SERIE CUADERNOS TECNOLÓGICOS

Cuadernos de isdefe

1

Capacidades Militares

en el Ámbito Europeo de la Defensa

CUADERNOS DE Isdefe

Isdefe

Capacidades Militares en el Ámbito Europeo de la Defensa

Volumen 1

Serie Cuadernos Tecnológicos

Cuadernos de Isdefe

AUTORES

J. Daniel González Galdo / Alfredo Peña Ruiz

Begoña Rojo Carralero

Violeta Ruiz Aldea

Alberto Domínguez Abecia / Fernando J. Senent Gómez

Cesar Heras Menor de Gaspar

Isaac Domínguez Santos

Benito Fernández García / Daniel Benavente López / Salvador Llopis

Yolanda Jaén González / Rocío Mora Picazo / Sergio Vicente López

Título original: Capacidades militares en el ámbito europeo de la Defensa

C/ Beatriz de Bobadilla, 3 -28040 Madrid
www.isdefe.es

Primera edición: Junio 2024

ISBN: 978-84-09-62256-6
No comercial
Depósito legal: M-14807-2024

Editorial: Ingeniería de Sistemas para la Defensa de España SA SME MP
Coordinador: Juan Manuel García Montaño
Equipo de edición y revisión de estilo: Juan Manuel García Montaño, J. Daniel González Galdo, Mª del Rocío Manjón Pérez
Diseño y maquetación: Iliana Aguilar Jiménez
Grabación y edición vídeos: Favorit Comunicación

Impreso por Byprint Madrid
Impreso en España – *Printed in Spain*

Queremos mostrar nuestro agradecimiento a las siguientes personas y organizaciones por hacer posible la primera edición de este libro con su colaboración o contribución:

General de Brigada. D. César de Cea Quijano

Coronel D. José Daniel Vázquez del Pozo y colaboradores del EMACON / EMAD

D. Emiliano Mata Verdejo

D. Efren Yániz Igal

Área de RRII de Isdefe

"El campo de batalla es una escena de caos constante. El ganador será el que controla el caos, tanto el propio como el de los enemigos."

Napoleón Bonaparte

PRÓLOGO

La tecnología ha sido tradicionalmente un factor determinante de los cambios en la sociedad y del arte de la guerra, favoreciendo a aquel que ha sabido obtener y utilizar la ventaja tecnológica. A su vez, la pervivencia de una sociedad y de las propias personas que forman parte de ella, dependen del resultado de la guerra; por ello, se puede concluir que el bienestar e incluso las vidas de los ciudadanos, están condicionadas por la efectividad de los ejércitos que los defienden.

A lo largo de la historia, los ejércitos vencedores han sido aquellos que han sido capaces de llegar más lejos, con mayor fuerza y precisión y más rápido que sus oponentes. Así, gran parte de la creatividad tecnológica del ser humano ha estado consagrada a incrementar el radio de acción, aumentar la potencia y precision de las acciones de fuego, el ritmo de la maniobra, y el tempo de las operaciones.

Hoy en día, ya no existen las retaguardias seguras, debido a las nuevas plataformas y armas que pueden superar la velocidad del sonido, como los misiles hipersónicos; e incluso igualar la velocidad de la luz, como los cañones láser, guiados con precisión con la ayuda de señales emitidas desde satélites. Además, desde la revolución industrial, la letalidad de las armas convencionales ha aumentado en más de cinco órdenes de magnitud. Resulta inquietante que dos de los contendientes en los dos conflictos activos más intensos posean armas nucleares capaces de provocar una catástrofe de proporciones incalculables. En definitiva, se puede afirmar que la humanidad está cerca de alcanzar los límites físicos asociados a los parámetros teóricos de espacio y tiempo.

Sin embargo, la aplicación en el ámbito militar de tecnologías emergentes y en gran medida asociadas a la transformación digital, como la inteligencia artificial o la robótica, promete ser una revolución por sus efectos sobre el ritmo de las operaciones. Esto conlleva consecuencias organizativas y cambios doctrinales profundos que tendrán un carácter disruptivo, que sin duda exigirán un cambio de mentalidad en los jefes de las diferentes unidades en combate. Hoy, en una era de cambio tecnológico exponencial donde la supremacía ha pivotado hacia el ámbito civil, las Fuerzas Armadas deben no solo adaptarse, sino anticipar y moldear el futuro, asegurando una superioridad tecnológica en un entorno global impredecible e hiperconectado.

Por otra parte, en un entorno donde la guerra híbrida y las acciones en la zona gris se están convirtiendo en la norma, las capacidades tecnológicas deben complementarse con un profundo entendimiento de la política global, la psicología humana y la estrategia económica. La guerra del futuro no se librará solo en los campos de batalla tradicionales, sino en las mentes y corazones de la población civil, en las bolsas de valores y en las redes de información.

El éxito de las operaciones militares en este complejo entorno operativo depende de la integración y la coordinación de todas las capacidades disponibles en los distintos dominios: terrestre, marítimo, aéreo, espacial, cibernético y cognitivo. Esta citada integración y tratamiento de la información, responde al concepto de operaciones multidominio (Multi Domain Operations). Supone una transición a una forma sofisticada y muy avanzada del arte de la guerra en un ecosistema digital, que descansa en la superioridad de la información y en la agilidad en la toma de decisiones. Se logra mediante la adopción de tecnologías capaces de automatizar procesos y de asegurar una elevada conectividad e interoperabilidad, características distintivas de la solución tecnológica que lo habilita, conocida como nube de combate. Para operar en el multidominio también es necesario un cambio de mentalidad basado en un profundo conocimiento técnico y táctico sobre las capacidades disponibles, de modo que se consiga una profusa delegación de decisiones y una fluida compartición de información, lo cual tiene inconvenientes, que hay que asumir, pero que son compensados sobradamente por la ventaja operativa que supone la descentralización en la toma de decisiones.

Sin embargo, la mera posesión de tecnología avanzada y superior a la del adversario no garantiza la victoria. La historia está repleta de ejemplos donde la superioridad técnica ha sido anulada por tácticas innovadoras o combatientes con una decidida voluntad de vencer. Hay que tener en cuenta que tan importante es la preparación física, técnica y táctica, como la moral y psicológica. Esto último resulta cada vez más complicado en un contexto hiperdinámico y con sobrecarga de información. La resiliencia en condiciones adversas y la habilidad para operar bajo extrema presión son atributos que ninguna tecnología puede sustituir completamente, por lo que tanto la formación como el desarrollo de las virtudes intangibles del soldado siguen siendo tan esenciales como siempre.

Con estos desafíos en mente, resulta indispensable identificar y comprender cuáles son las tecnologías más útiles para las Fuerzas Armadas, a fin de incorporarlas plenamente en sus capacidades militares. El presente cuaderno atiende de forma extraordinaria a ese propósito, mediante la difusión de ese conocimiento entre la sociedad española, a la que sirven nuestras Fuerzas Armadas y de la que esperan recibir lo que necesitan para el mejor cumplimiento de su misión.

Teniente General Fernando García González-Valerio
Jefe del Estado Mayor Conjunto de la Defensa

CAPACIDADES MILITARES EN EL ÁMBITO EUROPEO DE LA DEFENSA

ÍNDICE


59%
6169.6
0%
34%
4521.2
4521.2

CAPÍTULO 1

Introducción

Daniel González Galdo
Alfredo Peña Ruiz

El presente cuaderno pretende dar una visión global, desde un punto de vista divulgativo, de cómo el desarrollo tecnológico está afectando a las capacidades militares, dentro del marco geoestratégico actual, y las consecuencias que está teniendo la aplicación de dichas capacidades en los ámbitos de actuación: Terrestre, Naval, Aéreo, Espacial y del Ciberespacio.

La fuerte demanda de recursos naturales por parte de países en desarrollo, como del sudeste asiático, está reconfigurando el panorama geopolítico y, no cabe duda de que el desarrollo tecnológico está siendo utilizado como una de las palancas claves de esta reconfiguración. En este sentido, la UE se enfrenta al reto fundamental de posicionarse adecuadamente en este nuevo escenario. Para ello, debe ser consciente primero de cuál es su posición actual; segundo, cuál quiere que sea esa posición en el futuro; y finalmente diseñar y tomar las medidas correctas para posicionarse adecuadamente.

El problema abarca todos los aspectos de la sociedad, incluidos los políticos, económicos, comerciales, de seguridad y de defensa. Sin embargo, en el presente cuaderno nos limitaremos a aquellos referidos a la defensa, y más particularmente a las capacidades militares necesarias.

En cuanto al alcance geográfico, se focaliza en el ámbito europeo, señalando el papel que España desempeña en determinados desarrollos, y su comparación con el resto de los competidores mundiales que luchan por ejercer el liderazgo en tecnología.

No se busca ofrecer una relación exhaustiva de las capacidades que precisan las fuerzas armadas europeas, lo cual estaría dentro del alcance de trabajos más específicos, sino que se trata más bien de situar al lector y proporcionarle una visión general de la dimensión y tipología de los retos que nos ofrece la aplicación de las tecnologías a la hora de afrontar el futuro próximo.

1. CONTEXTO GENERAL

Desde una perspectiva de defensa, y con vistas a entender las implicaciones tecnológicas sobre las necesidades militares, podemos entender que la evolución del actual contexto geoestratégico está caracterizada por tres factores estratégicos.

El primer factor se refiere al desplazamiento del centro de poder global hacia Asia, derivado de su fuerte desarrollo económico de las últimas décadas y la necesidad de recursos para mantenerlo. Cualquier estimación de las futuras capacidades militares debe considerar las diferentes implicaciones y consecuencias de los acontecimientos, así como de las acciones en una u otra dirección que los actores globales (incluida la propia UE) puedan llevar a cabo.

Relacionado con esto, se puede observar como en las últimas décadas han surgido potencias no tradicionales que han expandido su influencia por todo el mundo. Esto comporta un incremento de su presencia política y económica, pero también militar. Se espera que esta expansión continúe en las próximas décadas, y estas potencias vayan ganando influencia en zonas de África y América Latina. China, India y otros países del sudeste asiático son claro ejemplo de esta tendencia.

Por otro lado, ello está provocando un cambio de posición en las potencias consideradas tradicionales. Países como EE.UU. están replanteándose en los últimos años su estrategia global con un claro enfoque hacia Asia. Aunque se espera que estas potencias tradicionales sigan manteniendo una fortaleza económica y militar, las prioridades para garantizar sus intereses se están viendo redefinidas y su posición en la geoestrategia global es, en ocasiones, incierta.

Como segundo factor estratégico, se observa una mayor intensidad en los vectores de amenaza tradicionales en Europa. En particular, tanto la amenaza en el este europeo como la inestabilidad en el norte de África se están viendo incrementadas en los últimos años.

Desde el punto de vista de la amenaza en el este, las tensiones vienen siendo incrementales en los últimos años, incluida la invasión de Ucrania por parte de Rusia. Más allá de la relevancia que puedan tener eventos concretos, la UE debe plantearse cuál es la posición y la relación de futuro que quiere mantener con los países de la zona, con Rusia en particular, pero también con otros como Turquía o los del Medio Oriente. Esta relación tendrá una componente política y económica, pero sin duda también una militar con el fin de evitar posibles conflictos como los actuales en esta zona del mundo.

En este sentido, se prevé que el uso de tácticas de guerra híbrida, la promoción de la desinformación y el apoyo al extremismo y al nacionalismo desde estos países se vean incrementados en las próximas décadas.

Desde una perspectiva más mediterránea, se observa un claro aumento del interés comercial en la zona del norte de África que está atrayendo a actores diferentes a los tradicionales. De hecho, en la actualidad, China es el mayor inversor en la región de Oriente Medio y Norte de África (zona MENA), donde se postula como proveedor de infraestructuras y tecnología.

Como elemento potenciador de estos vectores tradicionales es necesario considerar también la creciente polarización interna de la sociedad europea. Aspectos como el aumento del populismo o la falta de confianza en los gobiernos, junto con las campañas de desinformación, han sido identificados como tendencias que estarán presentes en las próximas décadas.

Como **tercer factor estratégico** a considerar, y en relación directa con la tecnología, se aprecia una **globalización de la amenaza** por la que cada vez más, se difumina la caracterización del adversario, que puede actuar desde cualquier parte del globo. En este último factor no solo influye el alcance cada vez mayor de los sistemas de armas sino también el fuerte desarrollo de sistemas y nuevas tácticas en el espacio exterior y en el ciberespacio que ofrecen la posibilidad de actuar a muy larga distancia.

Si observamos estos tres factores desde la perspectiva de la Unión Europea (EU), vemos como uno de los principales retos es la concepción diferente que los Estados miembros tienen tanto de la amenaza, como del conjunto de capacidades necesarias para enfrentarla. La concepción de la soberanía a nivel nacional, y no europea, sin duda es el principal factor para ello.

Si bien actualmente parece existir un deseo de avanzar en la defensa y la seguridad europea desde la integración del sector industrial, se ha señalado también que lo deseable sería considerar la creación de una Defensa y Seguridad Europea Común, en la que la soberanía europea prevalezca sobre la de los Estados miembros. Esto iría más allá de la actual Política Común de Seguridad y Defensa (PCSD), que permitiese la organización de la defensa europea en su totalidad, incluyendo su aspecto industrial.

De una forma u otra, el factor industrial juega un papel preponderante y surge la interrogante sobre cómo incentivar y fortalecer la Base Tecnológica e Industrial de la Defensa Europea (BTIDE) a través de programas cooperativos que no solo la estimulen, sino que también la organicen y revitalicen. Y todo ello, respondiendo de manera efectiva a las necesidades de capacidad militar, y valorando aspectos como el impacto en el tejido industrial a nivel individual de los Estados miembros, la gestión de redundancias y la posibilidad de especialización a nivel regional o nacional.

Cabe mencionar en este punto la aportación a la Autonomía Estratégica Europea (EU-SA, de sus siglas en inglés) que, si bien se refiere de forma general, a la capacidad de la Unión Europea para actuar sin dependencia de terceros países, la defensa, y en particular la industria de la defensa juegan un papel relevante.

2. LAS NUEVAS TECNOLOGÍAS

No cabe duda de que el factor tecnológico supone un elemento clave en lo que se refiere a la defensa y a la seguridad. A lo largo de la historia, la tecnología ha transformado constantemente la forma en la que se han llevado a cabo las operaciones militares, tanto desarrollando sistemas de armas más complejos y con mayores capacidades que daban origen a la aparición de nuevas tácticas y procedimientos, como mejorando los procesos de información y de toma de decisión. Todo ello genera además un salto tecnológico en materia de defensa con potenciales adversarios, que ha supuesto y supone un elemento disuasorio frente a posibles conflictos.

Este apartado quiere ofrecer una visión general de cómo las tecnologías pueden, potencialmente, afectar a las capacidades militares. Para ello, se describen brevemente y a modo de ejemplo, algunas de las tecnologías que previsiblemente pueden tener mayor impacto. Si bien en foros más especializados se habla de las tecnologías emergentes y disruptivas, no se pretende aquí realizar una revisión exhaustiva ni establecer una relación detallada de sus aplicaciones militares. El rápido desarrollo tecnológico haría obsoleto rápidamente cualquier análisis que procurase tal objetivo.

Las tecnologías que se presentan se han seleccionado de entre las consideradas por las principales organizaciones internacionales de las que España forma parte. En particular para la UE y OTAN, y son las siguientes: Inteligencia Artificial (IA), Internet de las Cosas (IoT) y Big Data, Blockchain, robótica y sistemas autónomos, tecnologías cuánticas, biotecnologías, armas hipersónicas, tecnologías espaciales y nuevos materiales.

2.1. Inteligencia Artificial (IA)

La IA está cambiando el mundo en que vivimos, y sus aplicaciones, son cada vez más relevantes tanto en el entorno civil como en el militar. Existe ya cierto consenso en que la IA pueda superar a la inteligencia humana en tareas específicas como traducción de idiomas o incluso la conducción y operación de vehículos en determinadas circunstancias límite o complejas.

Desde el punto de vista militar, su impacto está siendo también significativo, afectando a todas las capacidades militares, tanto en los nuevos dominios como en los tradicionales. Algunos ejemplos de capacidades que se ven potenciadas mediante la IA incluyen la detección y adquisición de objetivos, los sistemas autónomos o las herramientas de planificación y apoyo a la toma de decisión. También es crucial analizar el impacto de la aplicación de la IA y realizar los cambios adecuados para aprovecharlo en lo relativo a organización y doctrina, incluyendo el desarrollo de nuevas técnicas, tácticas y procedimientos.

Sin embargo, la implementación de la IA también presenta nuevos desafíos que deberán ser considerados. Aspectos como la verificación y validación de los algoritmos, la ciberseguridad o el grado de autonomía en la toma de decisión que se quiera ofrecer a los sistemas son aspectos que considerar detenidamente. A medida que se exploran las posibilidades de la IA para mejorar la efectividad de las operaciones, deben tenerse en cuenta los riesgos asociados al uso de esta tecnología.

La IA debe permitir a las Fuerzas Armadas (FAS) anticiparse y reaccionar en un escenario cambiante e incierto, incluyendo la capacidad de gestionar adecuadamente todo el espectro del conflicto, con total garantía y confianza en los sistemas autónomos y de apoyo a la toma de decisión basados en IA.

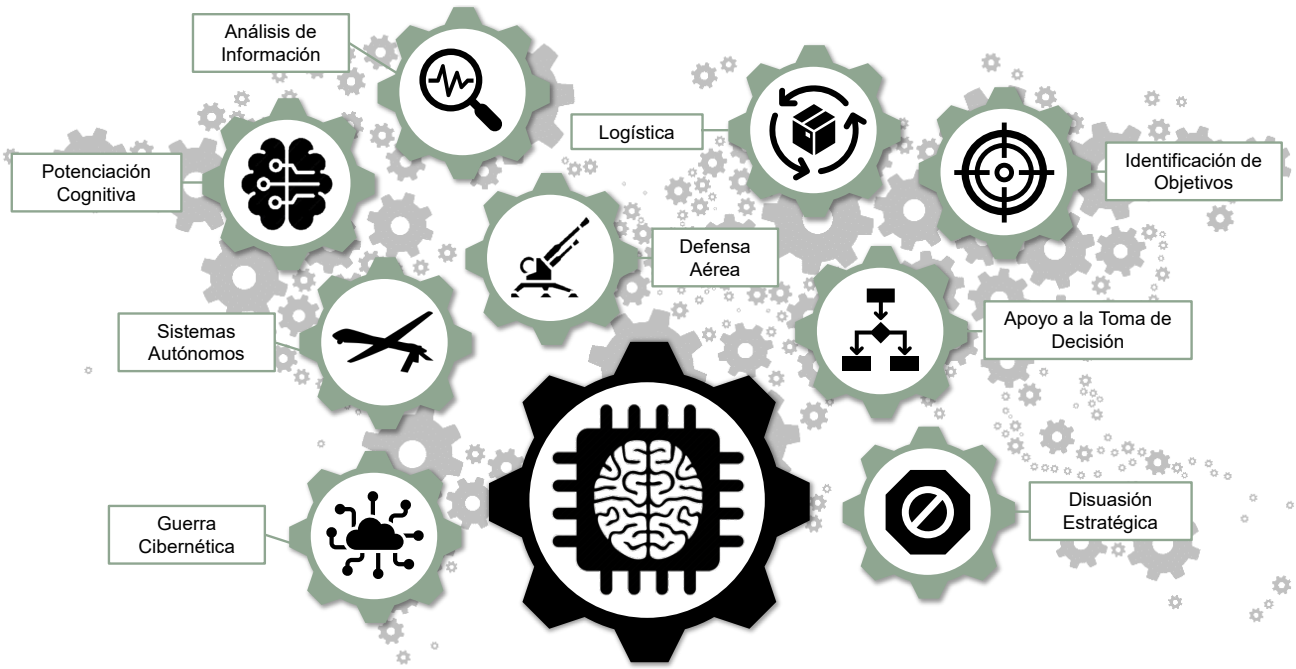


Ilustración 1. Posibles Aplicaciones Militares de la inteligencia Artificial

2.1.1. Posibles Aplicaciones Militares

Sistemas de apoyo a la toma de decisión. Es una de las principales aplicaciones de la IA. Estos sistemas podrán desarrollar planes de acción más complejos basados en el análisis de enormes cantidades de datos y así ponerlos a disposición del mando para la toma de decisiones.

A causa de la creciente velocidad con la que desarrolla la acción y a la reducción constante de los tiempos de reacción, es muy probable que, a corto y medio plazo, deba confiarse la toma de decisiones no críticas o rutinarias a las herramientas autónomas. Esto exige generar un nivel de confianza adecuado y establecer los mecanismos de control y validación apropiados para garantizar que las decisiones tomadas sean las más beneficiosas. Además, los sistemas de IA pueden ayudar en la identificación de objetivos de alta prioridad y en la asignación de recursos adecuados. La identificación de objetivos en el entorno táctico se ve mejorada gracias al desarrollo de sistemas de reconocimiento automático en tiempo real. Una mejor identificación y reconocimiento de objetivos permitirá una respuesta más eficaz evitando a su vez causar daños colaterales.

En la defensa contra nuevos tipos de amenaza aéreas. En combinación con otras tecnologías como el IoT, la IA también tiene aplicaciones en la defensa contra nuevos tipos de amenaza aéreas incluyendo municiones de hipervelocidad o sistemas autónomos. El uso de algoritmos de IA permite la identificación, caracterización y reconocimiento en tiempo real de la amenaza y el establecimiento de las contramedidas adecuadas.

Una de las principales aplicaciones de la IA consiste en dotar de autonomía de acción a los sistemas y plataformas. Los sistemas autónomos actuales ya disponen de cierta capacidad de maniobra no supervisada, y en algunos casos incluso capacidad de decisión ante una situación de enfrentamiento.

El empleo de armamento autónomo levanta muchas dudas desde el punto de vista ético y moral, pero no debe obviarse su uso por parte de adversarios que carezcan de este tipo de restricciones. Dada la precisión y velocidad de respuesta necesarias para contrarrestarlos, los sistemas de armas propios deben disponer de capacidad de actuación autónoma. Reviste una especial importancia la definición de las reglas de enfrentamiento en estos casos, con el fin de mantener la efectividad en la respuesta a la vez que se cumple con las restricciones legales en vigor.

En relación con lo anterior se halla la necesidad de definir el adecuado nivel de participación del ser humano en la decisión del sistema, desde el control pleno, la supervisión

o la delegación completa. Cada caso particular demandará una mayor o menor involucración por parte del operador humano, considerando el contexto de la operación, la presencia de no combatientes, el tipo de amenaza, la madurez del sistema basado en IA, etc.

Ciberespacio. Otro dominio en el que la IA ya está presente de forma muy relevante es en el del ciberespacio. Algoritmos basados en IA tienen la capacidad de analizar flujos de datos dentro de las redes digitales y localizar debilidades sobre las que ejecutar ataques cibernéticos. Muchos de estos ataques pueden ser realizados incluso sin que la víctima sea consciente del ataque, con las consecuencias que esto puede tener a lo largo del desarrollo de una operación. De igual manera, se pueden utilizar sistemas basados en IA con intenciones defensivas para detectar los ataques cibernéticos, incluidos espionaje, intrusiones, sabotajes o comportamientos sospechosos en general.

Desde un punto de vista estratégico, la IA puede tener un impacto muy significativo en la disuasión. Por ejemplo, son diversos los estudios que apuntan a la posibilidad de que mediante esta tecnología se pueda detectar con facilidad y de manera rápida los puntos de lanzamiento, así como las trayectorias de los misiles balísticos, y por tanto facilitar la neutralización efectiva de un ataque. Ejemplos como éste abren todo un nuevo escenario geopolítico lleno de incertidumbre en el que los mecanismos actuales de disuasión se verían afectados significativamente.

Por otra parte, cabe la posibilidad de que sea la capacidad cibernética, apoyada en sistemas de IA, la que pueda llegar a jugar ese papel disuasorio de nivel estratégico. Aquellos países que dispongan del conocimiento y las herramientas para incapacitar los servicios críticos de otro, en un momento dado, tendrán a su disposición una herramienta de disuasión de primer orden.

Logística militar. Un área donde mayor impacto tendrá la aplicación de sistemas apoyados por la IA (combinados con otras tecnologías como la fabricación aditiva o el gemelo digital) será el campo de la logística militar. La influencia de la IA se extenderá a varios aspectos de la cadena de suministro, así como al mantenimiento de equipos, sistemas y plataformas. Aspectos como el tratamiento estadístico de los datos, combinado con el procesado automático basado en IA, y el mantenimiento o reparación automatizados implican mejoras significativas en todo el proceso de apoyo logístico.

Capacidades cognitivas del ser humano. Otra de las aplicaciones que ofrecen los sistemas basados en IA es la potenciación de las capacidades cognitivas del ser humano. En particular, y a modo de ejemplo, los sistemas de reconocimiento de voz y traducción automática permiten una mejor interpretación del lenguaje y, sin duda, reducen la barrera idiomática. La fácil y rápida comprensión de las lenguas nativas, combinada con un aumento en la información disponible, ayuda a la identificación temprana de amenazas y reduce los riesgos de posibles malas interpretaciones o errores humanos.

Análisis de información. Finalmente, hay que destacar la capacidad de los sistemas basados en la IA para el análisis de información no estructurada, como informes, documentos, noticias, publicaciones en redes sociales, patrones de comportamiento y otros tipos de datos en favor de una mejor capacidad de inteligencia. Entre otras muchas aplicaciones, esto puede incluir herramientas específicas para la gestión de campañas de desinformación, identificación de falsos medios de comunicación, información falsa (Deep fakes) o comportamientos engañosos.

2.1.2. Retos Asociados a la Implementación

Como vemos, el uso de la IA se está extendiendo rápidamente y se prevé que tenga un impacto significativo en el campo militar. Sin embargo, la implementación de sistemas militares basados en IA también plantea importantes desafíos.

Uno de los mayores retos es la falta de estándares y procedimientos adecuados para la Verificación y Validación (V&V) de los sistemas que integran la IA. La V&V es esencial para garantizar que los sistemas funcionen correctamente, y cumplan con los requisitos de los usuarios antes de ser certificados y desplegados en un entorno real.

En el caso particular de la IA, al tratarse de soluciones no deterministas y cuyo comportamiento puede evolucionar con el uso y la experiencia adquirida, se complica especialmente este requisito. En este sentido será especialmente relevante el desarrollo de capacidades de simulación que permitan reproducir infinidad de posibles situaciones y comportamientos con los que validar las soluciones ofrecidas por el sistema de IA. Igualmente, el establecimiento de políticas adecuadas de certificación es un requisito fundamental para garantizar la resiliencia y la confianza en todos los niveles y dominios.

Otro desafío importante es la interoperabilidad de los sistemas, que requiere un esfuerzo significativo en cuanto a definir, desarrollar e implementar arquitecturas abiertas,

estándares y regulaciones para el desarrollo de la IA, así como para el intercambio y transferencia de conocimiento (sistemas pre-entrenados) y soluciones.

La utilización de la IA no debe tener como objetivo reemplazar la contribución humana, sino complementarla. Para ello, es necesario desarrollar nuevos modelos operativos que permitan la cooperación entre sistemas tripulados y no tripulados, de modo que las Fuerzas Armadas sean más efectivas y eficientes.

Desde este punto de vista, es necesario definir los criterios y protocolos de colaboración Humano-Máquina (MUM-T, de sus iniciales en inglés) en base a las capacidades que ofrezca la tecnología. En particular, entre las tecnologías habilitantes para MUM-T se incluyen algoritmos de inteligencia artificial y técnicas de aprendizaje automático, redes de comunicación avanzadas, tecnologías de sensores, interfaces hombre-máquina, realidad virtual o aumentada, o robótica y autonomía.

Otros retos significativos alrededor de la implementación de sistemas basados en IA provienen de las vulnerabilidades relacionadas con las amenazas cibernéticas, así como la dependencia de los datos para alimentar los algoritmos. La proliferación de sistemas altamente digitalizados y el uso de algoritmos complejos los convertirán en particularmente vulnerables a los ciberataques.

Por último, destaca por su importancia el reto de afrontar el diferente estado de desarrollo de sistemas y algoritmos basados en IA en Europa frente a otros países, así como la dependencia de terceras empresas no europeas.

2.2. Internet de las Cosas

El Internet de las cosas, también conocido como IoT, supone la sensorización de cualquier elemento del mundo físico con el fin de caracterizarlo y disponer de información en tiempo real sobre su entorno y sobre su estado. Uno de sus principales propósitos es el de monitorizar y actuar sobre cualquier dispositivo en remoto ofreciendo así una conciencia sobre el entorno y facilitar así la toma de decisiones.

Las aplicaciones que pueden tener el IoT desde el punto de vista militar cubren casi todo el espectro de tareas, desde las asociadas a la inteligencia y la gestión de la información, hasta aquellas directamente relacionadas con el combate o el apoyo y sostenimiento de operaciones. Desde el punto de vista de los sistemas, multitud de plataformas, incluyendo buques, aeronaves, vehículos terrestres, sistemas autónomos y sistemas de armas, se verán afectados por las tecnologías IoT. Aspectos como la miniaturización permitirán también implantar este tipo de tecnología en pequeños dispositivos portátiles, facilitando incluso la monitorización de los combatientes a través del uso, por ejemplo, de sensores integrados.

Desde el punto de vista de los dominios militares se contempla que el impacto del IoT afecte a todos y cada uno de ellos. En los dominios tradicionales (Tierra, Mar y Aire) tanto combatientes como vehículos y otros activos estarán equipados con sensores IoT. Particularmente, se espera un desarrollo significativo de IoT en el entorno submarino, donde los futuros desarrollos en tecnologías inalámbricas, sensores acústicos, comunicaciones y vehículos autónomos proporcionarán una conciencia situacional mejorada por debajo de la superficie.

2.2.1. Posibles Aplicaciones Militares

Una de las principales aplicaciones que se identifican para el IoT es la capacidad de recopilar grandes cantidades de datos y generar inteligencia a partir de ellos. El uso de redes extensas de sensores desplegados en todos los dominios e integrados en la mayoría de los dispositivos y plataformas, provenientes de múltiples fuentes, ofrecerá un entorno descentralizado que proporcione una visión operativa común de la situación, facilitando así la toma de decisión.

Esto tiene un impacto fundamental en los sistemas CIS, tanto en la capacidad de los mismos para tratar los datos y la información, como en la necesidad de desarrollar algoritmos avanzados de integración, fusión y generación de inteligencia.

Desde el punto de vista logístico, el IoT puede ser un gran facilitador de la eficiencia logística y el mantenimiento de equipos y sistemas. Combinado con otras tecnologías como Big Data, el IoT ofrecerá una mayor visibilidad en toda la cadena de suministro, permitiendo una mejor previsión de las necesidades de mantenimiento. Esto ayudará a la planificación logística y a gestionar los recursos de manera más efectiva, reducir cuellos de botella o mejorar la gestión de los inventarios.

Para la gestión de flotas y equipos, incorporar sensores y sistemas de monitorización en todo tipo de plataformas, sistemas de armamento y municiones, proporcionará información crítica en tiempo real sobre su posición,

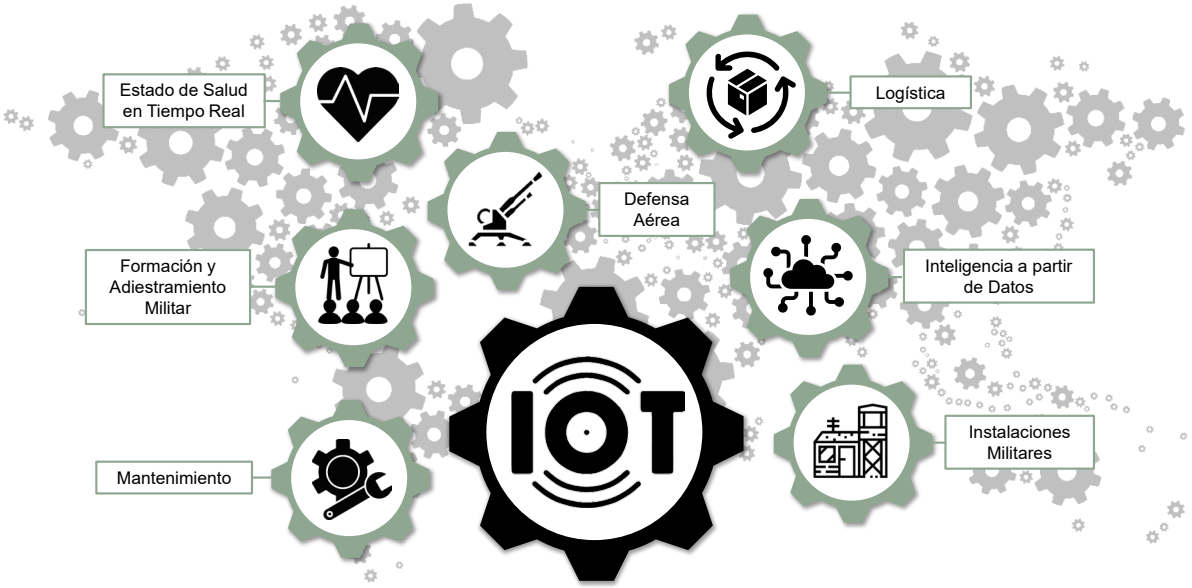


Ilustración 2. Posibles Aplicaciones Militares de Internet de las Cosas

velocidad, combustible, estado y otros parámetros. Esto ayudará a reducir los costes asociados a la movilidad de estos elementos y disminuirá el esfuerzo operativo asociado.

Otra de las aplicaciones donde la tecnología IoT tendrá mayor impacto es en los sistemas de defensa antiaérea. Puede observarse como las amenazas aéreas están en constante evolución con la inclusión de sistemas autónomos o misiles hipersónicos que tienen características físicas y vectores de ataque muy diferentes a los de plataformas tradicionales. Esto exige capacidades de detección y defensa antiaérea mejoradas con redes extensas de sensores que proporcionen información en tiempo real.

