías y aplicaciones (Figura 1)

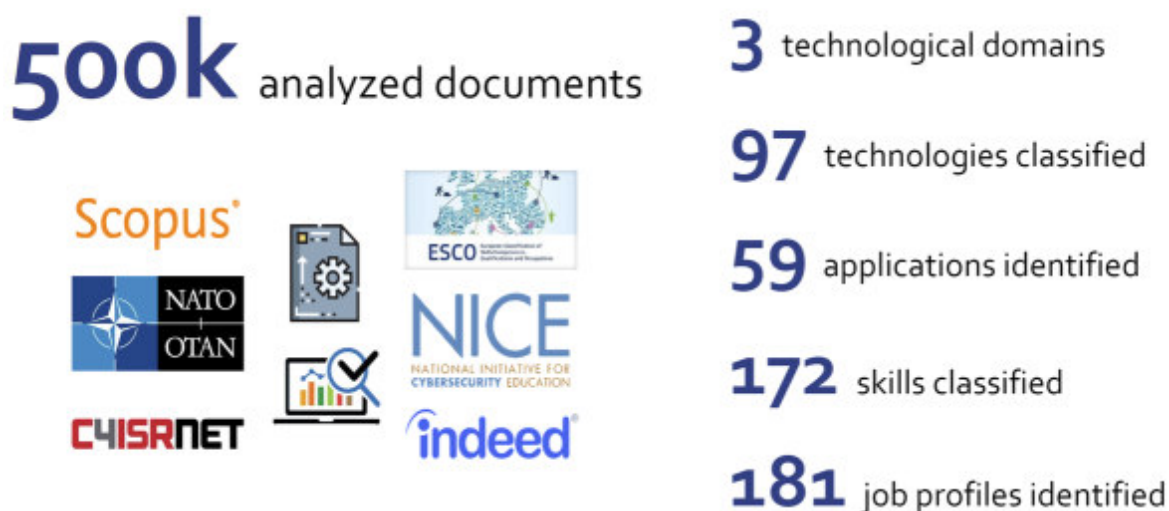


Figura 1. Parámetros del estudio bibliométrico ASSETS+.

Los resultados de este estudio han sido muy relevantes para la selección de las líneas recogidas en este informe. En las Figuras 2 y 3, se presentan a modo de ejemplo dos análisis relevantes de este estudio que muestran el peso de los conceptos, sus interrelaciones y la “matriz de relevancia”, en la que se estudian tecnologías específicas y su relevancia para operaciones concretas de defensa.

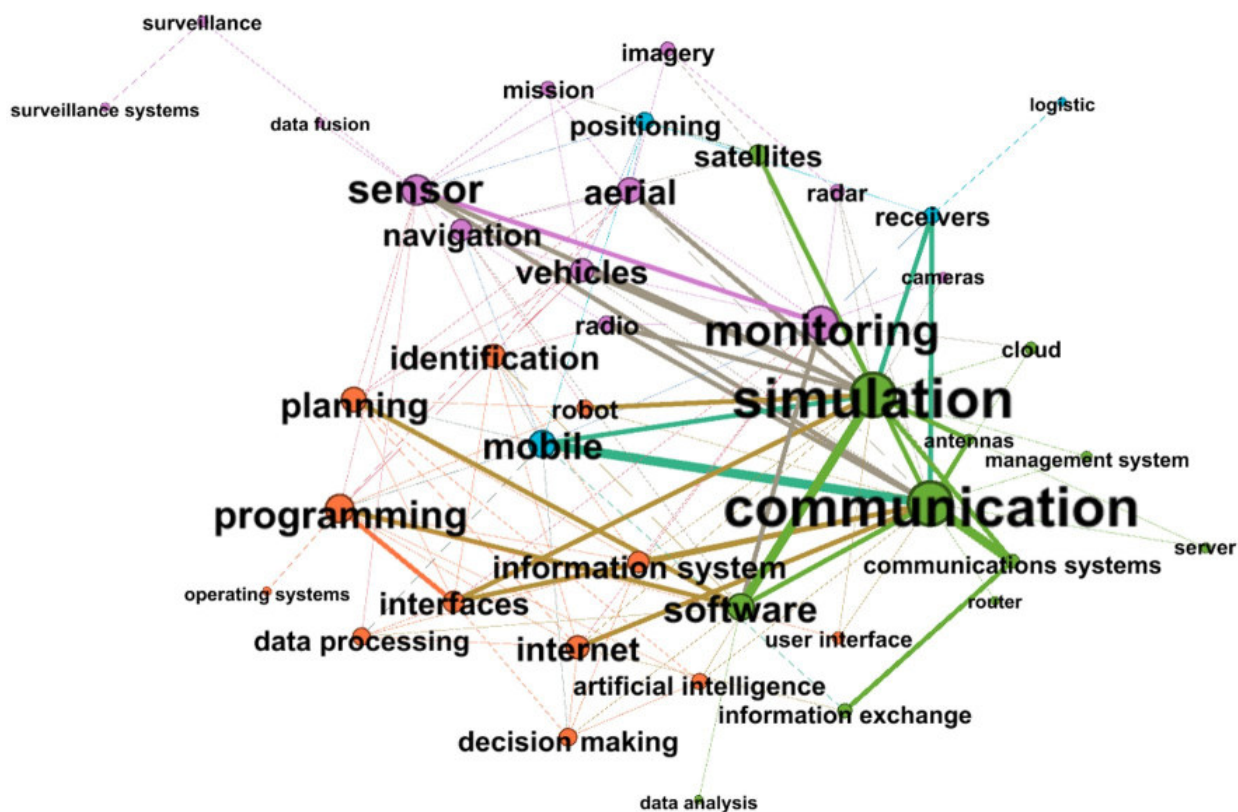


Figura 2. Mapa de peso-relación de diferentes keywords en el estudio bibliométrico de ASSETS+.

keyword	Mission planning	Mission control	Reconnaissance	Surveillance	Routing	Scheduling	Assignment	Coverage	Rescue	Target tracking	Combat simulation	Military vehicle manufacturing	Missile guidance	Anomaly detection	Trajectory tracking	Path planning	Space technologies	Cyber security	Cyber resilience	Aeronautics	land armours	Naval	Underwater	Satellite	Weapons	Fighter aircrafts
Artificial Intelligence	8	8	7	7	6	6	7	7	6	7	7	6	6	6	5	7	8	7	5	5	0	7	6	6	7	4
Autonomous system	8	9	8	8	6	6	7	7	6	8	8	6	6	5	6	7	8	6	5	6	0	7	7	7	7	4
Robotics	7	7	6	7	5	5	5	6	5	6	6	5	5	4	5	6	7	5	3	4	0	6	6	6	6	3
Simulation	9	10	8	9	7	7	8	8	7	8	10	7	7	6	7	8	9	7	6	7	0	9	7	8	9	5
Optimization	8	9	8	8	7	7	7	8	6	8	8	7	6	6	6	7	8	6	5	7	0	8	6	7	8	5
Sensor	9	9	8	9	7	7	7	8	7	9	8	7	7	7	7	8	9	7	5	7	0	8	7	8	8	5
Explainable artificial intelligence	4	4	3	4	1	1	3	3	2	3	3	2	1	1	0	3	4	4	3	0	0	3	2	2	3	0
Blockchain	1	1	0	2	1	0	0	1	0	2	0	0	0	1	1	0	2	2	0	0	0	0	0	1	1	0
Deep learning	7	7	6	7	5	5	6	6	5	6	7	5	6	5	5	6	7	6	5	5	0	6	5	6	7	4
Reasoning network	7	8	7	7	6	6	7	7	6	7	7	5	6	5	5	7	7	6	4	5	0	7	5	6	7	4
Edge computing	7	7	6	7	6	5	6	6	5	6	7	6	5	5	5	6	7	6	4	6	0	6	5	6	6	4
Signal processing	8	8	8	9	6	6	7	8	6	8	8	6	6	6	7	7	8	6	4	6	0	8	7	8	8	5
Image Semantic Segmentation	3	3	3	3	3	2	3	3	3	3	3	3	3	2	1	3	3	2	1	2	0	3	2	3	3	1
Machine learning	8	8	7	7	6	6	6	7	6	7	7	6	6	5	6	7	8	6	5	5	0	7	6	6	7	4
Fog computing	5	5	5	5	4	4	4	5	4	5	5	4	5	3	4	5	5	3	1	4	0	5	4	4	5	3
Neural network	7	7	6	7	5	6	6	6	5	6	7	5	5	5	5	6	7	5	4	5	0	6	5	6	6	4
Big data	8	8	7	8	6	6	7	7	6	7	7	6	6	6	6	7	8	7	5	6	0	7	6	7	7	5
Adversarial machine learning	5	5	4	5	3	4	4	4	3	4	4	4	4	4	3	4	5	4	4	3	0	4	3	4	5	2
Clustering	6	6	5	6	5	5	5	6	4	6	6	4	4	4	4	5	6	5	3	4	0	6	4	5	5	3
Internet of Things	7	7	6	7	6	6	6	6	5	6	7	5	6	5	5	6	7	6	5	5	0	7	5	6	7	4
Soft robotics	5	5	5	5	4	4	4	5	4	5	5	4	4	3	3	5	5	4	2	4	0	5	4	5	5	1
3D printers	3	3	3	3	3	2	3	3	3	3	3	3	3	3	2	3	3	1	0	2	0	3	2	3	3	0
SG	4	5	4	4	3	3	2	3	3	4	4	3	3	2	3	4	5	2	1	3	0	3	3	4	4	1
Object Co-segmentation	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cyber physical system	7	7	5	6	5	5	5	6	5	6	6	4	5	4	4	6	7	7	6	4	0	6	4	5	6	2
Computer vision	8	8	7	7	6	6	7	7	6	7	8	6	6	5	6	7	8	6	5	6	0	7	6	7	7	4
Sentiment analysis	5	5	4	4	3	1	3	4	3	4	4	2	2	3	2	4	5	4	3	2	0	4	1	3	4	0
Reinforcement learning	6	6	5	5	4	4	5	5	4	5	5	4	4	3	4	5	6	5	3	4	0	5	4	5	6	2
Support vector machine	6	7	6	7	5	5	6	6	5	6	6	5	5	5	5	6	7	5	4	5	0	6	5	6	6	4
Cloud computing	6	7	6	6	5	5	5	6	5	6	6	5	5	4	5	6	7	6	4	5	0	6	4	6	6	3
Autonomous vehicle	8	8	7	8	6	6	6	7	6	7	7	6	6	5	6	7	8	6	5	6	0	7	7	7	7	4
Machine translation	6	7	6	6	5	5	6	6	5	6	6	5	5	4	5	6	7	5	4	5	0	6	4	6	6	3
Natural language processing	7	7	6	7	6	6	6	7	6	7	7	6	6	5	5	7	7	6	5	5	0	7	5	6	7	4
Augmented reality	7	7	6	7	5	6	6	6	6	7	7	5	6	4	5	6	7	5	4	5	0	7	5	6	7	4
GPS	7	8	7	8	6	5	6	7	6	7	7	5	6	5	6	7	7	5	3	5	0	6	6	7	7	4
Fuzzy logic	6	6	5	6	4	5	5	5	4	5	6	4	5	4	4	5	6	4	3	4	0	5	4	5	6	3
Voice recognition	7	7	6	6	5	5	6	6	5	6	6	5	5	4	4	6	7	5	3	4	0	6	4	5	6	4
Human Machine Interaction	8	8	7	7	6	6	7	7	6	7	8	6	6	5	6	7	8	6	5	5	0	7	6	6	7	4
High performance computing	8	8	7	8	6	6	7	7	6	7	8	6	6	6	6	7	8	7	5	6	0	7	6	7	7	4
Structures and Materials	7	8	7	7	5	6	6	7	6	7	8	7	6	5	5	6	8	5	4	6	1	7	5	7	7	5

Figura 3. Matriz de relevancia tecnología-misión.

Sin embargo, este estudio se centra únicamente en tres ámbitos tecnológicos: C4ISTAR, Ciberseguridad y Plataformas Autónomas y Robótica, por lo que en base a otras fuentes y criterios que tienen en cuenta las publicaciones y tendencias actuales se han considerado adicionalmente áreas muy relevantes como son los nuevos materiales o las tecnologías de producción de energía. Por ello, de acuerdo con criterios de relevancia para el sector de la defensa y seguridad y el análisis de resultados bibliográficos se han seleccionado las líneas que se detallan en la Tabla 1 agrupadas en las siguientes seis categorías:

- I. **Tecnologías de la Información:** se incluyen doce tecnologías concretas, algunas de ellas agrupadas en las subcategorías de Inteligencia Artificial, y de Tecnologías cuánticas

- II. **Materiales y químicos:** se describen seis tecnologías que incluyen desde nuevos materiales, hasta generación de energía y fabricación aditiva, así como detección y neutralización de sustancias prohibidas o peligrosas.
- III. **Plataformas autónomas:** se consideran seis líneas tecnológicas, algunas de ellas clasificadas bajo el epígrafe de “drones” y otras como “anti-drone”.
- IV. **Sensores:** se seleccionan cuatro tecnologías que incluyen sensores activos y pasivos, tanto electromagnéticos como ópticos o acústicos, y su explotación y procesado.
- V. **Robótica:** se incluyen dos tecnologías, aquellas directamente relacionadas con el desarrollo de robots y otras asociadas a sistemas de potenciación de las capacidades humanas.
- VI. **Comunicaciones:** se seleccionan tres categorías relacionadas con los sistemas de comunicación relacionadas con las redes y los sistemas de radio definida por software y con la temática de la nube de combate.

	Nº de referencias desde 2020 (x1000)
I. TECNOLOGÍAS DE LA INFORMACIÓN	
I.1. Tecnologías cuánticas	
Quantum radar	19,3
Quantum computing	35,4
Quantum communications	20
1.2. IA	
Toma automatizada de decisiones	20
OSINT	6,3
IA generativa	31,1
IA explicable	23
Combatiente del futuro: Detección de estrés, fatiga, nerviosismo, etc..	0,36
Mantenimiento y logística predictivos, detección de corrosión	29,9
Gemelo digital	39,1
Realidad aumentada	192
Receptores fotónicos	16,9
II. MATERIALES y QUÍMICOS	
Metamateriales	18,4
Materiales para el combatiente (blindaje, tejidos)	9,9
Detectores de explosivos, drogas, etc.	37,4
NRBQ: detección y neutralización	7,4
Pilas de combustible: power-producing technologies	0,6
Fabricación aditiva	93,3
III PLATAFORMAS AUTÓNOMAS	
Tecnología y misiles hipersónicos	9,9
III.1 Unmanned systems	
Enjambres y colaboración entre plataformas	17,5
AI based navigation	4,8

Propulsión	13,6
III.2 Anti-dron	
DEW	16,2
Láseres de alta potencia	15,7
IV SENSORES	
Sensores ISTAR: IA y big-data	16
Sistemas radar AESA, C-RAM y pasivos	1,8
Procesado de señales acústicas	22,4
Identificación de emisiones con IA	20,9
V ROBÓTICA	
Robots	54,4
Sistemas de potenciación de capacidades humanas	17,3
VI Tecnologías de comunicaciones	
Nube de combate	0,24
Radio software y radio cognitiva	27,9
Redes definidas por software	17,7

Tabla 1. Tecnologías analizadas

El número reflejado debe considerarse solo como mero indicativo, ya que el dato obtenido depende de qué palabras concretas se introduzcan en el buscador, de manera que se filtren resultados indeseados o no relevantes. Sin embargo, sí que puede considerarse como una aproximación a un “mapa de calor” de las distintas tecnologías, representado en la Figura 4.

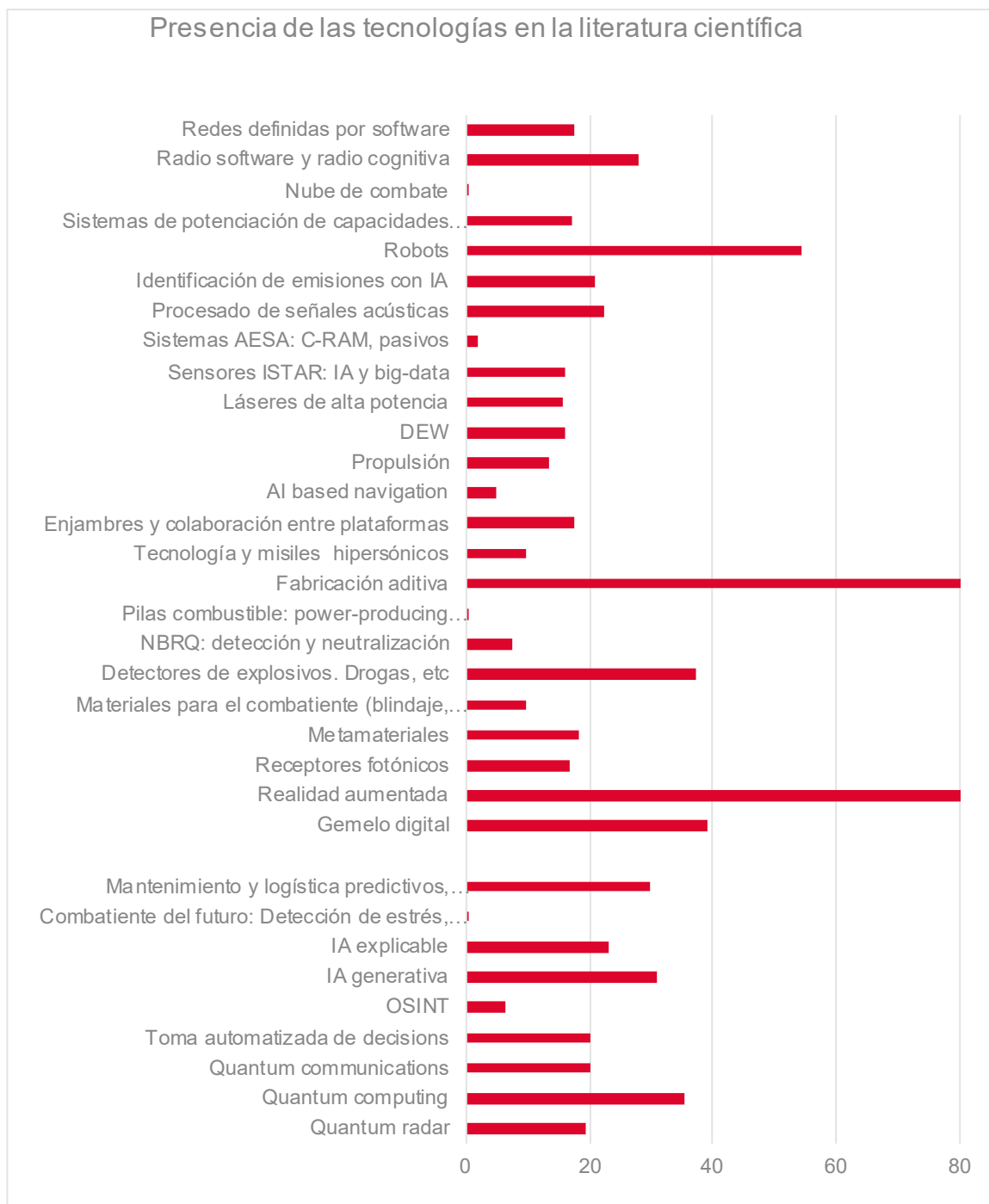


Figura 4. Mapa de calor de las tecnologías estudiadas.