El uso de IoT en todos los niveles de recopilación, procesamiento y análisis de datos permitirá la detección de estas amenazas y la determinación de su trayectoria de vuelo de manera más rápida y eficaz, permitiendo una toma de decisión (ya sea autónoma o no) más ágil y efectiva.

Desde el punto de vista del combatiente a pie, una de las áreas de aplicación más significativa será la utilización de dispositivos portátiles y sensores para monitorizar su estado de salud en tiempo real. Este tipo de tecnología permitirá un diagnóstico y tratamiento más temprano y efectivo de enfermedades y lesiones. Además, la monitorización biométrica, en conjunción con aplicaciones de realidad aumentada proporcionará la posibilidad de realizar tratamientos o adelantar actuaciones médicas en tiempo real.

Las aplicaciones de salud no se limitarán únicamente al diagnóstico y tratamiento de enfermedades y lesiones, sino que también serán fundamentales en las misiones de Búsqueda y Rescate en Combate (CSAR) así como en misiones de Evacuación Médica (MEDEVAC). El IoT permitirá realizar una mejor planificación de estas operaciones y una monitorización de pacientes en situaciones críticas.

La tecnología IoT puede también revolucionar la forma en que se gestionan las bases y se garantiza la seguridad en las instalaciones militares. La sensorización de cualquier elemento dentro de la base permitirá una automatización y manejo inteligente de información que proporcione mejor gestión de recursos, cobertura de necesidades del personal y en general un mejor apoyo a las operaciones a la vez que se reduce la cantidad de personal necesario para cubrir estos servicios. El uso de sensores IoT para identificar intrusos, mediante tecnologías como reconocimiento facial, escaneo de retina, huellas dactilares y otros datos biométricos, evita accesos controlados, así como el acceso a información y sistemas críticos.

Además, vehículos y plataformas de grandes dimensiones como es el caso de los buques, pueden beneficiarse de la tecnología IoT convirtiéndolas en “bases inteligentes” móviles con capacidades mejoradas que permitan una mejor operación dentro del buque.

Finalmente, los dispositivos IoT pueden proporcionar diferentes formas de apoyo a la formación y adiestramiento militar, mejorando la eficiencia y el realismo de los entrenamientos. Por un lado, los sensores pueden utilizarse para monitorizar al personal militar durante el entrenamiento, tanto en entornos locales como remotos, y proporcionar información valiosa sobre la calidad del entrenamiento. Además, el IoT en conjunto con otras tecnologías como el Big Data, la realidad aumentada o la IA, pueden recrear ciertos entornos complejos y situaciones específicas en base a datos reales que ofrezcan entrenamiento más eficiente, rápido y realista en entornos seguros.

2.2.2. Retos Asociados a la Implementación

Tal y como observamos, la tecnología IoT ha irrumpido en el campo militar y está transformando la forma en que las Fuerzas Armadas operan en el campo de batalla. Si bien esta tecnología aporta grandes beneficios, también conlleva nuevos desafíos que deben ser abordados.

La principal preocupación que se puede identificar es la referida a la **ciberseguridad.** Los sistemas que utilizan IoT están más expuestos a los ciberataques y con la llegada de las redes inalámbricas de alta capacidad se requerirá el fortalecimiento de las capacidades de protección, a fin de evitar interrupciones de servicio, intrusiones o acciones de guerra electrónica, entre otros.

Otro desafío importante que presenta el IoT es la necesaria **interoperabilidad** de los diferentes dispositivos conectados. Se espera que el número de suministradores, así como de tecnologías y protocolos utilizados, sea elevado, con lo que será necesario establecer estándares de interoperabilidad para asegurar el adecuado funcionamiento de todos ellos de forma conjunta.

Tampoco se puede ignorar el impacto que puede tener la sobrecarga de dispositivos en las necesidades de **suministro energético.** Si bien es previsible que los dispositivos no sean demasiado exigentes a título individual, el elevado número de los mismos sí puede suponer un reto para generar, almacenar y distribuir adecuadamente la energía necesaria.

Finalmente, no puede dejar de considerarse el cambio que puede suponer para los operadores de los sistemas hacer frente a la gestión de **grandes cantidades de información.** Será necesario establecer los mecanismos adecuados para evitar una sobrecarga de información y realizar una gestión efectiva de la capacidad cognitiva de operadores y personal involucrado en la gestión de la información y toma de decisión.

Para hacer frente a estos desafíos se requerirá una serie de soluciones técnicas, como la implementación de avanzadas soluciones criptográficas, sistemas de procesado y tratamiento de datos o dispositivos de almacenamiento de gran capacidad y bajo consumo de energía.

2.3. Robótica y Sistemas Autónomos (RAS)

Actualmente la robótica y los sistemas autónomos están estrechamente relacionados con el uso de la IA, de modo que esta última haga posible su funcionamiento sin necesidad de control por parte del ser humano. Esto permite afrontar de manera autónoma una amplia variedad de tareas, entre ellas el transporte y el apoyo logístico, actividades ISR o de guerra electrónica, e incluso de combate.

En cualquier caso, el papel del operador humano no dejará de ser relevante, al menos en la toma de decisiones más complejas, así como en la supervisión de las operaciones. La mencionada colaboración entre humanos y máquinas, definiendo los roles que cada uno debe jugar en cada situación particular, quizá sea uno de los mayores retos para generalizar el uso de sistemas autónomos.

Entre los beneficios que proporciona la automatización podemos destacar la reducción de la exposición al riesgo del operador humano, el efecto multiplicador que tiene el uso de múltiples sistemas autónomos o la posibilidad de operar en entornos mucho más hostiles y bajo condiciones físicas mucho más adversas.

2.3.1. Posibles Aplicaciones Militares

El uso de robots y sistemas autónomos facilita el cumplimiento de los objetivos de una forma más precisa, rápida y controlada, minimizando la exposición del personal en el campo de batalla.

Quizá la aplicación más evidente para el uso de estos sistemas es la que tiene que ver con el desarrollo de misiones ISTAR, donde se contempla una amplia gama de tareas, incluyendo las de vigilancia de áreas de interés, obtención de información en tiempo real, recopilación y análisis de información, o la adquisición de objetivos, entre otras.

El uso de estos sistemas permite, asimismo, que tareas rutinarias y repetitivas como la vigilancia de fronteras, se realicen con una supervisión humana mínima, aumentando el área de supervisión con el personal imprescindible.

Con respecto a la capacidad de combate, la utilización de sistemas autónomos permite la acción de fuego desde entornos mucho más expuestos a las acciones del adversario, así como una mejor y mayor capacidad de maniobra al no estar condicionados por las limitaciones físicas del cuerpo humano ni verse influenciados por factores emocionales.

Su uso combinado con el de armamento de precisión, permite también minimizar los daños colaterales. Además, el empleo de estos sistemas facilita la aplicación de tácticas de saturación, como ocurre con los enjambres.

Otra posible aplicación de los sistemas autónomos consiste en completar o mejorar las capacidades de transporte, al permitir el transporte de carga y personal de forma automatizada, optimizando la ejecución de operaciones, y reduciendo las necesidades de personal asociadas. La combinación de diferentes medios de transporte, tripulados y autónomos, con diferentes tamaños de carga permite rediseñar las redes de suministro y una mejor integración entre el transporte estratégico, operacional y táctico, haciendo posible la evolución hacia una logística bajo demanda.

Se espera también que, en un futuro próximo, estos sistemas desempeñen un papel importante en el ámbito de la sanidad operativa, tanto durante el combate, como en los hospitales de campaña. El uso de robots médicos para la telemedicina, o el establecimiento de procedimientos quirúrgicos autónomos para tratar y estabilizar al personal de forma remota, permitirá llevar a cabo actuaciones sanitarias de forma más rápida, reduciendo la necesidad de personal médico especializado en el campo de batalla. Igualmente, estos sistemas pueden utilizarse para el suministro de material sanitario o la búsqueda de supervivientes en un entorno contaminado, entre otras actividades.

En términos generales, el uso de robots y sistemas autónomos redundará en una mayor eficiencia en el apoyo logístico a través de la gestión y distribución automatizada de suministros en todos los dominios, bien bajo demanda o de forma anticipada, la ejecución de tareas de mantenimiento rutinario, preventivo e incluso correctivo mediante capacidades avanzadas de auto reparación, reduciéndose así la huella logística.

En lo que respecta a la guerra electrónica, los sistemas autónomos pueden facilitar la detección y neutralización de amenazas haciendo uso del espectro electromagnético, mediante contramedidas electrónicas.

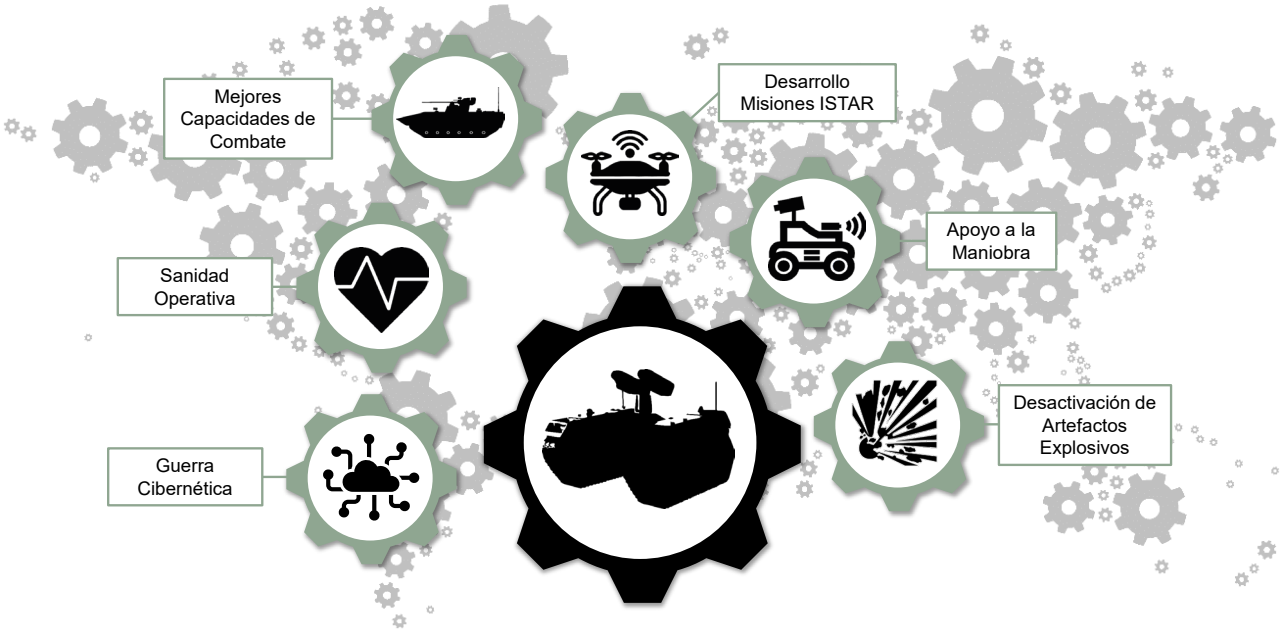


Ilustración 3. Posibles Aplicaciones Militares de la Robótica y los Sistemas autónomos (RAS)

Desde el punto de vista de la protección, es conocido el uso de robots para la detección y desactivación de Artefactos Explosivos Improvisados (C-IED de sus siglas en inglés), siendo previsible en que un futuro próximo las capacidades de estos materiales se vean incrementadas con mayor autonomía, mayor alcance y área de cobertura.

En cuanto al apoyo al combate de los ingenieros, estos sistemas son capaces de realizar diversos trabajos de mantenimiento, construcción o recuperación de infraestructuras, o de recuperación de sistemas y plataformas deteriorados. Esto permite la prestación de apoyos de forma remota, prescindiendo de la intervención humana in situ, lo que redundará en la minimización de tiempos y la reducción de la huella logística en operaciones.

2.3.2. Retos Asociados a la Implementación

El análisis en detalle desde la perspectiva MIRADO-I (siglas que respectivamente identifican a material, infraestructura, recursos humanos, adiestramiento, doctrina, organización e integración) contribuye a la integración completa de estos sistemas en las operaciones. Este análisis ayudará a definir el papel más adecuado de los robots y sistemas autónomos en las operaciones, así como el grado de sustitución o reemplazo de los sistemas tripulados actuales. Conseguir que tanto el personal ejecutante como los responsables de la toma de decisiones sean plenamente conscientes de las oportunidades, limitaciones y consideraciones generales de los robots y sistemas autónomos, aumentará significativamente la probabilidad de éxito en su implementación rápida y eficiente en el ámbito militar.

Para su uso en operaciones, los sistemas autónomos deben cumplir varios requisitos de rendimiento y de seguridad de modo que sean capaces de operar con todas las garantías. Sin embargo, algunos de estos aspectos aún no se han abordado o resuelto por completo.

Grado de supervisión humana o de autonomía que se les quiera dar. Esto dependerá de múltiples factores, entre los cuales cabe destacar los cambios doctrinales necesarios para aprovechar plenamente las ventajas, garantizando al tiempo que operan de forma fiable, segura y de acuerdo con las leyes y regulaciones en cada caso.

La resolución de los aspectos éticos y legales. Es un desafío crítico, que exigirá un profundo análisis de casos de uso y la elaboración de la legislación y regulación adecuada para el desarrollo y despliegue de robots y sistemas autónomos en operaciones militares.

Ciberseguridad. El nivel de digitalización y las necesidades de comunicaciones de estos sistemas hacen que la ciberseguridad sea un aspecto que considerar. Habrá que dotar a estos sistemas de las medidas de protección adecuadas para evitar ataques cibernéticos, capaces de tomar el control del sistema, interrumpir sus operaciones o acceder a información confidencial. A su vez, deben ser resistentes contra medidas electrónicas.

Riesgo de caer en manos del adversario. El riesgo de que estos sistemas puedan caer en manos del adversario, y esto le permita conocer la tecnología utilizada y aplicarla a sus propias capacidades es un aspecto relevante que tener muy en cuenta. El hecho de que se trate de sistemas con tecnologías de última generación y que puedan actuar en profundidad en zonas de conflicto, los hace especialmente vulnerables ante este riesgo. Por ello, es necesario implementar mecanismos y técnicas anti-manipulación en todas las etapas de su desarrollo.

Aspecto energético. Necesario para la alimentación de estos sistemas autónomos. Los desarrollos en propulsión eléctrica e híbrida tienden a generalizarse, requiriendo sistemas de almacenamiento más eficaces y de mayor capacidad, fuentes de energía miniaturizadas, supercondensadores, generadores de energía renovable o celdas de combustible de hidrógeno y cargadores eléctricos rápidos, por poner solo algunos ejemplos. Así mismo, otras soluciones no eléctricas, como los biocombustibles o los combustibles sintéticos, están siendo consideradas para su uso en los sistemas de propulsión de los sistemas autónomos.

2.4. Tecnologías Cuánticas

En el contexto del presente cuaderno, podemos entender la tecnología cuántica como aquella que aprovecha los principios y comportamientos de la física cuántica en aplicaciones tecnológicas de diferente índole, como la informática, los sensores o las comunicaciones, produciendo un gran impacto en la obtención, proceso, cifrado y transmisión de los datos.

Las principales ventajas que ofrece esta tecnología son el incremento exponencial en la capacidad de cálculo, el incremento en la velocidad y capacidad de las comunicaciones, el aumento sustancial de la seguridad cibernética, y la mejora significativa en la capacidad de sensorización y captación de información del entorno.

Los efectos de la aplicación de la tecnología cuántica serán sin duda disruptivos, si bien a su vez será necesario evaluar adecuadamente los plazos de implementación en función

del nivel de madurez. Así, hay potenciales aplicaciones cuya materialización puede estar más cercana en el tiempo, mientras que para otras es probable que no se vea en un largo plazo.

2.4.1. Posibles Aplicaciones Militares

Una primera aplicación de las tecnologías cuánticas se refiere al **desarrollo de operaciones en el ciberespacio,** tanto de índole ofensivo como defensivo. Los avances tecnológicos en la computación cuántica permitirán nuevos vectores de ataque y aumentar la efectividad de los métodos clásicos de hacking.

En las operaciones de defensa cibernética, los algoritmos de cifrado y protección aprovecharán la criptografía cuántica para hacer que los ataques de seguridad de la información sean considerablemente más complejos.

Por otra parte, las comunicaciones se verán directamente afectadas por los desarrollos de las tecnologías cuánticas debido a mejores capacidades de transmisión, pero sobre todo de seguridad en la información. En este sentido, estas comunicaciones seguras serán un habilitador clave para la conexión e interoperabilidad entre sistemas y dispositivos en el campo de batalla, como drones, aviones, barcos, combatientes y puestos de mando.

Uno de los campos donde se desarrollará más la tecnología cuántica es la de la capacidad de procesado de información y datos, que combinada con la IA producirá un salto cualitativo en las herramientas de apoyo a la toma de decisión. Esto permitirá contar con capacidades de mando y control distribuido más efectivas, integrando grandes cantidades de información y con asesoramiento inteligente por parte de los sistemas.

Con respecto a las capacidades de vigilancia, reconocimiento e inteligencia, las tecnologías cuánticas mejorarán significativamente la conciencia situacional de las fuerzas, mejorando por un lado la precisión, la sensibilidad y la protección de los dispositivos, y por otro, aumentando la capacidad de obtención y análisis de grandes cantidades de datos.

Particularmente en el entorno submarino, las tecnologías cuánticas pueden producir un importante cambio en sus tácticas, técnicas y procedimientos. El desarrollo de tecnologías cuánticas permitirá una mejor detección de objetivos, así como unas comunicaciones efectivas bajo la superficie.

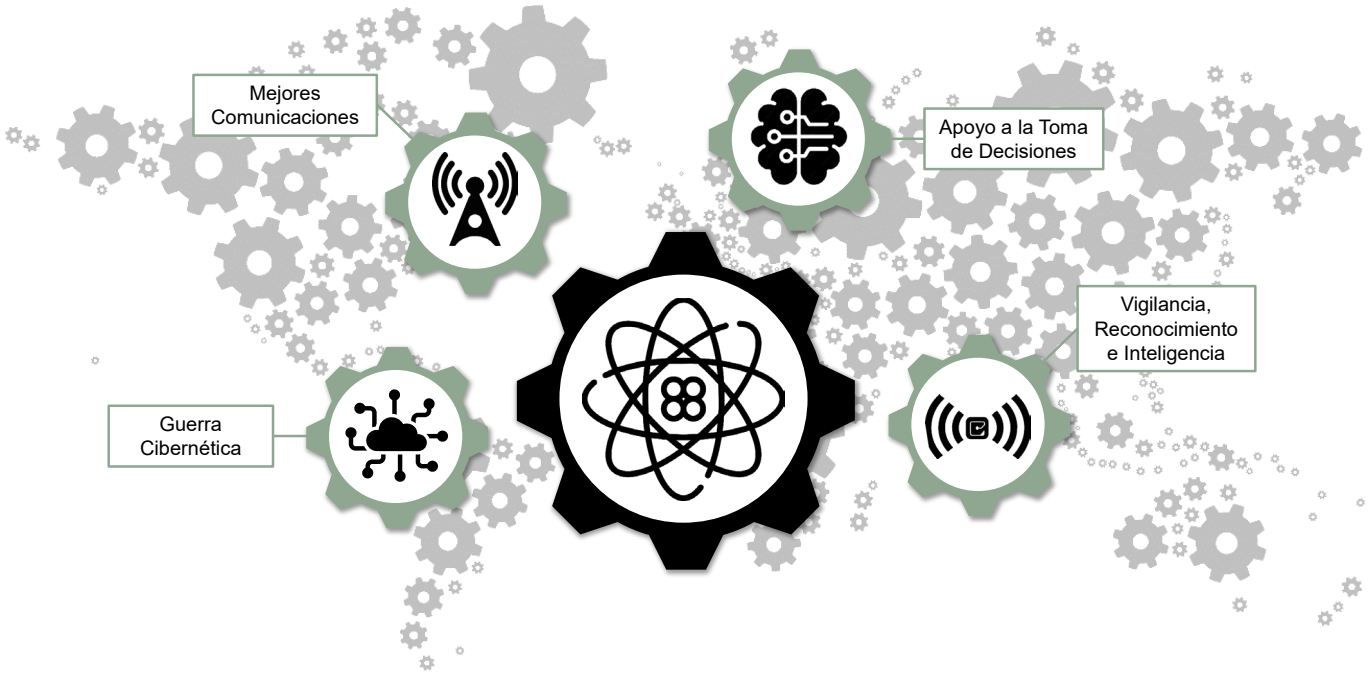


Ilustración 4. Posibles Aplicaciones Militares de las Tecnologías Cuánticas

2.4.2. Retos Asociados a la Implementación

Los plazos de implantación de las tecnologías cuánticas pueden variar de forma sustancial de unas aplicaciones a otras. A pesar de las perspectivas prometedoras, presentan problemas muy específicos que pueden causar dificultades en su integración en los sistemas militares. Por ello, habrá que incorporar paulatinamente estas tecnologías según estén disponibles, sin dejarse llevar por exageraciones sobre sus posibilidades o su grado de madurez, que conduzcan a expectativas no cubiertas.

Además, es necesario considerar el impacto que los nuevos sistemas de cifrado cuántico tienen sobre sistemas heredados con medios de ciberseguridad anticuados. Éstos últimos pueden no ser compatibles y requerir actualizaciones significativas, o aun siendo compatibles, pueden convertirse en puntos débiles del sistema comprometiendo la seguridad general del mismo.

También hay tener en cuenta los requisitos físicos y ambientales que deben cumplir las ubicaciones de los ordenadores cuánticos, que puede conllevar dificultades de despliegue, accesibilidad y seguridad.

Finalmente, un aumento en la complejidad tecnológica debido al desarrollo de la tecnología cuántica podría superar la capacidad de las cadenas de suministro, y potencialmente plantear problemas en cuanto al mantenimiento de los sistemas o dispositivos futuros.

2.5. Biotecnología y Mejora Humana

El término biotecnología se refiere a la aplicación de técnicas y procesos biológicos para desarrollar productos en apoyo a las capacidades del soldado y de las operaciones militares. Ejemplos de estos productos se refieren a alimentos y suplementos nutricionales, medicamentos biotecnológicos y farmacología, desarrollo de combustibles, biodegradación de residuos o ingeniería de tejidos.

El concepto de mejora humana tiene que ver con todas aquellas soluciones orientadas a la mejora de las capacidades del soldado, sean biotecnológicas o no. Los avances en este campo incluyen soluciones como exoesqueletos, integración de sensores, nuevos materiales o nanotecnología.

Al hablar del concepto de mejora humana asociado al de biotecnología, no nos referimos al uso de tecnologías relacionadas con la genética con el fin de potenciar las capacidades del ser humano. Son muchos los países que ya han renunciado explícitamente a la utilización de técnicas de ingeniería genética para mejorar las capacidades del soldado, tanto físicas como cognitivas.

2.5.1. Posibles Aplicaciones Militares

Monitorización de los combatientes. Una de las principales aplicaciones que se contemplan como parte del concepto de mejora humana es la de monitorización de los combatientes. El uso del IoT junto con capacidades de seguimiento biométrico facilitará una monitorización más precisa tanto del estado de salud como anímico del individuo. Se abre la posibilidad de disponer de múltiples sensores integrados en la ropa y el equipamiento del soldado, o incluso implantados, para monitorizar todo tipo de parámetros que, combinados y analizados adecuadamente, permitan un diagnóstico de su estado. En determinados casos, este diagnóstico puede realizarse de manera automática, y recomendar al soldado tomar determinadas acciones como alimentarse o tomar determinados medicamentos.

La implementación de estas tecnologías trae también consigo una mejora significativa en la conciencia situacional del soldado. El uso de microsensores avanzados y otras tecnologías como la Realidad Aumentada (RA) ofrecen la posibilidad de potenciar esa conciencia de la situación proyectando en tiempo real información de utilidad para la realización de la misión.

Integración efectiva de las capacidades humanas. El uso extensivo de sistemas no tripulados exige una integración efectiva de las capacidades humanas con la robótica y los sistemas autónomos. Dispositivos no invasivos permitirán una implementación fácil y rápida de esta capacidad de colaboración hombre-máquina, aunque pueden tener ciertas limitaciones y sobrecargar físicamente al operador. En el corto y medio plazo al menos, no se ve factible una integración más invasiva que conecte el cerebro y/o el tejido nervioso con las computadoras que permita una interacción extensiva en todos los procesos cognitivos. En cualquier caso, estas interfaces permitirán un aumento en la conciencia situacional y la optimización de los procesos de toma de decisiones.

Ámbito del adiestramiento e instrucción. Las tecnologías de neuroestimulación y farmacéuticas se están investigando para mejorar los resultados obtenidos al comprenderse de forma detallada cómo se está desarrollando el entrenamiento. En el

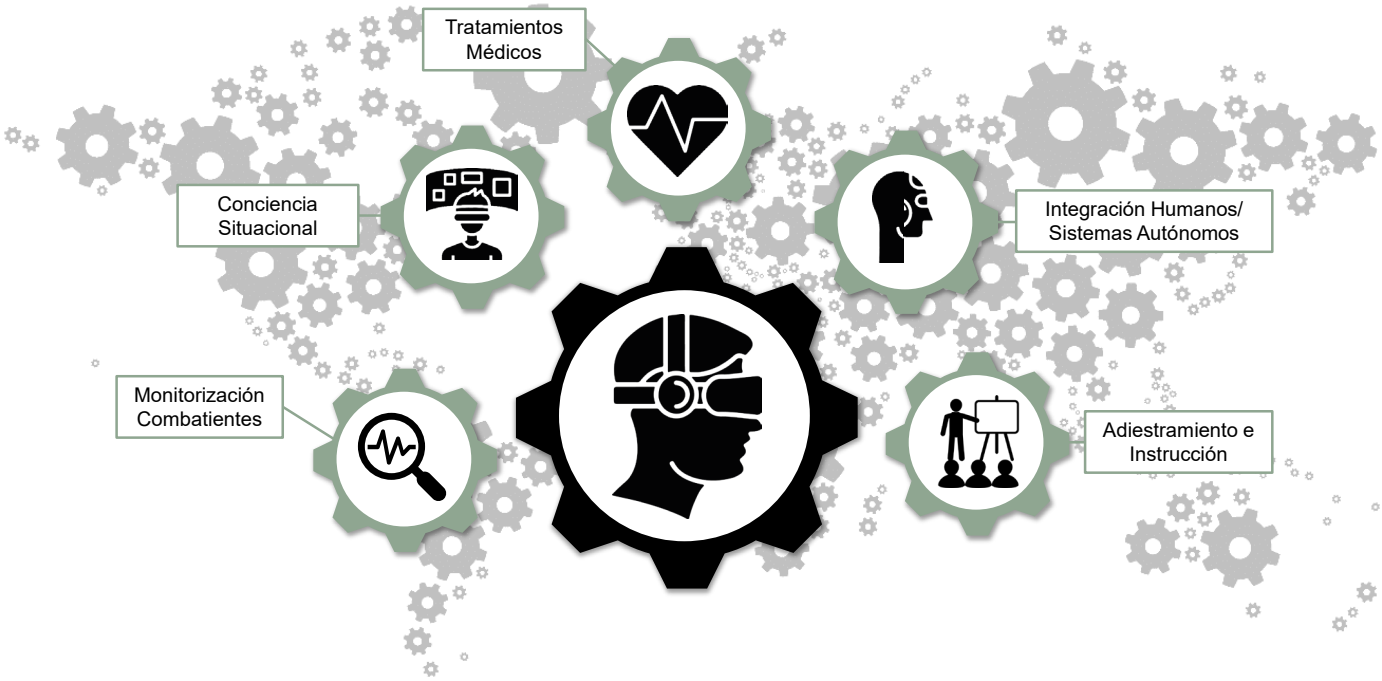


Ilustración 5. Posibles Aplicaciones Militares de la Biotecnología y la Mejora Humana

futuro, las interfaces cerebrales podrían utilizarse no solo para la monitorización, sino también para estimular y mejorar áreas relevantes del cerebro.

Tratamientos médicos. Estas tecnologías permiten la realización in situ de tratamientos médicos que hasta ahora solo eran posibles en instalaciones con capacidades específicas. Las tecnologías relacionadas con la telemedicina, por ejemplo, con la posible ayuda de cirugía asistida por robots, permiten la realización de tratamientos especializados en escalones donde, hasta el momento, no eran posibles. Otras tecnologías como los biomateriales y la fabricación aditiva pueden utilizarse para fabricar órganos artificiales u otros materiales de carácter biológico, como sangre sintética.

2.5.2. Retos Asociados a la Implementación

La aplicación de materiales novedosos y biotecnologías en el ámbito militar plantean algunos desafíos que deben abordarse y resolverse antes de su aplicación generalizada. Estos problemas incluyen las implicaciones legales y morales del uso de la genética, la toxicidad e incompatibilidades fisiológicas de los nanomateriales o aquellos relacionados con la sobrecarga cognitiva y la mejora biológica.

Existen incertidumbres sobre los nanomateriales y su seguridad para la salud y el medio ambiente que están actualmente obstaculizando su desarrollo. Es necesario definir los riesgos y los medios para la implementación de estas tecnologías mediante un enfoque seguro, integrado y responsable.

Por último, además de las dudas éticas y legales, estas tecnologías todavía presentan otros desafíos, especialmente en lo que respecta a la ingeniería de metamateriales, por las limitaciones físicas derivadas de las propiedades mecánicas, térmicas y ambientales aceptables.

2.6. Sistemas de Armas Hipersónicos

El armamento hipersónico supone un elemento multiplicador de las amenazas cinéticas que añade nuevas dificultades a las estrategias de protección y defensa.

Debido a su velocidad, maniobrabilidad y trayectoria, este tipo de armamento supone un desafío en términos de tiempo de detección que modifica radicalmente la concepción de la disuasión y defensa antimisil. Esto implica el desarrollo de nuevas contramedidas y sistemas complejos de detección y alerta temprana multidominio.

2.6.1. Posibles Aplicaciones Militares

Alcanzar objetivos en profundidad. Sin duda, como principal aplicación de este tipo de armamento, se encuentra la capacidad de alcanzar objetivos en profundidad de forma rápida y precisa, reduciendo la capacidad de reacción por parte del adversario. Esto permite tanto alcanzar objetivos de alto valor a grandes distancias, como contrarrestar las medidas de denegación de acceso.

Capacidad nuclear. La incorporación por parte de determinados actores en vectores hipersónicos puede suponer un cambio de paradigma en lo que a disuasión se refiere. Esto conllevaría un replanteamiento de las estrategias nucleares actuales, aumentando la inestabilidad del panorama estratégico.

A pesar de la falta de consenso sobre si suponen un cambio de paradigma o no, lo que sí que parece claro es que para contrarrestarlos se requiere el desarrollo de sistemas de defensa mucho más sofisticados y efectivos, tanto para la protección a nivel táctico como estratégico.

2.6.2. Retos Asociados a la Implementación

La amenaza del armamento hipersónico plantea importantes desafíos que requerirán el desarrollo de sistemas de detección, alerta temprana e interceptación multidominio.

El desafío para detectar esta amenaza con suficiente tiempo y antelación obliga establecer redes de sensores que sean capaces de detectar el propio lanzamiento de los misiles. Para ello, dominios como el espacial, el marítimo o el cibernético tendrán especial relevancia, pero, será sobre todo la interconexión e interoperabilidad de los sistemas de defensa en el multidominio lo que pueda ofrecer una capacidad de respuesta eficaz.

Esto requiere, por un lado, de importantes desarrollos en la arquitectura de sensores espaciales, sistemas no tripulados, radares, etc., pero también de capacidad de procesado en tiempo real de toda la información proporcionada. Así, algoritmos basados en IA o la computación cuántica para fusionar y procesar información lo suficientemente rápido pueden jugar un papel relevante.

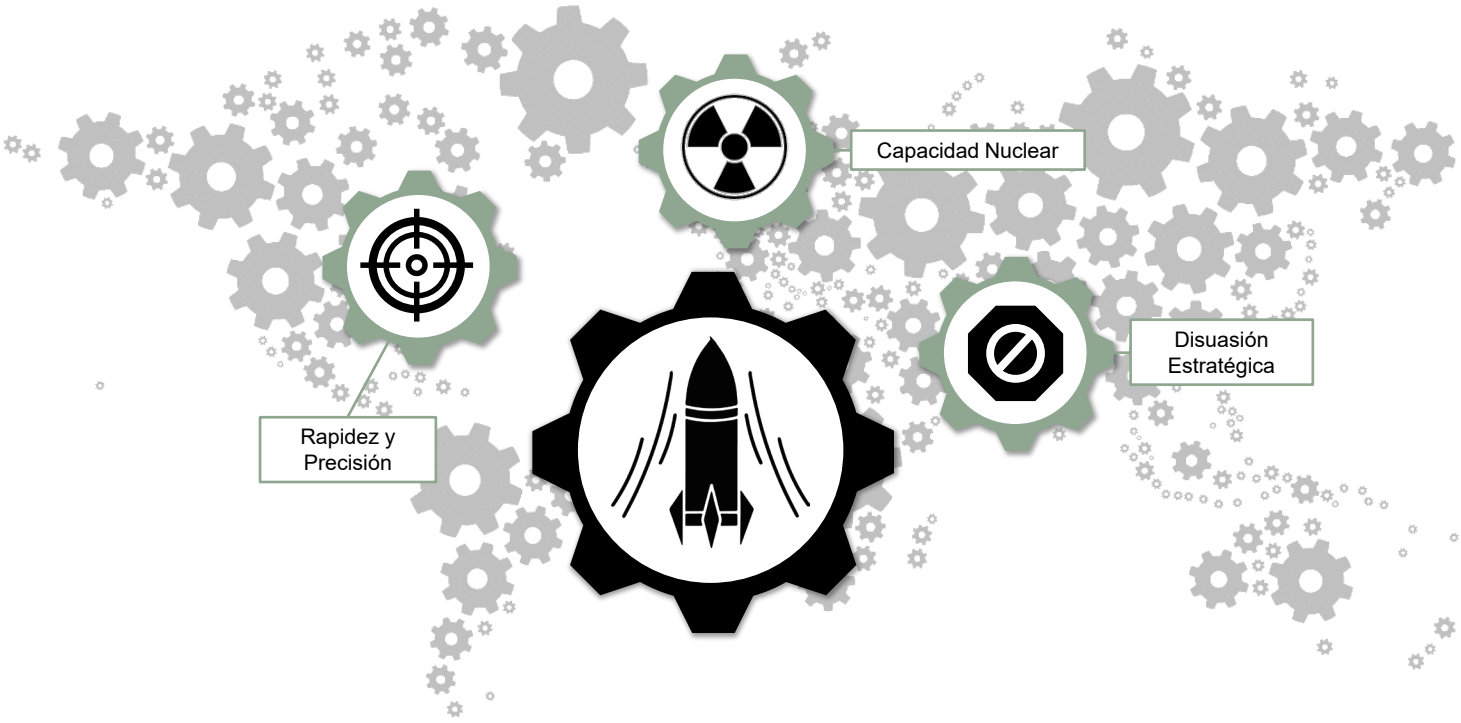


Ilustración 6. Posibles Aplicaciones Militares de los Sistemas de Armas Hipersónicas

Con respecto a la interceptación, se precisan sistemas de defensa que se encuentren más integrados y estratificados que las defensas actuales de misiles balísticos. Por otro lado, los efectores no cinéticos deben también considerarse como una posible solución efectiva, especialmente cuando se afrontan ataques por saturación. Estos pueden incluir sistemas de guerra electrónica, las armas de energía dirigida o de pulsos electromagnéticos.