2. FACTORES DE INFLUENCIA

El desarrollo de las líneas tecnológicas identificadas de relevancia para el sector de la defensa y la seguridad puede verse influenciado por los principales factores que se han identificado y especificado en la Tabla 2.

FACTORES DE INFLUENCIA	
Factores geopolíticos y geoestratégicos	<ul style="list-style-type: none"> • <u>Conflictos bélicos</u> y aumento de la inestabilidad que fomenten la inversión y desarrollo en tecnologías específicas. Por ejemplo, los conflictos actuales han puesto de manifiesto la importancia del desarrollo de plataformas autónomas, así como de sistemas de defensa frente a dichas plataformas (como las tecnologías anti-dron). • Definición de <u>prioridades y líneas de ruta</u> en el desarrollo de ciertas tecnologías de defensa por parte de los estados u organizaciones internacionales (OTAN, EDA, ...) que aceleren el avance tecnológico. Estas prioridades marcadas por decisiones estratégicas o necesidades actuales impactan de manera directa en el desarrollo y selección de temáticas de los programas de investigación y desarrollo (EDF, Coincidente,...). A nivel nacional y europeo, las principales líneas estratégicas actuales están marcadas por los documentos “2023 EU Capability Development Priorities” de la EDA, la Estrategia de Tecnología e Innovación para la Defensa (ETID) del 2020, y “NATO 2022 Strategic Concept”. • El <u>control de la exportación</u> de ciertas tecnologías también puede marcar el desarrollo tecnológico de determinadas líneas y el alcance de ciertas capacidades tecnológicas a nivel nacional
Factores tecnológicos	<ul style="list-style-type: none"> • Aparición y desarrollo de <u>tecnologías disruptivas</u> hasta TRLs altos que fomenten el desarrollo de nuevas aplicaciones y ciertas tecnologías. Por ejemplo, los desarrollos en computación cuántica que pueden llegar a aumentar extraordinariamente las capacidades de computación de los superordenadores actuales pueden actuar de habilitadores de nuevos enfoques y aplicaciones de tecnologías de inteligencia artificial de mayor complejidad gracias a la capacidad de procesar mayores cantidades de información en menor tiempo. • La <u>convergencia de tecnologías</u> puede igualmente fomentar el desarrollo, innovación y aparición de nuevas aplicaciones y capacidades en base a sinergias. Un ejemplo es la convergencia de las tecnologías de comunicaciones, sensores e inteligencia artificial en sistemas que aportan capacidades integradas o la aparición del concepto sistema de sistemas. • Desarrollo de <u>tecnologías de uso dual</u> que puede tener un efecto la velocidad, financiación y dirección de desarrollo de ciertas tecnologías y aplicaciones. Este factor es especialmente relevante en las tecnologías de comunicaciones de banda ancha (como sistemas de comunicaciones móviles o, incluso actualmente, sistemas de comunicaciones por satélite) o en las

	tecnologías de inteligencia artificial, cuyo desarrollo está fuertemente marcado por aplicaciones civiles.
Factores normativos	<ul style="list-style-type: none">• El desarrollo de <u>legislación internacional o nacional</u> sobre el uso de ciertas tecnologías también puede impactar en el desarrollo de las mismas. En este aspecto es importante resaltar el desarrollo actual de legislaciones en relación con el uso de plataformas autónomas o de la inteligencia artificial.
Factores económicos	<ul style="list-style-type: none">• La <u>evolución económica</u> puede impactar en el desarrollo de tecnologías de menor coste frente a aquellas tecnologías que requieren una mayor inversión para su desarrollo.
Factores ambientales	<ul style="list-style-type: none">• El <u>fomento de tecnologías sostenibles</u> puede fomentar el desarrollo, la financiación y la innovación de aquellas tecnologías que presentan un menor impacto en el medio ambiente. En este sentido se puede comentar como ejemplo los “Starter Projects” sobre proyectos de economía circular en defensa de la EDA o el desarrollo y producción de combustibles alternativos como el hidrógeno “verde”, sintetizado mediante el uso de energías renovables.

Tabla 2. Factores de influencia en el sector de la defensa y la seguridad.

3. IDENTIFICACIÓN DE TENDENCIAS

En base a los seis grupos temáticos de tecnologías relevantes en el sector de la defensa y la seguridad, se han identificado líneas tecnológicas cuyo desarrollo presenta un impacto actual y otras líneas emergentes que se espera que presenten un impacto importante a más largo plazo (en los próximos 5 a 10 años).

3.1. TENDENCIAS ACTUALES

3.1.1. INTELIGENCIA ARTIFICIAL

Toma automatizada de decisiones

Se espera un crecimiento sostenido del mercado de la IA de más del 15% en los próximos años. En la actualidad, más del 80% de los nuevos desarrollos o líneas de I+D incorporan la IA, y un gran número de decisiones hoy en día son informadas o directamente tomadas por una IA.

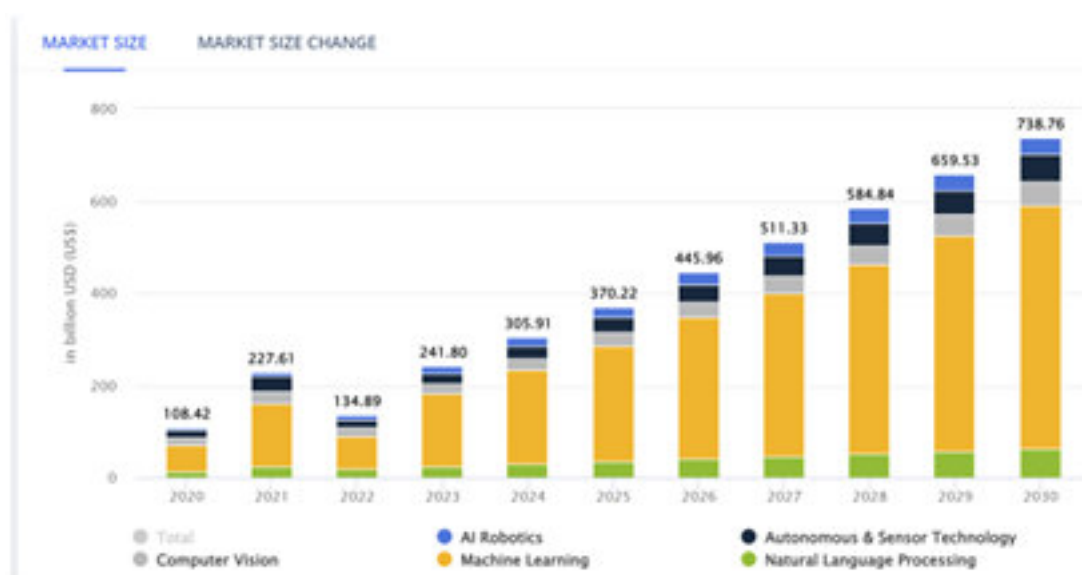


Figura 5. Prospectiva de mercado de la IA en los próximos años [Statista Market Insights].

Un amplio número de artículos analizados tratan sobre los impactos sociales que tiene la toma automatizada de decisiones. En concreto se identifican los principales riesgos generados por el uso de sistemas algorítmicos, las deficiencias del marco jurídico en materia de protección de datos a estos efectos y pone de manifiesto la necesidad de una mayor intervención regulatoria en la utilización pública y privada de los sistemas automatizados de procesamiento de datos y toma de decisiones. Sin duda, estos aspectos van a ser claves en el futuro inmediato.

Sin embargo, la posibilidad de que la IA “alucine” está siempre presente y el reto de lograr certificar decisiones basadas en IA es un reto pendiente en el que se está trabajando. Actualmente, y para defensa especialmente, la opción de dejar la decisión final al humano es la que prevalece (“Man in the loop”). Sin embargo, las alternativas denominadas “Man ON the loop” y “Model in the loop” se están abriendo paso de forma muy potente.

OSINT

Un buen número de artículos analizados muestran una visión general del uso de OSINT y analizan las diferentes plataformas que utilizan OSINT, así como los fines con los que lo utilizan. Los artículos hacen

especial hincapié en las amenazas que conlleva el uso malintencionado de OSINT y las medidas para combatir dichas amenazas. La referencia [9] describe el estado actual de la OSINT y hace una revisión exhaustiva del paradigma, centrándose en los servicios y técnicas que mejoran el campo de la ciberseguridad. Uno de los ámbitos donde más se está avanzando es en la extracción del sentir de sociedades, analizando estados de ánimo, sentimientos y opinión social, en base al estudio de publicaciones en las redes sociales, una enorme fuente de información abierta.

La OSINT se está beneficiando de los grandes avances tecnológicos en cuanto a generación, disponibilidad de información y capacidad de proceso, pero se encuentra también varios retos, principalmente derivados de la falta de estructura y fiabilidad de los datos, y hacia los que se está dirigiendo mucha actividad.

Pros ✓	Cons X
Huge amount of available information	Complexity of data management
High capacity of computing	Unstructured information
Big data and machine learning	Misinformation
Complementary types of data	Data sources reliability
Flexible purpose and wide scope	Strong ethical/legal considerations

Figura 6. Ventajas y retos actuales de la OSINT [9]

IA generativa

La irrupción de Chat-GPT a finales de 2022 ha generado una reacción cadena de avances en la que muchos competidores están luchando por ofrecer los mayores avances (Figura 7).

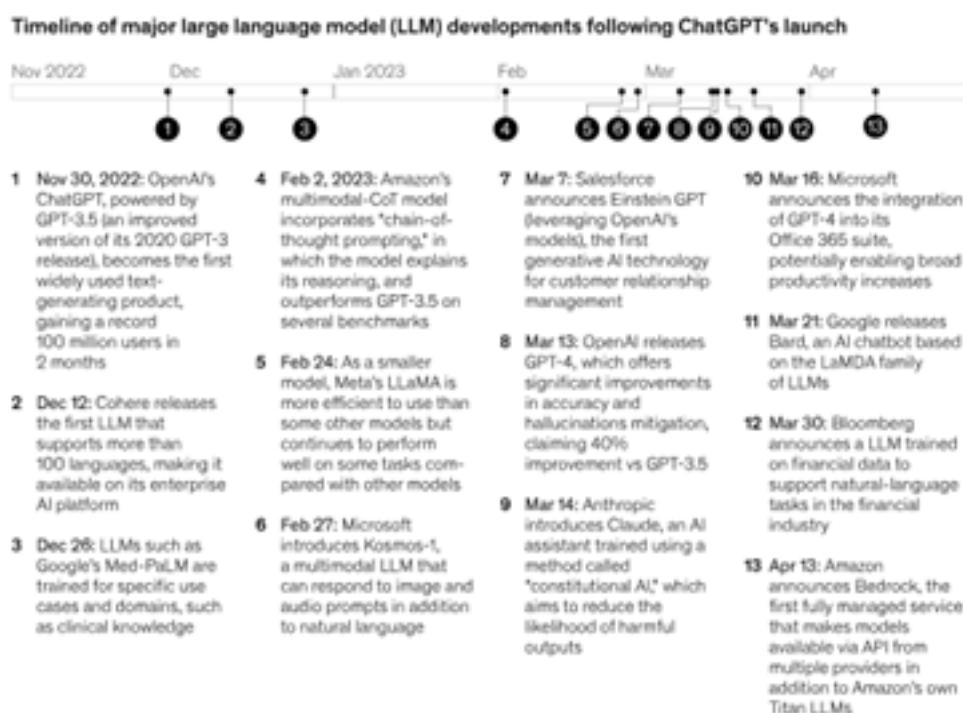


Figura 7. Principales hitos de la IA generativa tras ChatGPT [10].

Debido a la irrupción de la IA generativa, los expertos señalan que se alcanzarán capacidades “de nivel humano” entre 10 y 40 años antes de lo que se estimaba hace solo 5 años. El gráfico siguiente (Figura 8) muestra las estimaciones de estas habilidades humanas que se hacía en 2017 (línea discontinua) frente a la actual.

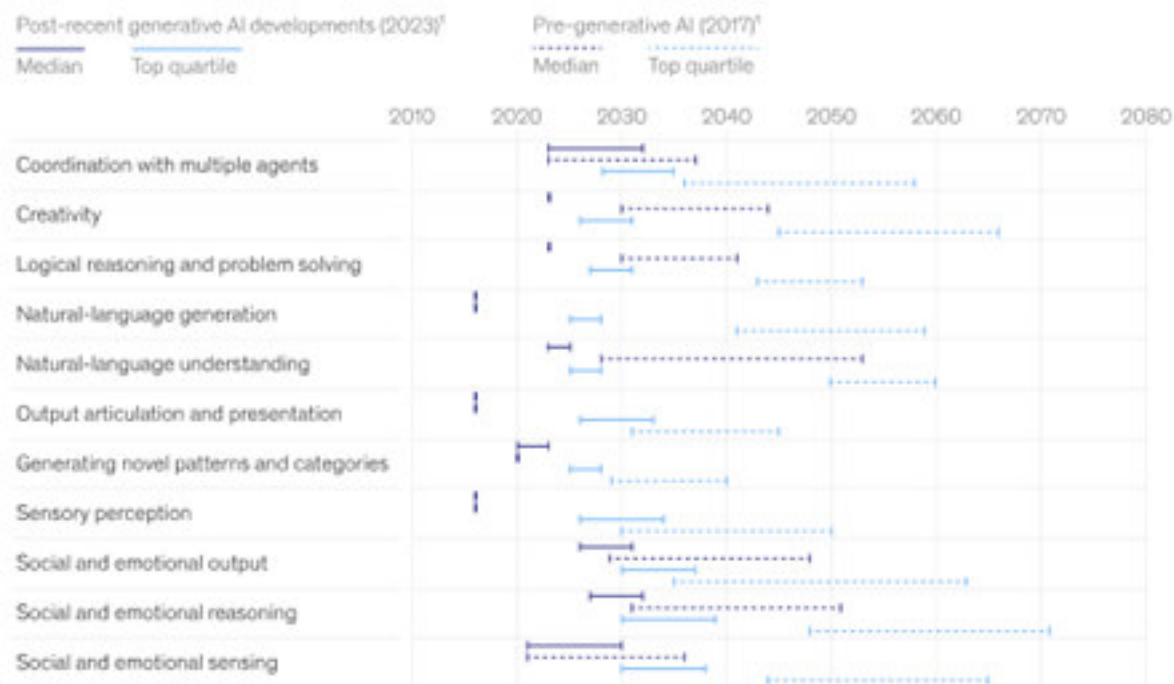


Figura 8. Estimación de las capacidades de la tecnología para emular las capacidades de nivel humano en los próximos años [10].

En relación con su potencial para defensa y seguridad, se estima que tendrá un impacto decisivo en las siguientes áreas:

- Mejora de la conciencia situacional. La IA generativa podrá leer de manera integrada la información obtenida por la enorme cantidad de sensores desplegados en el campo de batalla e interpretar y mostrar una descripción entendible y sintética de la situación para ayudar a la toma de decisiones en tiempo real.
- Mejora de los procedimientos de entrenamiento militar y simulación. De hecho, es en la formación en general donde la IA generativa está despertando más interés. Por ejemplo, en [11] se presenta un análisis sobre la irrupción de esta herramienta y cómo puede ser utilizada en el ámbito formativo, así como sus limitaciones y usos erróneos.
- Avances en los vehículos autónomos. Es uno de los campos donde la IA es más evidente. Tanto la de tipo generativo como la orientada a la toma de decisiones autónomas.
- Ciberdefensa y ciberseguridad. Adelantándose a las posibles amenazas

Uno de los mayores retos es la carga computacional que la implementación masiva de estas técnicas requiere.

IA explicable

Sin duda, la IA despierta muchos recelos. Y una de las razones principales es el hecho de que los algoritmos operan como una “caja negra” que no permite entender por qué en un momento dado se obtiene un cierto resultado, o como evitar que la IA “alucine”.

Desde hace ya años, la EDA ha manifestado el interés en utilizar IA explicable en el ámbito de la defensa, para caminar hacia una IA más robusta, controlada y segura. Un buen número de artículos analizados sobre esta temática muestran diferentes técnicas de IA explicativa y el empleo de diferentes algoritmos de Deep learning en diferentes sectores para los que son muy útiles y optimizan la producción y el desarrollo. La referencia [12] examina la literatura existente y las contribuciones ya realizadas en el campo de la IA explicable, incluyendo una perspectiva hacia lo que aún queda por alcanzar. Además, resume los esfuerzos previos para definir la explicabilidad en el aprendizaje automático y en distintos modelos de machine learning.

Combatiente del futuro: Detección de estrés, fatiga, nerviosismo, etc.

Como se ha dicho, al análisis de sentimientos humanos, es un área de gran potencial para la IA. Sin duda, el combatiente del futuro es un programa que puede beneficiarse de estos avances. Se han analizado un buen número de artículos que corresponden a estudios sobre métodos de predicción del nivel de estrés en combatientes, los efectos que causan el estrés y la fatiga en el organismo y a la psicología del combatiente, como por ejemplo en la toma de decisiones, y las causas con las que está relacionado el aumento del nivel de estrés. Como ejemplo, la referencia [13] describe un prototipo de asistente inteligente para la monitorización del estrés (SMA) para profesionales que deben hacer frente a la exposición a factores de estrés físico y psicológico extremos.

Mantenimiento y logística predictivos

Esta es una de las áreas donde la IA tiene un mayor interés en el campo civil y en la industria en general. Por ello, hay un gran número de artículos técnicos que se dedican a este campo, y de los que el ámbito de defensa puede incorporar ideas y tecnologías. Aparte de algoritmos concretos, en muchos trabajos publicados se resumen las metodologías fundamentales sobre enfoques basados en datos para el mantenimiento predictivo en diferentes industrias e instalaciones de ingeniería. Llevan a cabo investigaciones sobre los distintos campos de aplicación del pronóstico de máquinas, así como algoritmos de DL (Deep learning) y ML (machine learning) para el mantenimiento predictivo. La referencia [14] trata de dar un enfoque general y revisar la bibliografía actual relativa al mantenimiento predictivo y los sensores inteligentes en las fábricas inteligentes.

Para algún ejemplo concreto, pueden verse también los documentos [15] y [16] generados por la propia cátedra ISDEFE-UPM y donde se analizan soluciones a uno de los problemas más habituales encontrados: la falta de suficientes datos etiquetados y fiables (Figura 9).

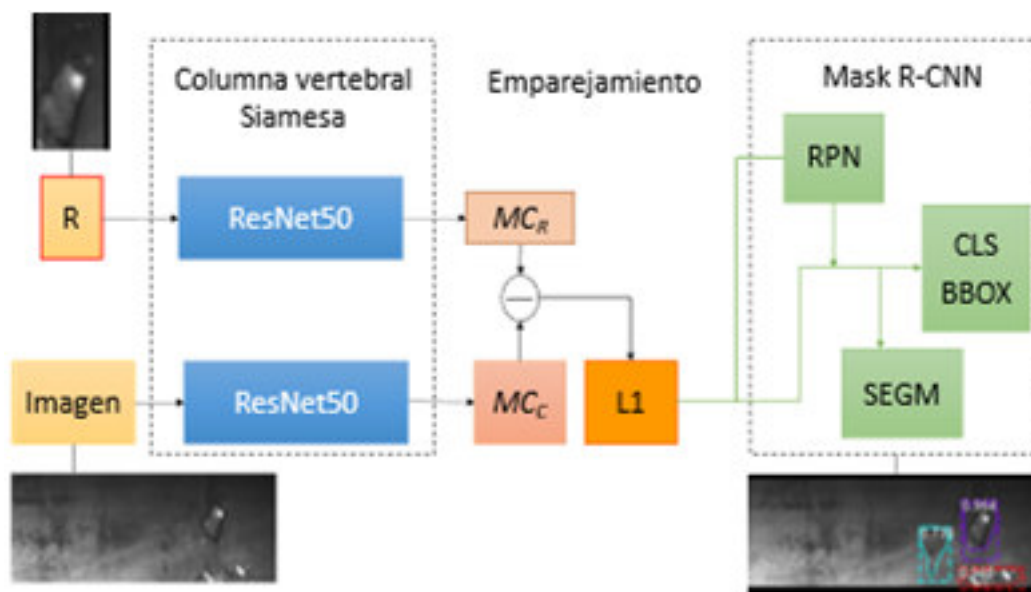


Figura 9. Posible alternativa al reto de aplicar IA en entornos de escasez de datos suficientes para el entrenamiento [16].

3.1.2. GEMELO DIGITAL

El desarrollo de gemelos digitales es otro ámbito que ha despertado gran interés en los ámbitos de defensa, por el impacto que supone respecto al diseño, mantenimiento, conocimiento y mejora de los complejos sistemas desarrollados en los últimos años: buques, plataformas en general, sistemas de comunicaciones, sensores, sistemas de armas, etc.

Un buen número de artículos analizados corresponden a estudios genéricos sobre lo que es un gemelo digital y lo que aporta, así como directrices para su explotación para smart manufacturing y mantenimiento. El resto de referencias se centra principalmente en describir desarrollos de gemelos digitales de sistemas concretos. La referencia [17] presenta un estudio sistematizado y clasificado de toda la bibliografía sobre el tema, por lo que puede ser considerada un buen análisis del estado del arte.

3.1.3. REALIDAD AUMENTADA

Un buen número de referencias analizadas analizan el uso de la tecnología de la realidad aumentada en diferentes sectores y como se ha desarrollado para satisfacer las necesidades de esos sectores. El sector más repetido es el de la formación. Otros artículos hablan de la irrupción de la realidad aumentada y los componentes de diseño de los sistemas de RA.

Sin duda, la RA tiene un enorme potencial también para el combatiente del futuro. Existen, por ejemplo, ambiciosos programas internacionales para crear bases de datos de geografía humana geolocalizada. Presentar información en tiempo real al combatiente, acerca por ejemplo de ubicaciones de agua, etiquetado de edificios, marcado de conflictividad de zonas, etc., será una ayuda altamente valiosa. Los avances en la actualidad están orientados a la creación de dichas bases de datos, así como a los avances tecnológicos que permitan la miniaturización y ergonomía de los equipos.

La referencia [18] presenta las estructuras básicas de los cascos de realidad aumentada y realidad virtual, describe sus principios de funcionamiento. Analiza nuevos dispositivos que ayudan a mejorar el rendimiento de la RA y la RV y ofrece una perspectiva para los posibles desarrollos de las futuras pantallas de RA.



Figura 10. Soldado portando un prototipo de Integrated Visual Augmentation System (IVAS)

3.1.4. MATERIALES PARA EL COMBATIENTE (BLINDAJE, TEJIDOS)

Un buen número de los artículos que se han analizado exponen pruebas de resistencia de los blindajes corporales de distintos materiales y los tejidos en impactos balísticos en diferentes condiciones (intemperie, elevación de la temperatura corporal, etc.). Otros artículos analizados exponen materiales adicionales buscando reducir costes y cantidad de material manteniendo las propiedades necesarias y que además sean más sostenibles. La referencia [19] expone la sustitución de los materiales que componen los cascos de protección balística de los combatientes por un material reciclable y biodegradable que además la reducción de capas de volumen de este nuevo material es mayor al porcentaje de reducción de protección.

3.1.5. DETECTORES DE EXPLOSIVOS, DROGAS, ETC.

La detección de explosivos es otro de los grandes retos tecnológicos pendientes. Hoy por hoy, en pleno siglo XXI, el método más fiable es la utilización del olfato de un animal que fue domesticado en el neolítico. Sin duda se espera que la tecnología pueda hacerlo mejor en los próximos años.

Varias referencias estudiadas exponen los principales métodos de detección de explosivos y se centran en la optimización de los sensores que imitan el sentido del olfato para detectar estas amenazas (nariz electrónica). Otras referencias explican métodos de procesamiento de los datos sensoriales para la detección precisa de drogas y explosivos, el uso de tecnología de terahercios, e incluso el uso de bacterias modificadas genéticamente. El artículo [20] ofrece una visión global de la detección de trazas de explosivos (DTE), destacando los retos que plantea y proporcionando una comprensión de los principios, ventajas y limitaciones de cada tecnología, relacionándolos con los sistemas actuales.

3.1.6. *NRBQ*

La defensa Nuclear, Radiológica, Biológica y Química (NRBQ) es cada vez más necesaria por un posible aumento de estos ataques realizados por células terroristas [21]. Esto es debido a la alta disponibilidad y cercanía con las tecnologías que lo permiten. Un clásico análisis de situación se describe en la referencia [26], en el que la disponibilidad de material nuclear en un hospital, su distribución a través de la Dark Web y su utilización usando un dron como vector, ponen de manifiesto la alta facilidad con la que un grupo terrorista puede acceder a la tecnología necesaria.

No hay un gran número de referencias en la literatura científica abierta sobre este tema, pero la mayoría de ellas se centran en la monitorización y detección de ataques o eventos NRBQ, usando tecnologías químicas, sensores, drones, etc.

3.1.7. *PILAS DE COMBUSTIBLE: POWER-PRODUCING TECHNOLOGIES*

Un amplio número de artículos analizados se centran en la investigación para el descubrimiento de distintos materiales y métodos de fabricación para mejorar el rendimiento de las pilas de combustible y simplificar sus componentes. Otra tendencia muy destacada es el estudio de reacciones para la producción de hidrógeno que con las pilas de combustible ofrecen una alternativa energética descarbonizada. La referencia [22] presenta el último estado de desarrollo de la tecnología de pilas de combustible PEM (membrana electrolítica polimérica) y sus aplicaciones en la energía portátil y de transporte y describe la gestión de los materiales y del transporte de agua/térmico para el diseño y el control operativo de las pilas de combustible.

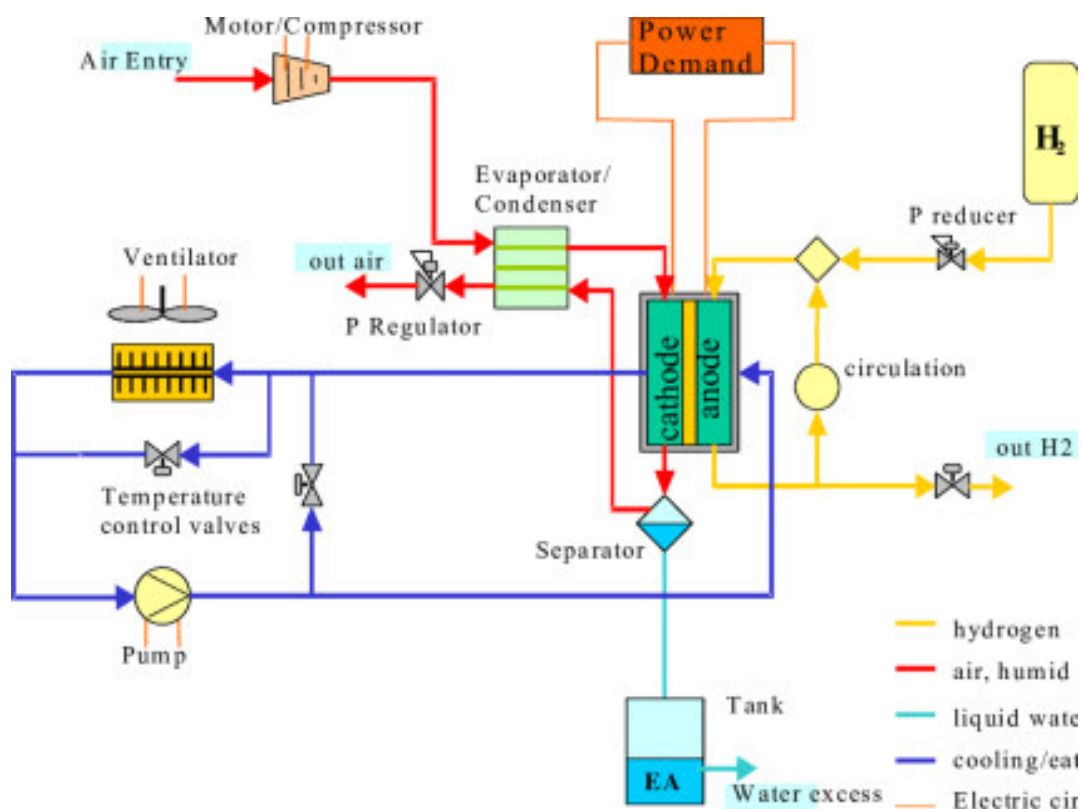


Figura 11. Ejemplo de una pila de combustible PEM [22]

3.1.8. FABRICACIÓN ADITIVA

La mayor parte de los trabajos que se están publicando actualmente resumen el estado actual de las tecnologías punteras de fabricación aditiva y sus aplicaciones en los diferentes campos e industrias. Presentan el estado del arte, al tiempo que se resumen los principales escenarios de aplicación. La referencia [23] refleja los últimos avances y tendencias en fabricación aditiva y se adhiere a las normas ASTM y otras; incluye capítulos sobre temas que abarcan toda la cadena de valor de la AM, como la selección de procesos, el software, el posprocesamiento, los impulsores industriales de la AM y proporciona una amplia gama de preguntas técnicas para garantizar una comprensión exhaustiva de los conceptos tratados.

Hay 10 tendencias destacadas en este ámbito (Figura 12), pero las tres siguientes son las que se espera que tengan un mayor impacto:

- Powder Bed Fusion (PBF): La fusión en lecho de polvo se utiliza principalmente para piezas funcionales de bajo volumen en todas las industrias y para la impresión de piezas únicas, como piezas de máquinas, plantillas y accesorios. Los componentes creados a partir de la impresión 3D por PBF presentan propiedades mecánicas comparables a las del mecanizado y la fundición. PBF también admite una amplia gama de materiales y permite el desarrollo simultáneo de múltiples piezas. Los métodos de PBF más comunes son la sinterización selectiva por láser (SLS), la fusión por haz de electrones y la fusión selectiva por láser (SLM). Los avances en este campo se centran en mejorar la pureza del polvo y reducir la dispersión del tamaño de las partículas. Aunque las mejoras de hardware aceleran enormemente las aplicaciones de PBF, las propiedades mejoradas del polvo ampliarán sus casos de uso. Además, las nuevas

empresas están desarrollando materiales de impresión 3D de bajo coste para hacer que el PBF sea más asequible.

- **Automatización de procesos:** Aunque la impresión 3D automatiza el desarrollo de piezas individuales, los fabricantes utilizan flujos de trabajo digitales y sistemas de automatización para optimizar aún más las líneas completas de fabricación basadas en impresión 3D. Por ejemplo, el procesamiento automatizado de piezas elimina la intervención manual después de la producción de componentes, lo que aumenta el rendimiento de la producción. En consecuencia, las nuevas empresas ofrecen soluciones de software y hardware de diseño y procesamiento independientes de las impresoras que automatizan los procesos de fabricación aditiva. Permiten el desarrollo de piezas de alta velocidad, la fabricación bajo demanda y la creación rápida de prototipos, al tiempo que mejoran la flexibilidad de impresión y minimizan los residuos. Además, las líneas de impresión 3D automatizadas reducen los costes de mano de obra y eliminan los errores manuales.
- **Nuevos materiales:** Las propiedades del material de base y del aglutinante, junto con los métodos de impresión 3D, tienen un impacto significativo en las propiedades mecánicas del producto impreso. Es por eso que las startups están desarrollando materiales novedosos para aplicar la fabricación aditiva en diversos casos de uso. Además, los materiales inteligentes, la cerámica, la electrónica, los biomateriales y los compuestos encuentran uso en el desarrollo de componentes con propiedades avanzadas. Permiten la impresión 3D de productos no convencionales como dispositivos médicos, electrónica de consumo y órganos bioartificiales. Además, las nuevas empresas están extrayendo materiales imprimibles en 3D de alto valor a partir de flujos de desechos para reducir los requisitos de material virgen y las emisiones.

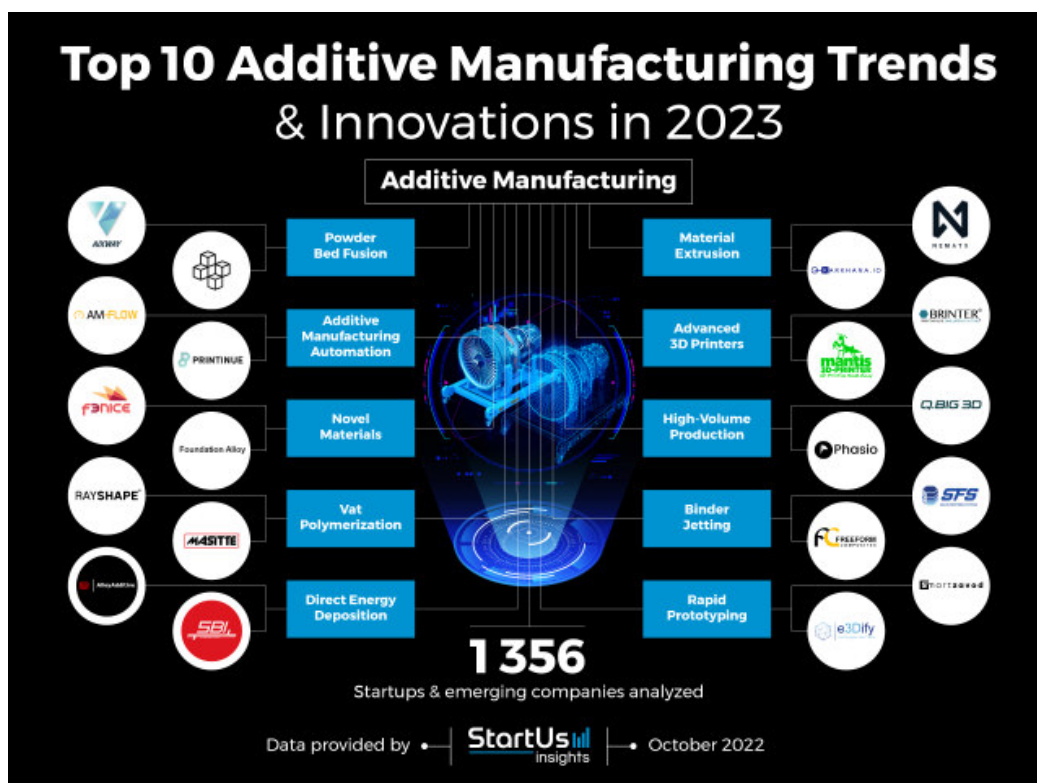


Figura 12. Principales tendencias actuales de evolución de la fabricación aditiva [StartUs insights].

3.1.9. UNMANNED SYSTEMS

Misiles hipersónicos

La tecnología de misiles hipersónicos es una amenaza que ya es una realidad y contra la cual no se está suficientemente preparado. Un amplio número de referencias recientes hablan sobre el aumento del desarrollo de las armas hipersónicas y la amenaza que pueden suponer para la seguridad, pues son muy difíciles de detectar e interceptar. Además, afirman que se trata de un sector que todavía tiene un amplio margen de crecimiento y mejora. Otros artículos tratan el control de este tipo de armamento para reducir riesgos o exponen diferentes mecanismos de vuelo de misiles hipersónicos. La referencia [24] revisa el desarrollo del vehículo hipersónico basado en el concepto “air-breathing” y su tecnología de guiado y control, que tiene un gran valor militar y económico potencial debido a sus características: alta velocidad, largo alcance y respuesta rápida. Los avances en propulsión de los próximos años son clave para el desarrollo de esta capacidad.

Enjambres y colaboración entre plataformas

Los enjambres son ya otra realidad que representa una gran amenaza potencial (véase sección 5.2 Antidrón). Un amplio número de artículos analizados exponen algoritmos de inteligencia de enjambre en la colaboración de múltiples plataformas (principalmente UAV). Entre los algoritmos destacan: prevención de colisiones, asignación de tareas, planificación de trayectorias y reconfiguración de formaciones. Otros artículos tratan el tema de cooperación entre enjambres y humanos para llevar a cabo distintas tareas.

La inteligencia distribuida y la colaboración con plataformas tripuladas son los ámbitos que más crecimiento se espera que experimenten los próximos años. En el entorno europeo el gran programa NGWS/FCAS (Figura 13) es paradigmático, donde un caza avanzado trabaja en colaboración con un grupo de drones. La explotación de esta configuración con sensores avanzada, despliegue de nube de combate, inteligencia distribuida, etc. son ámbitos en los que vamos a ver desarrollos en los próximos años.



Figura 13. Concepto del futuro caza europeo FCAS [Airbus]

La referencia [25] recopila y clasifica comportamientos básicos de enjambres en organización espacial, navegación, toma de decisiones, etc. Aplica esta taxonomía para clasificar una serie de aplicaciones de robótica de enjambre existentes en los ámbitos de la investigación y la industria. Por último, ofrece una visión general de las plataformas de investigación que pueden utilizarse para probar y evaluar el comportamiento de los enjambres, los sistemas que ya están en el mercado y los proyectos dirigidos a un mercado específico.