Por último, hay que mencionar que la gran cobertura geográfica que requerirían los sistemas de defensa antimisiles hipersónicos implica establecer un mayor nivel de cooperación entre las fuerzas aliadas.

2.7. Nuevas Tecnologías Espaciales

A medida que se reducen las barreras tecnológicas y se acotan los costes de producción, puesta en servicio y operación, los servicios espaciales continúan proliferando cada vez con mayor celeridad y con mayor participación de actores estatales, no estatales y comerciales. En particular, la componente comercial del espacio tiene un fuerte potencial de crecimiento con el desarrollo de servicios por parte de entidades comerciales que tradicionalmente venían ofreciéndose por órganos estatales.

Los servicios de comunicaciones y observación de la tierra se están viendo potenciados, ofreciéndose capacidades desde el espacio antes impensables en términos de coberturas, anchos de banda de comunicaciones o resolución de sensores.

El mercado que esto supone lleva a que sean muchas las empresas que están invirtiendo en actividades relacionadas con el diseño y producción de satélites (incluidos nano y micro), puesta en servicio o el desarrollo de servicios específicos. Esto ha llevado a que el espacio pase de ser un dominio copado por entidades estatales, a ser un entorno altamente congestionado en el que son muchos y muy variados los actores que participan.

Este contexto tiene un impacto muy significativo en lo que a capacidades militares se refiere, como capacidad habilitadora por un lado y como entorno en el que es necesario proteger los intereses nacionales por otro.

2.7.1. Posibles Aplicaciones Militares

Como capacidad habilitante, el espacio proporciona una serie de servicios críticos que es necesario garantizar durante las operaciones militares. Tanto los servicios de comunicaciones, como los de observación y sensorización se ven incrementados muy significativamente por el desarrollo de tecnologías espaciales. Disponer de conectividad de gran capacidad, acceso a internet o de imágenes en tiempo real de cualquier parte del mundo supone sin duda una mejora significativa en el desarrollo de las operaciones.

Las comunicaciones por satélite potencian muchas otras capacidades como las de vigilancia, inteligencia, identificación y seguimiento, o mando y control distribuido. Igualmente, facilitan las operaciones en el multidominio, proporcionando cobertura a activos terrestres, navales y aéreos sin depender de infraestructura terrestre.

Con las actividades de observación se ven potenciados los servicios de alerta temprana, análisis de objetivos o de evaluación de amenazas y daños, proporcionando una imagen 24/7 completa y exhaustiva del campo de batalla en tiempo real.

Por otro lado, como consecuencia del aumento del número de actores, el dominio espacial está cada vez más congestionado, hasta el punto de que se ha convertido en un dominio de conflicto potencial en sí mismo.

Existen iniciativas para desplegar sistemas espaciales con capacidad de enfrentamiento tanto sobre la superficie terrestre, como contra otros dispositivos y plataformas espaciales. Igualmente, se contempla la capacidad de interceptar plataformas satelitales desde emplazamientos en la superficie terrestre. Todo ello por no mencionar la generación constante de basura espacial y el riesgo que supone para las plataformas en servicio.

Esto obliga a dotar a los sistemas satelitales de los correspondientes sistemas de protección (incluyendo capacidad de maniobra, auto reparación o lanzamiento rápido de satélites para restituir un servicio), así como al desarrollo de capacidades militares que puedan operar en el dominio espacial y contrarrestar posibles acciones por parte de un potencial adversario.

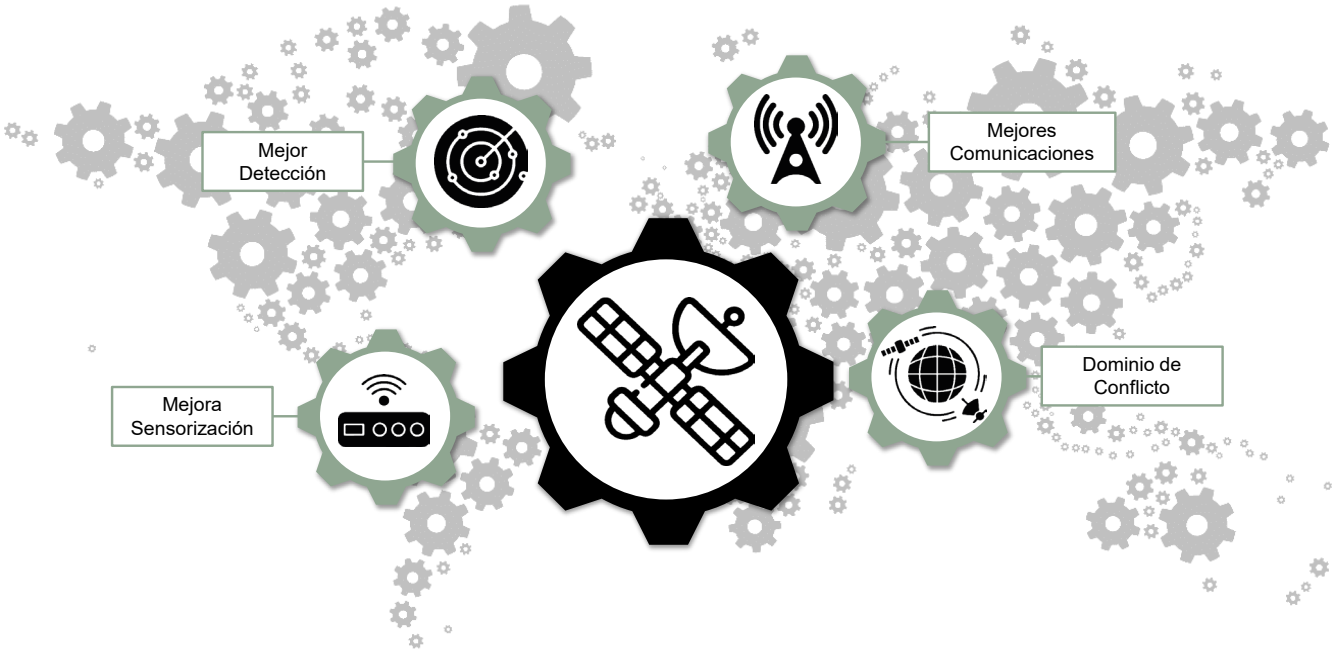


Ilustración 7. Posibles Aplicaciones Militares de Nuevas Tecnologías Espaciales

2.7.2. Retos Asociados a la Implementación

Protección de los sistemas espaciales. Es uno de los principales retos a considerar frente a amenazas tanto intencionadas como accidentales. Las capacidades espaciales son vulnerables tanto a la basura espacial (intencionada o no) como a los ataques, sea desde la superficie terrestre o desde plataformas en vuelo o en órbita.

Más allá de las amenazas cinéticas, los sistemas son también vulnerables a ataques cibernéticos, como la suplantación y el bloqueo o la interferencia electromagnética. Así mismo, también son vulnerables a los fenómenos naturales como tormentas solares.

La protección de estos sistemas requiere dotarles de capacidades de maniobra mejoradas para evitar impactos, de protección electromagnética, cibernética, o incluso el diseño de estrategias que proporcionen la adecuada redundancia al sistema completo, de forma que la pérdida de una plataforma no suponga un impacto significativo en el servicio.

Conciencia situacional del entorno espacial. Más allá de la protección de los sistemas, será necesario disponer de los medios para desarrollar una conciencia situacional estratégica del entorno espacial que permita comprender la posición de cada uno de los actores en el espacio, sus acciones y como afectan al resto de dominios. Esta conciencia situacional debe ser compartida para coordinar operaciones y misiones conjuntas y combinadas, asegurando una perspectiva y una capacidad de respuesta globales.

Hay que destacar el hecho de que mayoritariamente son inversores comerciales y privados los están liderando el desarrollo de las capacidades espaciales. En el ámbito militar deberán aprovecharse los avances surgidos en el sector civil y hacer uso de forma segura y con garantías de los servicios ofrecidos por las entidades privadas.

Marco regulatorio y adaptación de la docrtina. Desde el punto de vista regulatorio, se abre todo un abanico de necesidades relacionadas con los derechos de uso y ocupación del espacio, coordinación de la actividad espacial o la explotación de servicios. En relación con las necesidades militares, es necesario evaluar qué requisitos deben cumplir estas regulaciones para garantizar y asegurar la independencia en el uso de los servicios ofrecidos desde el espacio.

Finalmente, el desarrollo de operaciones en el espacio implica la generación o adaptación de la doctrina para hacer uso de este dominio y explotar plenamente sus beneficios. Esto implicará investigar, desarrollar y comprender el marco legal y regulatorio que rige el uso del espacio y desarrollar nuevos conceptos y estrategias operativas.

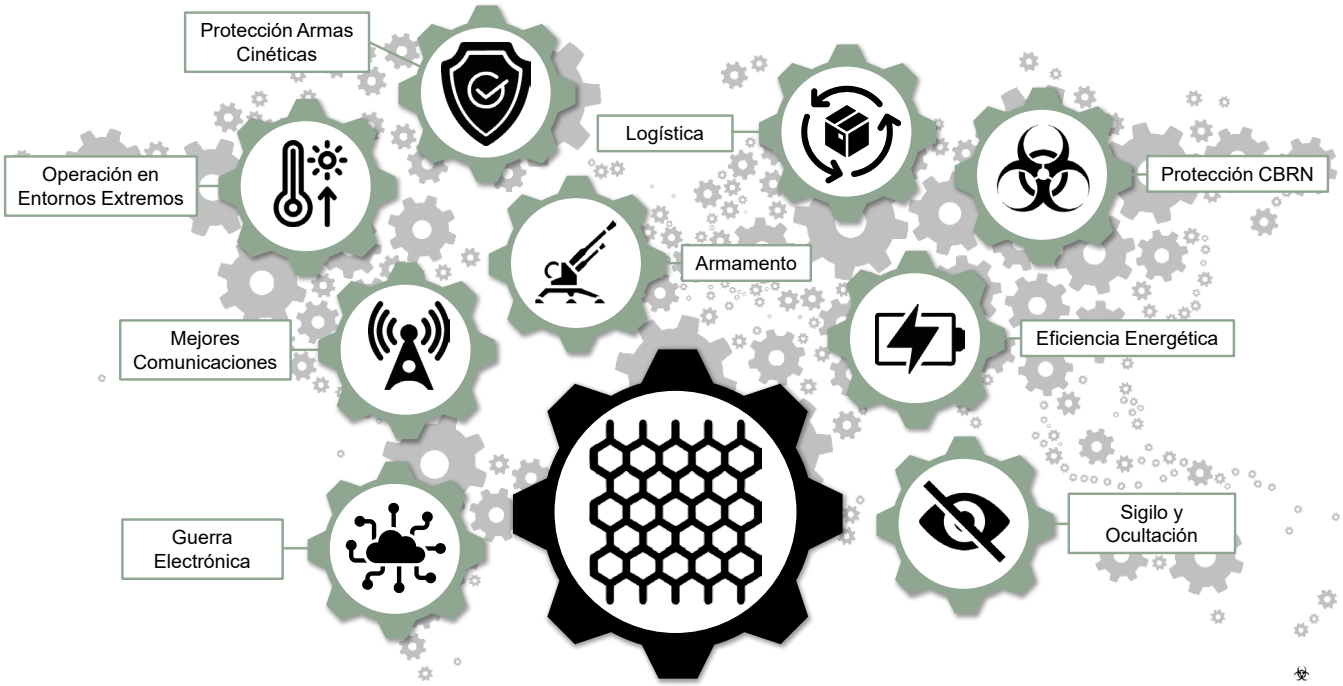


Ilustración 8. Posibles Aplicaciones Militares de Nuevos Materiales Avanzados

2.8. Nuevos Materiales Avanzados

Los avances en nuevos materiales y técnicas de fabricación tienen un efecto significativo en una amplia gama de capacidades militares, pues sus aplicaciones son numerosas. Estos desarrollos incluyen nuevos metales y superaleaciones, técnicas de producción más baratas y de menor consumo energético, fabricación aditiva, materiales estructuralmente reactivos, metamateriales, biología sintética, nanotecnología, diseños furtivos, etc.

2.8.1. Posibles Aplicaciones Militares

Los desarrollos actuales en materia de armamento apuntan al uso de materiales avanzados para el desarrollo de municiones inteligentes, de alta precisión o de hipervelocidad. Los metales, los compuestos, los materiales absorbentes de energía y las partículas de dimensiones nanométricas permiten la fabricación de municiones de alta energía, con la posibilidad de focalizarla en un objetivo reducido. De esta forma, se produce un efecto más efectivo y preciso, evitando daños colaterales. Además, el uso de metamateriales puede reducir el nivel de exposición de la munición, y por tanto su identificación y el seguimiento de su trayectoria.

Con relación a los futuros sistemas C4ISR, el uso de sistemas de comunicaciones basados en metamateriales proporciona capacidades avanzadas de comunicación que permitirán hacer un mejor uso del espectro electromagnético. Las antenas basadas en metamateriales aumentan la potencia de salida, mejoran la direccionalidad y aumentan el rango de frecuencias posibles. Esto, además de mejorar las capacidades de comunicación, es de utilidad en el campo de la guerra electrónica, tanto ofensiva como defensiva.

Otra aplicación de los metamateriales puede consistir en la mejora de las capacidades de los sensores y dispositivos Electro-Ópticos (EO) o Infrarrojos (IR), lo que permitirá una mayor fidelidad para la obtención de información a largas distancias, así como dar cobertura a áreas de mayor extensión. Gracias a una mayor capacidad de detección e identificación, se podrá disponer con mejor conciencia situacional y de tiempo adicional de reacción ante amenazas.

En cuanto a la supervivencia y protección, son diversos los nuevos materiales que proporcionan ocultación o protección ante diferentes amenazas, como las derivadas de agentes CBRN, impactos cinéticos, condiciones climáticas o capacidades de ocultación.

Las amenazas CBRN modernas requieren de métodos avanzados de identificación, protección y descontaminación donde los nuevos materiales juegan un papel relevante. La nanotecnología ofrece grandes oportunidades para el desarrollo de sensores en miniatura capaces de detectar partículas peligrosas con un consumo de energía mínimo. Del mismo modo, otras tecnologías como las superficies auto descontaminantes proporcionan una protección activa adicional contra estas amenazas.

Por otra parte, los nanomateriales, compuestos avanzados o metamateriales, proporcionan propiedades mecánicas únicas que se pueden usar para brindar mejor protección y resistencia contra armas cinéticas u otros impactos. Estos resultan de utilidad en componentes blindados para vehículos, estructuras o equipos personales.

Así mismo, la capacidad de vehículos y personal para operar en entornos extremos, incluidos bajo el agua o el espacio exterior, se ve potenciada por el uso de nuevos materiales. Estos permitirán el desarrollo de componentes y equipos más duraderos, como revestimientos y vestimenta inteligente, siendo menos vulnerables a temperaturas extremas, presiones, fenómenos atmosféricos, etc.

Los metamateriales, los materiales de baja observabilidad o aquellos con capacidad de blindaje electromagnético, entre otros, ofrecen una reducción significativa de las firmas visibles, infrarrojas, de radar e incluso acústicas. Esto dará lugar a una amplia gama de equipos, sistemas, plataformas o vestimenta con altas capacidades de discreción y ocultación.

Otra aplicación de nuevos materiales se refiere a los avances en el desarrollo de baterías y otras soluciones energéticas de alta eficiencia como células de combustible o supercondensadores. El desarrollo de baterías más ligeras, pequeñas, eficientes y con mayor capacidad, permite el uso extensivo de plataformas eléctricas e híbridas, como sistemas autónomos, bases autosuficientes, armas de energía dirigida, dispositivos portátiles, sistemas C4I, etc.

Por último, en el área de la logística en operaciones, la fabricación aditiva tiene el potencial de cambiar los procedimientos de mantenimiento y las cadenas de suministro. Con la suficiente madurez, esta tecnología podría permitir la producción descentralizada de partes y componentes, incluyendo repuestos para vehículos y sistemas, armas y municiones, e incluso suministros médicos.

No obstante, aún está por determinar cómo estos nuevos materiales avanzados y técnicas de fabricación podrían reducir los costes de sostenimiento de la fuerza en zona de operaciones. También debe considerarse que es poco probable que el volumen de suministros se reduzca, ya que las materias primas aún necesitarían ser transportadas al teatro de operaciones, si bien su disponibilidad sería mayor y su transporte más sencillo.

2.8.2. Retos Asociados a la Implementación

La aplicación de materiales inteligentes al dominio militar presenta algunos desafíos que deben abordarse y resolverse antes de su aplicación generalizada.

Por una parte, el desarrollo de la fabricación aditiva y la utilización de nuevos materiales avanzados pueden tener profundas implicaciones en la seguridad. Su uso extensivo puede acelerar significativamente la proliferación de armas, afectando de forma generalizada a la estabilidad. Esto puede requerir el establecimiento de nuevas medidas preventivas y marcos de regulación para evitar que civiles y actores no estatales no autorizados accedan a las tecnologías de fabricación de armas.

Resulta imprescindible una adecuada evaluación del grado de madurez de las tecnologías en este campo, pues muchas de ellas se encuentran aún en estadios tempranos de desarrollo, y su aplicación efectiva no se espera en el corto y medio plazo.

Con respecto a la fabricación aditiva, es importante destacar el desafío relacionado con la propiedad intelectual. Disponer de la capacidad de fabricar en el campo de batalla las piezas y componentes necesarios implica disponer de los diseños e información de detalle de estos. Es necesario asegurar una política de derechos de propiedad intelectual que garantice el uso de estas técnicas sin consecuencias legales o de apropiación indebida por parte de terceros.

2.9. "Blockchain"

La tecnología de Blockchain proporciona una forma segura y confiable de registrar cualquier tipo de información de forma descentralizada. Su principal característica es la creación de registros digitales inmutables que pueden ser utilizados en una amplia variedad de aplicaciones, entre ellas, el registro de transacciones, contratos o gestión de cadenas de suministro asegurando la integridad y privacidad de los datos.

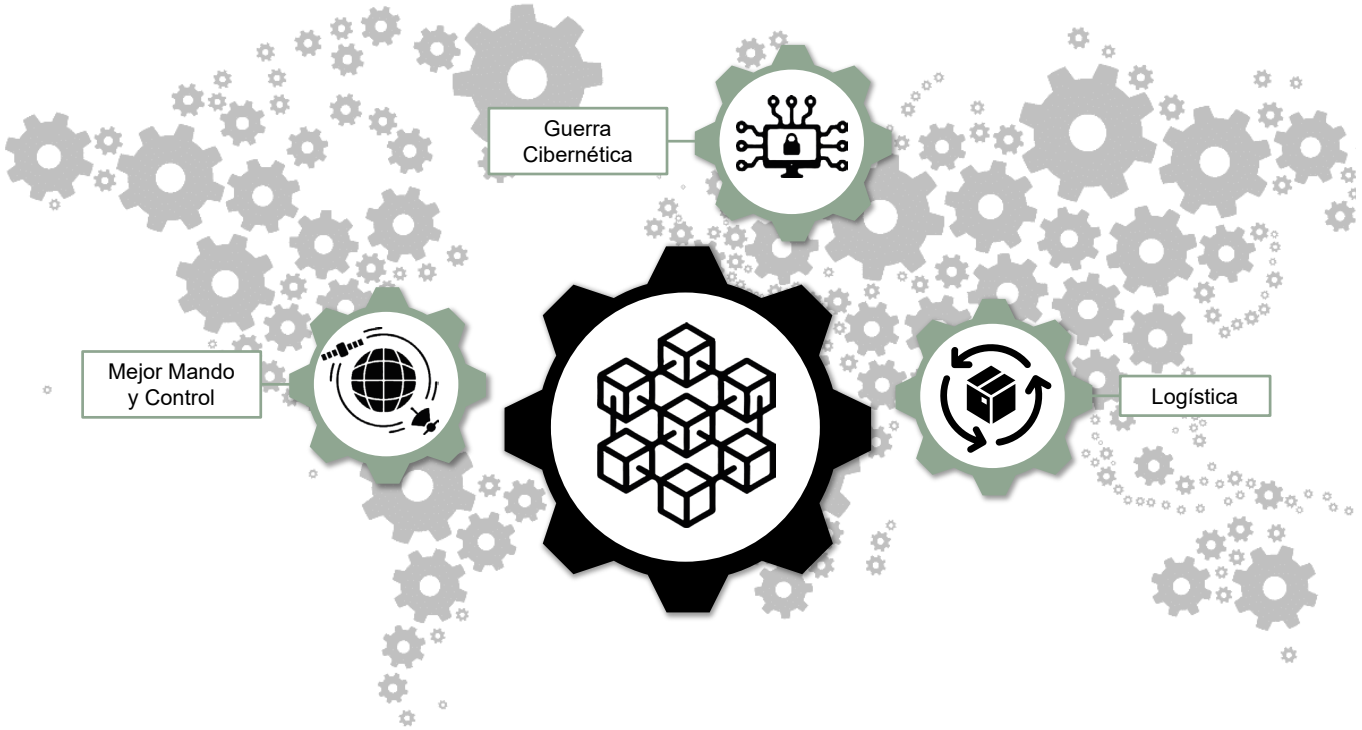


Ilustración 9. Posibles Aplicaciones Militares del Blockchain

Desde el punto de vista militar, sus aplicaciones afectan a prácticamente todas las capacidades, destacando el mando y control al garantizar la autenticidad de la información a lo largo de toda la cadena de mando, o la logística al permitir una mejor gestión de las cadenas de suministro.

2.9.1. Posibles Aplicaciones Militares

Desde el punto de vista del mando y control, Blockchain permite al mando garantizar la autenticidad de información, así como asegurar la adecuada transmisión de las órdenes. Como principales ventajas, Blockchain permite ejecutar el ciclo de decisión de forma más precisa, ágil y con mayores niveles de automatización.

En cuanto a la ciberdefensa, Blockchain añade una capa adicional de seguridad al permitir la autenticación y validación de los datos almacenados en tiempo real. El modelo descentralizado de Blockchain dificulta cualquier manipulación de los datos o, en cualquier caso, permite hacer patente cualquier manipulación.

El campo de la logística puede beneficiarse de Blockchain de forma significativa, con un impacto claro en la eficiencia y seguridad de las cadenas de suministro. Por sus características, Blockchain puede convertirse en una herramienta integral en la cadena de valor logística, aumentando la visibilidad en toda la red de proveedores, garantizando el origen de piezas y repuestos o facilitando la localización. Asimismo, facilita la identificación de las personas involucradas en todo el proceso, así como la certificación de piezas y componentes. Todo ello facilita enormemente el intercambio de componentes o personal especializado entre organizaciones o Fuerzas Armadas de diferentes países.

2.9.2. Retos Asociados a la Implementación

La implementación de las tecnologías asociadas al Blockchain se enfrenta a diferentes desafíos, como la escalabilidad, el consumo energético o la falta de regulación.

Con respecto a la escalabilidad, cabe destacar que Blockchain tiene ciertas limitaciones en cuanto a los recursos de computación y almacenamiento que precisa según se van acumulando registros y transacciones. Sin duda, este es un reto tecnológico que deberá abordarse desde el punto de vista militar antes de cualquier implementación concreta.

El consumo energético es actualmente un factor a tener en cuenta, siendo necesario trabajar en el desarrollo de soluciones más sostenibles y eficientes.

A su vez, dentro del sector de Defensa, es necesario evaluar el impacto que tiene en la doctrina y procedimientos y establecer políticas y directrices adecuadas para su implementación y uso.

A lo largo de los capítulos siguientes analizaremos, no de forma exhaustiva, cómo las tecnologías descritas afectan a las capacidades militares en los diferentes dominios. Por esto, nos referiremos a ellas genéricamente como tecnologías, sin entrar en una clasificación, que pudiera resultar artificial, entre emergentes y disruptivas o no.

3. OPERACIONES MULTIDOMINIO (MDO)

Si bien aún no se ha consensuado una definición específica en los marcos doctrinales nacionales, OTAN o en las FAS de países de referencia para el término “dominio”, podemos entender que se refiere a los espacios físicos y no físicos de una operación. Así, a los dominios tradicionales aéreo, marítimo y terrestre, se le ha unido recientemente el dominio espacial, ciberespacial y cognitivo.

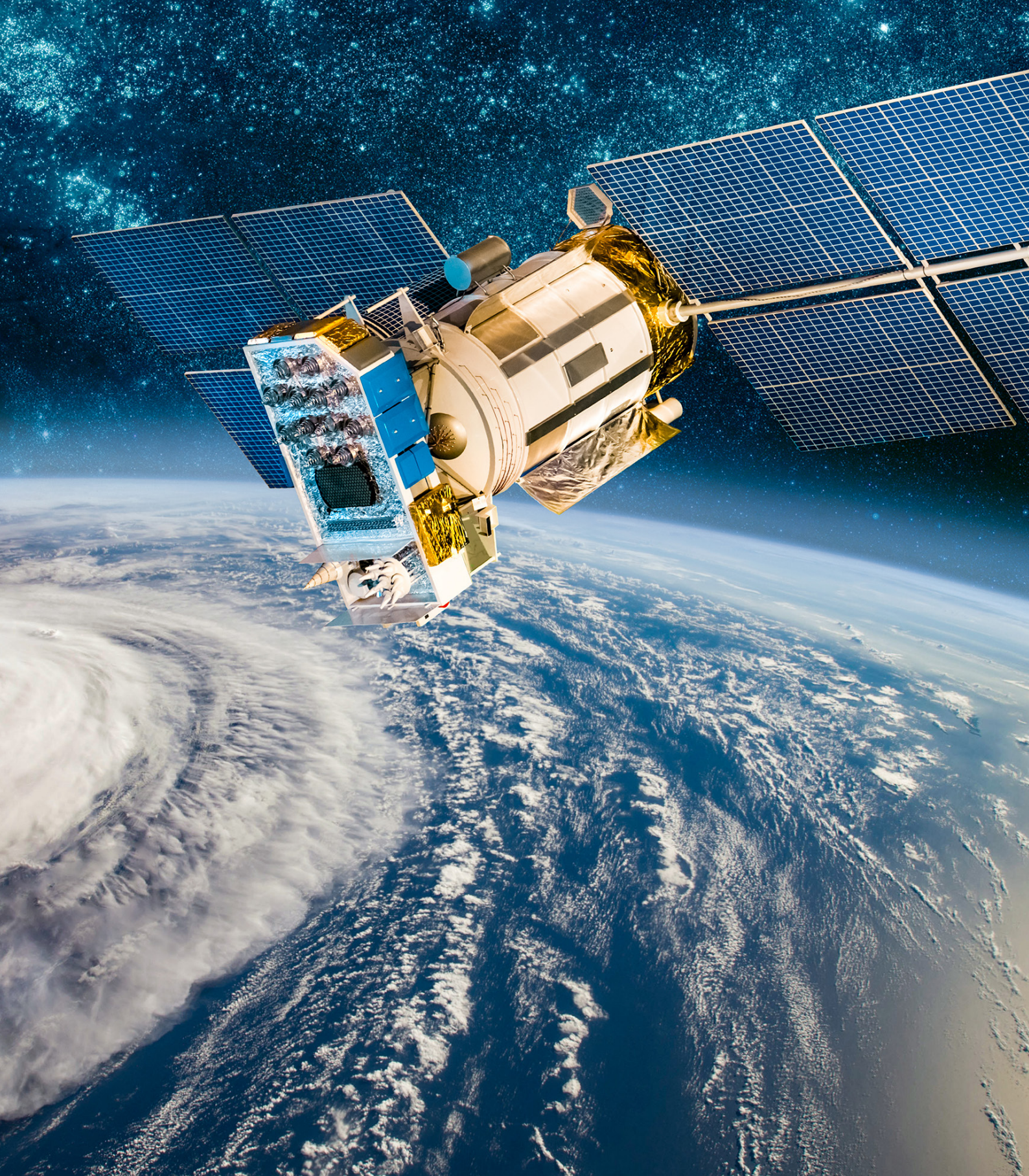
En consecuencia, las operaciones multidominio se caracterizarían por la capacidad de operar en diversos dominios de forma simultánea, con una coordinación y control distribuidos, y de manera ágil y rápida a través de los mismos.

El fuerte desarrollo tecnológico actual provoca que las fronteras entre dominios se vuelvan tan difusas que afecten, no solo al empleo de los sistemas de armas como tales, sino también a la forma en que se llevan a cabo las operaciones, o a las estructuras y doctrinas militares vigentes.

Las mejoras en alcance y precisión de los sistemas y del armamento han posibilitado acciones más eficientes entre tierra, aire y mar, a la vez que las tecnologías de comunicaciones avanzadas han permitido “romper” los ciclos de decisión y distribuirlos entre varios dominios, contando con sensores, mando y control y efectores distribuidos.

En referencia a los nuevos dominios, cabe destacar como desde el dominio cibernético, es posible hacer uso de métodos asimétricos para afectar y dañar servicios críticos a través de herramientas fácilmente accesibles, de bajo coste y en general, difíciles de rastrear. No puede descartarse que este dominio traiga consigo un nuevo tipo de conflicto en el que operadores y ordenadores se enfrenten para limitar o eliminar los servicios esenciales del adversario, condicionando seriamente las actuaciones en otros dominios.

Por último, se debe considerar la importancia que está tomando el dominio cognitivo de forma global y desde el punto de vista de las operaciones militares. Sin duda se trata de un campo que siempre ha tenido influencia en las operaciones militares, pero la accesibilidad actual del ciberespacio y la proliferación de tecnologías de comunicación, incluidas las redes sociales digitales, ofrecen una nueva dimensión que es necesario tener en cuenta.



BIOGRAFÍAS

J. DANIEL GONZÁLEZ GALDO

Licenciado en Química Industrial por la Universidad Complutense de Madrid, Master en Seguridad Internacional por la Universidad de la Rioja y MBA por la Escuela de Organización Industrial.

Tiene 24 años de experiencia en el ámbito de Defensa. Actualmente es Jefe del Área de Planeamiento en Isdefe cuya misión es la de dar apoyo a clientes, tanto nacionales como internacionales, en el planeamiento de capacidades de Defensa y Seguridad. Entre sus actividades se incluyen el desarrollo y aplicación de metodologías para la identificación y caracterización de amenazas, definición de escenarios de conflicto, análisis de riesgos o desarrollo de capacidades.

Previamente desarrolló su carrera profesional durante más de 10 años en el ámbito de las TIC, particularmente en la asistencia técnica para el seguimiento y control de programas de Mando y Control y Comunicaciones de Defensa.

ALFREDO PEÑA RUIZ

Ingeniero de Telecomunicaciones por la Universidad de Alcalá de Henares y cuenta con 17 años de experiencia en el ámbito de la Defensa y Seguridad.

Actualmente ocupa el cargo de Coordinador en el Área de Planeamiento y Seguridad prestando asistencia técnica en Estado Mayor Conjunto del Estado Mayor de la Defensa.

Entre sus actividades se encuentran la aplicación de metodologías y herramientas de apoyo para el planeamiento, tanto en el ámbito nacional como el europeo y el asociado al desarrollo de capacidades militares en el marco de las OISD.

Gran parte de su conocimiento del planeamiento de capacidades europeas ha sido adquirido gracias a los trabajos desarrollados para la Agencia Europea de Defensa durante los últimos 10 años.

Con anterioridad ha participado en el seguimiento de las iniciativas en materia de defensa europeas, el estudio y análisis de las capacidades industriales y tecnológicas de la industria de defensa nacional, así como en el desarrollo de capacidades de I+D del Ministerio de Defensa.

CAPÍTULO 2

Planeamiento de Capacidades Europeo

Begoña Rojo Carralero

Europa enfrenta cambios significativos en su contexto internacional, con un aumento de amenazas como ciberataques y amenazas híbridas, que combinan tácticas de guerra tradicionales y modernas. Esta nueva situación requiere cambios en las capacidades militares, con un enfoque en la investigación, desarrollo y adquisición de nuevas tecnologías, todo a un costo elevado. Para abordar estas amenazas compartidas, se necesitan respuestas coordinadas y estrategias de defensa conjuntas entre países europeos y aliados, asegurando la interoperabilidad de las fuerzas.