Navegación basada en IA

La necesidad de controlar los UAV de forma remota en entornos complejos limita la capacidad de los mismos y disminuye la eficiencia de todo el sistema. Por ello, muchos investigadores están trabajando en la navegación autónoma de UAV donde estos pueden moverse y realizar las tareas asignadas en función en su entorno. Con los recientes avances tecnológicos, la aplicación de la inteligencia artificial (IA) ha proliferado. La navegación autónoma de UAV es un ejemplo de una aplicación en la que la IA desempeña un papel fundamental en el suministro de características fundamentales de control humano. La referencia [26] realiza un completo resumen de todas las técnicas existentes sobre navegación autónoma basada en IA, sus limitaciones y tendencias de futuro (Figura 14):

- **Nuevos enfoques:** el aprendizaje federado (FL) encabeza la lista de nuevos enfoques. El objetivo de FL es entrenar un modelo de IA de forma distribuida en múltiples dispositivos utilizando conjuntos de datos locales sin compartirlos. Además, FL previene los ciberataques de forma natural, ya que los UAV no requieren compartir datos. FL se puede integrar con cualquier algoritmo de IA para la navegación autónoma de UAV y reduce la complejidad del espacio y el tiempo mediante el uso del aprendizaje central. Sin embargo, aún no se ha implementado para la navegación autónoma de vehículos aéreos no tripulados, lo que requiere su exploración. Además, la implementación de enfoques basados en ontologías para la navegación de un enjambre de vehículos aéreos no tripulados todavía no ha sido adecuadamente analizada. Karimi et al. utilizó un enfoque basado en ontología para navegar robots en un sitio de construcción en que puede modificarse para usarse en la navegación en enjambre de UAV en futuras investigaciones.
- **Consumo de energía:** los vehículos aéreos no tripulados utilizan baterías como fuente de energía principal para respaldar todas las actividades, incluidos el vuelo, la comunicación y el procesamiento. Sin embargo, las capacidades de las baterías de los UAV son insuficientes para vuelos prolongados. Muchos investigadores han aplicado diferentes algoritmos, como esquemas de sueño y despertar, incorporación de dispositivos móviles de vanguardia para computación externa y uso de energía solar, para optimizar el uso de energía de los UAV. Resolver el problema energético mediante la recolección de energía durante el vuelo es una dirección para futuras investigaciones. Sin embargo, una visita autónoma a una estación de carga que utilice IA también puede resolver este problema.
- **Potencia computacional:** los UAV son de tamaño muy pequeño en comparación con otros vehículos. Así, sus capacidades de memoria y energía son bajas, lo que les confiere un bajo poder computacional. Por el contrario, la implementación de enfoques de IA basados en optimización y aprendizaje requiere una alta potencia computacional. Superar esta cuestión sigue siendo un problema de investigación abierto. El desarrollo de enfoques de IA eficientes con bajo consumo de energía computacional puede ser una solución clave a este problema. Por lo tanto, es necesario explorar adecuadamente esta área.
- **Amenazas físicas:** Las amenazas físicas son muy recurrentes cuando se trata de misiones de vigilancia y UAV SaR (search and rescue). Anteriormente se han implementado muchos enfoques de IA para evitar obstáculos. Sin embargo, no existe ninguna solución que evite amenazas físicas repentinas. En consecuencia, las soluciones basadas en IA para evitar amenazas físicas requieren una investigación en profundidad.

- **Tolerancia al fallo:** Los fallos ocurren con frecuencia en vehículos en movimiento. El manejo de fallos de software es muy fácil de lograr con un programa de emergencia integrado. Sin embargo, faltan soluciones basadas en inteligencia artificial para fallos difíciles de manejar, como problemas de hardware, fallos de equipos y fallos de comunicación entre componentes. Por lo tanto, esta área sigue siendo un problema de investigación abierto.
- **Escasez de datos de aprendizaje:** Este es un problema recurrente en muchos ámbitos de la IA. Como avance representativo de lo que se está haciendo, la referencia [27] investiga la eficacia de bases visuales de preentrenamiento de imágenes en lenguaje contrastivo (CLIP) y amplía una de las bases produciendo un agente capaz de navegar hacia objetos que no se utilizaron como objetivos durante el entrenamiento.

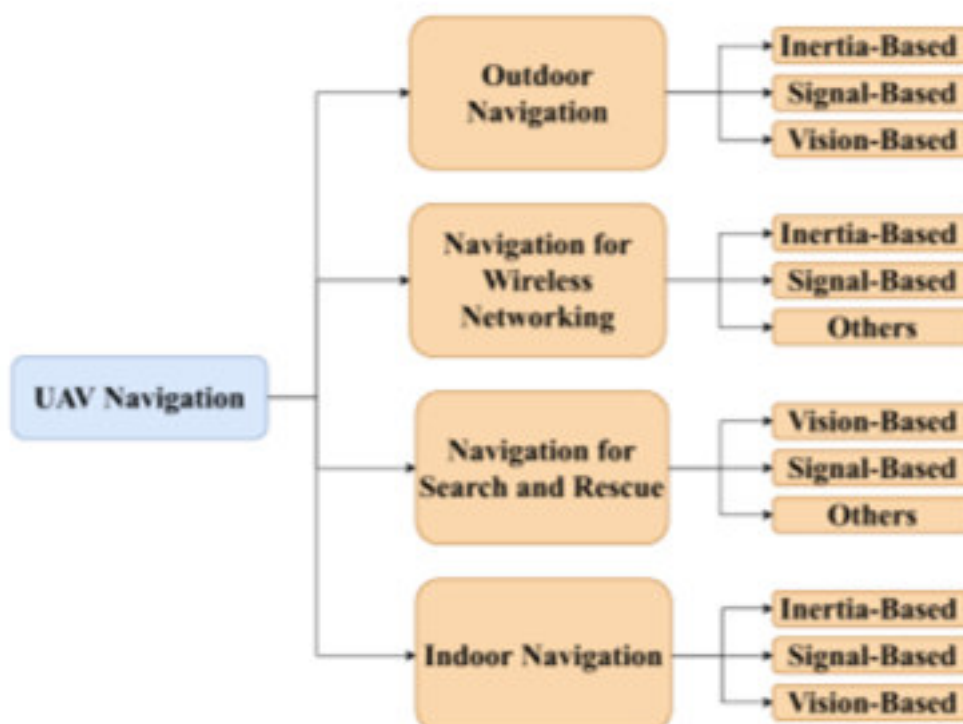


Figura 14. Taxonomía de la navegación autónoma de UAVs por aplicaciones y tipo de información de base [26].

Propulsión

Un amplio número de referencias analizadas exponen el estado del arte de las tecnologías de los sistemas de propulsión eléctrica y propulsión híbrida de transportes, así como evaluar su viabilidad tratando de utilizar energía renovable y sostenible. Otros artículos se centran en el éxito de nuevos sistemas de propulsión espacial eléctricos. La referencia [28] representa el estado actual y perspectivas de futuro exponiendo los fundamentos de la propulsión eléctrica.

3.1.10. SISTEMAS ANTI-DRON

El mayor esfuerzo de I+D en la actualidad se está poniendo en la neutralización, ya que el tema de la detección está bastante bien resuelto. Sin embargo, la identificación, y más en concreto la distinción entre drones y pájaros para automatizar lo más posible la vigilancia es otro de los temas calientes.

Armas de RF de energía dirigida

En este ámbito concreto, se desarrolló en la cátedra un estudio específico que se recoge en [29]. Los ámbitos más significativos de I+D son:

- El desarrollo de tecnologías asequibles de generación de potencia de RF, tales como el magnetrón relativista, los osciladores MILO y BWO o los Klystron relativistas.
- El desarrollo de sistemas de alimentación y de suministro de energía pulsada a dichos generadores, tales como generadores de Marx.
- El desarrollo de antenas capaces de soportar la enorme energía generada.
- La construcción de sistemas integrados completos (Figura 15)



Figura 15. Sistema de energía dirigida Ranets-E, de fabricación rusa [online].

Láser de alta potencia

Al igual que en el caso anterior, el reto principal es la generación de potencia suficiente para producir la neutralización del UAV. Un amplio número de referencias analizadas exponen nuevos materiales con los que se fabrican nuevos láseres de alta potencia que consiguen mejores prestaciones. Otros artículos presentan sistemas láser de alta potencia fabricados y cuantifican sus prestaciones.

Aunque no es exactamente esta temática, es interesante señalar otra perspectiva observada del uso de esta tecnología, que es el empleo de láseres de alta potencia para cargar la batería drones en vuelo y aumentar su tiempo de operación.



Figura 16. Dron alimentado mediante un láser [Northwestern Polytechnical University].

Clasificación drones vs. pájaros con IA

La tendencia más fuerte es el empleo de la firma microdoppler para realizar la clasificación (Figura 17). Sin embargo, está ganando mucha fuerza el empleo de técnicas basadas en comportamiento y aprendizaje automático, que pueden emplearse con virtualmente cualquier sensor. Esta es una de las líneas que se está actualmente trabajando en la cátedra y que ha generado el documento breve recogido en la referencia [30].

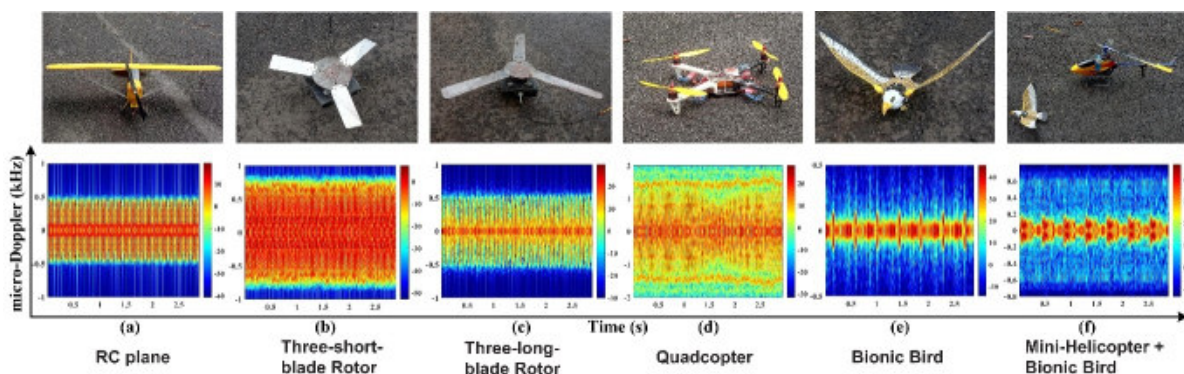


Figura 17. Firma microdoppler de distintos drones [31]

3.1.11. *SENSORES ISTAR: IA Y BIG-DATA*

Sin duda la detección de objetos y la extracción de información a partir de imágenes captadas por sensores ISTAR es la línea más importante. Se proponen nuevos algoritmos continuamente, pero otros grandes retos son conseguir bases de datos suficientes y significativas, procesar y almacenar de manera eficiente grandes cantidades de datos, y conseguir resultados con planteamientos de IA explicable. La referencia [32] es interesante por realizar un análisis exhaustivo de las técnicas y retos pendientes.

3.1.12. SISTEMAS AESA, C-RAM Y RADARES PASIVOS

Un amplio número de referencias analizadas exponen mejoras para aplicar a las distintas funcionalidades del sistema AESA (Active Electronically Scanned Array) y a los sistemas C-RAM (Contracohetes, artillería y mortero) e incrementar sus prestaciones y su rendimiento, así como reducir limitaciones. Otros artículos de este campo ofrecen soluciones alternativas al sistema AESA y realizan una comparativa entre las prestaciones del sistema alternativo con el sistema AESA. Incluso la realización de técnicas AESA utilizando múltiples nodos en sistemas multiestáticos.

El campo de los radares pasivos ha incrementado mucho su presencia en la literatura científica los últimos años. Una línea muy interesante, aparte de descripciones prácticas de despliegue de sistemas, son los avances en procesado multi-iluminador y multiestático.

La referencia [33] expone las tecnologías subyacentes que suponen una ventaja competitiva en los nuevos sistemas radar avanzados:

- Los componentes de Nitruro de Galio para los front-end de radiofrecuencia
- Los convertidores A/D y D/A de alta velocidad para la generación ágil de formas de onda sofisticadas
- El aumento de las capacidades de proceso en tiempo real para dotar a los sistemas de capacidades cognitivas
- Los buses de alta velocidad para la realización de fusión de sensores en tiempo real

3.1.13. PROCESADO DE SEÑALES ACÚSTICAS

Este es un campo muy amplio y que tiene diversas aplicaciones en el ámbito de la defensa. Resaltamos a continuación las tres tendencias principales observadas en el panorama de I+D:

- Detección de drones utilizando su firma acústica
- Clasificación de sonidos mediante aprendizaje automático, en particular para la detección de eventos de disparos, clasificación de armamento en base al sonido, etc.
- Técnicas para procesamiento de señal de los sonar, reducción de ruidos y aumento de capacidades subacuáticas.

La referencia [34] expone los fundamentos de la teoría del campo acústico y el procesamiento de señales espaciotemporales.

3.1.14. IDENTIFICACIÓN DE EMISIONES CON IA

Este es un ámbito bastante específico de la vigilancia espectral, y de la guerra electrónica, y no es un ámbito especialmente prolífico en publicaciones científicas. La identificación de señales de comunicaciones y radar usando redes neuronales es la mayor tendencia, dentro de la cual se están investigando el desarrollo de nuevos algoritmos y nuevamente técnicas sobre cómo abordar la escasez de datos etiquetados y fiables. En este sentido, la referencia [35] realiza un estudio bastante completo del estado del arte actual y las tendencias para los próximos años.

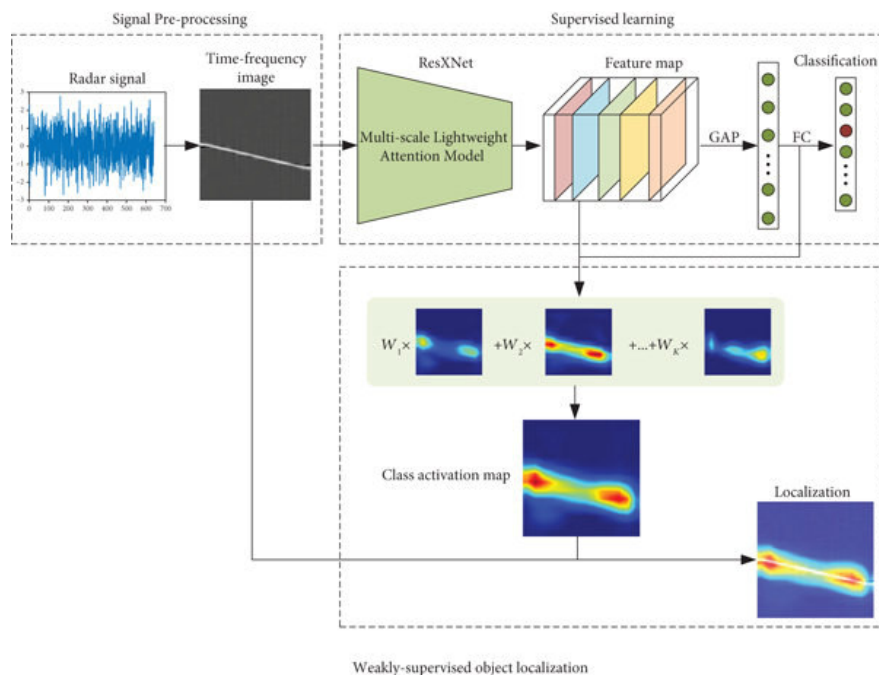


Figura 18. Esquema de aprendizaje supervisado para la clasificación de señales radar [35]

3.1.15. ROBOTS

Según la revista Spectrum del IEEE, en su número de prospectiva de enero define el año 2024 como el año del robot humanoide. Buena prueba de ello son numerosos desarrollos que están realizándose en esta línea (Figura 19).

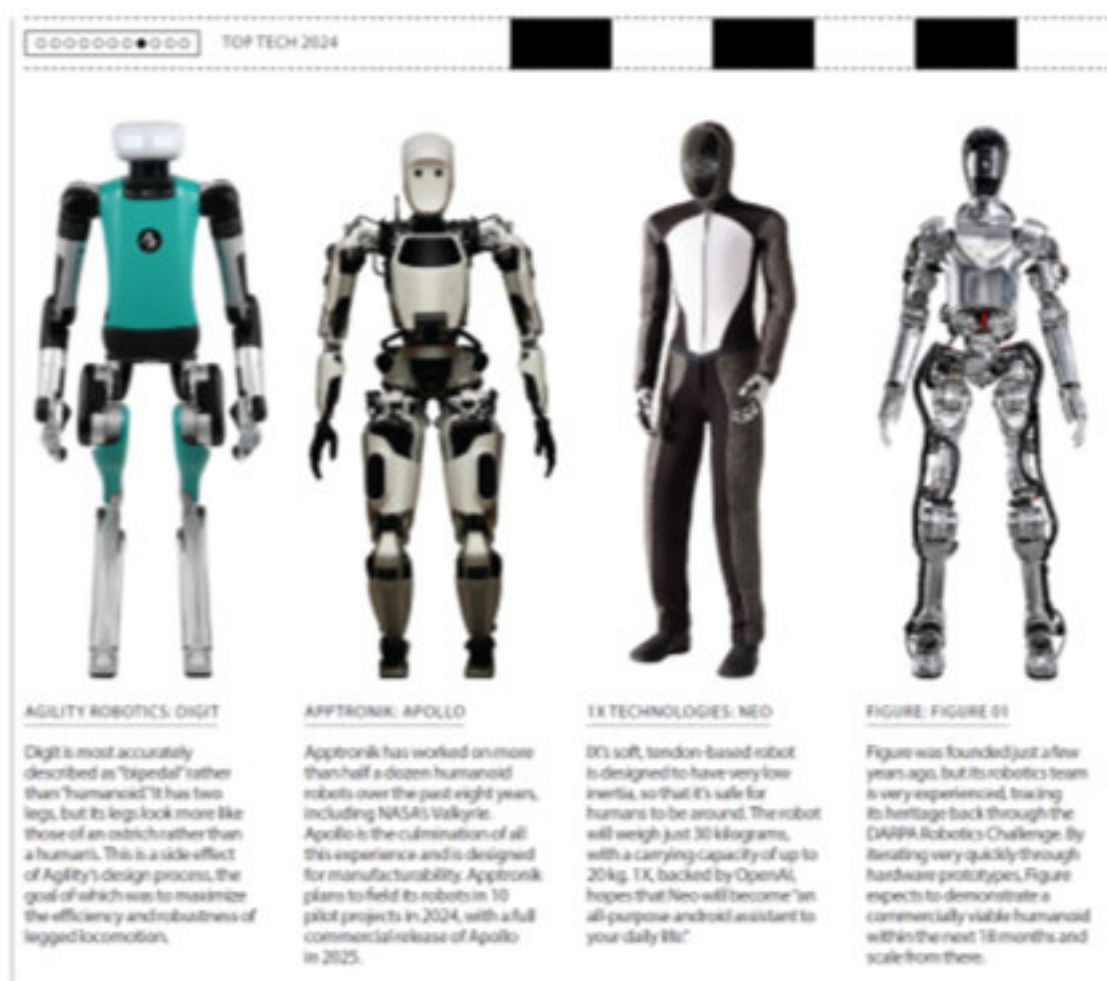


Figura 19. Prototipos de robots humanoides en desarrollo [IEEE Spectrum, enero 2024]

Yendo al campo de las publicaciones más técnicas, un amplio número de referencias analizadas abordan el tema de percepción del entorno de los robots y sus respuestas ante los estímulos, así como la capacidad de procesamiento, respuesta rápida y adaptación en tiempo real de los robots. Otras líneas se centran en las aplicaciones prácticas de los robots en diferentes sectores, sobre todo el de la medicina. Uno de los campos con más publicaciones es el relativo a los avances en el software de control. La referencia [36] aborda precisamente el diseño de sistemas operativos para robots y su uso eficiente.

Sin duda, y dentro de este ámbito, la dotación de IA a los robots es una tendencia de futuro muy clara y tiene un enorme potencial. Sin embargo, todavía se está en una situación bastante incipiente, exceptuando quizá los trabajos de Boston Dynamics. La Inteligencia IA generativa, tiene el potencial de alcanzar niveles de verdadera comprensión humana. La clave para ello es integrar el sistema computacional de IA con un robot. El robot debe poseer movilidad, sentidos (como el tacto, la visión y el oído) y la capacidad de interactuar con objetos físicos, lo que permitirá al sistema experimentar realimentación sensorial inmediata de cada acción que realice. Este circuito de realimentación permite que el sistema aprenda y comprenda. El enfoque actual sobre la IA en la robótica está pasando de la cuestión de qué tareas pueden realizar los robots para las personas a qué tipo de información puede proporcionar un robot a la "mente" de la IA. Al permitir que la IA explore y experimente con objetos reales, le será posible alcanzar una comprensión más profunda, muy parecida a la de un niño humano.

Con esta integración de la IA y la robótica, podemos esperar ver avances significativos en una amplia gama de aplicaciones.

3.1.16. SISTEMAS DE POTENCIACIÓN DE CAPACIDADES HUMANAS

Una sencilla definición del aumento de capacidades humanas procedente del ejército del Reino Unido es “la aplicación de la ciencia y la tecnología para mejorar temporal o permanentemente las prestaciones humanas”. Ello ha podido llevarse a cabo con el desarrollo de mejora del rendimiento, el uso de prótesis externas u otras internas, mediante la administración de fármacos, o modificando su código genético. El resultado puede esquematizarse en la Figura 20 en la que se representa este aumento potencial de capacidades, incluyendo las tecnologías que las soportan.

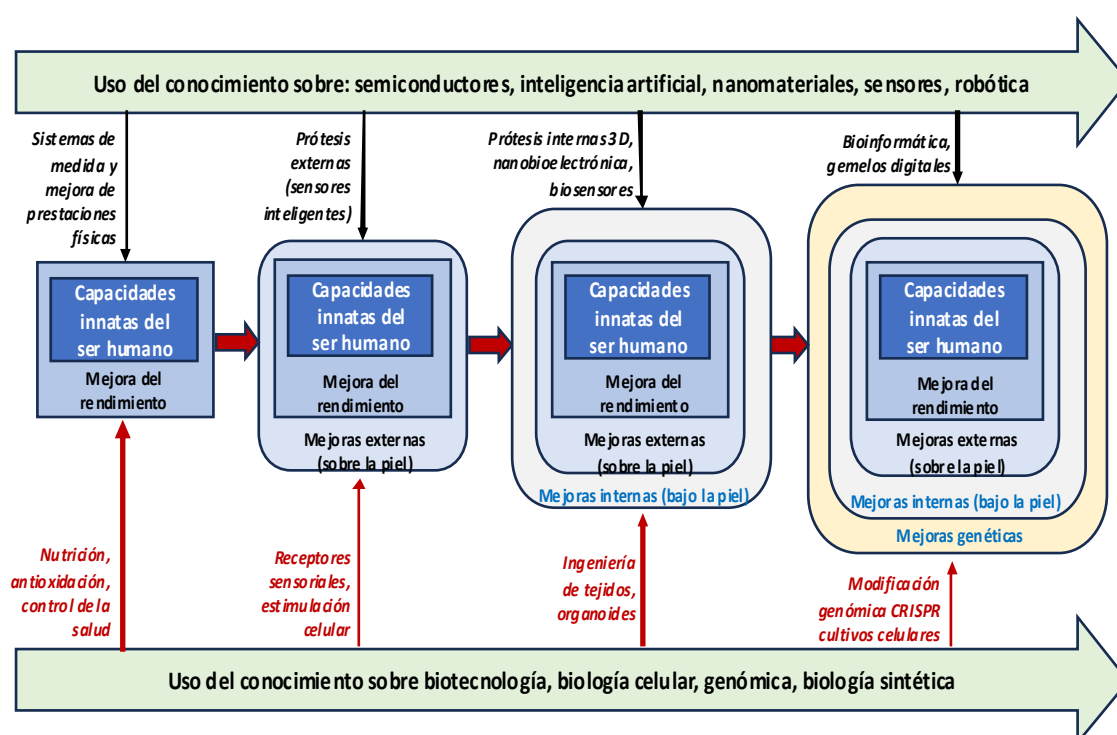


Figura 20. Fase de aumento de capacidades humanas [37]

Ha sido en las últimas dos décadas, al unísono con la rápida evolución de la biología celular, genómica, la nanotecnología, o las tecnologías de la información y las comunicaciones, cuando ha sido posible pensar en actuar sobre el cuerpo humano para mejorar sus capacidades sensoriales, motoras, cognitivas o sociales resultado de millones de años de evolución de la especie humana.

Desde la perspectiva de defensa y seguridad, las tecnologías de aumento de capacidades humanas, tanto las sensoriales, las motoras, las cognitivas o las sociales, se han considerado prioritarias en el contexto de la OTAN en su visión 2020-2040 con el objetivo de aprovechar el desarrollo de tecnologías emergentes y disruptivas para obtener la superioridad en conflictos militares. Dado el carácter clasificado de muchos de los proyectos en realización, no es fácil determinar el grado real en el que se han desarrollado, pueden emplear, o el impacto que pueden tener en el caso de su uso. En todo caso, su maduración acelerada permite pensar en su posible utilización real de manera efectiva a finales de la presente década o al comienzo de la próxima de manera generalizada en el ámbito militar, generado, a

su vez, problemas éticos relevantes en su uso en operaciones militares que es necesario debatir y regular en lo posible.

Un aspecto interesante de este campo es que aquí, además de las tecnologías más típicas como las TICs, electrónica, software, etc., irrumpen con mucha fuerza las tecnologías biológicas, y en particular, la genética. Esto ha disparado el número de publicaciones en torno a aspectos éticos, regulatorios y de seguridad, que sin duda van a ser clave en el desarrollo o no de estas tecnologías genéticas.

En estos aspectos, la referencia [38] se centra en las capacidades motoras, analizando todas las técnicas disponibles y los retos pendientes.

3.2. TENDENCIAS EMERGENTES

3.2.1. ARMAS HIPERSÓNICAS

Las armas hipersónicas se caracterizan por volar toda o gran parte de su trayectoria a través de la atmósfera, esto es, a cotas inferiores a 100 km, siendo capaces de maniobrar a velocidades hipersónicas (superiores a Mach 5) y permaneciendo la mayor parte del tiempo fuera del horizonte de radar.

Se trata de un tipo de amenaza aérea emergente que presenta nuevos retos para los sistemas de defensa antiaérea actuales. En primer lugar, las armas hipersónicas acortan los tiempos de reacción debido a su alta velocidad. Además, su menor altitud en comparación con los misiles balísticos dificulta su detección (Figura 21). Por otro lado, su gran maniobrabilidad dentro de la atmósfera, tanto en altura como lateralmente, dificulta su neutralización.

Las armas hipersónicas pueden aprovechar su alta energía cinética para realizar un impacto directo (*hit-to-kill*), o también pueden incluir una ojiva, que puede ser nuclear o convencional. Además, en régimen hipersónico la disociación del aire se vuelve significativa, lo que lleva a la formación de un escudo de plasma alrededor del vehículo. Esto puede perjudicar las comunicaciones entre el vehículo y el sistema de comando y control (C2), e incluso impedir que el misil (o planeador) navegue y se guíe por sus propios medios. Además, los altos factores de carga relacionados con maniobras de alta exigencia y las altas tasas de calor producidas por la resistencia atmosférica generan importantes riesgos para la aeroestructura del vehículo.

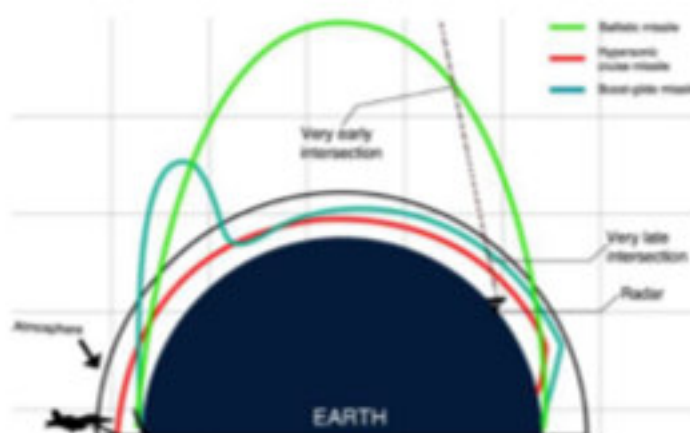


Figura 21. Perfiles de trayectorias de armas hipersónicas frente a balísticas

Existen dos tipos principales de armas hipersónicas: los misiles de crucero hipersónicos (en inglés, *Hypersonic Cruise Missile* o HCM) y los vehículos planeadores hipersónicos (en inglés, *Hypersonic Glide Vehicles* o HGV).

Los HCM son una versión mejorada de misil de crucero que alcanza velocidades hipersónicas, utilizando habitualmente para ello un motor de combustible sólido, un sistema de propulsión tipo ramjet o scramjet, o bien un ciclo de propulsión combinado. Los ramjet alcanzan velocidades de Mach 6, mientras que los scramjet (*supersonic combustion ramjet*) son supuestamente capaces de superar Mach 10. No obstante, se trata de una tecnología en estado de desarrollo. De hecho, lograr que un scramjet mantenga el régimen operativo de vuelo hipersónico sostenido se ha comparado con “mantener una cerilla encendida en medio de un huracán” [3]. La mayoría de los diseños de HCM proporcionan un alcance inferior a 2000 km y habitualmente vuelan a baja cota, entre 20 y 30 km de altitud, debiendo permanecer dentro de la atmósfera ya que los motores (exceptuando los cohetes sólidos) utilizan el aire como gas de propulsión. Generalmente, los HCMs son lanzados desde plataformas aéreas y la mayor parte del tiempo vuelan a velocidades constantes.

Los HGV son una clase de vehículos que, al no disponer de un motor para la propia propulsión, deben ser inicialmente acelerados por un misil balístico hasta alcanzar la velocidad de separación deseada. En la fase inicial, el planeador se encuentra en la parte superior del lanzador y es impulsado por él. Una vez que han finalizado las etapas de propulsión, el vehículo planeador es liberado y sigue una trayectoria balística hasta su regreso a la atmósfera, que da lugar habitualmente a un ‘rebote’ del vehículo como consecuencia del impacto con la atmósfera. Posteriormente, el vehículo sigue una trayectoria aproximadamente horizontal, es decir, sin grandes variaciones de altitud, gracias a las fuerzas de sustentación aerodinámicas, antes de ejecutar la fase terminal en la que realiza una maniobra de picado hacia su objetivo. El hecho de que un HGV pueda planear hasta su blanco permite un aumento en el alcance de estas armas en comparación con los misiles balísticos. Además, los HGV tienen una gran capacidad de maniobra que puede ser utilizada para evadir sistemas de defensa, sortear sistemas de detección o dificultar la predicción de su blanco. Por último, un lanzador puede portar varios HGV, lo cual dificulta su intercepción tras la fase de separación.

Aunque no se encuentran entre las principales amenazas hipersónicas, los vehículos de reentrada maniobrables (en inglés, *Manoeuvrable Reentry Vehicle* o MaRV), además de alcanzar altas velocidades, tienen cierta capacidad de maniobra en la fase terminal, por lo que constituyen también un desafío para los sistemas de defensa antimisiles. Los MaRVs siguen una trayectoria balística hasta la reentrada en la atmósfera. Posteriormente, tienen la habilidad de maniobrar durante la fase terminal de vuelo, describiendo una trayectoria impredecible hasta sus blancos.

Finalmente, existen otras armas que han sido catalogadas como amenazas hipersónicas, tales como los misiles aerobalísticos maniobrables, los FOBS (Fractional Orbital Bombardment System), o incluso aviones hipersónicos.

Actualmente, varias naciones están desarrollando plataformas hipersónicas tipo glider o planeadores. Estos incluyen el Hypersonic Technology Vehicle (HTV-2) de los EE. UU., el DF-ZF de China, y el Avangard de Rusia, que se lanzan desde un sistema de propulsión tradicional antes de alcanzar la velocidad hipersónica. Estas plataformas son diseñadas para deslizarse a través de la atmósfera a altísimas velocidades, reduciendo significativamente el tiempo de vuelo en comparación con los misiles balísticos tradicionales. Además, los avances en materiales avanzados, como las aleaciones refractarias y los sistemas de control aerodinámico, están permitiendo que los vehículos sobrevivan al intenso calor generado a velocidades hipersónicas.

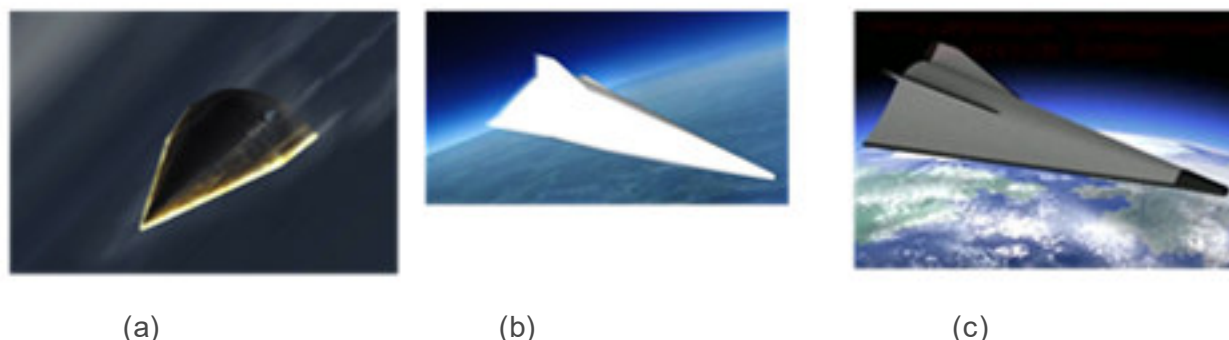


Figura 22. (a) HTV-2 Vehículo glider hipersónico experimental, DARPA Falcon Project. (b) Vehículo hipersónico DF-ZF (c) vehículo ruso Avangard HGV .

3.2.2. TECNOLOGÍAS CUÁNTICAS

Las tecnologías cuánticas en general están llamadas a tener un papel protagonista en aplicaciones de defensa y seguridad, tal como se describe en [39]. En esta referencia se hace un completo listado de muchas tecnologías y su estado de madurez, visualizando un escenario futuro de conflicto donde lo cuántico es omnipresente (Figura 23).



Figura 23. Escenario futuro de conflicto con fuerte presencia de tecnologías cuánticas [39]

Quantum radar

Un amplio número de artículos analizados corresponden a estudios teóricos sobre la comparativa de las prestaciones entre el empleo de radar cuántico y el de radar clásico y las mejoras potenciales. También se discuten diferentes esquemas de implementación para radar cuántico, sentándose las bases teóricas de un radar cuántico moderno en la referencia [40].

Sin embargo, el foco en la actualidad está puesto sobre la posibilidad de su implementación práctica: estudios de viabilidad, coste, dificultades, ... En [41] se realiza un análisis exhaustivo de los avances de los últimos años y las líneas de trabajo actuales. Destaca el reciente desarrollo de sistemas prácticos para generar fotones entrelazados en bandas de microondas. Algunos ejemplos se muestran en la Figura 24.

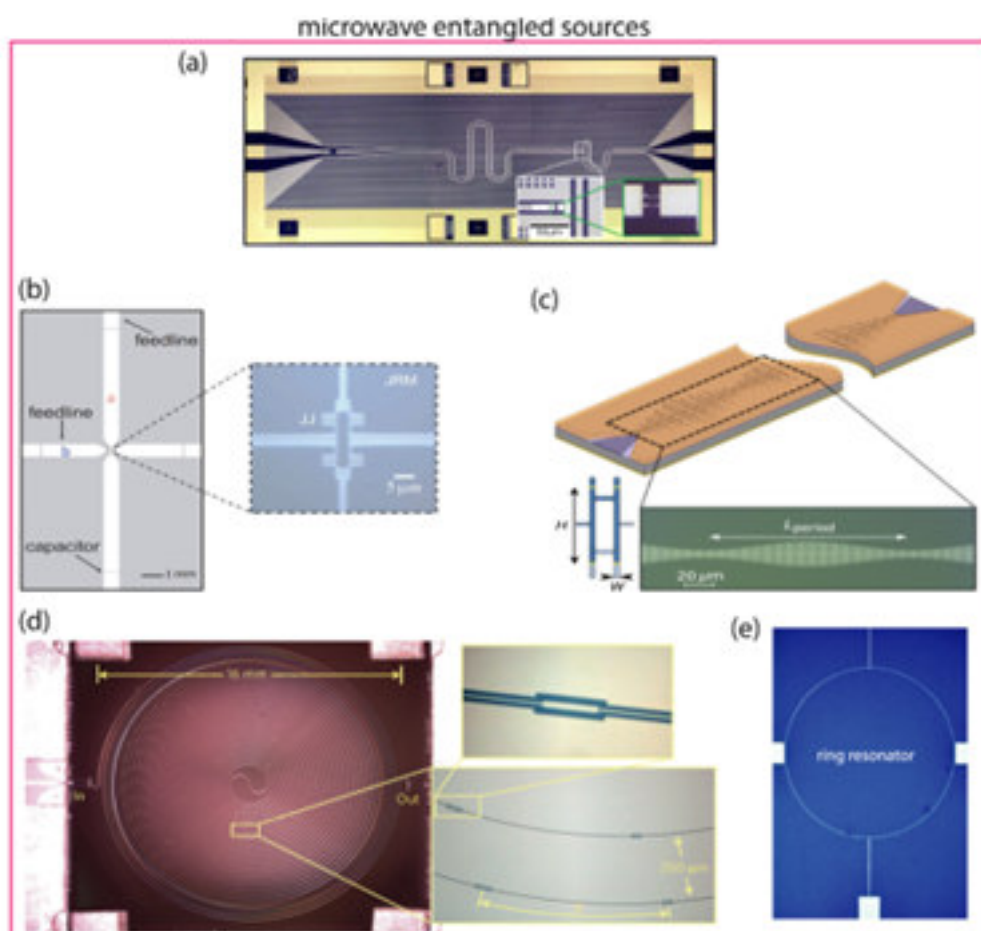


Figura 24. Fuentes de fotones de microondas entrelazados [41]

Estos avances permiten ser moderadamente optimistas respecto a lo que está por venir. Aunque existen dos obstáculos principales en el desarrollo del radar cuántico operativo. En primer lugar, el requisito de intensidades de señal extremadamente bajas para beneficiarse de la iluminación cuántica supone un desafío formidable. En segundo lugar, lograr las temperaturas extremadamente bajas necesarias para generar entrelazamientos sigue siendo un obstáculo importante. En el contexto de las aplicaciones de mejora de la precisión, los tiempos de integración necesarios plantean también un gran desafío práctico. Un enfoque para abordar estos retos pasa por identificar condiciones específicas donde la iluminación cuántica puede ofrecer ventajas significativas incluso en condiciones en que se dan las limitaciones expuestas, como escenarios con jamming intenso.