La cooperación entre países europeos es esencial para fortalecer la soberanía y autonomía estratégica de la Unión Europea en defensa. Para ello, es crucial contar con una industria de defensa europea fuerte y competitiva, clave para la implementación de la Política Común de Seguridad y Defensa (PCSD). La Estrategia Global para la Política Exterior y de Seguridad de la UE, aprobada en 2016, impulsó diversas iniciativas para avanzar hacia una Europa de la Defensa. Entre estas se encuentran el Plan de Acción Europeo de la Defensa (EDAP), la Cooperación Estructurada Permanente (PESCO), y la Revisión Anual Coordinada de la Defensa (CARD).

Adicionalmente, la Brújula Estratégica, aprobada en marzo de 2022, y el Plan de Desarrollo de Capacidades (CDP) de la Agencia Europea de Defensa (EDA), son instrumentos clave para establecer prioridades en el desarrollo de capacidades y fomentar la cooperación europea en defensa. Durante el primer semestre de 2022, la Comisión Europea presentó medidas para fortalecer la industria europea de defensa, con énfasis en adquisiciones y programación conjuntas. En España, la Estrategia de Seguridad Nacional 2021 y la Directiva de Defensa Nacional 2020 incluyen entre sus objetivos reforzar la base tecnológica e industrial de defensa, permitiendo mantener un alto nivel tecnológico en las capacidades operativas de las Fuerzas Armadas, en sintonía con las directrices europeas.

1. ORÍGENES DE LA POLÍTICA DE SEGURIDAD Y DEFENSA EN EUROPA

Los orígenes de la arquitectura europea de seguridad y defensa se remontan a los años posteriores a la Segunda Guerra Mundial. A partir de finales de la década de los cuarenta, varias iniciativas facilitaron una mayor cooperación en toda Europa como, por ejemplo, la firma del Tratado de Bruselas en 1948, que sembró las semillas de la Unión Europea tal y como la conocemos en la actualidad, y la creación de la Comunidad Europea del Carbón y del Acero en 1951, que puso recursos estratégicos para Europa bajo una autoridad supranacional.

A finales de los años sesenta, la Comunidad Europea comenzó a explorar diferentes formas de armonizar las políticas de sus miembros. De este modo, en la Cumbre de La Haya, celebrada en diciembre de 1969, los líderes europeos encargaron a sus Ministros de Asuntos Exteriores que analizaran la viabilidad de alcanzar una mayor integración en el ámbito político.

En respuesta a esta petición, se creó el concepto de Cooperación Política Europea (CPE) en el que se definían sus objetivos, incluyendo la armonización de las posiciones en algunos aspectos de política exterior, procedimientos consultivos y, en su caso acciones comunes. El CPE sirvió de base para la Política de Seguridad Común introducida en el Tratado de Maastricht. Con su entrada en vigor en el 1993, este Tratado creó un marco institucional único en la Unión Europea, basado en tres pilares, el segundo de los cuales era la Política Exterior y de Seguridad Común (PESC).

La PESC incluye por primera vez "todas las cuestiones relacionadas con la seguridad de la Unión, incluida la posible elaboración de una política de defensa común, que podría conducir a una defensa común".

Sin embargo, desde el tratado de Maastricht, no fue hasta finales de los años noventa (tras la guerra de los Balcanes y un paso al frente de Reino Unido) hasta que se crearon disposiciones concretas para una Política Europea de Seguridad y Defensa (PESD) común dotada de capacidades tangibles para la gestión de crisis.

A finales de los noventa, a través de numerosas cumbres del Consejo Europeo, se definieron las capacidades militares y civiles necesarias para cumplir con las conocidas como "misiones de Petersberg", que comprenden tareas humanitarias y de rescate, así como tareas de mantenimiento e imposición de la paz, incluyendo estas últimas acciones de combate en la gestión de crisis correspondiente.

Desde que en el año 2003 la PESD entró en funcionamiento, la Unión Europea ha llevado a cabo más de treinta y cinco misiones y operaciones de crisis. Además, la Unión Europea presentó su primera Estrategia Europea de Seguridad en diciembre de 2003, en la que se describen las principales amenazas y desafíos a los que Europa se enfrentaba en ese momento.

Con la entrada en vigor del Tratado de Lisboa, el 1 de diciembre de 2009, la PESD pasó a denominarse Política Común de Seguridad y Defensa (PCSD). La PCSD ofrece un marco para la Unión Europea en el ámbito de la defensa y la gestión de crisis, incluidas la cooperación y la coordinación en materia de defensa entre los países miembro. Como parte integrante de la PESC, la PCSD ha dado origen a estructuras políticas y militares internas de la Unión Europea, lo que ha permitido abordar misiones y operaciones militares y civiles en el extranjero.

El Tratado de Lisboa aprobó formalmente la ampliación de las "misiones Petersberg", que a partir de ese momento incluirían operaciones conjuntas de desarme, tareas humanitarias y de rescate, tareas de asesoramiento y asistencia militar, tareas de prevención de conflictos y mantenimiento de la paz, tareas de las fuerzas de combate en la gestión de crisis, incluyendo el establecimiento de la paz y la estabilización posterior al conflicto. Además, estas misiones pueden contribuir a la lucha contra el terrorismo, incluso apoyando a terceros estados en la lucha contra el terrorismo en sus territorios.

2. LA ESTRATEGIA GLOBAL DE LA UNIÓN EUROPEA Y LAS INICIATIVAS ASOCIADAS EN EL ÁMBITO DE DEFENSA

La actual Estrategia Global para la Política Exterior y de Seguridad de la Unión Europea (EUGS) se elaboró entre los años 2013 y 2016, siendo finalmente presentada ante el Consejo Europeo en junio de 2016. Manteniéndose vigente hasta ese momento la Estrategia de Seguridad de 2003.

La intención de la EUGS es dar protección a los intereses vitales de la Unión, avanzando a través de cinco prioridades estratégicas:

1 La seguridad de la Unión,

2 la resiliencia estatal y social en el este y en el sur,

3 una aproximación integrada a las crisis y los conflictos,

4 unos órdenes regionales cooperativos,

5 y una gobernanza global para el siglo XXI.

Estas prioridades constituyen el eje central de la EUGS, identificándose para cada una de ellas diferentes ámbitos de actuación, no solo exclusivos del ámbito de la defensa, sino otros como la energía, alimentación, relaciones internacionales con otras regiones como África, Asia, Latinoamérica y países del Caribe, el Ártico, países al Este de Europa, así como con países como Estados Unidos, Rusia, China, etc.

Los aspectos de seguridad y defensa son un ámbito específico dentro de la prioridad denominada "seguridad de la Unión", que cuenta con otros cuatro ámbitos: el contraterrorismo, la ciberseguridad, la seguridad energética, y la comunicación estratégica.

Uno de los lemas de la Estrategia, es *From Vision to Action*, por ello pone en marcha diversos Planes de Implementación – o de acción - concretos que permita continuar con el desarrollo de las distintas políticas de la UE, entre ellas la PCSD.

Con este nuevo impulso, el Consejo de la Unión proporcionó la orientación necesaria para avanzar en la Defensa Europea, abarcando ámbitos como la MPCC, PESCO, CARD, EDAP, el Fondo Europeo de Defensa (EDF), el Fondo Europeo para la Paz (EPF) o la movilidad militar y la cooperación UE-OTAN.

De las iniciativas de defensa y seguridad enumeradas el EDF representa una innovación particular. Por primera vez, permite utilizar una dotación presupuestaria dentro del marco financiero plurianual 2021-2027 de la Unión Europea para financiar las actividades relacionadas con la innovación, la investigación y desarrollo en el sector de la defensa europea. Por ello, la Comisión Europea creó en enero de 2020 una nueva Dirección General de Industria de Defensa y Espacio (DG DEFIS) a partir de la anterior Dirección General de Mercado Interior, Industria, Emprendimiento y PYME (DG GROW), para la gestión e impulso del EDF.

Así mismo, basándose en la EUGS, en 2020 también se presentó una nueva iniciativa para desarrollar una Brújula Estratégica de la Unión Europea, cuyo objetivo sería proporcionar una orientación co-militar para la seguridad y la defensa de la Unión Europea. Dicha Brújula Estratégica se presentó en 2022 bajo el lema:

> *"Por una Unión Europea que proteja a sus ciudadanos, defienda sus valores e intereses y contribuya a la paz y la seguridad internacionales"*

Ésta incluye un análisis común de las amenazas para los países de la Unión Europea y los desafíos a los que se enfrentan, además de fijar objetivos precisos para su desarrollo.

Más conocido como el *Strategic Compass*, este documento tiene como finalidad reforzar y orientar la aplicación concreta del nivel de ambición (LoA) de la UE , ofreciendo una evaluación común de nuestro entorno estratégico (retos y amenazas) garantizando que las diferentes iniciativas puestas en marcha tengan el impacto deseado, estableciendo objetivos más específicos y actualizados a la luz de la evolución del entorno de seguridad, y estableciendo etapas claras para medir los avances alcanzados.

El *Strategic Compass* proporciona guía política y objetivos específicos en cuatro líneas de trabajo a alcanzar entre 2022-2030:

- **ACTUAR** en la gestión de crisis, misiones y operaciones, estructuras de mando y control, capacidad de despliegue rápido.
- **SEGURIDAD** mejorar la resiliencia, inteligencia, política de ciberdefensa, estrategia espacial, etc.
- **INVERTIR** incremento del gasto, desarrollo de capacidades y la cooperación en materia de defensa, crear un centro de innovación en defensa.
- **TRABAJAR ASOCIATIVAMENTE** en el desarrollo de asociaciones estratégicas: OTAN, Naciones Unidas, y bilateralmente.

El 15 de febrero de 2022, la Comisión Europea aprobó dos comunicaciones que contribuyen a alcanzar los objetivos establecidos en el *Strategic Compass*.

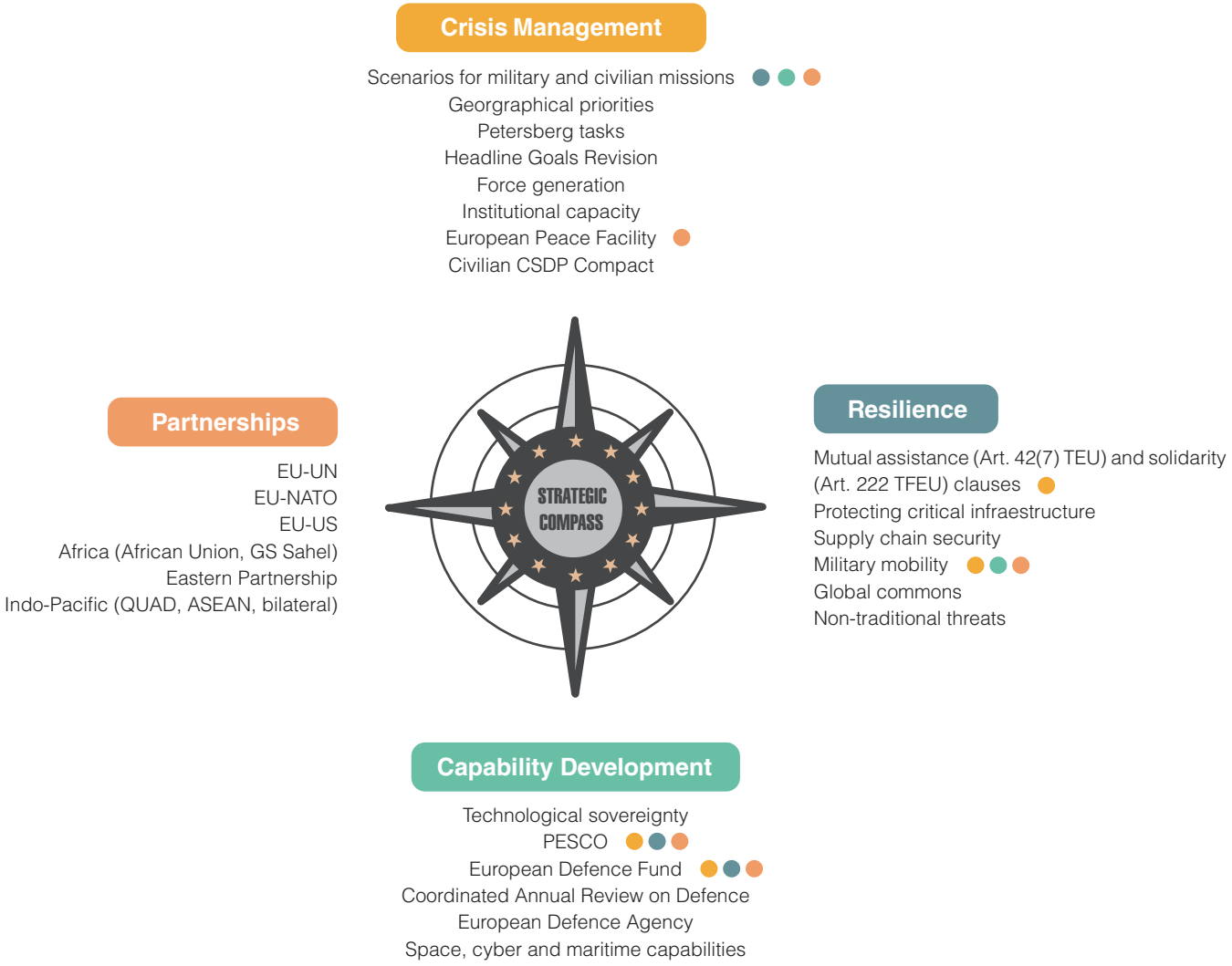


Figura 1. Esquema ámbitos Strategic Compass. (Fuente CE).

En la primera de las comunicaciones se identifican algunas medidas a tomar para fortalecer la competitividad del mercado europeo de defensa (ej. exenciones de IVA, reducción controles exportación armas y aumento de bonificaciones en EDF) y la resiliencia europea (ej. inversiones en espacio, contrarrestar amenazas híbridas, etc.). La segunda, establece una hoja de ruta en innovación y tecnología (ej. identificar tecnologías críticas, potenciar sinergias I+D+i civil y de defensa, mitigar las dependencias estratégicas de fuentes externas y coordinar las acciones con EEUU y OTAN).

ACTORES EN EL PLANEAMIENTO DE CAPACIDADES EUROPEO

Las instituciones europeas reguladas en el artículo 13 del Tratado de la Unión Europea (TUE) son el Parlamento Europeo, el Consejo Europeo, el Consejo de la Unión Europea, la Comisión Europea, La EDA, el Tribunal de Justicia de la Unión Europea, el Banco Central Europeo y el Tribunal de Cuentas.

El Parlamento Europeo, el Consejo y la Comisión están asistidos por un Comité Económico y Social, así como por un Comité de las Regiones que ejercen funciones consultivas.

Se describen a continuación las que intervienen principalmente en materia de Seguridad y Defensa, que son el Consejo de la Unión Europea, la Comisión y la EDA, incluyendo también el Consejo Europeo con objeto de distinguirlo del Consejo de la Unión Europea.

Consejo Europeo

Es la institución de la Unión Europea que define las guías y prioridades políticas generales de la Unión Europea. Creado por el Tratado de Maastricht -aunque venía funcionando informalmente-, no adquiere su carácter de institución de la Unión Europea hasta el Tratado de Lisboa de 2009. El Consejo Europeo está integrado por los Jefes de Estado o Gobierno de todos los países de la Unión Europea.

También asume la representación exterior de la Unión Europea en asuntos relacionados con la PESC. El Consejo Europeo celebra cumbres trimestrales en las que los líderes de la Unión Europea marcan las grandes líneas de las políticas europeas.

Consejo de la Unión Europea

El Consejo es un órgano decisorio esencial de la Unión Europea, en la mayoría de los casos junto con el Parlamento Europeo por el procedimiento de codecisión. También denominado de manera informal 'El Consejo', es el principal centro de decisión política y legislativa. Se encarga de negociar y adoptar la legislación de la Unión Europea junto con el Parlamento Europeo.

Está formado por los ministros de los gobiernos de cada país y se encarga de representar a los gobiernos de los Estados Miembros, adoptar la legislación europea y coordinar las políticas de la Unión Europea. Adopta formaciones de los diferentes ministros de cada país de la Unión Europea, en función del tema que se vaya a tratar.

Entre sus funciones se encuentra la de desarrollar la PESC de acuerdo al Consejo Europeo. Además, celebra acuerdos internacionales relativos a diversas materias y adopta el presupuesto de la Unión Europea. Cada país de la Unión Europea ejerce la Presidencia por turnos de seis meses.

En el segundo semestre del 2023, lo desempeñó España, tras haber relevado a Suecia que lo ejerció durante el primer semestre del mismo año.

La Comisión Europea

El mandato de la Comisión Europea, establecido en el Tratado de la Unión Europea, es promover el interés general de la Unión Europea y adoptar las iniciativas adecuadas con este fin. Así mismo, se encarga de velar por que se apliquen los Tratados y las medidas adoptadas por las instituciones en virtud de éstos, ejecutar el presupuesto y gestionar los diferentes programas, y ejercer funciones de coordinación, ejecución y gestión, de conformidad con las condiciones establecidas en los Tratados.

La Comisión Europea está dirigida por un grupo de 27 comisarios, denominado "el Colegio de Comisarios", y entre todos se encargan de marcar las prioridades políticas y estratégicas de la Comisión. Se encuentra organizada en departamentos, conocidos como "Direcciones Generales", y cada cinco años se nombra un nuevo "Colegio de Comisarios".

El Consejo Europeo nombra al Alto representante de la Unión para Asuntos Exteriores y Política de Seguridad por mayoría cualificada y de común acuerdo con el Presidente de la Comisión para un mandato de cinco años. El Alto representante de la Unión para Asuntos Exteriores y Política de Seguridad es a la vez el Vicepresidente de la Comisión Europea (HR/VP), ejercido por el español Josep Borrell en el periodo comprendido entre los años 2019 al 2024.

La Agencia Europea de Defensa

Creada en 2004, la Agencia Europea de Defensa (EDA) ayuda a los Estados Miembros a mejorar y desarrollar de forma colaborativa y conjunta sus capacidades militares y de defensa. Su experiencia y sus grupos de trabajo con expertos (Equipos de Proyectos y Grupos Tecnológicos de Capacidad) le permiten cubrir un amplio espectro de actividades del ámbito de la defensa, entre las que se destacan la armonización de los requisitos y necesidades para la consecución de capacidades operativas, la investigación e innovación para el desarrollo de demostradores tecnológicos, la gestión de proyectos y la formación y adiestramiento a través de ejercicios en apoyo de las operaciones de PCSD.

La EDA trabaja también para fortalecer la industria de la defensa europea y actúa como facilitador e intermediario entre las partes interesadas del ámbito militar de los Estados Miembros y las políticas de la UE que inciden en la defensa La EDA, como agencia intergubernamental del Consejo de la UE y cuyo consejo de dirección está formado por los Ministerios de Defensa de los 27 Estados miembros, desempeña un papel esencial al facilitar el desarrollo de las capacidades de las Fuerzas Armadas en Europa que sustentan la PCSD de la UE, estando recogidas su misión y cometidos en el propio Tratado de Lisboa.

El Parlamento Europeo

El Parlamento Europeo ejerce la función legislativa y la función presupuestaria, además de ejercer funciones de control político y de representación de los ciudadanos. Es elegido por un periodo renovable de dos años y medio, equivalente a la mitad de la legislatura y está formado por:

- 1 presidencia.
- 705 eurodiputados, elegidos de forma directa.
- 7 grupos políticos. Los diputados componen estos grupos políticos, que no se organizan por nacionalidades, sino por afinidades políticas.
- 26 comisiones. Los diputados trabajan en comisiones para preparar las actividades de las sesiones plenarias del Parlamento Europeo.

3. INICIATIVAS EUROPEAS EN MATERIA DE DEFENSA

3.1. El Plan de Acción Europeo de la Defensa (EDAP)

El Plan de Acción Europeo de la Defensa es una iniciativa puesta en marcha por la Comisión Europea en noviembre de 2016 con el objetivo principal de promover una Base Europea Tecnológica e Industrial de la Defensa (EDTIB) sólida y competitiva. Se materializa en distintos paquetes de medidas encaminadas a fomentar las inversiones y reforzar el mercado único de defensa.

Este plan se fundamenta en tres pilares, junto con la implantación de nuevas políticas de la Unión Europea más amplias:

- Fondo Europeo de Defensa (EDF).
- Fomento de las inversiones en las cadenas de suministro de defensa.
- Reforzar el mercado único de defensa.

De estos tres pilares, el principal es el EDF, que tiene como objetivo general estimular la competitividad, la eficiencia y la capacidad de innovación de la EDTIB en toda la Unión.

3.2. La Cooperación Estructurada Permanente (PESCO)

El artículo 42.6 del Tratado de la Unión Europea (TUE. Tratado de Lisboa de 2009) establece que “los Estados miembros que cumplan criterios más elevados de capacidades militares y que hayan suscrito compromisos más vinculantes en la materia para realizar las misiones más exigentes establecerán una cooperación estructurada permanente en el marco de la Unión”.

Esta cooperación (lo que conocemos como PESCO) se rige por el artículo 46 del TUE, su protocolo 10 y la normativa desarrollada en posterioridad.

Finalmente, esta iniciativa fue puesta en marcha por acuerdo del Consejo de la Unión Europea en el año 2017. Son 25 los países que firmaron el acuerdo en ese año (toda la Unión

Europea a excepción de Reino Unido, Malta y Dinamarca), ratificando el compromiso de colaborar de un modo más vinculante a la PCSD, así como permitir el seguimiento de las acciones llevadas a cabo para cumplir este compromiso. Recientemente se ha unido también Dinamarca.

La notificación se elaboró sobre la base de la propuesta conjunta que España, Alemania, Francia e Italia, trasladaron en una carta de las 4 ministras de Defensa al Alto Representante y al resto de los países de la Unión Europea el 21 de julio 2017. Estos cuatro Estados miembro constituyen aún hoy el grupo denominado PESCO4.

En diciembre de ese mismo año se adoptó la Decisión para el establecimiento de la PESCO, que constituyó el lanzamiento formal de la iniciativa (11 de diciembre de 2017). En la Decisión se relacionan los Estados miembros participantes, los compromisos asumidos, y la gobernanza establecida.

La Decisión establece la PESCO, pero no determina su duración. Tan solo señala que habrá dos fases iniciales consecutivas (años 2018-2020 y 2021-2025), que al principio de cada fase habrá que especificar los objetivos más precisos para el cumplimento de los compromisos más vinculantes, y que después de 2025, se llevará a cabo un proceso de revisión para evaluar si se han cumplido todos los compromisos de PESCO y decidir si se contraen nuevos compromisos, “con vistas a abrir un nuevo capítulo hacia la integración de la seguridad y la defensa europeas”.

Sus principios de aplicación recogen un conjunto de veinte compromisos vinculantes para todos los Estados participantes, entre los cuales se encuentra el incrementar los presupuestos de defensa, con un nivel de inversión en investigación hasta alcanzar un 2% del total de presupuesto de defensa, teniendo además el objetivo de destinar un 20% del gasto total a inversiones reales. El compromiso PESCO subraya la necesidad de potenciar el desarrollo de proyectos colaborativos y el uso cooperativo de capacidades, así como el impulso del desarrollo de capacidades militares en el marco de la CARD.

La primera revisión estratégica PESCO se llevó a cabo en 2020. Como resultado, el Consejo de la UE proporcionó orientaciones para la Fase 2021-2025 en términos de objetivos generales, objetivos políticos claves, procesos, así como incentivos para mejorar el cumplimiento de los compromisos más vinculantes. Se prevé una próxima revisión para 2025.

Con el fin de demostrar la voluntad de cumplir los veinte compromisos vinculantes acordados, los países miembros se comprometen a presentar anualmente un Plan Nacional de Implantación (NIP), que describe el avance a nivel nacional producido en el cumplimiento de dichos compromisos. A efectos de transparencia, todos los Estados miembros pueden acceder a los NIPs de los demás participantes.

Figura 2. Resumen de los 20 compromisos PESCO.

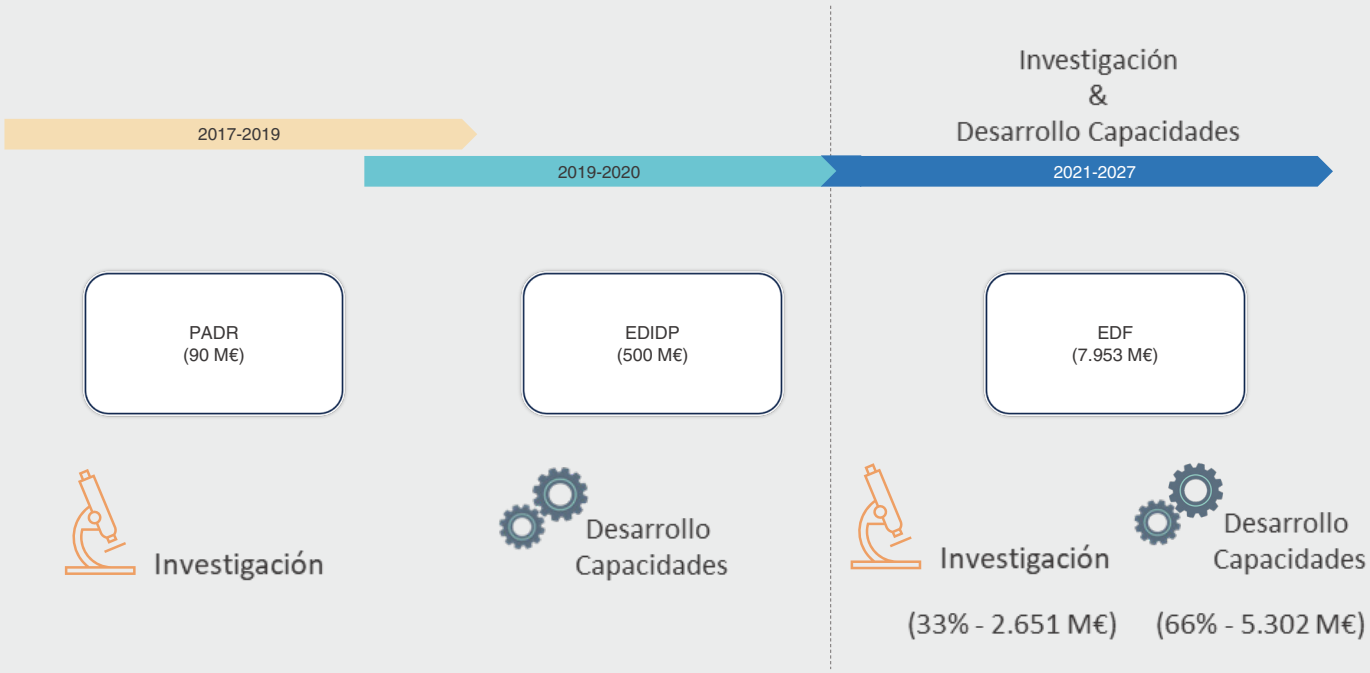


Figura 3. Visión General Fondo Europeo de Defensa y Programas Preparatorios previos (PADR y EDIDP).

3.3. El Fondo Europeo de Defensa (EDF)

El EDF supone que, por primera vez, la Unión Europea, a través de la Comisión Europea, pone a disposición del tejido industrial europeo una financiación para las actividades de investigación y desarrollo de capacidades militares.

Este fondo busca incentivar las acciones colaborativas y la cooperación transfronteriza entre entidades jurídicas de toda la Unión, en particular las Pequeñas y Medianas Empresas (PYMES) y las empresas de mediana capitalización (MIDCAPS), fomentando un mejor aprovechamiento del potencial industrial de la innovación, la investigación y el desarrollo tecnológico, en todas las etapas del ciclo de vida de los productos y tecnologías de defensa.

El fondo tiene previsto un presupuesto de cerca de 8.000 millones de euros entre los años 2021-2027, de los cuales un tercio aproximadamente se dedicará a financiar la investigación colaborativa en defensa y el resto para financiar proyectos de desarrollo colaborativo de capacidades.

Previo al lanzamiento del EDF en 2021, la Comisión Europea puso en marcha en 2017 la Acción Preparatoria para Investigación en Defensa (PADR) y en 2019 el Programa de Desarrollo Industrial de Defensa Europeo (EDIDP) para permitir, tanto a los Estados miembros, como a la Base Industrial adaptarse a los requisitos de participación en el EDF, como se muestra en la siguiente imagen.

El EDF se implementa a través de Programas de Trabajo anuales estructurados en 17 categorías, que se han configurado para permanecer estables durante el marco financiero plurianual 2021-2027. La financiación se concede a través de llamadas de propuestas competitivas anuales.

Puesto que uno de los distintivos del EDF es fomentar la cooperación industrial, los proyectos presentados tienen como exigencia que deben estar formados por consorcios de al menos tres entidades (públicas o privadas) que estén establecidas en, al menos, tres Estados miembros distintos.

Si bien el EDF está dirigido a entidades establecidas en la Unión o en un país asociado, su propio reglamento contempla la excepción que permite que entidades establecidas en la Unión, pero controladas por un tercer país, o por una entidad de un tercer país, puedan resultar beneficiarias de las acciones a subvencionar en el marco del EDIDP/EDF.

Para estos casos, la entidad debe poner a disposición de la Comisión garantías aprobadas por el Estado miembro en el que esté establecida sobre el beneficio de su contribución a la Unión Europea.

3.4. La Revisión Anual Coordinada de la Defensa (CARD)

A través de la CARD, la Agencia Europea de Defensa, el Estado Mayor de la Unión Europea (EUMS) y los Estados miembros llevan a cabo un proceso que proporciona una visión general de las capacidades existentes, así como de los planes para invertir en programas de defensa de los diferentes Estados miembros.

Así mismo permite analizar la situación actual de las capacidades prioritarias de la UE, acordadas en el Plan de Desarrollo de Capacidades (CDP), y las carencias identificadas en el *EU Headline Goal Process* (HLGP), medir el progreso de la cooperación en defensa y evaluar el potencial de desarrollo de capacidades adicionales.

El primer ciclo de la CARD se llevó a cabo en 2019-2020 e identificó seis áreas prioritarias (*six focus areas*) y cincuenta y seis oportunidades de colaboración en *Research & Technology*. Los proyectos asociados a las áreas y oportunidades tendrían un impacto positivo significativo en la mejora de las capacidades de la Unión Europea.

El segundo ciclo de la CARD se inició en diciembre 2021, llevándose a cabo la reunión bilateral nacional con los miembros de la EDA y el EUMS en abril 2022. El informe final de la CARD se ha presentado en el segundo semestre de 2022. El contenido de las seis áreas prioritarias identificadas se resume a continuación:

1) Actualizar, modernizar o adquirir una capacidad de carros de combate. Sustituir gradualmente las flotas existentes durante la próxima década y más allá.

2) Modernizar los sistemas de protección del soldado y la conciencia situacional del combatiente como núcleo de la protección de la fuerza individual y de la eficacia operativa en todos los tipos de operaciones durante la próxima década, basándose en una arquitectura comúnmente compartida para todos los subsistemas relacionados que utilicen tecnología de vanguardia.

3) Reemplazar los buques de patrulla costeros y de alta mar dentro de la próxima década y más allá, para satisfacer los crecientes requisitos operativos para garantizar la seguridad marítima adyacente al territorio europeo. Un buque de superficie de clase de patrulla europeo (EPC2S) representa un enfoque a escala de la UE para las plataformas navales modulares adaptables a diversas cuencas marítimas y a los requisitos/programas de los pMS.

4) Desarrollar la capacidad de contrarrestar los sistemas aéreos no tripulados de baja velocidad/baja visibilidad (*Counter-UAS*) para mejorar la protección de las fuerzas, así como contribuir a establecer una norma europea para la lucha contra el acceso y la denegación de área (A2/AD). Esta última está vinculada a la defensa aérea y de misiles, que podría integrarse en un contexto más amplio de gestión aérea civil.

5) Desarrollar un enfoque europeo de la defensa en el espacio para mejorar el acceso a los servicios espaciales y la protección de los activos basados en esta dimensión. Esto implicaría abordar sistemáticamente los requisitos de defensa en el desarrollo de capacidades espaciales y racionalizar los esfuerzos fragmentados de los países miembros y las instituciones de la UE.

6) Llevar los actuales esfuerzos prioritarios de los países miembros en materia de movilidad militar un paso más allá, mediante su mejora. Perfeccionar los medios de transporte (transporte aéreo y marítimo) y las instalaciones logísticas, así como la resistencia de los sistemas y procesos informáticos relacionados en condiciones de guerra híbrida (protección de puertos, ciberdefensa) para mediados de los años veinte.

Las actividades relacionadas con la I+T abarcan la Inteligencia Artificial (IA), la ciberdefensa, las nuevas tecnologías de sensores, los materiales emergentes y los sistemas de propulsión energéticamente eficientes, así como los sistemas no tripulados y la robótica.

3.5. El Plan de Desarrollo de Capacidades (CDP)

El CDP identifica las prioridades de capacidad en las que los Estados miembros deben centrar sus esfuerzos comunes. Se ha definido como el «impulsor» para la investigación y tecnología, la cooperación en armamento y para el desarrollo industrial.

En 2023, la Junta Directiva de EDA, en formato de Directores de Capacidades, respaldó la revisión de CDP y aprobó las veintidos prioridades para el desarrollo de capacidades de la Unión Europea derivadas del mismo. Este acto tuvo una importancia estratégica particular ya que el CDP es una de las referencias para la implementación de las principales iniciativas europeas de defensa, como la Revisión Anual Coordinada sobre Defensa, la Cooperación Estructurada Permanente y el Fondo Europeo de Defensa.

La identificación de estas prioridades se basa en cuatro áreas denominadas «STRANDS», que analizan a corto plazo las lecciones aprendidas de las operaciones en curso. A medio plazo, se identifican oportunidades de colaboración entre países reflejadas en las programaciones de recursos de los Estados miembros y a través de la información volcada en la herramienta EUCLID. A largo plazo, analiza la evolución del panorama estratégico y las tendencias tecnológicas e industriales.

Time			
Tasks	Shorter Term (Strand A+D)	Mid Term (Strand C)	Longer Term (Strand B)
	HLG 2010 Lessons Identified	Plans & Projects "Landscaping"	Long Tem View

Figura 4. Esquema CDP- Strands para priorización.