Quantum computing

La computación cuántica puede suponer una mejora muy significativa de las capacidades de los sistemas de defensa y espacio, aunque se está todavía lejos de un computador cuántico completamente funcional. Tampoco se prevé que vayan a substituir a los computadores clásicos. La computación cuántica puede emplearse en la simulación de sistemas muy complejos, en optimización y en criptografía. Numerosos países y organizaciones, tales como la NASA, están invirtiendo mucho dinero en desarrollar estas tecnologías, lo que demuestra su interés. Por ejemplo, el laboratorio QuAIL (Quantum Artificial Intelligence Laboratory) es una colaboración entre la NASA, Google y la USRA (University Space Research Association).

Los computadores actuales, sin embargo, utilizan qubits ruidosos y muy susceptibles de errores. Se estima que son necesarios entre 500 y 1000 qubits físicos para generar un único qubit lógico libre de errores. Un ordenador cuántico funcional debería tener al menos unos 200 qubits lógicos, es decir unos 200.000 qubits físicos. De acuerdo, al roadmap de IBM (Figura 25), dicho objetivo se alcanzará en torno a 2030. Otro gran problema que limita su despliegue es su gran inestabilidad. Es muy complicado mantener el estado cuántico de los qubits durante periodos de tiempo largos ya que son extremadamente delicados y muy sensibles a cambios en el entorno, temperatura, ruido, etc.

Un buen número de artículos analizados corresponden a estudios de tecnologías para aumentar el rendimiento y estabilidad de la computación cuántica, tales como el empleo de nuevos procesadores fotónicos, mejoras de circuitos, manipulación de átomos, empleo de nuevos materiales, etc. [42]

Desde el punto de vista de la seguridad, es muy conocido que uno de los algoritmos ya desarrollados para estos ordenadores, el algoritmo de Shor, es capaz de romper el encriptado RSA, que domina los actuales sistemas de cifrado. En particular hay que estar prevenidos ante la estrategia de ataques HNDL (Harvest Now Decrypt Later), por la que se sabe que delincuentes están almacenando ahora información sensible encriptada, con la intención de desencriptarla cuando el ordenador cuántico está disponible.

Quantum communications

Las comunicaciones cuánticas están más desarrolladas que la computación cuántica. De hecho, la Comisión Europea está desarrollando una infraestructura de comunicación cuántica segura para proporcionar servicios de conectividad fiables y seguros en toda la UE: la EuroQCI. Aun así, hay que tener muy en cuenta que el líder mundial en esta tecnología hoy por hoy es China.

Un amplio número de artículos analizados exponen una visión general sobre las líneas de comunicación cuántica y los avances más recientes y analizan técnicas, implementaciones y componentes para desplegar redes cuánticas seguras de gran tamaño y mejorar la eficiencia de las tecnologías cuánticas existentes. Uno de los aspectos clave es la distribución de claves cuánticas (QKD) a largas distancias. Como ejemplo, la referencia [43] demuestra una red de comunicación cuántica espacio-tierra integrada que combina una red de fibra a gran escala de más de 700 enlaces QKD de fibra y dos enlaces QKD espacio libre de alta velocidad satélite-tierra.

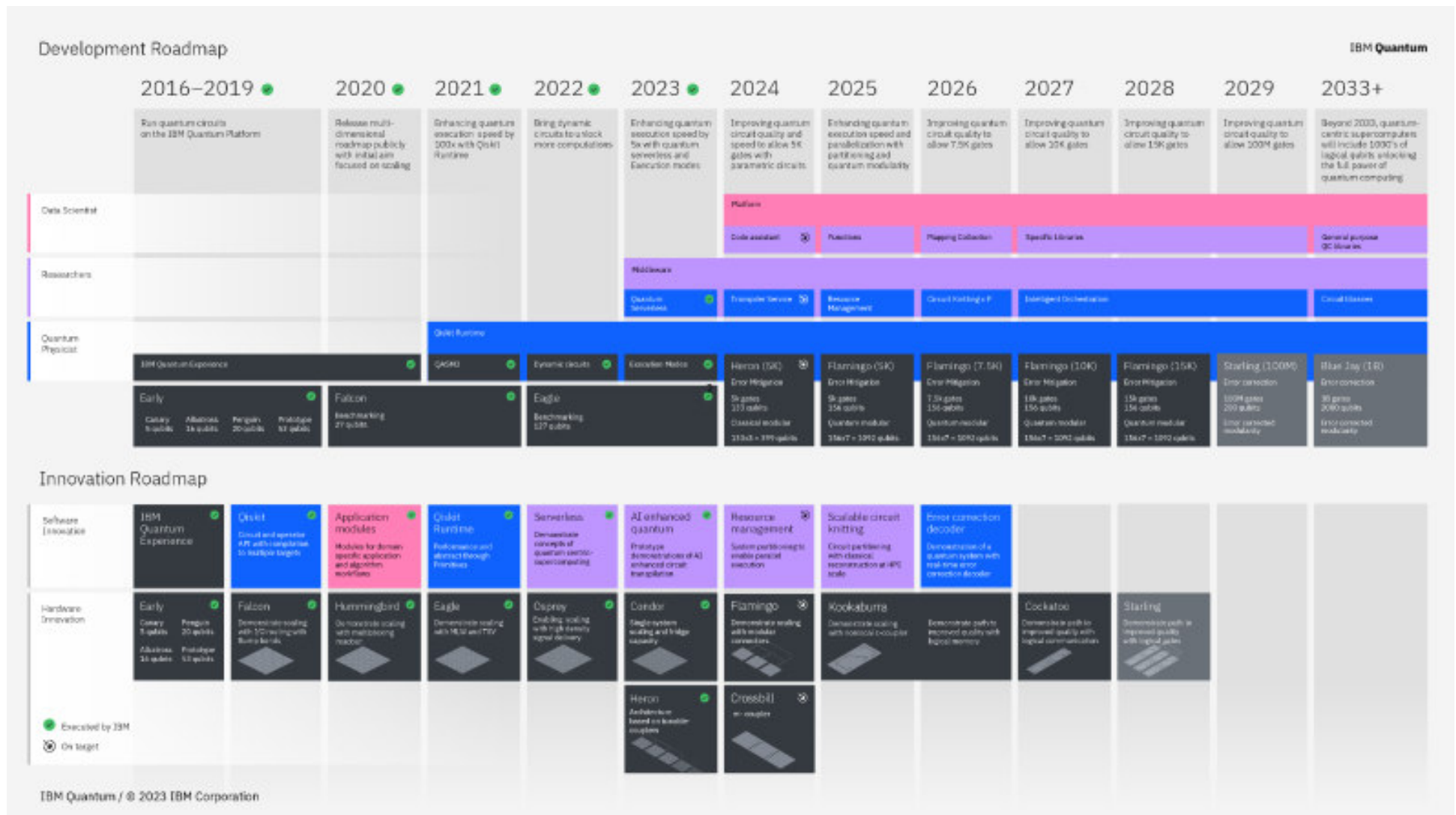


Figura 25. Roadmap de computación cuántica de IBM [IBM Quantum]

3.2.3. RECEPTORES FOTÓNICOS

Sin duda, uno de los campos donde el desarrollo de esta tecnología tiene un mayor impacto es en los receptores ESM para guerra electrónica. Este tipo de sistemas tienen virtualmente anchos de banda instantáneo de varias decenas de gigahercios. Sin embargo, tienen todavía poca penetración en los sistemas reales. Una descripción detallada de esta tecnología y de sus retos pendientes puede encontrarse en la referencia [44].

3.2.4. METAMATERIALES

Aunque los metamateriales se están utilizando para muchas aplicaciones, en particular relacionadas con ondas electromagnéticas (antenas, polarizadores, superficies selectivas en frecuencia), posiblemente el reto más interesante es el de la invisibilidad al radar, e incluso a la luz (ver figura 26). La referencia [45], analiza los avances obtenidos en este ámbito desde 2008 hasta 2023. La potencial aplicación a camuflaje es evidente.

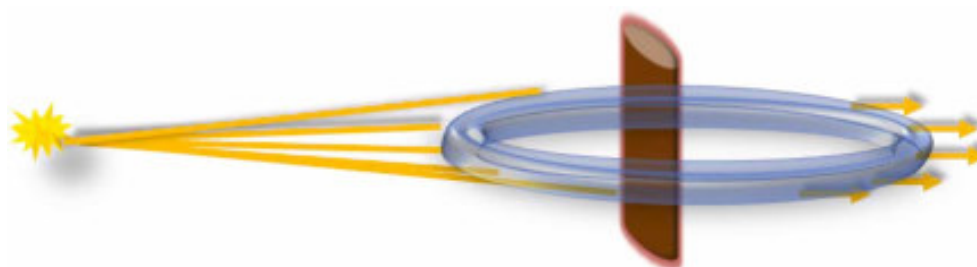


Figura 26. Principio básico de invisibilidad óptica, consistente en la desviación de los rayos de luz.

Más madura está la invisibilidad radar, o al menos, la reducción drástica de RCS mediante estos materiales compuestos. También en el campo de infrarrojos y de aislamiento acústico se están realizando muchos progresos. La referencia [46] recopila los principales avances recientes en esos campos.

Otro ámbito en el que los metamateriales aparecen como una tecnología de gran potencial es sobre el control de la transferencia de calor, logrando prestaciones sin precedentes en la transferencia de calor utilizando estructuras artificiales.

3.2.5. NUBE DE COMBATE

El desarrollo de la nube de combate es algo que se está haciendo más desde el entorno industrial que desde el académico, por lo que la revisión bibliográfica no es un mecanismo del todo fiable para estimar el grado de desarrollo.

Uno de los avances más significativos que está ya en proceso es la nube de combate asociada al sistema europeo FCAS. Representa un cambio de paradigma: del caza de combate tradicional, operado de forma independiente, se pasará a un “sistema de sistemas” interconectados que estará integrado por un avión de combate de siguiente generación (NGF), diversas plataformas no tripuladas, remote carriers (RC), y una Nube de Combate (Combat Cloud).

Esta Nube de Combate será el elemento habilitador del sistema de sistemas que, apoyándose en medios de conectividad avanzada (enlaces de datos de banda ancha entre vehículos, satelitales, oportunistas, ópticos...), permitirá una gran disponibilidad de información y, gracias a la aplicación de Inteligencia Artificial, Big Data y Edge Computing, convertirá esa información en conocimiento, permitiendo el Combate Colaborativo y la superioridad Aérea a través de capacidades y servicios colaborativos Multiplataforma sin precedentes (Figura 27).



Figura 27. Concepto de nube de combate del FCAS [AIRBUS]

Desde el punto de vista de publicaciones científicas, un amplio número de referencias analizadas revisan las principales amenazas presentes en las tecnologías de nube, comparan los ataques realizados en las tecnologías de nube y analizan métodos de protección de información [47] y mecanismos para combatir y eliminar las amenazas. Otros artículos analizan nubes de próxima generación y sus posibles algoritmos.

3.2.6. 6G

Actualmente, 5G promete velocidades varias veces más rápidas que las redes 4G LTE y con una latencia significativamente menor. Naturalmente, podemos esperar que las redes 6G utilicen frecuencias más altas y que proporcionen una capacidad sustancialmente mayor y una latencia mucho menor. Las proyecciones actuales exigen que 6G alcance una velocidad máxima de un terabit por segundo (Tbps), que es 100 veces más rápido que 5G.

6G utilizará equipos de radio más avanzados y una mayor diversidad de ondas de radio que 5G, incluyendo bandas de frecuencia por encima de 30GHz, que ofrece una enorme capacidad en distancias cortas. Todas las redes 6G tendrán tecnología de computación EDGE integrada, no un complemento como el 5G actual, lo que brindará beneficios como un mejor acceso a capacidades de inteligencia artificial y soporte para dispositivos y sistemas móviles sofisticados.

Más allá de amplificar las aplicaciones para una mejor conectividad y rendimiento, el diseño de la red 6G del mañana debería utilizar inteligencia artificial y aprendizaje automático (para mejorar la asistencia y la eficiencia), respaldar mayores resultados de sostenibilidad, aumentar la seguridad (para fomentar la confianza y la confiabilidad) y expandir y mejorar la conectividad con áreas remotas. del mundo.

La red 6G debe ser más eficiente que la 5G y consumir menos energía. La eficiencia energética lograda a través de la digitalización es fundamental para una industria móvil más sostenible debido al crecimiento previsto en la generación de datos. La red 6G puede impulsar las aplicaciones necesarias para que esto suceda.

La red debe ser algo más que segura. También debe ser fiable. Si bien la privacidad es un componente importante de la seguridad, es esencial la entrega de datos consistente, confiable y rápida de extremo a extremo, como la necesaria para respaldar la operación segura y eficiente de vehículos sin conductor sin preocupaciones sobre fallos de latencia potencialmente peligrosos.

Si bien 5G es bien conocido por su arquitectura de red “cloud” basada en microservicios, las redes de próxima generación o la era 6G están estrechamente relacionadas con la orquestación y gestión de redes inteligentes. Por tanto, el papel de la Inteligencia Artificial (IA) es inmenso en el paradigma 6G previsto. Sin embargo, la alianza entre 6G y la IA también puede ser un arma de doble filo en muchos casos, ya que la aplicabilidad de la IA para proteger o infringir la seguridad y la privacidad.

La referencia [48] analiza qué podemos esperar y/o debemos potenciar del desarrollo de la tecnología 6G.

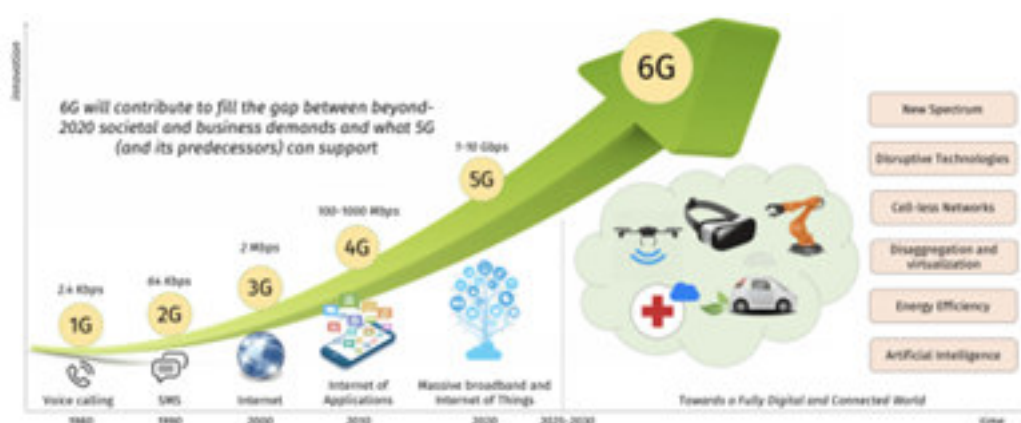


Figura 28. 6G: hacia un mundo totalmente digital y conectado.

4. ESCENARIOS FUTUROS

En base a las líneas tecnológicas y tendencias relevantes identificadas en el sector de la defensa y seguridad se han considerado y analizado una serie de escenarios futuros que podrían tener un gran impacto en el desarrollo de estas tecnologías. Estos escenarios, así como sus implicaciones, se presentan de manera sintética a continuación.

4.1. ESCENARIO #1 – ATAQUES MASIVOS CON DRONES

En los actuales conflictos bélicos se ha puesto de manifiesto la importancia de implementar sistemas de vigilancia y defensa que puedan hacer frente a posibles ataques basados en múltiples drones que operan de manera simultánea (aunque no necesariamente de forma cooperativa o en enjambre) y tratan de saturar las capacidades de defensa.

4.1.1. ANÁLISIS DEL ESCENARIO #1

Un ataque masivo con drones que pueden llegar a transportar decenas de kilogramos de carga explosiva trata generalmente de saturar los sistemas de defensa de tal forma que alguno llegue a impactar en el objetivo. De hecho, el uso táctico y generalizado de estos ataques se ha puesto de manifiesto en los conflictos bélicos actuales. Aunque se están realizando avances en coordinación de drones en arquitecturas de enjambre, la mayor complejidad y coste de estos sistemas hace que generalmente los ataques masivos se basen en un ataque simultáneo de múltiples drones que realmente no cooperan entre ellos.

Frente a estos ataques, los sistemas de defensa tradicionales podrían ser vulnerables debido a la saturación de sus capacidades y a la mayor maniobrabilidad de los drones. Por este motivo, los sistemas anti-dron actuales para la detección, clasificación y neutralización de drones deben mejorar su capacidad para hacer frente a múltiples ataques de drones de manera simultánea. En los conflictos bélicos actuales se han reportado ataques simultáneos de más de 100 drones.

Además, la mejora de la autonomía de las plataformas aéreas ha permitido desarrollar drones de coste limitado con alcances de más de 500 km, normalmente basados en sistemas de ala fija, por lo que estos ataques pueden ser lanzadas más allá de las fronteras o a largas distancias del objetivo. Incluso drones comerciales pueden ser adaptados para transportar cargas explosivas de hasta 10 kg con alcances de varias decenas de kilómetros.

4.1.2. PROBABILIDAD DEL ESCENARIO #1

Dada la disponibilidad actual y el bajo coste de las plataformas autónomas aéreas o drones y el aumento de sus capacidades y posibilidades de cooperación entre drones, se considera que la probabilidad de que las Fuerzas Armadas deban hacer frente a este tipo de ataques en misiones internacionales o por terrorismo es alta. De hecho, son escenarios que ya ocurren en los conflictos bélicos actuales con drones de mayor o menor complejidad, pero la mejora de la autonomía y la carga útil, así como la disminución de coste de los drones, puede suponer un aumento de este tipo de ataques.

La probabilidad de ataques masivos con drones que actúen de manera cooperativa en arquitecturas de enjambre se considera menor, especialmente en ataques terroristas, al requerir plataformas más complejas y de mayor coste. Generalmente estas plataformas cooperativas no se encuentran ampliamente disponibles, requieren desarrollos específicos y una mayor planificación de la misión.

4.1.3. *RIESGOS, OPORTUNIDADES Y MEDIDAS DE MITIGACIÓN DEL ESCENARIO #1*

El principal riesgo de este escenario se debe a que los sistemas de defensa tradicionales pueden ser vulnerables y verse saturados por un ataque masivo de drones que se basa en el número de unidades más que en su complejidad y altas capacidades. Además, la reducción de costes y aumento de disponibilidad de estas plataformas autónomas puede hacer proliferar este tipo de ataques masivos incluso en actos terroristas. Por ello, es necesario tener en cuenta este tipo de ataques en el desarrollo de los sistemas anti-dron y en la definición de estrategias frente a estas amenazas.

El desarrollo de las tecnologías asociadas a las plataformas autónomas en términos de menor coste y mayor autonomía, carga y cooperación entre plataformas también supone una oportunidad para el desarrollo de nuevas aplicaciones y mejora de capacidades en operaciones militares, de vigilancia o reconocimiento o de búsqueda y rescate. Sin embargo, deben analizarse de manera continua los nuevos riesgos que los avances en esta tecnología suponen en el ámbito de la seguridad y actualizar los sistemas de defensa anti-dron para hacer frente a las nuevas amenazas.

Para hacer frente a estas amenazas se proponen una serie de medidas basadas en fomentar el desarrollo tecnológico de los sistemas anti-dron:

- Fomentar el desarrollo e innovación de sistemas anti-dron, especialmente en tecnologías y sistemas para la neutralización de drones, como los sistemas de energía dirigida o láseres de alta potencia, que pueden hacer frente a múltiples ataques simultáneos.
- Con el objetivo de hacer viables sistemas redundantes, robustos y con amplia cobertura que puedan neutralizar múltiples drones de manera simultánea, se pueden promover tecnologías que reduzcan los costes y permitan su escalabilidad, flexibilidad y despliegue en función de las necesidades. En este aspecto se puede poner el foco en la neutralización simultánea de múltiples drones que presentan capacidades limitadas en lugar de en la neutralización de un solo dron de altas capacidades.
- Mejorar las estrategias autónomas y el tiempo de respuesta para hacer frente a ataques masivos haciendo uso de los avances en IA, cooperación entre nodos, fusión de datos o edge computing.

4.2. **ESCENARIO #2 – FUERTE DESARROLLO DE LA IA EN EL ENTORNO REGULATORIO EUROPEO**

Actualmente existe un importante esfuerzo para regular el uso de las tecnologías de inteligencia artificial, por lo que la aparición de nuevas regulaciones puede suponer un cambio de escenario que impacte en el desarrollo de estas tecnologías. Por ejemplo, a nivel de la Unión Europea se está regulando y definiendo el marco de aplicación de la IA, así como sus riesgos, en términos de privacidad, sesgos, seguridad, robustez, ... [49]. Además, la nueva regulación también puede tener un impacto en la creación y disponibilidad de bases de datos abiertas para el desarrollo de IA, pudiendo limitar la disponibilidad de datos, uno de los retos actuales para el desarrollo de nuevas aplicaciones especialmente en el ámbito de la defensa y la seguridad

4.2.1. *ANÁLISIS DEL ESCENARIO #2*

El desarrollo de normativas o regulaciones restrictivas puede tener importantes implicaciones en la limitación de la innovación y la aparición de desventajas normativas para el desarrollo de estas tecnologías a nivel nacional y europeo. Además, podría limitar la posibilidad de disponer de los datos necesarios para el entrenamiento de la IA llegando incluso a una saturación de sus capacidades.

4.2.2. *PROBABILIDAD DEL ESCENARIO #2*

Se considera que es altamente probable que se establezcan regulaciones que limiten a distintos niveles el desarrollo y aplicabilidad de la IA con el objetivo de solventar algunas problemáticas de seguridad, privacidad, derechos de autor, veracidad de la información o sesgos, entre otras.

4.2.3. *RIESGOS, OPORTUNIDADES Y MEDIDAS DE MITIGACIÓN DEL ESCENARIO #2*

Una regulación menos restrictiva de la IA puede suponer una mayor innovación y desarrollo más rápido de estas tecnologías a costa de no hacer frente a determinados riesgos que pueden tener implicaciones sociales y de seguridad. Por ello, es conveniente hacer una regulación adecuada y balanceada y poner en marcha mecanismos de innovación dentro del contexto normativo que eviten que aparezcan desventajas competitivas de la industria nacional o europea frente a otras naciones.

A continuación, se especifican algunas de las medidas de mitigación de un escenario con regulación restrictiva en la aplicación de la IA o de las plataformas autónomas:

- Promover el desarrollo de tecnologías de IA explicable y de bases de datos de calidad para el entrenamiento y desarrollo de IA que pueda ser certificable con el objetivo de asegurar su robustez y potenciar su desarrollo en aplicaciones críticas como la defensa y seguridad.
- Cooperación público-privada para fomentar la creación de datasets y la compartición de datos especialmente relacionados con aplicaciones de defensa y seguridad para fomentar el desarrollo de la IA en estos sectores.
- Cooperación público-privada para la definición de las regulaciones con el objetivo de analizar las implicaciones específicas de las nuevas normativas en el fomento de la innovación y el desarrollo de nuevas aplicaciones.
- Desarrollar nuevos mecanismos de innovación e inversión en estas tecnologías dentro del contexto normativo y regulatorio.
- Fomento de la estandarización y control de estas tecnologías para mantener su robustez y seguridad.
- Revisión periódica de la regulación, así como de su impacto para incorporar nuevos avances para realizar ajustes convenientes. Esta revisión se considera importante al tratarse al ser tecnologías de rápido avance y desarrollo con nuevas aplicaciones emergentes.

4.3. **ESCENARIO #3 – MAYOR USO DE MISILES HIPERSÓNICOS EN CONFLICTOS BÉLICOS**

Las plataformas y misiles hipersónicos constituyen una amenaza actual dado su desarrollo avanzado por parte de algunas naciones, incluyendo China (plataforma DF-ZF) y Rusia (plataforma Avangard), que implican riesgos importantes para la defensa debido a su alta maniobrabilidad, velocidad, alcance y autonomía que dificulta su detección y neutralización para los sistemas de defensa actuales. Por ello, el desarrollo de sistemas de defensa que hagan frente de manera efectiva y robusta a dichas amenazas se considera una necesidad a corto plazo.

4.3.1. *ANÁLISIS DEL ESCENARIO #3*

El desarrollo y avance de la tecnología de misiles hipersónicos también presenta retos tecnológicos en áreas relacionadas con la propulsión, materiales resistentes al calor y de baja observabilidad y sistemas de control, guiado y navegación. Sin embargo, varias naciones han presentado sistemas operativos de misiles y plataformas hipersónicas, por lo que su uso en conflictos bélicos se espera que aumente en los próximos años.

Dado que actualmente la tecnología de defensa antiaérea para la detección temprana e interceptación de este tipo de misiles no está suficientemente madura, existe la necesidad a corto plazo de desarrollar tecnologías, sistemas y estrategias para hacer frente a estas amenazas.

En este aspecto, las investigaciones realizadas generalmente proponen la integración de múltiples tecnologías y sensores que abarcan múltiples dominios (terrestre, naval, espacio y ciberespacio) incluyendo también información de inteligencia sobre localizaciones de lanzamiento y acopio de materiales. Por ello, el desarrollo de conceptos relacionados con sistemas de sistemas, la definición de interfaces y estándares para la interoperabilidad, y el procesado y fusión de información procedente de múltiples fuentes mediante IA son aspectos de gran importancia para este escenario.

4.3.2. *PROBABILIDAD DEL ESCENARIO #3*

Aunque la tecnología de misiles hipersónicos está suficiente avanzada y distintas naciones han presentado sistemas operativos, su uso generalizado en conflictos bélicos no se considera probable a corto plazo dado su alto coste. Sin embargo, la posible disminución del coste y aumento de robustez y alcance de estos sistemas puede suponer un incremento de su uso en conflictos bélicos, por lo que es crucial prepararse frente a este tipo de amenazas a medio plazo (5-10 años).

A pesar de esto, aunque su uso generalizado no se prevea inminente, su uso ocasional sí lo es, y de hecho ya se han usado misiles Fattah por Irán contra Israel el 1 de octubre de 2024.

4.3.3. *RIESGOS, OPORTUNIDADES Y MEDIDAS DE MITIGACIÓN DEL ESCENARIO #3*

El mayor riesgo actual asociado al desarrollo de la tecnología de plataformas y misiles hipersónicos es el de no disponer de una tecnología suficientemente madura y robusta que permita la detección y neutralización de dichos misiles de manera efectiva. Por ello, es necesario el avance tecnológico en diferentes áreas relacionadas con las tecnologías de sensores (radares terrestres y satelitales y sensores hiperespectrales), la guerra electrónica, los sistemas de neutralización y el procesado de datos y control automático de baja latencia (incluyendo técnicas de IA), así como la integración de dichas tecnologías en un sistema de sistemas.

El desarrollo de estas tecnologías y sus pruebas asociadas supone un alto coste, lo que implica un riesgo en su avance si no se asegura la financiación necesaria y se promueve su desarrollo en base a los programas y prioridades de defensa nacional.

El desarrollo de la tecnología de misiles hipersónicos también presenta oportunidades para el sector de la defensa nacional para promover nuevas capacidades industriales nacionales, innovaciones tecnológicas y colaboraciones internacionales de I+D.

Para hacer frente a los riesgos asociados a este escenario se proponen medidas que fomenten el desarrollo tecnológico de diferentes áreas implicadas en los sistemas de defensa:

- Fomentar el desarrollo y despliegue de sensores espaciales como radares SAR o sensores hiperespectrales que permitan detectar el lanzamiento de los misiles hipersónicos en las etapas iniciales, de reentrada o de vuelo.
- Promover los avances tecnológicos necesarios para que los radares terrestres de largo alcance o alerta temprana, como los radares OTH (over-the-horizon), mejoren sus capacidades para detectar plataformas hipersónicas a distancias suficientes para los tiempos de respuesta necesario.
- Desarrollar las tecnologías de defensa área para mejorar las capacidades de interceptación endoatmosférica de misiles de corto y medio alcance.

- Promover el desarrollo de sistemas de sistemas que permitan fusionar de manera efectiva la información de múltiples sensores, así como interceptar las amenazas. Para ello, se debe promover la cooperación naciones aliadas y la definición de interfaces que permitan la interoperabilidad de los sistemas, así como el intercambio de información relevante y el desarrollo de redes de sensores internacionales.
- Avanzar en las tecnologías de procesado y control autónomas y robustas basadas en IA para el procesado de grandes cantidades de datos multidominio y toma de decisión que permita disminuir el tiempo de respuesta frente a estas amenazas y mejorar su interceptación.

4.4. ESCENARIO #4 – DESARROLLO DE SISTEMAS DE COMPUTACIÓN CUÁNTICA OPERATIVOS

El desarrollo actual de las tecnologías de procesamiento cuántico y de algoritmos específicos para explotar los beneficios de estos procesadores emergentes, ponen de manifiesto el gran potencial disruptivo y de capacidades de estas tecnologías. Sin embargo, actualmente la mayoría de los sistemas pueden considerarse prototipos con importantes limitaciones (coste, gestión, estabilidad). Por ello un escenario de gran relevancia en la evolución de los sectores tecnológicos de la defensa y seguridad sería la aparición de sistemas de computación cuántica que sean operativos y estén disponibles a gran escala, por ejemplo, para el despliegue de infraestructuras de supercomputación nacionales o privadas.

4.4.1. ANÁLISIS DEL ESCENARIO #4

La principal implicación será el incremento de capacidad de computación que tendrá efectos en otras tecnologías como la inteligencia artificial, el procesado de grandes bases de datos (big data) o la ciberseguridad (criptografía). Existen ciertos problemas y simulaciones complejas cuyo tratamiento resulta inviable con los sistemas de procesamiento actual pero que podrían ser resueltos en un futuro próximo gracias a los computadores cuánticos.

Este desarrollo supondría además la necesidad de actualizar las infraestructuras y arquitecturas de computación nacionales con el objetivo de evitar un importante gap tecnológico frente a otras naciones que tengan disponibles esta tecnología. Además, tendría un importante efecto para la seguridad en relación con la criptografía ya que podrá comprometer los sistemas de cifrado actuales como RSA y requerirá seguir avanzando en tecnologías específicas para comunicaciones seguras.

Uno de los retos actuales para el desarrollo de esta tecnología es la definición de estándares que permitan en un futuro su interoperabilidad y escalabilidad.

Por tanto, el desarrollo de la computación cuántica no sólo supone grandes oportunidades sino también implica importantes riesgos.

4.4.2. PROBABILIDAD DEL ESCENARIO #4

Aunque en los próximos años se espera un continuo desarrollo de la computación cuántica principalmente en la mejora de la estabilidad y aplicabilidad de los sistemas, pudiendo hacer viable el despliegue de infraestructuras nacionales, se considera poco probable el escalado de esta tecnología para una utilización generalizada o de masas. Por tanto, este escenario se considera a largo plazo.

4.4.3. RIESGOS, OPORTUNIDADES Y MEDIDAS DE MITIGACIÓN DEL ESCENARIO #4

El desarrollo de la tecnología de computación cuántica supone grandes oportunidades en cuanto al incremento de la capacidad de computación pudiendo hacer viable nuevas aplicaciones y desarrollos tecnológicos en múltiples campos como la inteligencia artificial o la ciberseguridad.

En cuanto a los riesgos principales que tendría el desarrollo de esta tecnología se encuentra la vulnerabilidad de los sistemas de cifrado actuales y la posible aparición de importantes desigualdades tecnológicas entre los países que tengan disponible la tecnología y aquellos que no.

Por ello, se consideran las siguientes medidas principales para mitigar los riesgos de este escenario:

- Seguimiento de la tecnología de procesamiento cuántico con el objetivo de determinar la viabilidad e idoneidad temporal en el desarrollo de infraestructuras nacionales de supercomputación basadas en dicha tecnología.
- Fomento de la inversión público-privada en estas tecnologías para mantener un know-how de esta tecnología a nivel nacional o europeo y un punto de partida en caso de que se acelere el desarrollo de nuevas aplicaciones. De este modo, se trataría de evitar la aparición de desigualdades tecnológicas con otros países, que también pueden tener un importante impacto económico.
- Desarrollo e implementación en los sistemas de comunicaciones seguras de mecanismos y técnicas de seguridad que sean robustas frente a la computación cuántica o evitar la interceptación de posibles comunicaciones clasificadas. Se debe tener en cuenta que actualmente existen ataques HNDL (Harvest Now Decrypt Later), por lo que su riesgo futuro debe minimizarse con la aplicación de nuevas técnicas de cifrado o de comunicaciones de baja probabilidad de interceptación.

4.5. ESCENARIO #5 – DESARROLLO DE TECNOLOGÍAS 6G PARA APLICACIONES MILITARES

El desarrollo y expansión de las tecnologías de comunicaciones móviles 6G de banda ancha, incluyendo redes NTN (non-terrestrial networks) con cobertura global desde satélites, así como el desarrollo de técnicas de comunicaciones seguras y de sistemas y redes ad hoc desplegables, supondría una mayor aplicación de estas tecnologías en aplicaciones de defensa.

4.5.1. ANÁLISIS DEL ESCENARIO #5

La mayor aplicación de tecnologías 6G para aplicaciones militares gracias a la mejora de su robustez y seguridad supondría fomentar el desarrollo de aplicaciones emergentes como la realidad aumentada o la realidad virtual en el contexto del combatiente del futuro gracias a la mejora de la velocidad de transferencia de información y la reducción de la latencia. Además, estos avances estarían también implicados en el fomento del despliegue de sensores y actuadores IoT (Internet of Things) que permitirían aumentar la conciencia situacional en situaciones de conflicto, especialmente en entornos urbanos. La mejora de las capacidades de computación asociadas a las estaciones base de comunicaciones móviles y a los sistemas móviles, también permitiría implementar arquitecturas de computación basadas en Edge Computing con mayor flexibilidad y menor latencia, frente a arquitecturas de procesamiento centralizado en los nodos C2 (Command and control). La convergencia de múltiples tecnologías que se observa en las tecnologías 6G de comunicaciones, sensores e inteligencia artificial fomentaría el desarrollo de aplicaciones emergentes incluyendo en el sector de la defensa y la seguridad.

Una posible implicación es el desarrollo de técnicas de JCAS (Joint Communication and Sensing) en las estaciones base desplegadas en entornos urbanos. Estas tecnologías podrían ser revolucionarias para el sector de la seguridad en entornos urbanos, ya que la densa red de estaciones base se convertiría en una red de sensores que podrían hacer frente a amenazas de drones.

4.5.2. PROBABILIDAD DEL ESCENARIO #5

El desarrollo de las tecnologías de comunicaciones 6G de banda ancha terrestres es altamente probable debido a que viene marcado por la industria civil de comunicaciones y presenta importantes implicaciones económicas y sociales.

Un reto actual es la integración e interoperabilidad transparente para el usuario de las redes terrestres con las redes satelitales emergentes, lo que sería de gran interés para la aplicación de las tecnologías 6G en aplicaciones de defensa. Al tratarse de una tecnología de comunicaciones civiles, otro reto es el cumplimiento de los requisitos de robustez y seguridad necesarios para estas aplicaciones. Sin embargo, existe una probabilidad media de que las ventajas que suponen las tecnologías 6G en términos de ancho de banda, disponibilidad y latencia fomenten la superación de estos retos.

En cualquier caso, se debe comentar que el desarrollo y despliegue de la futura constelación europea para comunicaciones gubernamentales y seguras, IRIS² está aprobado y se espera que el primer lanzamiento de satélites se realice durante el año 2025.

4.5.3. RIESGOS, OPORTUNIDADES Y MEDIDAS DE MITIGACIÓN DEL ESCENARIO #5

El desarrollo de los métodos y técnicas necesarias para mejorar la robustez y seguridad de los sistemas 6G que habiliten su uso en aplicaciones de defensa presenta importantes oportunidades en el fomento de otras tecnologías como la realidad virtual o aumentada, sensores y aplicaciones de inteligencia artificial en operaciones tácticas. Todo ello permitiría la mejora de la conciencia situacional en entornos de conflicto y la mejora de capacidades del combatiente del futuro. Además, el uso dual de esta tecnología potenciaría su desarrollo en base a múltiples aplicaciones emergentes.

Los principales riesgos que se detectan se deben al aumento de dependencia en estas tecnologías de comunicaciones, cuya infraestructura está habitualmente controlada por empresas internacionales. Además, aunque hay un importante esfuerzo de estandarización y el desarrollo de las infraestructuras terrestres de comunicaciones móviles viene marcado por estos estándares, el desarrollo de las nuevas constelaciones satelitales (véase Starlink o OneWeb) no sigue actualmente estándares definidos, lo que puede limitar la escalabilidad e interoperabilidad de estos sistemas.

Por otra parte, existe el riesgo de que los requisitos y necesidades en términos de robustez y seguridad de la transferencia de información especificadas para las aplicaciones en defensa y seguridad no se integren en el desarrollo de estas tecnologías 6G, al estar marcado principalmente por el ámbito y la industria civil.