De la priorización en el corto, medio y largo plazo se derivan una serie de prioridades de desarrollo de capacidades europeas (*EU Capability Development Priorities*), que se desarrollan en los denominados *Strategic Context Cases* (SCC).

3.6. Adquisiciones Conjuntas en Materia de Defensa como Política Industrial Europea

A raíz de la agresión rusa contra Ucrania, los Jefes de Estado y de Gobierno se reunieron en Versalles, Francia, en marzo del 2022, para abordar tres dimensiones clave:

a) el refuerzo de nuestras capacidades de defensa,

b) la reducción de nuestra dependencia energética, y

c) el desarrollo de una base económica más sólida.

Tras esta reunión se invitó a la Comisión Europea a realizar un análisis sobre la falta de inversión en defensa, en coordinación con la EDA. Dicho análisis se presentó el 18 de mayo del citado año e incluye recomendaciones para potenciar la base industrial y tecnológica de defensa europea.

El informe identificó las siguientes carencias agrupadas en cuanto al gasto en defensa, las capacidades militares disponibles y la capacidad de la base industrial europea:

Carencias identificadas en el gasto en defensa:

Como consecuencia directa de la invasión rusa de Ucrania, los Estados miembros ya han anunciado aumentos de sus presupuestos de defensa cercanos a los 200.000 millones de euros adicionales en los próximos años. Aunque estos aumentos son esenciales, se producen después de años de importantes recortes y de una grave falta de inversión. De 1999 a 2021, el gasto combinado de defensa de la Unión Europea aumentó un 20%, frente al 66% de Estados Unidos, el 292% de Rusia y el 592% de China. Sin un enfoque coordinado, el aumento del gasto corre el riesgo de conducir a una mayor fragmentación y deshacer los progresos realizados hasta ahora.

Carencias industriales:

A pesar de la competitividad general del sector, la demanda está fragmentada y por ende la industria también sigue estructurada según las fronteras nacionales, a excepción de los sectores de la aeronáutica y los misiles. Existen dependencias para equipos clave de defensa para los que la EDTIB no ofrece soluciones propias.

Carencias identificadas en relación con las capacidades militares:

Se identifican tres prioridades urgentes: reponer los arsenales, sustituir los sistemas heredados de la era soviética y reforzar los sistemas de defensa aérea y de misiles.

Más allá de estas carencias urgentes de capacidades, se propone trabajar en una serie de capacidades estratégicas a medio y largo plazo en los ámbitos de la defensa aérea, terrestre, marítima, espacial y cibernética.

A raíz de este informe se creó la *Defence Joint Procurement Task Force* (DJPTF) para apoyar la contratación conjunta y reponer las existencias a la luz del apoyo prestado a Ucrania. Los trabajos desarrollados en el seno de esta *Task Force* serán implementados gracias al instrumento EDIRPA, herramienta diseñada para favorecer la adquisición conjunta a muy corto plazo y con carácter urgente, con lo que se pretende restablecer los stocks y disponibilidad previos al conflicto, además de favorecer asistencia futura a Ucrania. Este instrumento, dotado de un presupuesto de 500 millones de euros, será gobernado por una estructura con similitudes a la ya conocida para los EDF.

CAPABILITIES GAPS

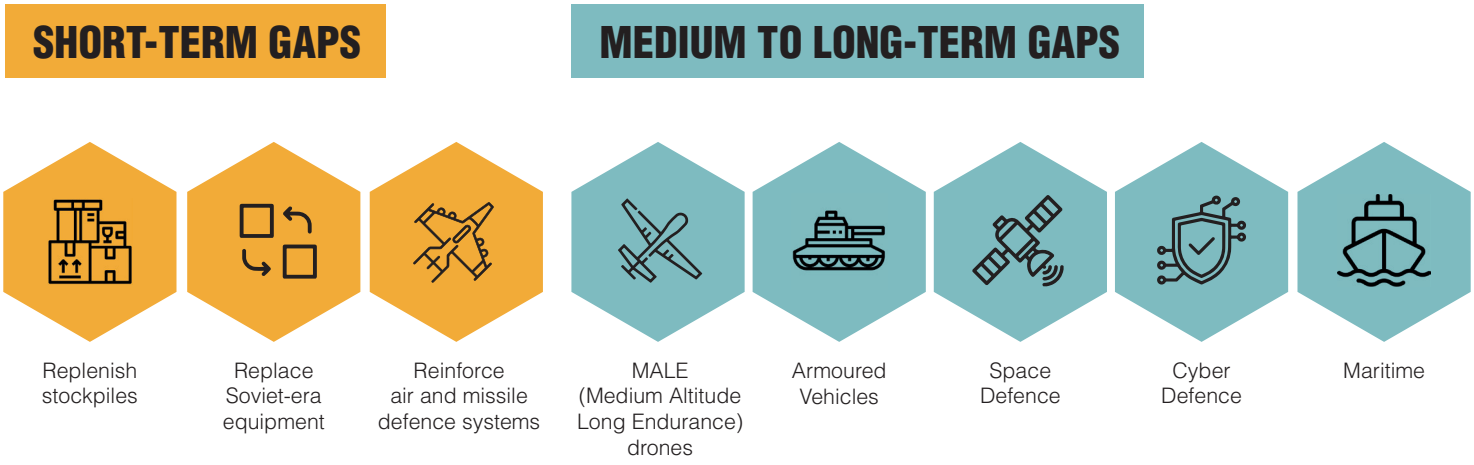


Figura 5. Carencias en el ámbito de capacidades europeas. (Fuente. CE).

En este caso, el marco de actuación será de dos años, finalizando el 31 de diciembre de 2024. Un Comité de Programas (*Programme Committee, PC*) elaborará un único Programa de Trabajo (*Work Programme, WP*) que cubrirá todo el periodo de duración de las adquisiciones conjuntas, y heredará la información de necesidades compilada hasta el momento en el seno de la DJTF.

En julio de 2022, los países miembros enviaron a la EDA un listado con posibles materiales objeto de adquisición. Con fecha de octubre del 2022, basándose en la respuesta de los Estados miembros, la DJPTF ha presentado siete áreas de interés común para la posible adquisición conjunta en diferentes categorías de equipos (es decir, 1. Equipos y suministros médicos, 2. Equipos de protección individual QBRN, 3. Sistemas y misiles antitanque, 4. Equipos y radios para soldados, 5. Municiones, explosivos, morteros y MLRS, 6. Misiles, defensa aérea, MANPADS, bombas, y 7. Armas portátiles).

Este instrumento a corto plazo allanará el camino hacia un marco de la Unión Europea para la adquisición conjunta de defensa. Para ello, en el tercer trimestre de 2022, la Comisión propuso un reglamento del Programa Europeo de Inversiones en Defensa (*European Defence Investment Programme* (EDIP)) y estableció las condiciones para que los Estados miembros formaran Consorcios Europeos de Capacidades de Defensa.

La exención del IVA para los Estados miembros que adquieran conjuntamente capacidades de defensa desarrolladas en colaboración continúa discutiéndose. Además, la Unión Europea proporcionará financiación asociada para proyectos de gran interés para la Unión.

Por otro lado, a medio plazo la Comisión propondrá una iniciativa sobre materias primas críticas, incluidas medidas legislativas, para facilitar, entre otras, el acceso de la industria de defensa a dichas materias primas críticas (CRM), fortaleciendo así la resiliencia y la seguridad del suministro de la UE.

Por su parte, el Banco Europeo de Inversiones (BEI), debería aumentar su apoyo a la industria de defensa europea y la adquisición conjunta más allá de su apoyo continuo al uso dual. Se ha solicitado al BEI que evalúe, en las circunstancias geopolíticas y de mercado actuales, qué pasos debería dar para fortalecer su apoyo a la defensa europea, incluyendo la capacidad de producción industrial, y adaptando, si fuera necesario, su política de préstamos, a la vez de invitar a los Estados miembros, sus accionistas, a apoyar este proceso.

Junto con las anteriores, la Comisión continuará poniendo en marcha nuevas acciones en el marco para la investigación e innovación de doble uso, para mejorar las sinergias entre los instrumentos civiles y de defensa.

4. LA INNOVACIÓN EN EL MARCO DE LA UNIÓN EUROPEA

Desde el año 2017, hay un nuevo marco para la cooperación transfronteriza en materia de I+D en el ámbito de la defensa. Como mencionamos anteriormente, el inicio fue a través de PADR y el EDIDP, y ahora, a través del Fondo Europeo de Defensa.

En febrero del año 2022, la Comisión se comprometió a mejorar la coordinación interna entre los programas e instrumentos de la UE, con el fin de aprovechar los enormes beneficios que se derivan de las sinergias entre la I+D+i civil y la de defensa, contribuyendo así a la defensa europea, impulsando la innovación y analizando las dependencias estratégicas.

Para implementar estas medidas, la Comisión está trabajando, en colaboración con otros organismos de innovación europeos como la EDA, el EIC (*European Innovation Council*) y el EIF (*European Investment Fund*). También lo hace con OTAN para asegurar el desarrollo de sinergias en innovación.

4.1. Plan de Innovación para la Defensa de la UE (EUDIS)

EUDIS es el marco a través del cual la Comisión propone aplicar una serie de medidas concretas para derribar las barreras de entrada, y poner en marcha una amplia gama de apoyos para ayudar a las empresas innovadoras de la UE a llevar sus ideas al mercado, y marcar una diferencia significativa para la defensa de la UE.

En cuanto a la financiación, la Comisión aprovechará parte del presupuesto del Fondo Europeo de Defensa (1.460 millones de euros), combinado con la cofinanciación de los Estados miembros (90 millones de euros), y también espera obtener entre 400 y 500 millones de euros de otras fuentes públicas y privadas. En términos generales, el Plan de Innovación para la Defensa de la UE supondrá una inversión total cercana a los 2.000 millones de euros durante la vigencia del actual MFP.

La Comisión anunció los siguientes instrumentos bajo el marco del EUDIS para fomentar la innovación en materia de tecnologías críticas, especialmente orientado a PYMES y MIDCAPs:

a) Acciones específicas en las convocatorias del EDF para apoyar los proyectos sobre tecnologías disruptivas y soluciones de defensa innovadoras y orientadas al futuro, fomentando en particular la participación de las PYMEs innovadoras, los laboratorios innovadores y las organizaciones de investigación y tecnología. Estas acciones adoptan diferentes formas, por ejemplo, *coaching* empresarial (WP2021); retos tecnológicos (WP2022), *hackathons*, *spin-in* y premios (WP2023 o posterior).

b) Mecanismo de combinación de inversiones en materia de defensa en el marco de InvestEU; aliviando los problemas relacionados con el acceso limitado a la financiación de las PYMEs que desarrollan tecnologías, al tiempo que proporcionaría capital de confianza y evitaría las adquisiciones hostiles por parte de entidades de terceros países. Permitir un mejor acceso a la financiación de capital para las PYMEs innovadoras de defensa y las empresas de mediana capitalización apoyaría su crecimiento y, finalmente, beneficiaría a la capacidad de innovación de la BTID.

c) CASSINI para la defensa: inspirado en la actual iniciativa CASSINI para apoyar a las empresas de nueva creación de la industria espacial. Les proporcionaría servicios como: desarrollo empresarial y redes (*matchmaking*, acelerador de empresas), y premios y concursos (*hackathons*, *mentoring*, etc.), complementando el mecanismo de combinación de inversiones en defensa antes mencionado.

d) HEIDI: una nueva incubadora de innovación en materia de nuevas tecnologías e innovación de doble uso. Actuará como plataforma para estimular, facilitar y apoyar la cooperación en materia de innovación en defensa entre los Estados miembros, garantizando al mismo tiempo las sinergias con las actividades conexas de la Comisión Europea, en particular el Plan de Innovación en Defensa de la Unión Europea, y la coherencia de los resultados con las iniciativas de innovación de la OTAN, como el Acelerador de Innovación en Defensa para el Atlántico Norte (DIANA).

e) Mayor apoyo a las redes de innovación. Las redes transfronterizas de innovación en materia de defensa, *Cross Border Innovation Networks* (CBDIN), desempeñarán el papel de intermediarios (empresa-centro) de la innovación y fomentar los proyectos de colaboración para incorporar soluciones innovadoras.

Los centros de investigación y las instalaciones de pruebas técnicas comprobarían la pertinencia de esas tecnologías en el ámbito civil e intercambiarían las mejores prácticas.

4.2. La Agenda Estratégica de Innovación (OSRA)

Las siglas de OSRA corresponden a *Overarching Strategic Research Agenda*. Esta iniciativa, lanzada por la EDA, ofrece un nuevo enfoque para alinear las agendas estratégicas de investigación de la Unión Europea (de ámbito dual) con las necesidades y requisitos operacionales de los Estados miembros.

El objetivo de esta Agenda es esbozar una hoja de ruta para la ejecución de los futuros programas de investigación del EDF.

5. CONCLUSIONES

Desde la entrada en vigor de las PESC en las que se incluían por primera vez cuestiones asociadas a la seguridad de la Unión Europea, y el posible establecimiento de una política de defensa común que derivara en una defensa europea común, se han dado importantes pasos a nivel europeo. La aprobación en 2016 de la EUGS ha tenido como consecuencia el establecimiento y desarrollo de diferentes iniciativas europeas en materia de defensa que impulsarán la Europea de la Defensa.

Estas iniciativas se encuentran en gran medida orientadas a una mayor cooperación en el desarrollo de las capacidades necesarias de acuerdo al contexto geoestratégico actual, además de ser la primera vez en la que la Comisión Europea se involucra de forma directa en el ámbito de la seguridad y defensa, llegando incluso a asignar una pequeña parte del presupuesto europeo de forma exclusiva al ámbito de defensa a través del EDF. Se trata del inicio de un conjunto de medidas más amplias en materia de política industrial de la Comisión Europea.

Además de ser una gran oportunidad para que Europa alcance de forma real una defensa común que garantice el cumplimiento de los objetivos de la PCSD, es una oportunidad única e irrepetible para la Unión Europea, dado que tendrá un gran impacto en los futuros sistemas a desarrollar en Europa en las próximas décadas.

Aprovechar dichas iniciativas facilitará la racionalización que sufre el mercado de defensa de forma tradicional, además de facilitar el desarrollo de capacidades militares europeas. Europa sufre la ineficiencia del gasto debido a las duplicaciones, la falta de interoperabilidad entre sistemas, las brechas tecnológicas y las insuficientes economías de escala para la industria y la producción. En torno al 80% del desarrollo de nuevos sistemas o plataformas es realizado fundamentalmente a través de la industria de defensa nacional, lo que conduce a una costosa duplicación de capacidades militares.

Así mismo, permitirá potenciar las capacidades de la EDTIB, posicionándola en una posición de ventaja frente a otros competidores en un momento en el que los presupuestos de defensa se encuentran en expansión derivado fundamentalmente a la situación de Ucrania. Aspectos estos considerados en la European Defence Industrial Dtrategy (EDIS).

Por otro lado, en un contexto europeo en el que la cooperación en el desarrollo y adquisición de capacidades deja de ser una opción para convertirse en una obligación debido a la complejidad y coste de los nuevos sistemas de armas, los países europeos deben ser conscientes de la necesidad de participar activamente en estas iniciativas.

Esta mayor cooperación demandará, por una parte, la armonización de los requisitos de nuevas capacidades, así como la coordinación de las estrategias de I+D, adquisición e industriales de los países europeos. Así mismo, la EDTIB deberá realizar un importante esfuerzo en la conformación de consorcios europeos con una vista a medio-largo plazo de las capacidades industriales y tecnológicas de la Industria de Defensa Europea.

En la actualidad, el EDF es el programa de I+D de la UE en materia de defensa, y a futuro el Plan de Innovación de la Defensa puesto en marcha por la Comisión Europea. Estos programas no van a cubrir el déficit de inversión en I+D+i, pero desde luego permitirá reducirlo, aprovechando las sinergias con otras iniciativas civiles/militares en curso, así como con las iniciativas de la OTAN.

El beneficio de las iniciativas europeas en materia de defensa va más allá del ámbito militar o de defensa, toda vez que puede generar un importante retorno de carácter industrial, incrementando la capacidad y el *know-how* de la EDTIB, su potencial exportador, y facilitando un innegable avance en tecnologías de carácter dual, civil-militar.

La participación en ellas no es una opción para el conjunto de los países europeos, sino una obligación, ya que es beneficioso para conseguir las capacidades que se requerirán por parte de la defensa europea para hacer frente a los escenarios futuros.

En los capítulos siguientes analizaremos grosso modo la influencia de las tecnologías en las capacidades de cada uno de los ámbitos del multidominio, como nuevo paradigma del conflicto, intentando vislumbrar si Europa (y España dentro de ella) está en condiciones de alcanzar la autonomía estratégica que pretende en competencia con los actores internacionales, y si los mecanismos descritos anteriormente, sobre la base de la estructura y organización de la Unión Europea, darán sus frutos para ir convergiendo en una real Base Industrial y Tecnológica Europea que soporte una autentica Defensa de Europa.

BIOGRAFÍAS

BEGOÑA ROJO CARRALERO

Ingeniero Industrial del ICAI. Durante los 20 años en los que ha formado parte de Isdefe, su trayectoria profesional ha estado orientada a la administración pública, en especial del Ministerio de Defensa y del sector empresarial de la defensa. Ha colaborado con el Estado Mayor y con la Secretaría de Estado de Defensa en la implantación del Planeamiento Nacional de la Defensa y su integración en los procesos OTAN y UE, así como fomentar la participación de la industria de defensa nacional, en las Iniciativas Europeas de Defensa.

Actualmente trabaja como adjunta al Director de Desarrollo de Negocio de la empresa GMV.

Es miembro de la Junta Directiva de la Asociación Nacional de Ingenieros del ICAI, del Comité de Tecnologías de la Defensa en el Instituto de la Ingeniería de España, y del Grupo de Trabajo de Ingeniería con Propósito en la Real Academia de la Ingeniería.

Cuenta con una Cruz al mérito naval con distintivo blanco concedida en 2017, por su trabajo apoyando al Estado Mayor de la Defensa.

CAPÍTULO 3

Capacidades Terrestres

Violeta Ruiz Aldea

El ámbito terrestre es básico para sostener todo esfuerzo bélico o apoyar de distintas formas la acción desde otros ámbitos. En palabras de Fehrenbach: “puedes volar sobre un terreno, bombardearlo, atomizarlo y limpiarlo de toda forma de vida, pero si quieres defenderlo, protegerlo y mantenerlo para la civilización, debes hacerlo sobre el propio terreno, como hicieron las legiones romanas, metiendo a sus hombres jóvenes en el lodo” [1].

Las guerras aún parecen ganarse y perderse por los elementos terrestres. El control desde otros ámbitos sobre lo que acontece en tierra, sobre su población o sobre sus líderes, es parcial.

Las fuerzas armadas ucranianas, desde la invasión de su territorio por Rusia en febrero del 2022, recibieron de la UE más de 77.000 millones de Euros en ayuda económica, militar y de protección civil en un periodo de poco más de año y medio. Esto nos recuerda el nivel de exigencia que supone una guerra preponderantemente terrestre.

Este capítulo pretende dar una visión general del desarrollo tecnológico asociado a las capacidades militares en el ámbito terrestre y en el marco de los compromisos internacionales de España para con la UE y la OTAN.

Se introducen los sistemas más significativos, los retos asociados a su operación y se mencionan finalmente dos aplicaciones de las nuevas tecnologías a las capacidades en el ámbito terrestre: la logística predictiva y el adiestramiento mediante simulación.

1. EVOLUCIÓN DEL COMBATE TERRESTRE HACIA LAS OPERACIONES MULTIDOMINIO

La doctrina militar, que describe la forma de empleo de las Fuerzas Armadas y establece las normas fundamentales con las que operan, evoluciona para enfrentar en cada momento nuevos desafíos.

La guerra ha cambiado de lugar. La guerra fría entre EE.UU. y Rusia nunca llegó a un conflicto armado; este se dio en otros lugares del mundo y a través de otros actores ('guerras proxy'). A menudo, los teatros de operaciones son áreas densamente pobladas, y la pérdida de vidas entre la población civil es políticamente inaceptable. Han cambiado los combatientes, una variedad de actores y grupos terroristas que hacen que la frontera con las fuerzas regulares sea difusa. Pero hay dos aspectos en los que la naturaleza y velocidad de los cambios constituyen una auténtica revolución.

Por una parte, las nuevas tecnologías han configurado un campo de batalla cada vez más letal: drones, plataformas semiautónomas o nanotecnología, integrados en sistemas y sofisticadas redes ISR (Inteligencia, Vigilancia y Reconocimiento), capaces de operar a distancias estratégicas, operacionales y tácticas. Por otra, estas nuevas tecnologías han multiplicado la forma y capacidad de gestionar la información: el control del ámbito de lo cognitivo persigue conseguir un efecto eficaz sobre el adversario, que es en definitiva el fin de la conquista de un objetivo militar (la situación política, económica y social; la opinión pública; los aspectos legales y el derecho internacional…). Hoy la guerra mundial informativa ha alcanzado su apogeo y existen varias versiones sobre la realidad que chocan abiertamente entre sí.

En occidente, la evolución de la doctrina ha venido liderada desde el Ejército estadounidense. Precisamente por su superioridad en el ámbito terrestre, sus adversarios han intentado alcanzar sus objetivos usando métodos poco convencionales de combate. Hay ejemplos en Vietnam, Iraq o Afganistán.

La doctrina de la Batalla Aeroterrestre (ALB) evolucionó en 2016 al concepto de la "Batalla Multidominio" (MDB) y, finalmente, a las "Operaciones Multidominio" (MDO) en 2018, que propone soluciones frente a múltiples niveles de enfrentamiento en todos los ámbitos (tierra, mar, aire, espacio, ciberespacio y cognitivo). Este es el problema militar a solventar. La amenaza, según se percibe desde la seguridad, está en el aumento de las capacidades A2 (Anti-Acceso) y AD (Denegación de uso de área) de Rusia y de China [i], para evitar la entrada de fuerzas expedicionarias a su territorio y, una vez dentro, limitar su libertad de acción. Hace siglos el imperio español usó fortificaciones costeras, torres de vigilancia y flotas de galeras como sistema anti-accesos.

El objetivo final es la defensa de la zona estratégica Asia-Pacífico (incluyendo Taiwán) en el caso de China, y las fronteras con países de la Alianza, en el caso de Rusia.

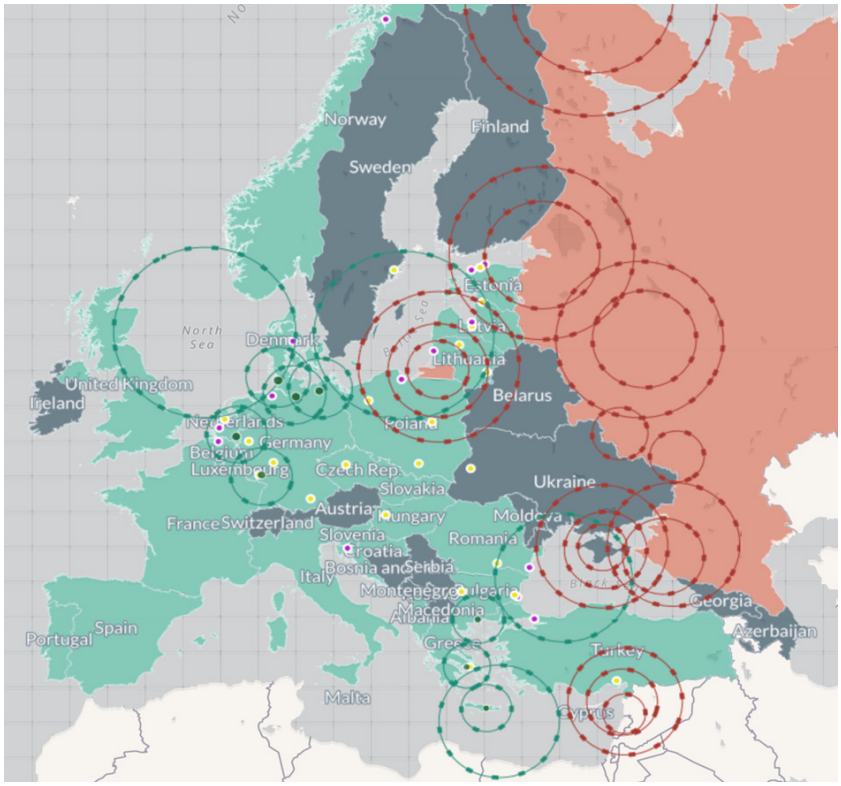


Figura 1 - Gráfico interactivo que muestra los sistemas A2/AD de Rusia (en rojo) y de la OTAN (en verde) en 2017. Los puntos amarillos son puertos de embarque y desembarque de tropas y equipo (por aire o mar) de la Alianza [2].

La idea central de las MDO es la rápida y continua integración de todos los ámbitos para disuadir al adversario y prevalecer en la contienda por debajo del conflicto armado. Si falla la disuasión, el Ejército, operando como parte de la Fuerza Conjunta, desintegrará los sistemas A2/AD del adversario y aprovechará la libertad de acción así obtenida para impedir que el adversario alcance sus objetivos y lograr los propios, forzando una vuelta a la contienda en una situación más favorable para EE.UU., sus socios y aliados. En 2022 el Ejército estadounidense publicó la última versión de su manual de campaña, que representa la adopción oficial de la doctrina por el Ejército de los EE.UU.

En cuanto a sus potenciales adversarios, es reveladora la importancia que tanto Rusia como China conceden al ámbito ciberespacial y al valor de la información (la 'quinta dimensión' o 'quinto dominio' de la guerra).

El reflejo de las MDO en el caso de Rusia viene a ser un 'combate colaborativo'. Se da prioridad a la 'calidad' del fuego (potencia y precisión) frente a la cantidad, y al ámbito espacial y del ciberespacio. China pone el foco en la habilidad para generar, explotar y proteger la información, buscando atacar centros de sistemas de mando, control, comunicaciones, computadoras, inteligencia y vigilancia (C4ISR) y debilitar así los enlaces y redes del adversario.

Los sistemas A2/AD son más que burbujas impenetrables dentro de un potente sistema anti-misiles de largo alcance o un sistema móvil de defensa aérea. Se complementan con la batalla en el ámbito cognitivo: una campaña de desinformación junto a amenazas de carácter económico puede crear discordia entre los adversarios, retrasando la decisión de actuar y forzando el combate bajo el umbral del conflicto armado. Las operaciones multidominio son la nueva forma de entender el espacio de batalla del futuro y preparar así a la Fuerza Conjunta para integrar los ámbitos no físicos (ciberespacial y cognitivo) en la consecución de sus objetivos.

2. CAPACIDADES MILITARES TERRESTRES EN OPERACIONES MULTIDOMINIO

Las capacidades militares en el ámbito terrestre incluyen tanto medios humanos y materiales (tecnología, logística, etc.) como la doctrina o el adiestramiento asociados a la operación.

Respecto de la capacidad tecnológica, la EDA (*European Defence Agency*) incluyó en la lista de prioridades de 2018 el combate terrestre (plataformas y protección de las fuerzas desplegadas) y el apoyo (movilidad, logística y ayuda médica). Los apartados siguientes refieren algunos aspectos del componente tecnológico, como son las plataformas terrestres, la nube de combate y otras aplicaciones de las nuevas tecnologías.

En el aspecto doctrinal, el concepto MDO está sujeto a múltiples interpretaciones con respecto a lo que supone a efectos prácticos. El Ejército estadounidense explica hasta cierto punto cómo las unidades penetran las capacidades del adversario y desintegran sus sistemas A2/AD, pero la lógica sobre la que se sustenta no está expuesta de forma explícita.

La idea es crear combinaciones de efectos (físicos, no físicos, mentales, morales) para debilitar y colapsar la voluntad de resistir del adversario. Estos efectos son el resultado de operaciones complejas entrelazadas dentro y a través de múltiples ámbitos. En consecuencia, la solución no es única.

La doctrina MDO del Ejército estadounidense establece los siguientes postulados:

1. **Calibrar el despliegue**, es decir, combinar posición y capacidad de maniobra en todas las distancias con un despliegue dinámico (fuerzas adelantadas, expedicionarias y anfitrionas) para disuadir al adversario y a la vez estar preparado para combatir. El espacio de batalla no se define por áreas geográficas, sino por la mezcla de capacidades disponibles en cada una. Este marco debe poder ser visualizado en tiempo real por el núcleo de planificación de los Estados Mayores, que se dota de personal experto de cada cuerpo (junto con oficiales de enlace y especialistas -incluso en lingüística y cultura local-), ajustado al ritmo de la batalla y a los turnos de trabajo.

2. Emplear **unidades multidominio resilientes** para operar en todos los ámbitos, desde cualquier localización al punto de conflicto. Son unidades tácticas escalables y organizadas en base a la tarea; poseen ISR, potencia de fuego y movilidad; pueden maniobrar sin flancos seguros, sin soporte durante largos períodos de tiempo ni comunicación constante con el cuartel general y conducir la filosofía "misión command" [ii]. El soldado es parte de un equipo interdisciplinar que integra experiencias y habilidades individuales para adaptarse a cada misión, integrando los avances técnicos a su alcance, a través de todos los ámbitos y desde cualquier localización.

3. **Converger capacidades**, o sea, integrar las capacidades de todos los ámbitos en el tiempo y en el espacio físico -una evolución del "combate Inter Armas" [iii] a nivel operacional- para crear ventajas físicas, virtuales y cognitivas frente al adversario.

   - Los elementos están organizados, entrenados, autorizados y equipados para acceder, planear y operar juntos a través de los múltiples ámbitos en todo momento, no sólo en conflicto. El Ejército se reorganiza para integrar fuerzas convencionales y de operaciones especiales, junto a las de sus socios y aliados.

   - Los sistemas son interoperables y están conectados, dentro de cada ámbito y entre los diversos ámbitos de operación, para compartir información en tiempo real. Puesto que las ventanas de oportunidad pueden surgir de la ventaja temporal ofrecida desde otro ámbito (aéreo, por ejemplo), el intercambio rápido y preciso de datos entre los diferentes actores operando en MDO es la llave del éxito, precisando de una estructura óptima de transferencia de datos junto a una de gestión de operaciones interoperable y flexible.

El Ejército estadounidense creó en 2017 la primera *Multi-Domain Task Force* (MDTF), pieza central en su reorganización en base al concepto MDO, con objetivo en el Indo Pacífico. Bajo el mando de la Fuerza Conjunta, las MDTF son capaces de operar a todos los niveles operacionales y sincronizar efectos (espacio, ciberespacio, información) y fuego de precisión de largo alcance. Una segunda MDTF se activó en 2021 en Alemania y la tercera en 2022 en Hawái.

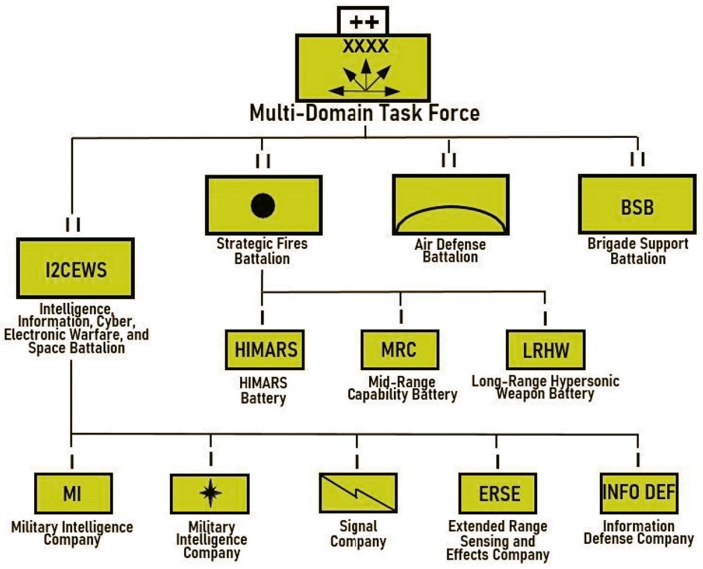


Figura 2 - Concepto de la organización de una MDTF genérica. Fuente: Chief of Staff Paper #1 Army Multi-Domain Transformation Ready to Win in Competition and Conflict, March 16, 2021, p. 12. https://sgp.fas.org/crs/natsec/IF11797.pdf

El Ejército español, por su parte, inició un proceso de cambio con horizonte en el año 2035 para afrontar el reto de mantener unas fuerzas terrestres preparadas y eficaces, la «Fuerza 35». En palabras del Jefe de Estado Mayor del Ejército , «El Ejército de 2035, componente esencial de la Fuerza Conjunta, estará capacitado para constituir organizaciones operativas flexibles y cohesionadas, dotadas de medios tecnológicamente avanzados y formadas por personal altamente motivado y preparado. Será capaz de operar en todo tipo de entornos y de integrarse en estructuras multinacionales para asegurar la protección de la población y el control del territorio y los recursos".

3. PLATAFORMAS TERRESTRES EN MULTIDOMINIO

Los medios materiales asociados al ámbito terrestre incluyen una variedad de sistemas y equipos cuya descripción exhaustiva excede el alcance de este trabajo. Nos limitamos aquí a considerar las principales 'plataformas terrestres' cuya tendencia es combinar capacidades en un tipo de vehículo, tripulado o no (incluyendo robots y drones), de combate o de apoyo, en base a los condicionantes de cada fabricante, cada ejército, y cada potencial escenario operativo.

3.1. Plataformas Tripuladas

3.1.1. Carros de Combate

Las plataformas de blindaje pesado o carros de combate (*Main Battle Tanks*, MBT) son el resultado de un proyecto de franceses y británicos a principios del siglo XX, empleando la palabra 'tanque' (de agua) como medida de decepción para mantener en secreto su fabricación y despliegue. Tras aumentar su potencia de fuego y protección, con el consiguiente aumento de peso y volumen, se añadieron capacidades electrónicas (para detectar al enemigo a más distancia y batirle allí) y aún hoy parecen seguir respondiendo a la necesidad de un 'carro universal' capaz de cubrir varias capacidades bajo un único diseño.

En **Europa** coexisten varias versiones de los Leopard alemanes (también adquiridos por Turquía), AMX Leclerc franceses, Challenger británicos y Ariete italianos. Los europeos sólo disponían de 5.000 MBTs en 2017 según la EDA; la mitad necesitarían ser actualizados en los próximos 20 años y unos 300 eran ya obsoletos. Bajo el proyecto estrella, el MGCS (*Main Ground Combat System*), se desarrolla el *European Main Battle Tank* (EMBT) francoalemán, del que poco se sabe al momento de escribir este capítulo, salvo que el proyecto parece haberse dilatado hasta 2040.

Rusia tiene en su arsenal la mayor flota de carros de combate del mundo, más de 12.000 unidades según varias fuentes. Además de los T-72 Ural y T-80 operando en la guerra de Ucrania, el T-90 es además un éxito comercial (exportado a varios países, entre ellos India, Venezuela, e Irak). El T-14 Armata es el MBT ruso de última generación. Se desplegó en Ucrania en julio de 2023. Se afirma que los MBT rusos son más ligeros que sus oponentes occidentales, pues el límite para la mayoría de los puentes en territorio de la antigua Unión Soviética es de 50 toneladas.

En comparación con el M1A1 Abrams estadounidense, el T-90 ruso es 18 toneladas más ligero, se impulsa con motor diésel (frente a la turbina de gas del Abrams) y aunque algo más lento, tiene mucha más autonomía.

China, con casi 6.000 MBTs en activo y varios diseños en producción para uso interno y exportación de la estatal *Norinco*, es el tercer país con mayor flota tras Rusia y EE.UU. Su MBT más popular es el Type 96, probado por el Ejército de Sudán contra los rusos T-72, aparentemente con ventajas significativas. El *Type 99A* es su carro de combate principal, 10 toneladas más ligero que el Abrams y alimentado por turbodiésel. Dentro de los carros de combate ligeros, el *Type 15* (ZTQ-15) pesa entre 33 y 36 toneladas para uso en áreas montañosas y terrenos inaccesibles para los MBT estándar (de unas 50 toneladas, como el Type 99).

España cuenta con *Leopard 2A4* adquiridos en los 90, de donde parten las unidades destinadas a apoyar a la fuerza ucraniana en la guerra contra Rusia. La versión más moderna con la que cuenta el Ejército español es el Leopardo 2E, montada y fabricada parcialmente bajo licencia en España.

Los MBT han crecido en armamento y con la incorporación de sistemas adicionales (dispositivos automáticos de carga o sistemas de protección, como luego veremos), aumentando su peso e impactando en su agilidad y movilidad. Algunos ejércitos están abandonando el MBT en favor de unidades blindadas más ágiles y ligeras, al considerar la merma de capacidades en ciertos teatros (terrenos con obstáculos, ciudades, etc.), donde otros tipos de plataformas son más adecuadas para apoyar unidades ligeras (divisiones aerotransportadas) o en entornos de difícil maniobrabilidad (montaña, zonas urbanizadas, etc.).

Imagen 1- El M1 Abrams estadounidense arriba y el ruso T-14 Armata abajo. Fuente: "Noticias de Israel".

3.1.2. Vehículos de Transporte y Otros Blindados de Combate

Además de los MBTs encontramos vehículos blindados más ligeros con diversa capacidad de combate y diseñados para apoyar la operación de aquellos y/o de la infantería: blindados de transporte de infantería -APC (*Armoured Personnel Carriers*)- con menor capacidad de combate; híbridos, entre los APC y los MBT, más ligeros en armamento y protección que el MBT; y vehículos de combate de la infantería -IFV (*Infantry Fighting Vehicles*) o AFV (*Armoured Fighting Vehicles*)-, algunos dotados de capacidades anfibias.

Las fuerzas ucranianas operaron en la guerra ruso-ucraniana algunos modelos de la familia de blindados rusos BMP, un AFV de la era soviética, hasta que recibieron en febrero de 2023 el M2 Bradley estadounidense.

China ha desarrollado más de una docena de vehículos de combate. El ZBL-09 (*Snow Leopard*) es un 8X8 diseñado para 'vestirse' tanto de APC como de AFV. Tanto Israel, con más experiencia en guerra de maniobras en tierra que muchos países, como Turquía, que ha pasado de ser un importador a marcar tendencia desde el inicio de la modernización de su industria de defensa en 2004, poseen sus propios diseños de MBT y de AFVs.

En Europa existe más de una docena de fabricantes con producción en serie de varios modelos de estos tipos de vehículos. Los alemanes disponen del blindado multi-misión *Boxer* y del *Puma*, que reemplaza al IFV *Marder* (enviado en apoyo a Ucrania). Los franceses reemplazaron su 6x6 de apoyo, el AMX-10 (también enviado a Ucrania), por el *Jaguar* RACV (*Reconaissance Armored Combat Vehicle*). Para misiones de reconocimiento y contra carro, Italia diseñó en los 90 el 8x8 Centauro, adquirido por España y actualizado como el VBM Frecia. España cuenta además con el Pizarro; el transporte Pegaso BMR -Blindado Medio de Ruedas- (un desarrollo español de los 70 actualizado a su versión M1); y su derivado Vehículo de Exploración de Caballería (VEC). Estos últimos serán reemplazados por los 8x8 Dragón del consorcio español *TESS Defence*. Se prevé el Vehículo de Apoyo de Cadenas (VAC) para reemplazar el TOA (Transporte Oruga Acorazado) M113 estadounidense en 2027.

Dentro de los proyectos PESCO impulsados desde la UE, el *Armoured Infantry Fighting Vehicle / Amphibious Assault Vehicle / Light Armoured Vehicle* (AIFV/AAV/LAV) pretende desarrollar y construir un prototipo de vehículo blindado ligero de infantería con capacidades anfibias. El proyecto está liderado por Italia, pero se desconoce cualquier otro detalle.

Imagen 2- Un BMP-2 ruso en dos instantáneas, supuestamente tomadas en Ucrania. Fuente: X (Twitter).

3.1.3. Vehículos Antiminas y Anti-emboscadas

Los vehículos anti-minas (*Mine Protected Vehicle*, MPV) y emboscadas (*Mine-resistant ambush protected*, MRAP) responden a la necesidad de protección específica ante una de las formas más rudimentarias de ataque mediante minas y dispositivos explosivos improvisados (IED) en general.

Se usaron en la Segunda Guerra Mundial, de forma intensiva en Rodesia y contra las fuerzas sudafricanas desde Angola, a Namibia y Zambia durante las guerras de frontera entre 1966 y 1990.

Sudáfrica respondió en 1980 con un vehículo monocasco, el MPV *Casspir*, aún en servicio en varios países y en operaciones de paz de Naciones Unidas. El modelo perfeccionado es el RG-31 *Nyala* de la británica BAE Systems. Más de una docena de países operan actualmente este modelo, entre ellos España.

EE.UU. hubo de abandonar los esfuerzos para reforzar los *Humvees* en Iraq ante el coste humano y la consiguiente repulsa de la opinión pública, para adquirir un diseño que derivó en el MRAP *Cougar*.

Rusia desplegó en Ucrania varios acorazados anti-minas de la familia *Typhoon-K*. Ucrania, por su lado, recibió una entrega inicial en 2022 de 50 unidades del anti-minas turco *Kirpi*.

En Europa, una historia de éxito es el Dingo alemán, en el que nunca ha muerto ningún soldado. En su versión más reciente es un 6x6 de 20 toneladas con capacidad de 12 soldados.

3.1.4. Plataformas de Lanzamiento

Aunque el concepto de lanzar múltiples municiones (proyectiles o cohetes) simultáneamente es antiguo, la primera plataforma con artillería autopropulsada por cohete, *Katyusha*, la usaron los rusos en la Segunda Guerra Mundial, montada en camiones ordinarios. Se trataba de aumentar la potencia de fuego de la artillería convencional; se sacrificaba precisión, pero se contaba con la ventaja de la movilidad.

Los sistemas actuales (*Multiple Launch Rocket Systems*, MLRS), dotados de control digital para guiar la munición y corregir la trayectoria de los cohetes, han probado ser un arma devastadora, no sólo por su capacidad destructiva sino psicológica, por el terror infringido en el área atacada. Pueden cargarse en unos minutos, lanzar una salva de una docena de misiles, y abandonar el lugar antes del contraataque. El alcance varía con los cohetes y/o misiles que puede montar y los objetivos pueden estar en tierra o en el aire (*Self-propelled Anti-Aircraft Artillery*, SPAAA).

Del M142 HIMARS (*High Mobility Artillery Rocket System*) estadounidense se dice que puede alcanzar blancos en un radio de 2 metros. Lanza 6 cohetes en menos de un minuto y misiles como el PrSM (*Precision Strike Missile*), con casi 500 kilometros de alcance. En la guerra ruso-ucraniana se enfrentan en el rango entre 70 y 90 kilometros con el BM-30 *Smerch* ruso. Éste monta cohetes de 300 mm y posee capacidad de guiado por GLONASS (equivalente ruso al GPS). Rusia también cuenta con la plataforma SAM (*Surface to Air Missile*) 50R6 *Vityaz*. China dispone de sistemas SAM HQ-9 a HQ-22, éste último del 2017.

Imagen 3 - Izda: RG-31 Mk5E del Ejército español. Fuente: Ministerio de Defensa de España
Dcha: Kirpi turco, capturado por el Ejército ruso durante la guerra de Ucrania según Bulgarianmilitary.com (Fuente: Twitter).

Imagen 4 - M142 HIMARS estadounidense en la imagen izquierda y varios BM-30 Smerch rusos a la derecha.
Fuente: Armed Forces EU. https://armedforces.eu/compare/rocket_artillery_M142_HIMARS_vs_BM-30_Smerch.

3.1.5. Otros Vehículos

Puede decirse que hay tantas otras plataformas como necesidades a cubrir: vehículos tácticos de alta movilidad (HMTV), vehículos ligeros multipropósito (LMV), de reconocimiento... El LMV de la italiana Iveco (en las fuerzas italianas denominado 'Lince') tiene más de 4,000 unidades producidas y está en servicio en una veintena de países, entre ellos España.

Una categoría especial la constituyen los vehículos de apoyo a la maniobra (como lanza puentes, o grúas) y de apoyo logístico a la maniobra: desde los de asistencia médica y evacuación a los destinados a la recuperación del material que ha resultado inoperativo (*Armoured Recovery Vehicles,* ARV).

En el caso de España, y respecto de las plataformas terrestres en general, no hay un 'suministrador nacional' capaz de satisfacer el grueso de las necesidades. General Dynamics, a través de su filial europea *European Land Systems* (Santa Bárbara Sistemas) en el caso de los vehículos de combate, seguido de IVECO, para vehículos todo terreno, de combate y transporte, son las firmas más representativas. De diseño y fabricación española son los vehículos de Alta Movilidad Táctica (VAMTAC) de la compañía UROVESA -una plataforma versátil de unas 3 toneladas de peso que está en servicio en más de una veintena de países-, y otros equipos de apoyo de la también española EINSA, como el vehículo aerolanzable o mula Falcata, y el ligero para operaciones especiales Neton.

3.2. Plataformas No Tripuladas

Obedecen al intento de minimizar el riesgo humano en el campo de batalla, si desestimamos la necesidad, en su caso, de que los humanos tengan que intervenir para recuperar el vehículo, o lo que quede de él.

Cuando se trata de vehículos terrestres se usan las siglas UGV (*Unmanned Ground Vehicle*), para reflejar que no tienen a bordo a ningún humano y que operan en contacto con el terreno (el equivalente de los UAV -*Unmanned Aerial Vehicle*- en el aire y los UUV-*Unmanned Underwater Vehicle*- en el mar). A menudo se les denomina también robots o sistemas robóticos, independientemente de su forma o tamaño.

> *"Aunque los UGV no disfrutan de la popularidad de los UAV, están igualmente destinados a ser las estrellas de todos los proyectos tecnológicos en las próximas décadas por sus muchas cualidades"*

Se diseñan con el objetivo final de adelantarse, manteniendo a los soldados a una distancia segura del ataque del adversario, aunque pueden configurarse para tareas diversas (de reconocimiento, logísticas, evacuación médica, de combate...), algunas potencialmente letales como la detección, eliminación de explosivos (*Explosive Ordnance Disposal*, EOD) y el despeje de minas. Informan de los datos que obtienen a un operador humano que lo controla de forma remota, pudiendo también incorporar modos de operación totalmente autónoma. El 'Telekino' del español Leonardo Torres Quevedo (1904) parece ser el primer ejemplo documentado de un vehículo controlado a distancia.

Sus desventajas residen en que presentan limitaciones tácticas y dependen de la comunicación con el operador remoto. El Uran-9 ruso, desplegado en Siria, experimentó problemas de cobertura y pérdida de control del operador humano, y el Uran-6, un antiminas operando en la guerra de Ucrania, requiere proximidad con el operador por los efectos de contramedidas electrónicas del adversario, incluso en condiciones favorables, lo que complica su uso táctico.

Por ello, en la última década, la investigación se ha centrado en tres áreas fundamentales:

- la movilidad en terrenos complejos;
- la comunicación en un EMS (espectro electromagnético) disputado;
- y el grado de intervención humana en la operación (hoy el ser humano está generalmente '*in the loop*' al decidir sobre el guiado o el uso de armamento de la plataforma). Desarrollar perfiles de misión autónomos (como regresar a la base por sí mismo) requiere gestionar referencias de navegación.

Si bien la IA puede mejorar el conocimiento de la localización, productos como el LIDAR (*Laser Imaging Detection and Ranging*), que permite medir distancias con un haz láser pulsado, no están aún maduros, amén de no ser totalmente compatibles con la necesidad de no ser detectado.

Rusia ya declaraba en 2015 su intención de desplegar armas cinéticas en plataformas controladas en remoto. Su AT/ARF Marker es un *UGV* de combate dotado de reconocimiento automático de equipos (catálogo de imágenes y AI), lanzador de misiles y UAV, y un largo etcétera de posibles combinaciones de armamento.

El turco FNSS Shadow *Rider*, un UGV de 13 toneladas (indistinguible de un blindado ligero pilotado, a ojos de los no expertos), opera de forma autónoma en misiones de amplio espectro como señuelo, para reconocimiento o apoyo logístico. Como ya hemos citado, la persona está siempre '*in the loop*' en su variante armada (la decisión de hacer fuego no la toma el sistema). La versión israelí para observación e interceptación es el *Guardium Avantguard*, un UGV que ha patrullado sin descanso su frontera con la franja de Gaza desde 2008. El ROBUST (*Robotic Autonomous Sense and Strike*) es un UGV de combate de 5 toneladas del que se desconoce si ha sido probado en combate.

Imagen 5- Robot Marker ruso (Figura: Wikipedia) a la izquierda y el THeMIS (Figura: Milrem Robotics) en la foto derecha.

En **EEUU**, Qinetic desarrollaba el UGV de transporte Titan con Milrem Robotics, creadora del THeMIS. El MULE (*Multifunction Utility/Logistics and Equipment*), un UGV logístico destinado a aliviar los más de 30 kilogramos que un soldado medio carga en operación, pero el proyecto se canceló en 2021 antes de los ensayos finales.

China tiene en servicio el Dragon & Horse II 8x8, un UGV propulsado por turbodiésel de más de 5 metros de largo capaz de transportar 1 tonelada de diversas cargas útiles.

En **Europa** es popular el *THeMIS* estonio, también adquirido por España. Alemania los envió a la fuerza ucraniana a finales de 2022, mientras en Twitter (ahora X) se pudo leer que Rusia ofrecía un millón de rublos a quien le trajera un *THeMIS* en buenas condiciones . Si las fuerzas ucranianas los usan predominantemente para evacuación de bajas (CASEVAC) y desminado de rutas, Rusia da a su *Marker* una misión más prosaica en esa guerra: destruir las plataformas terrestres que Ucrania recibe de la OTAN.

El Ejército español recibió a finales de 2022 el *Small Multipurpose Equipment Transport* (S-MET), una 'mula robótica' (una plataforma de carga) con capacidades de apoyo al combate. Actualmente se están evaluando prototipos como el UGV pesado de combate TRX de General Dynamics.

Cabe mencionar brevemente a los drones (UAVs) con carga de munición 'merodeadora' (*loitering munition*), también conocidos como drones *kamikaze*. En la guerra de Ucrania son los Lancet por el lado ruso y los *Switchblade 300* por el ucraniano (recibidos de EE.UU. en la primavera de 2022).

Imagen 6- Lancet-3 ruso (Foto X)

Una vez el operador activa el objetivo, se guían hasta él de forma autónoma, lo que les hace especialmente efectivos en blancos estáticos.

En septiembre de 2023, las fuerzas israelíes extendieron el uso del dron suicida *Maoz,* con munición merodeadora *Firefly*, de las fuerzas de operaciones especiales a la infantería.

Hoy la tecnología para hacer que sean las máquinas quienes combatan en el lugar de los humanos ya existe. Los robots autónomos (*killer robots*) descansan en su IA para tomar decisiones. Una Directiva del Departamento de Defensa estadounidense, de enero de 2023, pusó por primera vez el foco sobre la autonomía en sistemas de armas, y ello porque un plan de la OTAN sobre sistemas autónomos, de octubre de 2022, disponía como objetivo preservar la ventaja tecnológica de la Alianza en los llamados '*killer robots*'.

Los intentos de limitar su uso a través de la CCW (Convención sobre armas convencionales) han sido frustrados por EE.UU. y Rusia. Tal es el potencial de una tecnología cuyo uso por las grandes potencias puede ser sólo una cuestión de tiempo. Unir IA y armas puede ser el futuro de la guerra.

3.3. Retos de la Operación de Plataformas Terrestres

Idealmente, se pretende disponer de sistemas capaces de combatir durante toda la misión, es decir, transportar, comunicarse, disparar, protegerse y 'sobrevivir'.

Y para ello cada plataforma cubre un abanico, más o menos amplio de tareas, y tiene un entorno operativo para el que fue diseñada y en el que se puede obtener un desempeño óptimo.

En un informe de 1992 sobre la Guerra del Golfo las tripulaciones del MBT Abrams informaban de limitaciones operativas debido a las frecuentes paradas para repostar (alto consumo de combustible y fallos en las bombas) y limpiar los filtros de aire de la arena ambiental. Hubo problemas de repuesto, algunos de los cuales se habían agotado tras las primeras cien horas de combate terrestre. En palabras del personal de logística: *"el sostenimiento podría haberse convertido en un problema serio de haberse prolongado la guerra"*.

3.3.1. Protección vs Maniobrabilidad

La primera capacidad a preservar es la de permanecer en la contienda. De nada sirve poseer alto poder de fuego si la propia supervivencia de la plataforma y su tripulación se ve comprometida más allá de lo razonable.

La vieja lucha entre "lanza y coraza" que llevaba a aumentar el blindaje de los vehículos parece haber cedido paso a otras alternativas.

La detección de la plataforma por el adversario tiene que ver con su 'firma electrónica' (*signature management*), su interacción con diversas formas de radiación electromagnética (EMR) [iv]. Los vehículos militares son a menudo voluminosos y operan a altas temperaturas. Ello permite al adversario detectar su patrón o firma e identificar su naturaleza y localización con el sensor adecuado (el ojo humano, o un radar).

Modificar esta firma para reducir la probabilidad de ser detectado puede lograrse con camuflaje o enmascaramiento de reducción de firma multiespectral (*Mobile Camouflage Systems*, MCS), una cobertura que oculta el vehículo en longitudes de onda del espectro visible y radar infrarrojo, fundamentalmente. La sueca Saab es líder en estos sistemas de protección.

La letalidad y precisión del armamento actuales han forzado una evolución de los sistemas de protección pasiva (materiales cerámicos u otros, entre las capas de blindaje convencional), efectivos ante la artillería convencional, a los de protección activa o APS (*Active Protection Systems*). El M1 Abrams usa blindaje pasivo con uranio empobrecido; el T-90 ruso, uno de los MBT mejor protegidos del mundo, lleva blindaje reactivo Kontakt-5 y protección NBQ. Llegados al punto en que los MBT no pueden ser más pesados (e incapaces, por tanto, de maniobrar, ser transportados o simplemente avanzar en determinados terrenos sin hundirse y volcar), siendo aún vulnerables a cohetes y misiles guiados contra carro, la alternativa es detectar la amenaza y eliminarla antes de alcanzar la plataforma. Son los APS '*hard kill*', entre los que se encuentra el *Trophy* israelí: un sistema de radar activo con 360 grados de protección continua que clasifica la amenaza y activa, en su caso, las contramedidas adecuadas para neutralizarla. Los APS '*soft kill*', en cambio, son contramedidas no destructivas para crear interferencias con la firma del blanco (bloqueando señales infrarrojas o de radar) y reducir así -ahora de forma activa- la posibilidad de ser detectados.

La necesidad de blindados más ágiles y ligeros durante conflictos de estabilización como Afganistán, Iraq o Mali ha favorecido dotar a vehículos 8x8 de sistemas avanzados de protección y ataque para un más fácil despliegue -modelos 'expedicionarios'-, frente a los MBT (que siguen siendo las plataformas de referencia en conflictos de alta intensidad).

Si prima la agilidad para alcanzar el escenario de la contienda, ciertos desarrollos permiten que la plataforma sea transportada por aire y 'lanzada' literalmente al campo de batalla.

Aunque dependen de su control en remoto, los UGV son un ejemplo de versatilidad en cuanto que pueden configurarse para múltiples propósitos, pero cabe recordar sus limitaciones tácticas, además de ser un blanco fácil si no pueden autoprotegerse.

3.3.2. Logística

La frase se atribuye al General Pershing en la Primera Guerra Mundial, *"la infantería gana las batallas, la logística gana las guerras"*. A medida que la contienda se alarga, una base logística más sólida para mantener el esfuerzo bélico de forma ininterrumpida por más tiempo puede inclinar la balanza hacia la victoria. En sentido amplio, toda estrategia requiere de una cadena de suministro que la haga posible.

En la guerra ruso-ucraniana, los medios occidentales señalaban que Rusia, asumiendo una rápida intervención basada en su abrumadora superioridad militar, desatendió una adecuada planificación de su base logística para sostener una guerra prolongada. Así lo afirmaba en un artículo espléndido de 2022 el Coronel Ruiz Arévalo. Tras más de dos años de combates, quizá otros factores externos inclinen la balanza en esta guerra de desgaste.

El primer reto logístico se plantea con el transporte de las plataformas al escenario de operaciones, especialmente si no es accesible -o los vehículos no son aptos- para transitar por carretera y deben hacerse llegar por aire (el C5 Galaxy estadounidense puede albergar solo dos MBT M1 Abrams) o por mar (en barcos *Roll On – Roll Off*). La primera guerra del Golfo marcó el mayor reto logístico para EE.UU. desde la invasión de Normandía. Tropas y equipos fueron embarcados desde más de una treintena de puertos de todo el mundo en más de 500 barcos con destino a Arabia Saudí.

Por su parte, Rusia libra batallas en su periferia, lo que le permite el avance por tierra con una retaguardia capaz de albergar efectos logísticos a, digamos, un máximo de días de abastecimiento de reserva. Sin embargo, en los primeros meses de la guerra ruso-ucraniana, el tránsito a la fase táctica supuso abandonar su potente red de ferrocarriles para encontrar infraestructuras inutilizadas en las fronteras con Ucrania, lo que supuso un auténtico cuello de botella para sus blindados y una falta de medios para trasladar los recursos a vanguardia al ritmo y volumen requeridos.

Toda la cadena logística hacia el teatro de operaciones descansa en asegurar canales de suministro fiables; por ello, las rutas de suministro del adversario constituyen los objetivos prioritarios de cada contendiente. El ataque ucraniano a los puentes en la región de Kherson sobre el rio Dniéper en julio de 2022 obligó a los rusos a construir a toda velocidad un puente flotante que completó ese mismo mes. Los canales de suministro son esenciales para asegurar la energía para operar (el combustible), la munición y la capacidad de reparación necesarias en tiempo y forma para sostener el ritmo de las operaciones.

Disponer de resiliencia logística, es decir, clase VII según la doctrina logística de operaciones (armamento, material y animales, -recursos completos-) para realizar intercambios directos con las unidades de combate a medida que sus medios quedan inoperativos o son destruidos, es clave para mantener las capacidades operativas durante todo el conflicto.

Respecto de la munición, la guerra en Ucrania la ha quemado a un ritmo mayor del que EE.UU., el mayor donante de ayuda militar al país, puede producirla. En el primer trimestre de 2023, sólo un año después de la invasión rusa, las existencias estadounidenses de misiles tierra-aire *Stinger*, obuses y munición de 155 mm y misiles contra carro *Javelin* se habían agotado. Con un consumo de más de 30,000 proyectiles diarios -EE.UU. produce 11,000 al mes- , una logística a una escala industrial similar no se había visto desde la última guerra mundial. Ucrania disponía de munición de 152 mm de la era soviética, pero la guerra del Donbás desde 2014 dejó al país con posibilidad de enfrentar la invasión rusa durante un par de meses como mucho.

El Pentágono ha destinado fondos desde 2022 para ampliar su capacidad de producción, tanto de proyectiles como misiles, debiendo simultáneamente reponer munición en sus propios almacenes, todo lo cual sin que EE.UU. esté técnicamente 'en guerra' con nadie.

En cuanto a Rusia, también ha sufrido la merma de munición, pero es el segundo mayor suministrador de armamento a nivel mundial tras EE.UU. y parece probado que ha recibido de Irán y e otros de sus aliados munición y equipamiento.

Tampoco la industria europea está dimensionada para una producción que ya se había contraído las últimas décadas por la caída de la demanda, lo que, en casos como España, provocó que la industria de munición propia pasara a manos de compañías extranjeras.

3.3.3. Operabilidad e Interoperabilidad

En sistemas no tripulados se han mencionado retos a la operabilidad (capacidad de sortear obstáculos o la contaminación del área con otras frecuencias, entre otros). Son sistemas vulnerables al control del ciberespacio por el adversario, y sin los enlaces de comunicaciones el sistema carece absolutamente de utilidad. La IA, junto con sistemas de aprendizaje automático o ML (*Machine Learning*) para reconocer objetos y personas, abre el camino a la operación en modo autónomo (*man off the loop*), pero existe un obstáculo adicional: simplemente no se dispone de procesos de evaluación o certificación para probar que incluso el más básico UGV con funciones autónomas sea capaz de operar correctamente y con seguridad en entornos favorables, mucho menos en entornos complejos y hostiles (algo

En el terreno de la interoperabilidad, el reto es conseguir la capacidad de múltiples sistemas para permitir el intercambio de información y uso de la misma.

parecido pasa con los coches sin conductor en el mundo civil). No obstante, la capacidad de estos sistemas para comunicarse y operar de forma cooperativa entre ellos y con el ser humano es uno de los aspectos clave de las futuras operaciones militares y en general de la doctrina militar.

La interoperatividad supone que las fuerzas multinacionales puedan interactuar e interconectarse a través de distintas plataformas y medios, desde sensores a armamento, desde el soldado a su UGV o robot más cercano. Hablamos de que sistemas de distinta creación y con distintos datos sean capaces de comunicarse bajo un estándar común y sin errores. Integrar tecnologías a nivel multinacional para mejorar las capacidades, planes y operaciones dentro de la OTAN será un proceso lento, aunque se ha dado un impulso reciente a iniciativas como el Programa SPS (*Science for Peace and Security*) .

Adicionalmente, la mera implementación de la IA en los sistemas militares presenta retos en sí misma. Si humanos y máquinas deben trabajar en equipo, la cantidad de información que los futuros sistemas pueden recopilar en tiempo real será difícil de procesar por el cerebro humano sin ayuda. Las posibilidades, sin embargo, parecen infinitas.

4. RETOS PARA LA IMPLEMENTACIÓN DE LA NUBE DE COMBATE EN EL ÁMBITO TERRESTRE

Una iniciativa para la implementación de la nube de combate multidominio, esa red de información que conecta fuerzas aéreas, terrestres, marítimas, espaciales y cibernéticas, es el JADC2 (J*oint All-Domain Command and Control)* del Departamento de Defensa estadounidense. Conectando sensores y dispositivos de los sistemas a través de todos los ámbitos en una 'red de redes' integrada, se persigue mejorar las capacidades de mando y control (C2) para tomar decisiones y actuar a todos los niveles y fases del combate en tiempo real. La aplicación de IA y ML responden a la necesidad de gestionar la avalancha de datos de inteligencia, vigilancia, adquisición de objetivos y reconocimiento (ISR); analizando, distribuyendo y compartiendo la información en cada etapa del conflicto.

Implementar esta nube de combate supone también, por tanto, comunicar redes tácticas que cada fuerza ha desarrollado y operado en cada ámbito, con tecnologías específicas en cada caso.

En el ámbito terrestre, la conectividad a nivel táctico depende del desarrollo de redes MANET (*Mobile Ad hoc Network*) con cuatro características generales: fuerte conectividad, ancho de banda de muy alto nivel, seguridad y capacidad de supervivencia. La red se mueve a medida que lo hacen los nodos, pudiendo perderse los enlaces punto-a-punto por interferencias del terreno o por salir del alcance de otros nodos. Los soldados no pueden esperar minutos -a veces, ni siquiera segundos-, a que la red se estabilice. La amenaza del ciberataque electrónico y la operación en entornos EMS (espectro electromagnético) extremadamente restringidos pueden degradar o anular la transferencia de información y, consecuentemente, las decisiones y acciones derivadas. Además de poder direccionar la información en el menor tiempo posible, ésta deberá ser encriptada para controlar las amenazas y prevenir intrusos, mediante cortafuegos y otros elementos de gestión del tráfico.

El Ejército estadounidense viene trabajando en el concepto de una Red Táctica Integrada (ITN) con personal de mando y control, comunicaciones y computación y ciber-tecnología. Frente a la comunicación vía satélite más allá de la línea visual (*Beyond Line-of-sight*, BLOS), un sistema en modo alguno sencillo de operar que no está disponible siempre, la ITN busca combinar radio en la línea visual con nodos de comunicación satelitales fuera de ella.

En cuanto a la implementación de estas redes en una única nube de combate multidominio, a los retos del control del espectro electromagnético y la seguridad de la información se añade la interoperabilidad en el tratamiento de datos provenientes de distintas fuentes, algunos de los cuales serán compartidos, mientras que otros serán de uso exclusivo para ciertas unidades.

Existen iniciativas en todos los ejércitos relativas a la transformación digital, que harán realidad conceptos como la nube de combate y la posibilidad de conectar humanos y sistemas a redes inteligentes.

El **Ejército español** requiere de la necesidad de adquirir una nube táctica con capacidad para establecer redes 5G, una tecnología que puede habilitar nuevas capacidades operativas y facilitar un mando y control más eficiente. Cuenta desde 1996 con el Regimiento de Guerra Electrónica 31, encaminado al dominio del espectro electromagnético en beneficio de nuestras fuerzas en todas las operaciones en las que participe.

5. APLICACIÓN DE LAS NUEVAS TECNOLOGÍAS A LA LOGÍSTICA PREDICTIVA Y A LA SIMULACIÓN PARA EL ADIESTRAMIENTO

En otros capítulos de este trabajo se han introducido las nuevas tecnologías, entre ellas la IA o la robótica, a las que hemos hecho referencia también en este capítulo de capacidades terrestres. En este apartado se expone brevemente la importancia de estas tecnologías para afrontar el reto de la logística militar y del adiestramiento de las fuerzas terrestres.

5.1. La Logística Predictiva

La capacidad de prever posibilita atender necesidades futuras antes de que se evidencien, y permite disponer los medios dónde y cuándo sean necesarios, limitando la disrupción en las operaciones y aumentando la disponibilidad y fiabilidad de los medios, lo que revierte en una mayor eficiencia del conjunto de las capacidades terrestres. En suma, el reto es gestionar anticipadamente los riesgos a los que potencialmente se enfrentará la cadena de suministro. A este reto se pretende dar solución a través de lo que se ha denominado, logística predictiva, que se aplica en prácticamente todos los sectores de la industria, además de en el sector de la defensa.

Todos los ejércitos usan herramientas de gestión logística de mayor o menor grado de sofisticación, la más básica consistente en la identificación y registro de los activos, posiblemente su estado o condición, su localización y algún dato para predecir necesidades de mantenimiento. La información de suministros podrá incluir, por ejemplo, el nivel de almacenes (de combustible, de munición) a corto y medio plazo.

Una herramienta que controle, no sólo el mantenimiento de cada sistema de armas, sino las necesidades logísticas de todo un ejército, supone gestionar una cantidad de información mucho mayor. Analizarla para detectar patrones, predecir comportamientos y prever necesidades es algo inaccesible a la mente humana.

Aquí entra en juego **la Inteligencia Artificial.**

La IA permite combinar elementos como el *Big Data* o la capacidad de las computadoras para aprender sin instrucciones explícitas, mediante algoritmos y modelos estadísticos (ML). Al fin y al cabo, para el *software* de logística predictiva, la realidad es un conjunto más o menos grande de objetos del que se obtienen -y, en ocasiones, hacia el que se envían- datos.

La complejidad para dotar a los sistemas de IA de capacidades humanas (percepción visual, reconocimiento de voz o toma de decisiones) está asociada al tipo y nivel de información que es necesario obtener para su proceso posterior. Pensemos en un destacamento dotado de vehículos y sistemas con sensores y comunicaciones. Sólo pueden transportar lo indispensable para su operación y deberán conocer exactamente cuándo y dónde reabastecerse. Otra unidad soltará los suministros, que aquellos encontrarán mediante sensores y coordenadas, todo sincronizado para evitar la detección y el ataque. Quizá un vehículo se averíe o sufra daños. Sin previsión, se desconoce si la decisión correcta es abandonarlo y continuar la operación, o invertir recursos en su reparación. Detrás de todos estos movimientos hay decisiones que deben tomarse de forma inmediata en el teatro de operaciones teniendo en cuenta gran número de variables y factores.