En base a los riesgos detectados, se pueden proponer las siguientes medidas de mitigación en este escenario:

- Analizar los requisitos de los sistemas de comunicaciones para la aplicación de nuevas tecnologías como la realidad virtual o aumentada o inteligencia artificial en entornos tácticos y combatiente del futuro, con el objetivo de especificar unas guías que marquen la aplicabilidad de las tecnologías 6G en estos entornos y fomenten su desarrollo.
- Fomentar la colaboración público-privada tanto en el desarrollo de la tecnología, definiendo los requisitos necesarios para aplicaciones en defensa y seguridad, como en el despliegue y operación de los sistemas de comunicaciones para disponer de cierto control sobre las infraestructuras a nivel nacional y europeo.
- Fomentar los esfuerzos de estandarización a nivel nacional e internacional para promover la interoperabilidad entre redes tanto terrestres como satelitales.
- Definir métodos, desarrollar técnicas e implementarlas en las futuras redes de comunicaciones que permitan alcanzar los requisitos de robustez y seguridad de los sistemas 6G para aplicarlos en el ámbito de la defensa y la seguridad. Un ejemplo sería la implementación de las técnicas de network slicing que permitiría dar una mayor prioridad a las comunicaciones gubernamentales o militares en dichas redes frente a comunicaciones civiles, lo que mejoraría la robustez en aplicaciones críticas.

5. PROPUESTA DE ACCIONES

5.1. ACCIONES RECOMENDADAS

En base al análisis de tecnologías, tendencias y escenarios relacionadas con el sector de la defensa y seguridad realizado en este informe, se sugiere la implementación de una serie de acciones, principalmente basadas en el seguimiento de la evolución tecnológica y fomento del desarrollo de ciertas tecnologías relevantes. Dada la relevancia de los distintos escenarios analizados en relación con las tecnologías tratadas en este informe se priorizan las acciones en el siguiente orden:

1. Fomentar el seguimiento y desarrollo de las tecnologías de neutralización de drones, especialmente para hacer frente a ataques masivos.
2. Promover la aplicación de la IA en el ámbito de defensa y seguridad mediante el desarrollo de IA explicable que pueda ser certificada y el fomento de la creación y compartición de bases de datos relevantes para estas aplicaciones mediante la cooperación público-privada.
3. Mantener el seguimiento de la tecnología de misiles hipersónicos y de los sistemas antiaéreos para hacer frente a estas amenazas.
4. Mantener el seguimiento de la tecnología de computación cuántica y el análisis continuo de las implicaciones que los nuevos avances puedan tener en la seguridad y defensa nacional.

Estas acciones pueden implementarse mediante la organización de jornadas temáticas que pongan en contacto y fomenten la cooperación entre organizaciones públicas y privadas. Además, dichas jornadas facilitarían la identificación y presentación las necesidades operativas actuales de las Fuerzas Armadas así como la identificación de los actores relevantes nacionales en el desarrollo de esta tecnología.

Por otra parte, se debe seguir promoviendo la cooperación internacional en los ámbitos de la Unión Europea y la OTAN, especialmente en relación con la definición de la regulación asociada a aplicaciones de la IA, el desarrollo de la tecnología de computación cuántica y el desarrollo de sistemas de defensa internacionales frente a amenazas de misiles hipersónicos.

Finalmente, es importante promover el desarrollo de las tecnologías implicadas mediante la definición de las prioridades nacionales de desarrollo tecnológico y de los programas de I+D para hacer frente a los retos actuales y a los riesgos asociados de los escenarios futuros. De esta forma, se podrá desarrollar un marco estratégico sólido que permita a los actores implicados en el desarrollo de estas tecnologías a la vez que mitigar los riesgos asociados a los escenarios analizados.

5.2. PLAN DE SEGUIMIENTO

El continuo avance tecnológico en las líneas temáticas relevantes para la defensa y seguridad identificadas en este informe hace necesario un continuo seguimiento de las implicaciones de los nuevos avances y tendencias. Sin embargo, en base a la velocidad de desarrollo y relevancia tecnológica se considera prioritario mantener el seguimiento y realización de análisis tecnológicos de tres temas fundamentales a nivel del Nodo de Tecnologías de Defensa y Seguridad (Cátedra Isdefe-UPM) de la Red Horizontes:

- IA explicable para aplicaciones de defensa y seguridad.
- Tecnologías para la defensa frente a misiles hipersónicos.
- Sistemas anti-dron frente a ataques masivos de drones.

Dentro de estas temáticas, la tecnología de IA explicable se considera como línea prioritaria para realizar actividades de análisis y prospectiva para el Nodo de Tecnologías de Defensa y Seguridad en la próxima anualidad. En cuanto a las otras líneas, Isdefe está implicada en un grupo de trabajo de la Fundación Círculo sobre tecnologías de defensa frente a misiles hipersónicos. Además, los sistemas anti-dron se han

tratado de manera extensa en actividades previas por lo que se proponer realizar un seguimiento periódico sobre los nuevos avances y tendencias relevantes en este ámbito.

6. CONCLUSIONES

En este informe se han identificado y analizado las principales tecnologías y tendencias relevantes en el ámbito de la defensa y seguridad, en base a seis líneas tecnológicas:

- **Tecnologías de la Información** incluyendo la inteligencia artificial.
- **Materiales y químicos** relacionados con las tecnologías de fabricación aditiva y generación de energía
- **Plataformas autónomas** como el desarrollo de drones o de sistemas anti-dron.
- **Sensores** incluyen sensores activos y pasivos, tanto electromagnéticos como ópticos o acústicos.
- **Robótica** relacionada no sólo con el desarrollo de robots sino también con los sistemas de potenciación de las capacidades humanas.
- **Sistemas de comunicación** en el ámbito de las redes y los sistemas de radio definida por software y de la nube de combate.

El análisis de dichas tecnologías ha permitido identificar y definir una serie de escenarios relevantes con impacto en la seguridad y defensa nacional relacionados con los ataques masivos de drones, el desarrollo de la IA en aplicaciones de defensa, el uso de misiles hipersónicos, el desarrollo de la computación cuántica y el uso dual de las tecnologías de comunicaciones móviles 6G.

Las necesidades identificadas para hacer frente a los riesgos asociados con los tres primeros escenarios que se consideran de alta probabilidad a corto y medio plazo y efectos de gran impacto en el ámbito de la defensa, se han tomado de base para definir una serie de acciones recomendadas para promover el desarrollo de las tecnologías asociadas. Además, se han utilizado para definir las líneas temáticas de prioridad que podrían ser tratadas en la próxima anualidad dentro de las actividades del nodo de Defensa y Seguridad:

- IA explicable para aplicaciones de defensa y seguridad.
- Tecnologías para la defensa frente a misiles hipersónicos.
- Sistemas anti-dron frente a ataques masivos de drones.

En base a actividades previas y a otras actividades en las que se encuentra implicada ISDEFE, para la próxima anualidad, se considera de mayor relevancia el análisis de capacidades y de prospectiva tecnológica sobre IA explicable para aplicaciones de defensa.

7. ANEXOS

7.1. REFERENCIAS

[1] Programa del congreso DESE I+D 2023.

https://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Presentacion/deseid_2023/Documents/PROGRAMA%20DESEi+d%202023.pdf

[2] European Defence Agency. Capability Technology Areas (CapTechs)

[https://eda.europa.eu/what-we-do/research-technology/capability-technology-areas-\(captechs\)](https://eda.europa.eu/what-we-do/research-technology/capability-technology-areas-(captechs))

[3] Horizon Europe Work Programme 2023-2025. Cluster 3: Civil Security for Society.

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-6-civil-security-for-society_horizon-2023-2024_en.pdf

[4] Horizon Europe Work Programme 2023-2025. Cluster 4: Digital, Industry and Space.

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2023-2024/wp-7-digital-industry-and-space_horizon-2023-2024_en.pdf

[5] EDF Work Programme 2024: https://defence-industry-space.ec.europa.eu/edf-work-programme-2024_en

[6] Estrategia Industrial de Defensa 2023.

https://publicaciones.defensa.gob.es/media/downloadable/files/links/e/s/estrategia_industrial_de_defensa_2023.pdf

[7] Revista IEEE Spectrum. <https://spectrum.ieee.org/>

[8] Proyecto ASSETS+. Alliance for Strategic Skills addressing Emerging Technologies in Defence. assets-plus.eu

[9] Pastor-Galindo, J., Nespoli, P., Mármol, F. G., & Pérez, G. M. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. IEEE Access, 8, 10282-10304.

[10] McKinsey & Company, "What's the future of generative AI? An early view in 15 charts"

<https://www.mckinsey.com/~media/mckinsey/featured%20insights/mckinsey%20explainers/whats%20the%20future%20of%20generative%20ai%20an%20early%20view%20in%2015%20charts/whats-the-future-of-generative-ai-an-early-view-in-15-charts.pdf>

[11] Baidoo-Anu, D., & Owusu Ansah, L. (2023). Education in the era of generative artificial intelligence (AI): Understanding the potential benefits of ChatGPT in promoting teaching and learning. Available at SSRN 4337484.

[12] Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., ... & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information fusion, 58, 82-115.

[13] Lai, K., Yanushkevich, S. N., & Shmerko, V. P. (2021). Intelligent stress monitoring assistant for first responders. IEEE Access, 9, 25314-25329.

- [14] Pech, M., Vrchota, J., & Bednář, J. (2021). Predictive maintenance and intelligent sensors in smart factory. *Sensors*, 21(4), 1470.
- [15] Cátedra ISDEFE-UPM en Defensa y Seguridad. Big Data Aplicado a la Defensa y la Seguridad. Estado del Arte de las Tecnologías. Julio 2022.
- [16] Martín Pérez, C.L., del Blanco Adán, C. Detección de defectos en placas acero mediante el uso de técnicas de Few Shot Learning en aplicaciones militares. DESE I+D Noviembre 2023.
- [17] Jones, D., Snider, C., Nassehi, A., Yon, J., & Hicks, B. (2020). Characterising the Digital Twin: A systematic literature review. *CIRP journal of manufacturing science and technology*, 29, 36-52.
- [18] Xiong, J., Hsiang, E. L., He, Z., Zhan, T., & Wu, S. T. (2021). Augmented reality and virtual reality displays: emerging technologies and future perspectives. *Light: Science & Applications*, 10(1), 216.
- [19] Meliande, N. M., Silveira, P. H. P. M. D., Monteiro, S. N., & Nascimento, L. F. C. (2022). Tensile Properties of Curaua–Aramid Hybrid Laminated Composites for Ballistic Helmet. *Polymers*, 14(13), 2588.
- [20] To, K. C., Ben-Jaber, S., & Parkin, I. P. (2020). Recent developments in the field of explosive trace detection. *ACS nano*, 14(9), 10804-10833.
- [21] Koblenz, Gregory D. "Emerging technologies and the future of CBRN terrorism." *The Washington Quarterly* 43.2 (2020): 177-196.
- [22] Wang, Y., Diaz, D. F. R., Chen, K. S., Wang, Z., & Adroher, X. C. (2020). Materials, technological status, and fundamentals of PEM fuel cells—a review. *Materials today*, 32, 178-203.
- [23] Gibson, I., Rosen, D. W., Stucker, B., Khorasani, M., Rosen, D., Stucker, B., & Khorasani, M. (2021). Additive manufacturing technologies (Vol. 17, pp. 160-186). Cham, Switzerland: Springer.
- [24] Yibo, D. I. N. G., Xiaokui, Y. U. E., Guangshan, C. H. E. N., & Jiashun, S. I. (2022). Review of control and guidance technology on hypersonic vehicle. *Chinese Journal of Aeronautics*, 35(7), 1-18.
- [25] Schranz, M., Umlauf, M., Sende, M., & Elmenreich, W. (2020). Swarm robotic behaviors and current applications. *Frontiers in Robotics and AI*, 36.
- [26] S. Rezwani and W. Choi, "Artificial Intelligence Approaches for UAV Navigation: Recent Advances and Future Challenges," in *IEEE Access*, vol. 10, pp. 26320-26339, 2022
- [27] Khandelwal, A., Weihs, L., Mottaghi, R., & Kembhavi, A. (2022). Simple but effective: Clip embeddings for embodied AI. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 14829-14838).
- [28] Goebel, D. M., Katz, I., & Mikellides, I. G. (2023). *Fundamentals of electric propulsion*. John Wiley & Sons.
- [29] Cano Fernández, J. Análisis y Definición de un Sistema de Radiofrecuencia de Alta Potencia para La Anulación Física de Sistemas RPA. Trabajo Fin de Master. ETSI Telecomunicación. UPM. 2021
- [30] Clasificación de detecciones de radar de drones vs aves. Estado del arte. Cátedra ISDEFE 2024. (disponible próximamente)

- [31] Kumawat, H. C., Chakraborty, M., Raj, A. A. B., & Dhavale, S. V. (2021). DIAT- μ SAT: Small aerial targets' micro-Doppler signatures and their classification using CNN. *IEEE Geoscience and Remote Sensing Letters*, 19, 1-5.
- [32] Ding, J., Xue, N., Xia, G. S., Bai, X., Yang, W., Yang, M. Y., ... & Zhang, L. (2021). Object detection in aerial images: A large-scale benchmark and challenges. *IEEE transactions on pattern analysis and machine intelligence*, 44(11), 7778-7796.
- [33] 4 Game-Changing Underlying Technologies for Advanced Radar. <https://www.ni.com/en/solutions/aerospace-defense/radar-electronic-warfare-sigint/4-game-changing-underlying-technologies-for-advanced-radar.html>. December 2023
- [34] Ziomek, L. (2020). *Fundamentals of acoustic field theory and space-time signal processing*. CRC press.
- [35] Li, Peng. "Research on radar signal recognition based on automatic machine learning." *Neural Computing and Applications* 32.7 (2020): 1959-1969.
- [36] Macenski, S., Foote, T., Gerkey, B., Lalancette, C., & Woodall, W. (2022). *Robot Operating System 2: Design, architecture, and uses in the wild*. *Science robotics*, 7(66), eabm6074.
- [37] León Serrano, Gonzalo "Tendencias de las tecnologías para el aumento de las capacidades humanas", ELC, 2024.
- [38] Eden, J., Bräcklein, M., Ibáñez, J. et al. Principles of human movement augmentation and the challenges in making it a reality. *Nat Commun* 13, 1345 (2022). <https://doi.org/10.1038/s41467-022-28725-7>
- [39] Krelina, M. Quantum technology for military applications. *EPJ Quantum Technol.* 8, 24 (2021). <https://doi.org/10.1140/epjqt/s40507-021-00113-y>
- [40] Maccone, L., & Ren, C. (2020). Quantum radar. *Physical Review Letters*, 124(20), 200503.
- [41] Ricardo Gallego Torromé, Shabir Barzanjeh, *Advances in quantum radar and quantum LiDAR, Progress in Quantum Electronics, 2023, 100497, ISSN 0079-6727*
- [42] Zhong, H. S., Wang, H., Deng, Y. H., Chen, M. C., Peng, L. C., Luo, Y. H., ... & Pan, J. W. (2020). Quantum computational advantage using photons. *Science*, 370(6523), 1460-1463.
- [43] Chen, Y. A., Zhang, Q., Chen, T. Y., Cai, W. Q., Liao, S. K., Zhang, J., ... & Pan, J. W. (2021). An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, 589(7841), 214-219.
- [44] P. Ghelfi, F. Scotti, D. Onori and A. Bogoni, "Photonics for Ultrawideband RF Spectral Analysis in Electronic Warfare Applications," in *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 25, no. 4, pp. 1-9, July-Aug. 2019, Art no. 8900209, doi: 10.1109/JSTQE.2019.2902917
- [45] Muhammad Shaheryar Khan, R.A. Shakoor, Osama Fayyaz, Elsadig Mahdi Ahmed, *A focused review on techniques for achieving cloaking effects with metamaterials, Elsevier Optik, Volume 297, 2024, 171575,*
- [46] Xujin Yuan, Mingji Chen, Yin Yao, Xiaogang Guo, Yixing Huang, Zhilong Peng, Baosheng Xu, Bowen Lv, Ran Tao, Shenyu Duan, Haitao Liao, Kai Yao, Ying Li, Hongshuai Lei, Xu Chen, Guangfu Hong, Daining Fang, *Recent progress in the design and fabrication of multifunctional structures based on metamaterials, Elsevier. Current Opinion in Solid State and Materials Science, Volume 25, Issue 1, 2021, 100883,*

[47] Chinnasamy, P., Padmavathi, S., Swathy, R., & Rakesh, S. (2021). Efficient data security using hybrid cryptography on cloud computing. In *Inventive Communication and Computational Technologies: Proceedings of ICICCT 2020* (pp. 537-547). Springer Singapore.

[48] Dang, S., Amin, O., Shihada, B., & Alouini, M. S. (2020). What should 6G be?. *Nature Electronics*, 3(1), 20-29.

[49] European Commission, AI Act: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

7.2. ACRÓNIMOS

A/D	Analog/Digital
AESA	Active Electronically Scanned Array
AM	Additive Manufacturing
ASSETS+	Alliance for Strategic Skills addressing Emerging Technologies in Defence
ASTM	American Society for Testing and Materials
BWO	Backward wave oscillator
C4ISTAR	Command, Control, Communications, Computers, Intelligence, Surveillance, Target Acquisition, Reconnaissance
CLIP	Preentrenamiento de imágenes en lenguaje contrastivo
C-RAM	Contracohete, artillería y mortero
D/A	Digital/Analog
DEW	Directed-energy weapon
DL	Deep Learning
DTE	Detección de trazas de explosivos
EDA	European Defence Agency
EDF	European Defence Fund
EDT	Tecnologías Emergentes Y Disruptivas
ESM	Electronic Support Measures
ETID	Estrategia de Tecnología e Innovación para la Defensa
EU	Unión Europea
FL	Federated Learning

GPT	Generative pre-trained transformer
HNDL	Harvest Now Decrypt Later
IA	Inteligencia artificial
I+D	Investigación y desarrollo
ISTAR	Intelligence, Surveillance, Target Acquisition, Reconnaissance
MILO	Magnetically insulated line oscillators
ML	Machine Learning
NASA	Administración Nacional de Aeronáutica y el Espacio
NGWS/FCAS	New Generation Weapon System/Future Combat Air System
NRBQ	Nuclear, Radiológica, Biológica y Química
OSINT	Inteligencia de fuentes abiertas
OTAN	Organización del Tratado del Atlántico Norte
PBF	Powder Bed Fusion
PEM	Membrana electrolítica polimérica
QKD	Distribución de claves cuánticas
QuAIL	Quantum Artificial Intelligence Laboratory
qubit	Bit cuántico
RA	Realidad aumentada
RSA	Rivest, Shamir y Adleman
RV	Realidad virtual
SaR	Search and rescue
SLM	Fusión selectiva por láser
SLS	Sinterización selectiva por láser
SMA	Stress Monitoring Assistant
TIC	Tecnologías de la Información y la Comunicación
TRL	Nivel de madurez tecnológica
UAV	Unmanned Aerial Vehicle

UPM	Universidad Politécnica de Madrid
USRA	University Space Research Association
WP	Working Package