La aproximación a la logística predictiva por los ejércitos consiste básicamente en diseñar una estrategia en torno a las necesidades actuales y potenciales, y trabajar con expertos en las nuevas tecnologías para configurar un sistema capaz de alcanzar los objetivos de predicción de la forma más simple y práctica.

Palantir Technologies fue seleccionada en 2022 por el Ejército estadounidense para optimizar la cadena de suministro y el mantenimiento predictivo. Su *software* integra datos de suministros, sensores y mantenimiento, partiendo de sistemas existentes, para permitir un aprovechamiento más eficiente de sus activos globales.

España presentó en 2022 el proyecto de Sistema Integrado de Logística Predictiva del Ejército (SILPRE). Una vez desarrollado, será capaz de predecir el comportamiento y estado futuro de los materiales de las fuerzas terrestres, permitiendo la máxima disponibilidad operativa de los sistemas de armas con el mínimo coste. Se planean varias etapas: instalación de sensores para captar datos de los vehículos, repositorio de datos en la base logística, análisis con IA para establecer modelos de predicción, y aplicación de los modelos con automatización de procesos de mantenimiento.

Una herramienta de logística predictiva para apoyar los procesos logísticos de movimiento y transporte estratégicos, planeamiento y ejecución de despliegues, programación de movimientos en el teatro de operaciones y planeamiento del sostenimiento es el *software* LOGFAS (*Logistics Functional Area Services*) de la Agencia de Comunicaciones e Información (NCIA) de la OTAN. Se integra con un sistema de posicionamiento (basado en GPS, normalmente), lo que permite seguir los movimientos del material.

China ha desplegado soluciones de IA para mantenimiento y logística, incluyendo *software* de diagnosis y pedidos electrónicos (almacenes inteligentes), de la mano de Anwise Global Technology, el mayor fabricante de equipos inteligentes del país, centrado en electrónica y tecnologías aeroespaciales.

5.2. Tecnologías de Simulación para Adiestramiento

Una simulación imita la operación de procesos o sistemas del mundo real mediante modelos. Para simular el efecto de un aterrizaje sobre el tren de un avión pueden colocarse martinetes hidráulicos (en un banco de ensayos, por ejemplo), consiguiendo así un simulador físico donde el esquema teórico se expresa con un algoritmo que dicta la cantidad de presión a aplicar en cada instante para replicar la misma carga que sufre el tren en la realidad. En un grado de abstracción mayor, no es necesario disponer del tren ni de los martinetes; el esquema teórico (el modelo) parte de conocer en cada caso la reacción de los componentes del tren (ruedas, amortiguadores) y se expresa con un algoritmo que realiza la secuencia completa de golpear contra el suelo en un programa informático. La simulación es la ejecución de ese modelo (en el tiempo).

El potencial de la simulación es enorme, fundamentalmente por proporcionar al ser humano la posibilidad de realizar acciones sin los riesgos que conllevaría realizarlas en el mundo real. No hay sector, desde la ingeniería civil o las telecomunicaciones, pasando por la biología o la medicina, a las aplicaciones militares, que no haga uso de esta potente herramienta en alguno de sus procesos.

La simulación para adiestramiento militar, en particular, representa un modo único de reproducir situaciones de combate reales sin riesgos de lesiones y sin el coste operacional que supondría realizarlo en un entorno real, además de no estar limitado por las condiciones meteorológicas.

Descansa, por lo general, en un *software* para crear una maqueta visual del entorno y proceso a simular, pudiendo incluir elementos del mundo físico o no. El mundo real contiene infinidad de objetos e innumerables relaciones entre ellos. El reto tecnológico es proporcionar al ser humano una sensación todo lo más parecida a aquél. La realidad virtual (VR) permite construir una réplica tridimensional para que el ser humano pueda interactuar a través de sus sentidos, mediante dispositivos a tal efecto (cascos, gafas, guantes…). La realidad aumentada (AR) superpone elementos digitales a imágenes y localizaciones del mundo físico. La combinación de elementos de VR y AR se ha denominado realidad mixta (MR).

El manejo de las relaciones entre los objetos, -éstos toman acciones de forma autónoma y como consecuencia de la interacción con el ser humano- y, en general, de los procesos que tiene lugar en la simulación, se ha conseguido por el aumento de la capacidad computacional, que permite usar múltiples procesadores en una única computadora e incluso interconectar, en una misma red, múltiples simulaciones.

Un trabajo de la Universidad de Ingenieros del Ejército de Shijiazhuang en China define el adiestramiento con simulación como "u*n proceso que usa tecnología moderna de simulación basada en tecnología computacional, tecnología de realidad virtual, tecnología de simulación distribuida, y tecnología de IA, para simular la actuación de sistemas de armas, el entorno, el oponente, la misión y el proceso de combate con un alto nivel de fidelidad, lo que permite al equipo y a los alumnos sentir la atmósfera próxima al combate real, y maximizar su nivel de adiestramiento".*

Clasifica el adiestramiento militar con simulación según los diferentes niveles de aplicación:

- **Habilidades para operar y mantener el equipo o sistema**: busca simular su operación o el proceso de mantenimiento (desde la detección o previsión del fallo, análisis y eliminación).

- **Adiestramiento táctico:** refiere al mando de combate y ejercicios en torno a tareas de combate específicas, y suele acometerse con simulación real. Un club de *paintball* se transformó en 2014 para proporcionar a las fuerzas ucranianas adiestramiento táctico de combate.

- **Adiestramiento estratégico:** ayuda a los mandos a tomar decisiones estratégicas y a formar una manera de pensar estratégica. Se desarrollan modelos de simulación constructivos de planes militares, incorporando a veces factores sociopolíticos. A menudo se les refiere como 'juegos de guerra'.

En la primera categoría se encuentra el *software* de simulación de operación y mantenimiento que ofrece la mayoría de fabricantes de sistemas de armas.

Respecto a los simuladores de adiestramiento táctico, compañías como las estadounidenses Virtra y Sentient Digital, la australiana Bohemia Interactive, o Zen Technologies en la India, ofrecen esta clase de productos cuyo objeto principal es desarrollar las habilidades del soldado, esto es el soldado en preparación. De igual forma surgen a menudo adaptaciones militares de juegos comerciales ('*serious games*') como el *Steel Beasts* de la estadounidense eSim que usa el Ejército español para adiestramiento de plataformas terrestres. La frontera entre simuladores de juego y adiestramiento es a veces difusa, pero la finalidad los distingue claramente. La compañía china *DataExa* ha desarrollado un simulador de combate basado en IA e inspirado en el AlphaStar, programa de la británica DeepMind que reproduce el videojuego *StarCraft II*. A la postre, se trata de una competición de ingenio y recursos en los que ambos contendientes intentan prevalecer.

En cuanto a los "juegos de la guerra" propiamente dichos (adiestramiento estratégico y operacional), Rusia tiene difícil la exportación de sus productos de simulación debido al embargo. RPA RusBITech JSC ofrece soluciones de alta tecnología, integrando simuladores de armamento y equipo militar en un único campo de batalla virtual multidominio para adiestramiento en planeamiento operacional, reconocimiento, control y comunicación. En este sentido, está en línea con el proyecto de simulación distribuida (*Mission Training through Distributed Simulation*, MTDS) de la OTAN , para el adiestramiento colectivo en un mismo entorno de simulación. El reto tecnológico es la estructura capaz de albergar los distintos requisitos, estándares de interoperabilidad y patrones, a través de todos los ámbitos (tierra, mar o aire). En el ejercicio MTDS a gran escala de 2017 participaron las fuerzas aéreas de Alemania, Canadá, Noruega y Francia, con presencia de AWACS estadounidenses, objetivos en tierra y guerra electrónica. Salvo por la batalla real en el aire, la mayoría de los objetos eran de simulación constructiva. Aunque es viable conectar simuladores heterogéneos en misiones multinacionales, se reconoció que alcanzar cierto grado de madurez en estos ejercicios tomará tiempo.

6. ALGUNAS REFLEXIONES FINALES

Las acciones de las fuerzas terrestres en el campo de batalla han estado siempre marcadas por las características de los medios (vehículos, armamento, material…) disponibles ocultando cada bando en lo posible cualesquiera nuevas tecnologías que pudíeran conferirle una ventaja. Así ocurrió desde el uso de la espada y su perfeccionamiento, según la capacidad del ser humano de fundir los metales, hasta el mencionado *"tank water"* que camuflaba al carro de combate.

Quizás, lo novedoso de nuestros días es la velocidad con que se producen hallazgos en las tecnologías disponibles y su posible aplicación a las plataformas terrestres. En este sentido, la búsqueda de ese material ligero que sea tan resistente como el pesado como para que pueda armarse y protegerse adecuadamente, sigue siendo un campo de estudio, entre otros. A ello hay sin duda que añadir el salto que se ha producido en la automatización y robotización de las plataformas, visualizándose ya en el imaginario colectivo dedicado a la defensa una serie de combates, sobre todo a vanguardia, protagonizado por máquinas, o quizás mejor por humanos no biológicos (según palabras de Ray Kurzweil en su obra "La Singularidad está cerca"). Este escenario nos dirige a la importancia del dominio cibernético, donde discurren todas las señales que se transformarán en información, decisión y acción, y quien lo controle dispondrá de una clara ventaja militar.

Para lograr esto y satisfacer los requerimientos operativos necesarios habrá que hacer una fuerte inversión en I+D+i con objeto de que esa otra parte de la defensa, la industria, oriente sus esfuerzos a esas necesidades y saque provecho de todos los avances tecnológicos actuales que son de aplicación al sector defensa.

Invertir en I+D es beneficioso para la defensa e impacta positivamente en lo industrial, económico y social.

Los retos que supone la digitalización del ámbito terrestre en las operaciones multidominio son enormes, pero estamos ante la oportunidad de focalizar bien nuestras inversiones en estos momentos de crecimiento presupuestario, haciendo converger a todos los sectores industriales de la sociedad, entendiendo que el conflicto que estamos librando no es sólo cuestión de defensa, nos afecta a todos y todos debemos prepararnos para enfrentarlo y superarlo.

REFERENCIAS

1. Fehrenbach, T. R. (1963) This Kind of War. A Study in Unpreparedness. Nueva York: Macmillan Publishers.

2. Williams, Ian. Ian Williams, "The Russia – NATO A2AD Environment," Missile Threat, Center for Strategic and International Studies, January 3, 2017, last modified November 29, 2018, https://missilethreat.csis.org/russia-nato-a2ad-environment/.

NOTAS FINALES

[i] Ambos conceptos están relacionados y pueden superponerse; en esencia A2 implica generalmente capacidades de largo alcance para prevenir la entrada a un área operacional (defensa antiaérea, misiles balísticos y de crucero, fuego de largo alcance y artillería, armas de destrucción masiva, actividades de (des)información) y AD de corto alcance, para limitar la libertad de acción en un área operacional (técnicas de combate de guerrilla y, en confrontación directa, artillería, minas, agentes químicos, biológicos, radiológicos y nucleares).

[ii] En palabras del General Enseñat y Berea: "que los escalones subordinados asuman iniciativas y responsabilidades teniendo como frontispicio el cumplimiento de la misión y, por último, velocidad de operaciones, tanto en la toma de decisiones como en la ejecución de las mismas".

[iii] Busca integrar armas diferentes para el beneficio mutuo (por ejemplo, usar infantería y blindados en un ambiente urbano, donde ambos se apoyan mutuamente), frente a unidades militares con un único tipo de soldado o sistema de armas.

[iv] Ondas a veces visibles, -de la superficie de un carro de combate o de un arma-, a veces invisibles -ondas de radio o infrarrojas, reflejadas, emitidas o absorbidas por los objetos-.

BIOGRAFÍAS

VIOLETA RUIZ ALDEA

Ingeniero Aeronáutico por la Universidad Politécnica de Madrid, con estudios de posgrado en gestión de negocio por la Escuela de Organización Industrial y la Universidad de York en el Reino Unido, y una maestría en Economía por la Universidad Francisco Marroquín.

Ha trabajado desde 1990 para diversas compañías nacionales y multinacionales en el sector aeronáutico y de la energía, desde fabricantes de motores a líneas aéreas, con funciones y responsabilidades que van desde ingeniería de soporte, gestión de cartera de clientes y operaciones, desarrollo de negocio y comercial, a estrategia y consultoría, interactuando en ocasiones con el Ministerio de Defensa desde la industria.

Actualmente presta asistencia comercial y financiera a la Subdirección de Programas de la DGAM dentro de la Oficina de Programa del Sistema de Armas A400M de transporte estratégico para el Ejército del Aire y el Espacio.


705

CAPÍTULO 4

Capacidades Navales

Alberto Domínguez Abecia
Fernando Javier Senent Gómez

En este capítulo se presentan, de un modo divulgativo, las capacidades europeas y de las principales potencias mundiales, en el ámbito marítimo, con el principal objetivo de identificar las fortalezas y debilidades de la UE y determinar los principales campos de actuación de la industria de defensa europea en los próximos años.

Se inicia el capítulo hablando de cómo se prevé la evolución del combate naval hacia el conflicto multidominio, para posteriormente analizar las plataformas navales, tanto en su estado actual como en su evolución prevista y necesaria para poder afrontar los nuevos desafíos en zonas de conflicto.

Por su importancia en multidominio, también se desarrollan sendos apartados sobre la contribución de la futura nube de combate naval y los gemelos digitales de plataformas navales en el ámbito marítimo.

Finalmente, en las conclusiones se exponen una serie de consideraciones para mantener o impulsar las capacidades europeas dentro de un entorno mundial muy competitivo.

1. EVOLUCIÓN DEL COMBATE NAVAL HACIA EL CONFLICTO MULTIDOMINIO

En el ámbito de actuación marítimo, las Marinas de Guerra, se han centrado durante los últimos 20 años en ejecutar acciones que permitan conseguir influencia y efectos en tierra. Sin embargo, en virtud de su necesidad de expandir su acción en aguas nacionales e internacionales, estas van regresando a la guerra naval para la culminación de sus objetivos estratégicos, a un tipo de escenario que no se ha presentado en tiempos recientes. Afrontando de esta forma un combate en la mar en el que estén involucradas diferentes plataformas propias y adversarias.

La guerra naval toca quizás más ámbitos de actuación que cualquier otro tipo de enfrentamiento, ya que se extiende desde el espacio, pasando por el aire, y desde la superficie del mar hasta el propio lecho marino, además de las zonas litorales que son escenario de operaciones anfibias. Esta singularidad hace del combate naval un caso de estudio ideal a la hora de examinar cómo la innovación tecnológica afecta a los sistemas de combate y cómo éstos, a su vez, pueden integrarse eficazmente como parte de un Sistema de Sistemas (SoS), es decir, un enfoque multidominio.

Para que una determinada Marina de Guerra alcance la eficacia y la capacidad de supervivencia exigidas en escenarios de conflictos de alta intensidad, a gran escala y multidominio, cada vez más competitivos, es necesaria una importante inversión en sistemas de combate que los mantengan a la par de los rápidos avances tecnológicos de la industria actual, mejorando la integración entre activos y la comunicación de datos.

A medida que las tecnologías emergentes y disruptivas (Inteligencia Artificial (IA), Internet de las Cosas (IoT) y Big Data (BD), blockchain, robótica y sistemas autónomos, tecnologías cuánticas, biotecnologías, armas hipersónicas y nuevos materiales) se introducen en el campo de batalla moderno, el combate se desarrolla cada vez más en un entorno multidominio y la guerra naval no escapa a esta tendencia.

Dada su importancia estratégica en el contexto geopolítico actual, el ámbito marítimo se ha convertido en un polo tractor para la innovación.

Los sistemas de combate naval engloban todos aquellos elementos como sensores, actuadores, mando-control y comunicación que contribuyen directamente a las operaciones ofensivas y/o defensivas navales.

Abarca desde misiles, torpedos, artillería naval con munición guiada, aeronaves de guerra anti-submarina (ASW) y anti-superficie (ASuW), tripuladas o no; hasta los sensores necesarios para la detección e identificación de amenazas, los sistemas no tripulados, que amplían el alcance de un buque de guerra, y, en un futuro no muy lejano, las armas de energía dirigida (DEW) y sistemas hipersónicos.

Tanto el desarrollo de las DEW (incluidos láseres) como de sistemas hipersónicos (misiles que alcanzan velocidades iguales o superiores a Mach 5), tendrán gran efecto en los próximos escenarios de guerra naval, ya que la mejora en la rapidez y precisión de este tipo de armas acortará significativamente el tiempo de respuesta y toma de decisión, y repercutirá poderosamente en el futuro diseño de los ejércitos.

Centrándonos en estos dos últimos sistemas, el Proyectil de Híper Velocidad (HVP) es una nueva concepción de munición de gran calibre diseñada para el empleo en múltiples misiones. Este proyectil tiene un menor peso y una menor resistencia aerodinámica, lo que permite una alta velocidad inicial, maniobrabilidad y un intervalo de tiempo de disparo reducido. También ha incorporado componentes electrónicos que permiten un guiado preciso, convirtiéndolo en un proyectil de próxima generación capaz de adaptarse a las futuras amenazas de la guerra antiaérea y de superficie. Este proyectil reconfigurará la geometría del espacio de batalla e implicará el desarrollo de nuevas contramedidas y sistemas complejos de detección y alerta temprana multidominio.

Por su parte, el primer DEW en el ámbito marítimo fue desplegado en el año 2014 en el buque USS “Ponce”, transporte anfibio de la US Navy. La tecnología utilizada, de concentración masiva de fotones sobre un blanco, es ahora el arma más rápida que se haya creado para destruir objetos atacantes al disparar a la velocidad de la luz (Ref. 1X, 3X). Al operar en la parte invisible del espectro electromagnético, es un arma insonora e invisible y con una precisión única, pensada por el momento para derribar aeronaves y neutralizar lanchas rápidas. Este sistema de arma láser (LaWS) tiene un alcance de entre 1

y 10 millas (dependiendo de la potencia) y requiere de su propio sistema de generación de electricidad, pero tiene un reducido coste operativo, al no requerir ni munición ni una dotación específica de varias personas para su operación/mantenimiento. El LaWS promete ser una tecnología que se ampliará a todo el espectro bélico en el futuro, aunque su desarrollo no está exento de dificultades (movimientos del buque, mantenimiento de los disparos sobre objetivos en movimiento y de alta maniobrabilidad, etc.)

Además de los dos ejemplos anteriores, la artillería naval también está evolucionando rápidamente con otros nuevos diseños de alcances cinco veces mayores que los actuales y con capacidad de integración en operaciones multidominio. El Cañón de tipo Riel Electromagnético (EMRG) pretende destronar a los cañones retráctiles por medio del uso de la energía pulsada, proporcionada por un sistema de carga de condensadores que crea una alta corriente (8 a 32 MJ) a través de dos carriles conductores paralelos que generan el disparo. El EMRG (Electromagnetic Rail Gun) y la munición HVP antes mencionada, prometen combinarse para lograr alcances en artillería muy superiores a los actuales, con especial relevancia para el combate de superficie y misiones de bombardeo y fuego de apoyo naval sobre tierra. Este cambio sustancial requerirá en el futuro de una adecuada preparación de personal de operación y mantenimiento. Asimismo, deberán crearse nuevas doctrinas para su empleo, suponiendo también un desafío para la realización del entrenamiento y ejercicios de artillería a máxima distancia.

Por otra parte, **la robótica y la IA podían ser la llave para hacer frente a ciertos riesgos como los que afectan a las redes de comunicaciones y la autonomía de la toma de decisiones de Sistemas Marítimos No Tripulados (UMS).** No obstante, en esta área existe un debate en Occidente en el entorno de la ética y de la legalidad sobre su utilización en el conflicto y el riesgo de que tales tecnologías lleguen a estar disponibles por adversarios que no hacen frente a restricciones similares.

En relación con vehículos de apoyo, las principales potencias navales (EEUU, Reino Unido, Rusia, Francia, China, etc.) han integrado en sus flotas vehículos no tripulados (UV) embarcados, que tienen la ventaja de un menor coste de adquisición/operación, mejor rendimiento y mayor flexibilidad frente al helicóptero embarcado convencional. La implementación de las tres dimensiones (aire, superficie y submarina) de los UV requerirá de una nueva estructuración de las fuerzas, nuevas doctrinas, configuración de sistemas (mando y control, logístico, etc.) y tácticas que cambiarán la actual naturaleza del espacio de batalla naval. A nivel estratégico, permitirán optar a diferentes soluciones de planificación, desarrollo y empleo de fuerzas. El impacto principal de estas tecnologías en la guerra naval, en los niveles operacionales y tácticos, redundará en el aumento de las distancias tácticas en la geometría del combate, en un mayor tiempo de persistencia de medios en las áreas de operaciones (no limitados por factores humanos) y en una menor intervención humana en el combate a medida que se desarrolle aún más la IA.

El empleo de Sistemas Aéreos no Tripulados (UAS) en buques de medio y gran porte (fragatas y buques anfibios) operando en forma independiente o en pequeños grupos de superficie (SAG) implicará una serie de ventajas, no sólo en cuanto a mejorar el conocimiento de la situación táctica, sino que también en cuanto a optimizar una serie de factores logísticos que requieren las aeronaves embarcadas.

Existen también desventajas en el empleo de UAS como limitaciones operacionales en malas condiciones climáticas, dependencia sobre comunicaciones satelitales para largas distancias de operación, menor capacidad de carga de combate, etc. Por este motivo algunas Marinas de Guerra están empleando las aeronaves embarcadas en forma híbrida, es decir, un helicóptero tradicional junto a un UAS. Este es el caso, por ejemplo, de la US Navy en sus unidades de combate litoral (LCS) y de la US Coast Guard en sus unidades clase Legend que están operando el helicóptero no tripulado UAS MQ-8B Fire Scout junto al helicóptero Sikorsky SH-60 Seahawk.

Centrándonos ahora en el caso de las futuras fragatas F-110 españolas, está previsto que dispongan de un hangar y una cubierta de vuelo en popa desde la que podrán operar helicópteros y UAS. Las F-110 también incorporarán, junto al hangar, un espacio multi-misión que permitirá albergar contenedores y equipos de apoyo desplegables para vehículos aéreos, de superficie o submarinos no tripulados.

Y considerando todo lo anterior es importante destacar el gran impacto que pueden tener los ciber-ataques y, en consecuencia, la necesidad de la ciberdefensa. Las armas basadas en tecnología ciber tienen un potencial impacto estratégico con ataques que pueden inhabilitar infraestructuras navales críticas. Esto concede un poder desproporcionado a estados, o a actores no estatales, militarmente débiles. Parte del reto de este nuevo teatro de operaciones lo constituye la reducción del tiempo de aviso y las dificultades de conocer con una razonable certeza la procedencia de los ciberataques que difuminan la distinción entre guerra y paz. Las misiones en el ciberespacio serán

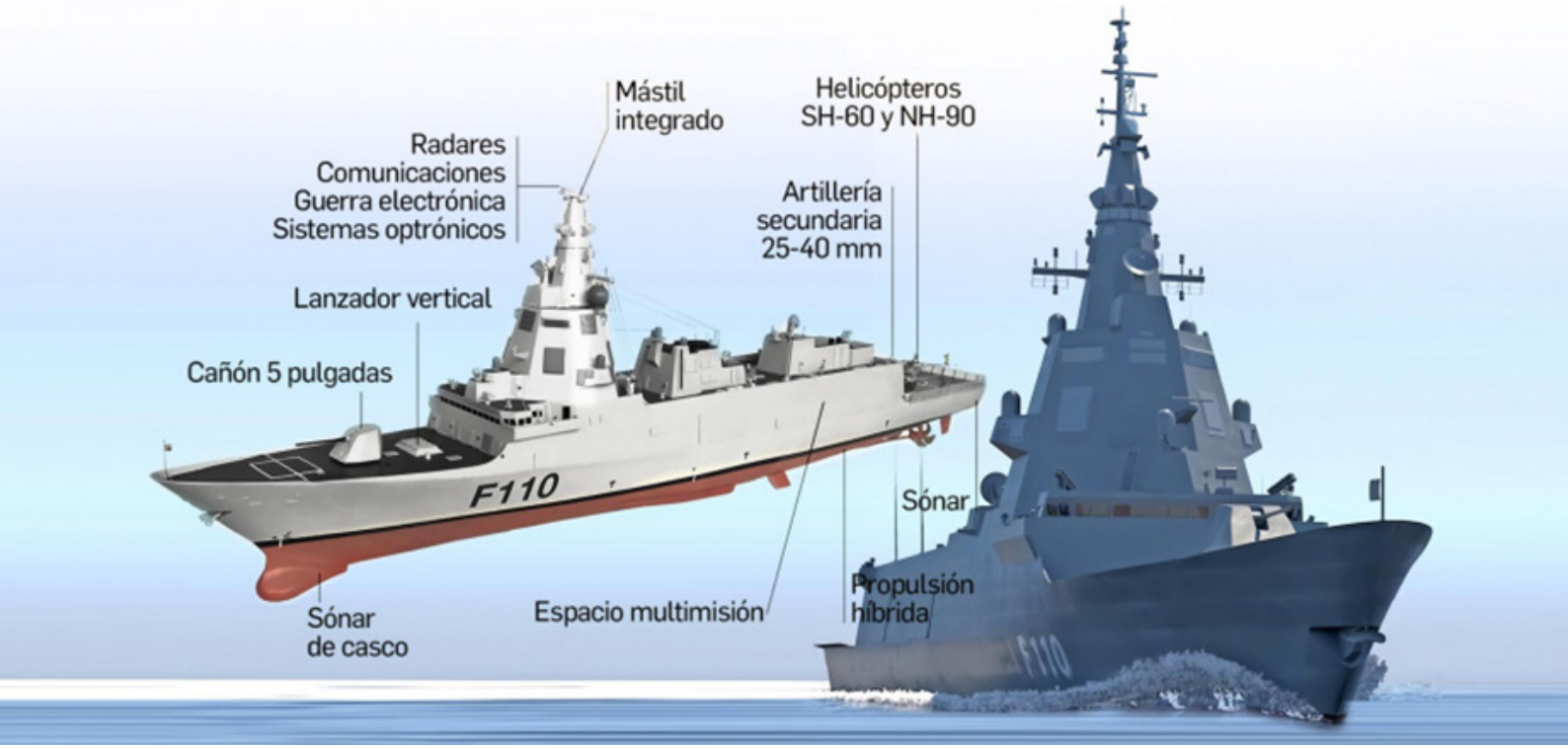


Imagen 1 – Fragata F-110 - Capacidades. Fuente: www.eldebate.com, 19 marzo 2022

también una parte integral de las futuras operaciones militares marítimas.

En España, los nuevos programas de adquisición de plataformas navales ya incluyen importantes capacidades de ciberdefensa. En este sentido, las empresas Navantia y Telefónica Tech han comenzado a trabajar en el desarrollo de un sistema de ciberseguridad reforzado para los submarinos de la clase S-80 y las Fragatas F-110 en estrecha colaboración con el Ministerio de Defensa. Esta solución de ciberdefensa nace con los estándares más exigentes en esta materia y dotará, a los principales sistemas, de protección ante ciber-ataques o intentos de intrusión. Además, podrá monitorizar, en tiempo real, el funcionamiento del sistema de combate, el sistema integrado de control de la plataforma y el sistema de comunicaciones, alertando ante la detección de cualquier posible amenaza. Estos sistemas permitirán la realización de análisis forense, que posibilitará el estudio de las incidencias para identificar su procedencia, el grado de la amenaza y el mecanismo usado para la intrusión para adoptar las acciones correctivas pertinentes.

Y finalmente, en el campo de la conectividad, la gestión de datos de alta tecnología y la integración de diferentes sensores de las fuerzas conjuntas mejorarán la capacidad de los buques para reaccionar ante ataques directos. La Capacidad de Enlace Cooperativo (CEC) es una red táctica automatizada en tiempo real diseñada en la última década que permite el control integrado de las armas a nivel conjunto y que compila todas las detecciones de radar disponibles para generar un panorama común en toda la fuerza. Así una unidad de superficie podría lanzar un misil antiaéreo sobre un misil enemigo lanzado desde tierra hacia una fuerza naval con la información de seguimiento proporcionada por una instalación en tierra. Esta nueva generación de sistemas data link y de mando y control automatizados permitirán una mayor integración de las distintas fuerzas navales, terrestres y aéreas en un teatro conjunto. Esta

tecnología actualmente se encuentra en desarrollo y será implementada en el medio plazo en las Marinas de Guerra de países desarrollados.

Sin duda, en el nuevo entorno multidominio, es la integración de los sistemas de combate naval con un enfoque SoS, lo que representa el verdadero cambio de las reglas de juego en la guerra naval, más que las tecnologías disruptivas individuales o los sistemas de combate individuales. Este enfoque SoS es la clave para construir flotas resistentes, versátiles y distribuidas que sean verdaderamente interoperables, también en un contexto multinacional. Para tener éxito y actuar como un verdadero multiplicador de fuerzas, este nivel de integración no sólo exige tecnologías de vanguardia que permitan la transferencia de datos, sino también, y esto es crucial, una doctrina clara en todos los aspectos, desde la composición de la flota, los niveles de versatilidad exigidos a las plataformas, el uso de sistemas autónomos, hasta la formación de oficiales en una nueva forma más distribuida de guerra en el mar.

En definitiva, las Marinas de Guerra tendrán que adaptarse a un contexto en el que las amenazas evolucionan constantemente, desarrollando un ciclo de adquisición, mantenimiento y actualización de los sistemas de combate más abierto a posibles cambios frecuentes de las necesidades.

2. PLATAFORMAS NAVALES EN EL MULTIDOMINIO

Desde el final de la Guerra Fría, los buques de guerra se han convertido en plataformas cada vez más complejas, que deben tener en cuenta nuevas y más peligrosas amenazas, así como disponer de las correspondientes contramedidas para las mismas. En consecuencia, los buques de guerra modernos tienden a estar equipados con sensores y sistemas de combate más complejos y diversos que sus predecesores, con el fin de garantizar su preparación en caso de conflicto con adversarios de similares características o casi similares. Por ello la mayoría de los buques de guerra incluyen armamento convencional como misiles de crucero, misiles antiaéreos y antibuque, artillería naval (incluidos los sistemas de defensa de punto (CIWS), ametralladoras, torpedos y helicópteros multifunción).

Mientras las nuevas tecnologías se incorporan rápidamente a los diferentes sistemas de armas de las principales Marinas de Guerra del mundo, las contramedidas no se están incorporando tan rápidamente y, en consecuencia, las plataformas empiezan a ser vulnerables a una gama más amplia de amenazas, como son las ya comentadas de misiles balísticos hipersónicos anti-buque y los sistemas no tripulados, además de las amenazas convencionales.

Así, el buque de guerra moderno ideal debe estar equipado con un gran número de sensores, contramedidas y sistemas de armas de última generación que aumenten sus capacidades tanto ofensivas como defensivas, al tiempo que se apoya en un moderno Sistema de Combate (CMS), capaz de gestionar todos los sistemas y los datos entrantes y conectado a una red integrada. Por esta razón, el coste global de este tipo de plataformas ha aumentado considerablemente en los últimos años. Se puede decir que actualmente, el 50% del coste de una fragata media es la propia plataforma del buque, y el otro 50% los sistemas que se integran en ella. Las restricciones presupuestarias, el aumento de los costes y los problemas de personal repercuten negativamente en la capacidad de la mayoría de las Marinas de Guerra para aumentar sus flotas. Aunque el aumento del coste por unidad de los buques hace que la pérdida potencial de cada uno de ellos sea mucho más perjudicial, los buques de guerra modernos deben ser más versátiles y capaces de operar solos o como parte de pequeños grupos. Por consiguiente, las Marinas de Guerra deben encontrar el equilibrio adecuado cuando tratan de repartir las capacidades de alta gama entre un mayor número de unidades (para aumentar la versatilidad, la capacidad de supervivencia y el alcance) y, por tanto, reducir el potencial impacto de la pérdida de un buque en la Fuerza Naval (Concepto letalidad distribuida).

La guerra de Ucrania ha proporcionado ejemplos de hasta qué punto la innovación tecnológica, incluso la referida al uso de sistemas no tripulados de bajo coste o de construcción artesanal, puede ser eficaz frente a un adversario no preparado. Tanto el hundimiento del buque insignia ruso del Mar Negro, el crucero lanzamisiles “Moskva”, como el ataque ucraniano contra la base naval de Sebastopol, se llevaron a cabo con la participación de vehículos no tripulados que provocaron el hundimiento o daño de buques de guerra infinitamente más caros y sofisticados. (Ref. 3).

En general, las Marinas de Guerra actuales tienden a adquirir buques diseñados para incrementar su ciclo de vida y, por tanto, la diferencia entre las curvas de obsolescencia de las plataformas navales y ciertos sistemas de combate es cada vez mayor. Aunque la instalación de sistemas modernos en buques mucho más antiguos suele ser difícil y poco rentable, **los diseños de los buques de guerra modernos deben tener en cuenta la evolución futura de la tecnología y las necesidades operativas para alargar la vida útil del buque**, retrasando lo máximo posible

su obsolescencia. Esto no es trivial, un planteamiento de este tipo requiere el desarrollo de sistemas abiertos y modulares que puedan someterse fácilmente a actualizaciones y mejoras para adaptarse a amenazas y requisitos operativos nuevos o cambiantes, tanto en lo que respecta a la fase de diseño y desarrollo como en la fase de ejecución que sustenta un programa de adquisición. El Departamento de Defensa de EEUU (DoD), por ejemplo, ha estado trabajando en la integración de un enfoque de sistemas abiertos modulares (MOSA) en los programas de adquisición de defensa. También la Unión Europea (UE), a través de su Fondo Europeo de Defensa (EDF), ha identificado la modularidad como un enfoque útil para el proyecto de Corbeta de Patrulla Modular y Multirrol (MMPC o EPC), destacando la ambición de aumentar la flexibilidad de los buques de segunda línea para llevar a cabo una gama más amplia de operaciones.

La creciente complejidad de los sistemas de combate también tiene implicaciones en la dotación de un buque en términos de número y de habilidades requeridas a cada uno de sus miembros, así como el tipo de formación y adiestramiento necesarios para operar tecnologías avanzadas que evolucionan a un ritmo más rápido, en comparación con décadas anteriores. Muchos de los sistemas más modernos también requieren menos personal, ya que ofrecen un mayor grado de automatización y una mayor fiabilidad y disponibilidad, dando así al menos una solución parcial a los problemas de personal a los que se enfrentan la mayoría de las Marinas de Guerra occidentales. Sin embargo, el aumento de la automatización, por sí misma, no conducirá a una trayectoria de disminución constante del número de tripulantes por debajo de cierto punto, ya que los buques seguirán necesitando un mínimo de operadores humanos que garantice la flexibilidad y la seguridad en las operaciones. Hay ejemplos de buques ya construidos que se han diseñado con un alto grado de automatización y con una dotación reducida, pero que una vez en operación se comprobó que no se podían realizar tareas habituales en un buque de guerra.

Los avances en tecnología satelital, así como en tecnologías de sensores y no tripuladas, ofrecen grandes oportunidades a las Marinas de Guerra que deseen ampliar el alcance de un CMS, mucho más allá de lo que era técnicamente posible hace sólo una década. Estas oportunidades, sin embargo, dependen de la capacidad de la flota para integrar adecuadamente una amplia gama de sistemas de combate naval y los datos que estos generan, en una arquitectura SoS cohesiva apoyada por un Sistema de Mando, Control y Comunicaciones (C3) integrado. En la práctica, en el ámbito de los CMS,

Las Fuerzas Navales apuestan cada vez más por la integración a nivel estratégico.

y no sólo táctico, como una forma de facilitar la interoperabilidad entre un mayor número de sistemas diversos, incluidos los no tripulados y los activos multinacionales.

Otro reto importante para la integración e interoperabilidad efectiva de los diferentes sistemas y plataformas es la necesaria adaptación de la doctrina. La interoperabilidad entre aliados y países socios, y entre medios tripulados y no tripulados también puede verse enormemente facilitada por un enfoque integrado de los sistemas de combate. Sin embargo, esto debe verse soportado por procedimientos compartidos respecto al procesamiento de datos y la comunicación, de forma que los diferentes sistemas puedan comunicarse entre sí de forma eficiente desde el diseño implementando arquitecturas abiertas, estándares y regulaciones para su desarrollo. Actualmente los aliados de la OTAN sólo disponen de una norma STANAG relativa a vehículos no tripulados que, aunque fue desarrollada para la interoperabilidad de vehículos aéreos no tripulados (UAV), también se utilizó en el contexto del proyecto OCEAN2020 para sistemas marítimos.

La Alianza trabaja actualmente en el STANAG 4817 (Multiple Area Control of Unmanned Platforms), que proporcionará normas comunes para el control de sistemas no tripulados en todos los ámbitos (aéreo, marítimo y submarino).

Un denominador común para la mayor parte de las Marinas de Guerra, aunque puede parecer una contradicción, es la tendencia a disponer de un mayor número de sistemas no tripulados de reducido tamaño y bajo coste de adquisición y operación y, al mismo tiempo, disponer de plataformas navales tripuladas de mayores dimensiones, probablemente para poder incorporar todos los nuevos sistemas y capacidades que está ofreciendo el desarrollo tecnológico actual, así como para poder disponer de las necesidades de generación de energía correspondientes.

2.1. Rusia y China

Con respecto a la implementación de todos estos conceptos, Rusia sigue aplicando al combate naval un enfoque centrado en las plataformas, mientras que China se ha mantenido firme en la adopción de una perspectiva de SoS en red. No obstante, ambos países esperan que la innovación tecnológica contribuya a mejorar algunas carencias o limitaciones en cuanto a las capacidades disponibles en sus respectivas Marinas de Guerra, especialmente en ASW (guerra anti-submarina) y C4ISR (mando, control, comunicaciones y computación (C4), inteligencia, vigilancia y reconocimiento (ISR).

Rusia y China se consideran vulnerables a los ataques relámpago de armas combinadas occidentales y por ello, ambos países han desarrollado doctrinas que hacen hincapié en inutilizar la infraestructura enemiga y atacar sus buques a mayor distancia, aprovechando al máximo la tecnología de misiles y submarinos, así como sistemas no tripulados como multiplicadores de fuerzas. No obstante, lo anterior, las sanciones impuestas a Rusia en 2022 a raíz de la guerra de Ucrania, además del propio conflicto, pueden afectar de forma muy importante a su desarrollo tecnológico.

2.1.1. Mando y Control

Las tecnologías disruptivas chinas en el ámbito naval, especialmente la guerra electrónica y C4ISR, se centran en implementar la guerra centrada en redes (NCW), cambiando una estructura de fuerza centrada en las plataformas a un SoS integrado y habilitado en red. Pekín ha optado por reforzar sus capacidades de operaciones conjuntas y acortar el ciclo de reconocimiento-ataque de su Marina de Guerra. Una sólida red ISR es especialmente significativa, ya que la falta de este tipo de capacidades adecuadas ha sido durante mucho tiempo un problema importante de las capacidades antibuque y ASW chinas.

2.1.2. Plataformas Tripuladas

La Marina de la Federación Rusa (VMF) tiene una larga tradición en situar la innovación y la disrupción tecnológica en el centro de sus conceptos operativos. Desde la caída de la Unión Soviética, y de nuevo tras la ronda de sanciones internacionales en 2014, la VMF ha llegado a considerar los nuevos sistemas navales como la clave para contrarrestar la superioridad percibida de sus pares en términos de tonelaje, número de buques y capacidades de proyección de fuerzas

La adopción por parte de China de sistemas de combate de nueva generación ha sido el resultado de la evolución doctrinal que acompaña a su ascenso como potencia militar mundial. La Marina del Ejército Popular de Liberación (PLAN) ha superado en los últimos años a la estadounidense como la mayor del mundo en número de buques, aunque no en tonelaje (la PLAN desplaza alrededor de 2 millones de toneladas repartidas en 335 buques, frente a los 4,5 millones de la US Navy repartidos en 305). Lo que indica que Pekín sigue dependiendo en gran medida de un gran número de buques más pequeños. Aunque los buques más pequeños suelen ser menos capaces que los grandes, un enfrentamiento naval de envergadura entre China y EEUU se produciría probablemente cerca de la China continental, donde los buques más pequeños de la PLAN podrían operar teóricamente bajo un paraguas de capacidades anti-acceso y negación de área (A2/AD) basadas en tierra.

La fragata polivalente Tipo 054 es la plataforma que mejor refleja el cambio de enfoque de China en el combate naval. Su operación comenzó a principios de la década de los años 2000, empleándose en un principio para la defensa del litoral y desde entonces ha evolucionado progresivamente hacia funciones de patrulla de Líneas de Comunicación Marítima (SLOC) y protección de portaaviones. Sus actualizaciones tecnológicas muestran las nuevas funciones de estos buques en la estrategia china: la modernización de sus sistemas anti-aéreos y de radar han reforzado su contribución a la defensa de área.

Y como ejemplo de la tendencia del incremento de las dimensiones de ciertas plataformas navales podemos citar a los cruceros Tipo 055, buques de 180m de eslora, que integran capacidades ASW, ASuW (guerra anti-superficie), AAW (guerra anti-aérea) y la posibilidad de lanzamiento de misiles de crucero.

Por último, la nueva generación de portaviones de la PLAN es casi una realidad con las pruebas de la primera unidad, el “Fujian”. Esta serie de portaviones son los primeros que han sido diseñados completamente con ingeniería nacional china y, entre otras novedades, disponen de sistemas electromagnéticos de lanzamiento de aviones (tecnología que sólo está al alcance de EEUU), lo que les permite operar aviones de mayor carga y alcance.

Imagen 2 – Type 054A (Jiangkai II) Class Frigate. Fuente: Revista Naval Technology, Type 054A (Jiangkai II) Class Frigate, 04 sep 2020

2.1.3. Plataformas no Tripuladas

La principal medida de actualización de la envejecida flota Rusa, ha sido la adopción de tecnologías disruptivas como los vehículos submarinos no tripulados (UUV). Por ejemplo, el Surrogat-W, es un UUV de reconocimiento encargado de realizar tareas que, de otro modo, supondrían el riesgo de revelar la posición de submarinos tripulados.

Por su parte, la necesidad China de mejorar las capacidades ISR de la flota de superficie le ha llevado a realizar una fuerte inversión en sistemas no tripulados, tanto en términos de UAV como de USV. Imágenes de la cubierta del buque "Shandong", por ejemplo, muestran que el portaaviones chino puede operar al menos dos tipos de drones de despegue y aterrizaje vertical (VTOL). La Marina Japonesa también tuvo algunos incidentes con UAV chinos de altitud media y largo alcance (MALE) y, sin duda, los UAV marítimos podrían mejorar la operación de los aviones especiales de la Fuerza Aérea de la Marina China encargados de misiones ISR, ASW y de guerra electrónica (EW).

Otro proyecto destinado a mejorar el complejo ISR de la PLAN es lo que se ha llamado "Zhu Hai Yun", la primera nave nodriza inteligente no tripulada del mundo, capaz de desplegar UAV y UUV con total autonomía. El "Zhu Hai Yun", aunque clasificado como buque civil, tendría evidentes aplicaciones militares.

2.1.4. Armamento Convencional

El segundo elemento central de Rusia para actualizar su flota ha sido el empleo de misiles hipersónicos y de crucero. La VMF está trabajando en la modernización de las capacidades de misiles anti-buque de la flota mediante un proceso conocido como "Kalibrisation", es decir, el equipamiento generalizado de misiles de crucero 3M14 Kalibr en diversos buques de la flota. Esto desempeñaría un papel crucial para la flota rusa en el Mar Mediterráneo. La próxima incorporación al arsenal ruso sería el misil de crucero hipersónico 3M22 Zircon, aún en desarrollo y supuestamente capaz de alcanzar velocidades de Mach 9 con un alcance de 1.000 km.

La expansión de la PLAN ha ido acompañada de importantes avances tecnológicos en misiles, tanto embarcados como terrestres. Destacan dos: el DF-21D (1.500 km de alcance) y el DF-26 (5.000 km de alcance), popularmente denominado el «asesino de Guam» por su capacidad para alcanzar la base naval estadounidense del mismo nombre en la segunda cadena de islas. Sin embargo, estas armas aún no se han utilizado en combate.

Otro campo en el que Pekín ha hecho grandes avances es el desarrollo de misiles de crucero anti-buque (ASCM) y misiles de crucero terrestres (LACM). El YJ-18, por ejemplo, supera al Harpoon estadounidense y puede lanzarse desde buques de superficie como los destructores tipo 052D y 055 y desde submarinos de ataque nuclear clase Shang II, pudiendo incluso desplegarse en submarinos de la VMF de la clase Kilo.

2.1.5. Otros Sistemas

Según diversos artículos, Pekín está estudiando el desarrollo de un arma de pulso electromagnético (EMP) de 80 GW y la ha probado en un lugar no revelado, derribando UAV que volaban a 1.500 m sobre el nivel del mar (Ref. 4).

2.2. Estados Unidos

La US Navy se está transformando de una fuerza compuesta de grandes plataformas tripuladas a otra con una mayor proporción de pequeños buques, aviones y vehículos submarinos tripulados y no tripulados. Pretende incorporar nuevos buques y aviones no tripulados, junto con tecnologías ya comentadas como armas hipersónicas y láseres, para mejorar la letalidad y la capacidad de supervivencia de la flota, y otras capacidades desarrolladas a través del Proyecto Overmatch (Ref. 2, 5) que proporcionen ventajas en la eficiencia y rapidez en la toma de decisiones. En el marco de este proyecto, la US Navy colabora con diversos socios industriales para perfeccionar los radares, la EW, los sonares de apertura sintética, las redes ópticas, los enlaces de datos por radiofrecuencia y otras tecnologías de comunicaciones, con el fin de seguir desarrollando las redes marítimas multidominio.

Se puede afirmar con seguridad que el tratamiento de la información, la velocidad y la reducción del ciclo de toma de decisiones para disminuir exponencialmente el

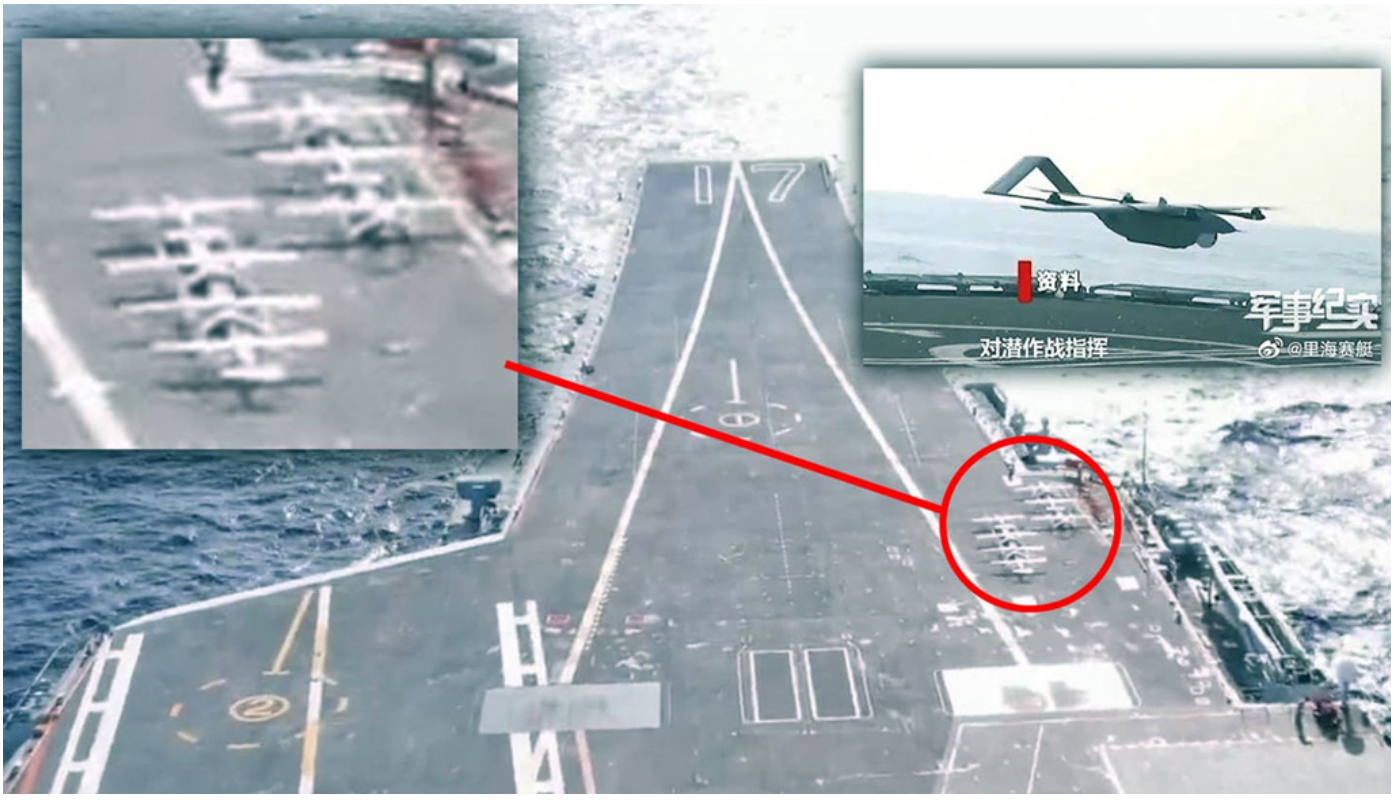


Imagen 3 – Chinese aircraft carrier Shandong with VTOL. Fuente: Revista The Warzone vía Weibo, Chinese Aircraft Carrier Seen With A Fleet Of Drones On Its Deck, 02 jun 2022

tiempo que transcurre entre el inicio de una tarea (orden, sensor receptor, etc.) hasta la ejecución (disparo, etc.) es la esencia del enfoque multidominio del Pentágono, en la guerra del futuro.

2.2.1. Mando y Control

En consecuencia, el mando y control (C2) puede ser el aspecto más importante del nuevo enfoque conceptual. Los comandantes de buques y otras unidades o grandes contingentes de tropas distribuidas pueden depender de los Centros de Operaciones en tierra para la inteligencia, la planificación y la dirección. Y adversarios con suficiente capacidad tecnológica podrían interrumpir las comunicaciones de largo alcance, lo que obligaría a la US Navy a desarrollar procesos y arquitecturas de C2 que se adapten a la disponibilidad real de las comunicaciones, en lugar de intentar construir redes que permitan a los mandos de la flota en tierra dirigir las operaciones en todas las condiciones de guerra. La US Navy persigue un C3 ágil como parte del JADC2 (mando y control conjunto multidominio) del Proyecto Overmatch. Este esfuerzo se basa en la interconexión y el procesamiento seguros de la información, ya que los nodos disgregados, los sensores espaciales, los drones aéreos, los submarinos, los buques de superficie e incluso los aviones de combate, pueden estar muy dispersos en una vasta zona de combate, pero estrechamente conectados por sensores de largo alcance y redes de comunicaciones. Este concepto hace hincapié en los sistemas no tripulados y exige elevar el procesamiento y la transmisión de información entre dominios como objetivo estratégico fundamental de la guerra.

De acuerdo con lo anterior, las redes basadas en IA, los enlaces de datos seguros por radiofrecuencia, los sensores y armas de mayor alcance, el procesamiento informático de alta velocidad y otras innovaciones que afectan al ciclo de toma de decisiones bélicas son, naturalmente, áreas de gran interés de la US Navy.

Centrándonos es aspectos más concretos, el proyecto Overmatch tiene por objeto la integración de una flota cada vez más heterogénea y es la principal prioridad de innovación de la US Navy. Liderado por el NAVWAR (Mando de Guerra de Sistemas de Información Naval), el proyecto incluye acciones para conectar las redes tácticas existentes, como CEC, Link-16 y TTNT (Tactical Targeting Network Technology), con redes más nuevas como el Datalink avanzado multifunción (MADL) de los aviones F-35 y Datalinks de vehículos no tripulados.

Con sistemas que operan en el aire, en tierra y en la superficie del mar y bajo ella,

> *el enfoque de la US Navy sobre el multidominio y el C3 es conseguir que casi todas sus plataformas se integren en varios dominios.*

Por ejemplo, los SSN (denominación para sus submarinos nucleares) despliegan ahora sistemas EW para generar efectos en el espectro electromagnético, así como misiles para lanzar ataques contra objetivos en el mar o en tierra. Aviones como el P-8A[a] Poseidon lanzan y gestionan sonoboyas como el sistema MAC (Multistatic Active Coherent) que puede detectar y rastrear submarinos enemigos de última generación a través de enlaces cooperativos entre unidades, de tal manera que toda unidad detectora bajo la superficie (sonares de casco, sonoboyas, UUV, sensores fijos) puede ser fuente y receptor a la vez, creando un entorno colaborativo en red multiéstatica en el que todos los sensores se aprovechan de las señales transmisoras del otro. Tanto las FFG (fragatas con misiles guiados o capacidad anti-arérea) como las DDG (destructores con capacidad anti-aérea) pueden realizar operaciones AAW, ASuW, ASW y guerra electromagnética (EMW). Con el anteriormente citado proyecto Overmatch se están ampliando sus capacidades C3 a un número y variedad crecientes de paquetes de fuerzas para hacer frente a los retos operativos de los mandos de las flotas. También hay interesantes iniciativas adicionales para crear la infraestructura necesaria utilizando sistemas de control comerciales. La adecuada combinación de capacidades C3 y de automatización será esencial para conseguir una flota más grande y cada vez menos tripulada.

2.2.2. Plataformas Tripuladas

Mientras que el C3 lidera los esfuerzos de innovación técnica y operativa de la US Navy, desde el punto de vista de las plataformas, la prioridad de adquisición son los SSBN (denominación para sus submarinos nucleares balísticos) de la clase Columbia que utilizarán un nuevo sistema de control de la propulsión e incorporarán las nuevas tecnologías en sensores y sistemas de combate desarrollados para el programa de submarinos SSN de ataque Virginia.

La US Navy también está priorizando el programa del destructor DDG(X), cuya llegada está prevista para mediados de la década de 2030, y que proporcionará una defensa aérea mejorada mediante lanzadores verticales de misiles de mayor capacidad, láser de alta energía, así como un mayor alcance ofensivo con misiles hipersónicos. El programa de FFG(X) Constellation class ha comenzado recientemente su construcción. Este diseño, basado en las fragatas multimisión europeas FREMM, desarrolladas por Francia e Italia, se centrarán en misiones ASW, al estar equipados con el sonar activo de baja frecuencia remolcado CAPTAS-4 del grupo francés Thales, además de otras misiones de escolta.

2.2.3. Plataformas no Tripuladas

Debido a los altos costes de adquisición y funcionamiento de sus plataformas tripuladas de superficie y submarinas, la US Navy prevé que los vehículos no tripulados ayuden a conseguir una flota más distribuida que pueda llevar a cabo operaciones a mayor escala que en la actualidad. Para ello se están priorizando esfuerzos para desarrollar equipos de trabajo, la infraestructura digital para gestionar las operaciones de los sistemas no tripulados y los procesos de despliegue de sistemas no tripulados para resolver problemas operativos importantes. Sin embargo, la US Navy ha tardado en introducir sistemas no tripulados más allá de los sistemas ISR, como son los pequeños UAV de a bordo RQ-21 Blackjack o Scan Eagle, los UUV cazaminas Mk-18, los planeadores oceanográficos SHARC y el gran UAV MQ-4C Tritón.

En el ámbito submarino, la US Navy está desarrollando una familia de sistemas de diversos tamaños. En la gama alta, el UUV extragrande Orca (XLUUV) está pensado para ser lanzado desde muelles o grandes buques anfibios, previsto para el despliegue de minas y pequeños UUV (SUUV) en lugar de misiones de vigilancia más extensas. La financiación del UUV de gran desplazamiento (LDUUV) Snakehead fue inicialmente paralizada por la US Navy en su propuesta de presupuesto para 2023, aunque es probable que se vuelva a activar. En la gama media, los MUUV están diseñados para ser lanzados desde buques, lanchas o tubos lanzatorpedos. Los Mk-18 Mod 1 y Mod 2 serán sustituidos por el Knifefish MUUV (UUV de tamaño medio) y con el tiempo, el Razorback MUUV proporcionará una plataforma MUUV común para operaciones cazaminas, la realización de misiones ISR y de otro tipo desde submarinos, utilizando el lanzamiento y la recuperación desde tubos lanzatorpedos.

El Lionfish SUUV (Ref. 2) es el programa de pequeños UUV más reciente. Con un diámetro de 10 pulgadas, el Lionfish podría ser lo suficientemente pequeño como para ser desplegado por sistemas de contramedidas submarinos, XLUUV y, potencialmente, lanzadores de sonoboyas aéreas. Las misiones de los SUUV incluirían ISR, pero también

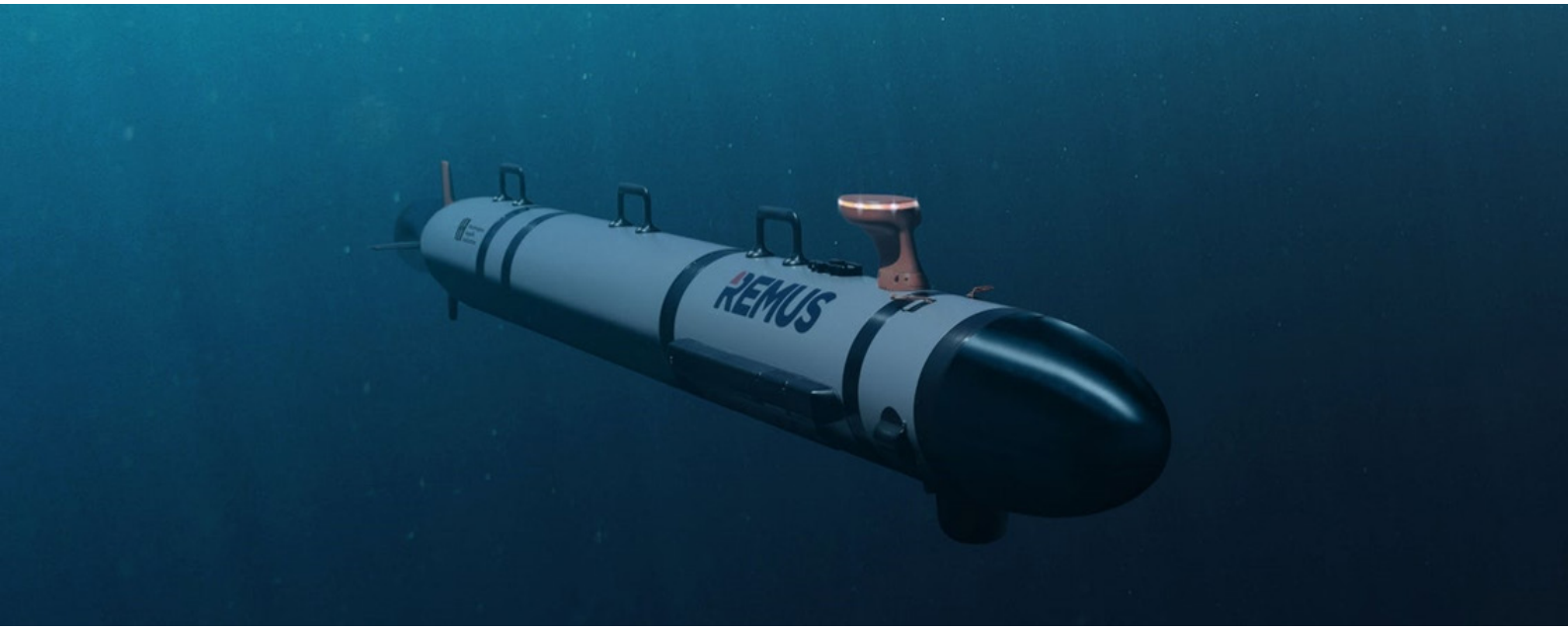


Imagen 4 - REMUS 300 SUUV. Fuente: Página web de Huntington Ingalls Industries, Inc. (HII) "hii.com/Newsroom", 30 mar 2022

podrían actuar como señuelos o interferentes de sonar. El modelo elegido para este programa es el REMUS 300 de Huntington Ingalls Industries.

Al igual que los UUV, la US Navy planea desplegar buques de superficie no tripulados (USV) de varios tamaños. Los grandes USV (LUSV) se están desarrollando para transportar cargadores de misiles que aumenten la capacidad de plataformas de superficie tripuladas. Los USV de tamaño medio (MUSV) están destinados a realizar misiones de reconocimiento y contra reconocimiento transportando sensores pasivos de radiofrecuencia e infrarrojos, inhibidores y señuelos EW, o iluminadores de radar para apoyar la detección multiestática por parte de plataformas tripuladas que lleven receptores de radar. Sin embargo, hay dudas sobre si estas misiones podrían ser realizadas de forma más asequible por USV más pequeños. Casi todos los pequeños USV de la US Navy son experimentales, como los USV Saildrone que está utilizando en Oriente Medio, aunque estos sistemas comerciales carecen de las comunicaciones reforzadas de los vehículos militares o de sensores como arrays de sonar y sofisticados dispositivos de inteligencia de señales. El USV de contramedidas de minas de pequeño tamaño (MCM) es el único programa USV formal, y aunque inicialmente se diseñó para remolcar ISS (Influence Sweep Systems), el USV MCM podría llevar a cabo misiones ISR, EW u otras en el futuro y será construido por el astillero Bollinger (Ref. 6).

2.2.4. Armamento Convencional

El proyecto CPS , que es la versión naval del misil hipersónico de largo alcance LRHW, está desarrollando un sistema de armas hipersónicas de largo alcance (3.000 kilómetros), capaces de alcanzar casi cualquier parte del mundo en cuestión de minutos a velocidades superiores a Mach 5 y con una gran capacidad de supervivencia frente a las defensas enemigas. La empresa Lockheed Martin será la encargada de integrar la capacidad de ataque hipersónico en los destructores de la clase Zumwalt, estando prevista su prueba inicial en el año 2025.

Además del desarrollo del misil hipersónico de ataque, la US Navy está modernizando el misil de ataque a tierra Tomahawk y los misiles interceptores de defensa aérea SM-6 para poder realizar ataques desde el ámbito marítimo. De aquí a la década de 2030, está previsto desarrollar una nueva arma de ASuW ofensiva para sustituir al misil anti-buque Harpoon y complementar al Tomahawk y al SM-6.

También se están introduciendo algunas mejoras en sus capacidades ASW. La versión más moderna del torpedo Mk-48 incorpora procesamiento digital de sonar y sistemas mejorados de guía y control. Para ayudar a los submarinos a contrarrestar ataques de torpedos y proporcionar a los aviones ASW una mayor capacidad de armamento, se desarrolló el Arma Compacta de Ataque Rápido (CRAW, un torpedo de aproximadamente 1/3 del tamaño del torpedo tradicional Mk-54 que llevan los buques de superficie), para los helicópteros MH-60R Seahawk y los aviones P-8A Poseidon.

2.2.5. Otros Sistemas

Como se ha comentado anteriormente, desde 2014, la US Navy ha desplegado y probado prototipos de sistemas de armas láser en los buques anfibios USS “Ponce” y “Portland”. En 2022 fue instalado en la DDG USS “Preble” el primer láser de alta energía (60kW) con deslumbrador óptico integrado y sistema de vigilancia (HELIOS), desarrollado por Lockheed Martin, para abatir misiles o cohetes, que podría alcanzar 120 kW en una futura versión (Ref. 1, 2). A más largo plazo, el Programa de Láser de Alta Energía Contra-ASCM (HELCAP) está desarrollando un láser de 300 kW.

2.3. Europa

La UE puede desempeñar un papel importante en el fomento de la cooperación entre sus Estados miembros a la hora de planificar el desarrollo y la adquisición de sistemas navales de combate de última generación. La Brújula Estratégica de la UE 2022 mencionaba el ámbito naval entre los sectores clave en los que los Estados miembros deben invertir para desarrollar capacidades nuevas y tecnologías innovadoras, con el fin de rellenar las lagunas existentes y reducir las dependencias de otros países. En particular, la UE da prioridad a conseguir capacidades interoperables que puedan garantizar la superioridad en el ámbito marítimo. Entre las prioridades de desarrollo de capacidades de la Agencia Europea de Defensa (EDA) figuran las categorías de maniobrabilidad naval y control submarino. Para impulsar el citado desarrollo de las capacidades europeas, la UE financia una serie de proyectos en el marco del EDF y de la iniciativa PESCO (Cooperación Estructurada Permanente).

2.3.1. Mando y Control

Desde la perspectiva del C2 y la integración de sistemas en el ámbito marítimo, la UE cuenta con grandes empresas como el grupo francés Thales, Navantia (su división de sistemas) e Indra en España, Leonardo en Italia, Atlas en Alemania, etc. que desarrollan productos innovadores, pero hasta ahora de forma individual. Existen algunos proyectos en curso a nivel europeo que podría ser la semilla de una intensa futura colaboración entre empresas.

PESCO MUSAS. tiene el propósito de crear una arquitectura de servicios C3 de vanguardia para la guerra antisubmarina, que permita a los Estados miembros de la UE contrarrestar las operaciones de denegación de zona del adversario. También en el ámbito de la guerra submarina, el proyecto SEANICE pretende desarrollar un sistema de guerra antisubmarina de nueva generación basado en la combinación de plataformas tripuladas y no tripuladas. Mediante el uso de las tecnologías más avanzadas, SEANICE tiene el objetivo de mejorar las capacidades de detección, seguimiento y clasificación de la UE.

E-NACSOS. pretende definir el estándar europeo para el intercambio y la fusión de información de sensores en tiempo real entre Sistemas de Combate, que fortalecerá la vigilancia colaborativa en las fuerzas navales europeas e incrementará la eficacia de las operaciones navales anti-aéreas y de superficie. El alcance incluye la implementación de demostradores nacionales de los países participantes, contemplando tanto pruebas simuladas como pruebas de mar con unidades reales. El programa está liderado por consorcio francés Naval Group y, además de Navantia, desde España participan también Indra y la Universidad de Vigo.

HARMSPRO. Proyecto de vigilancia y protección portuaria y marítima, tiene el objetivo de crear una nueva capacidad marítima que permita a los Estados miembros de la UE garantizar una vigilancia y protección adecuadas del tráfico y las estructuras marítimas, mediante una función C2 mejorada.

Entre los esfuerzos concluidos, se envuentra el proyecto ya citado **OCEAN2020** implementado por la EDA, dirigido por Leonardo y en el que participaron 43 socios de 15 Estados miembros, demostró la integración de los UV en operaciones navales, mediante demostraciones en el Mediterráneo y en el Báltico. Sus principales objetivos fueron: mejorar el reconocimiento del escenario marítimo en operaciones navales mediante la integración de sistemas no tripulados y la explotación y compartición en tiempo real de la información generada para mejorar la interoperabilidad, y la demostración de las nuevas capacidades en ejercicios de operación real y simulados.

2.3.2. Plataformas Tripuladas

La European Patrol Corvette (EPC) es uno de los proyectos más importantes para comprobar la viabilidad de una cooperación eficaz dentro la UE (Ref. 2, 7, 8, 9). El proyecto lo gestiona la Organización Conjunta de Cooperación en Materia de Armamento (OCCAR), actuando como contratista, por mandato de la Comisión Europea (CE), contratando al consorcio formado por Naviris (joint venture creada a finales de 2019 a partes iguales por Naval Group y el consorcio italiano Fincantieri.) y Navantia, como coordinadores, y otras 40 empresas de 12 países. Su objetivo es diseñar un buque de unos 110 metros de eslora y 3.000 toneladas, modular y polivalente, capaz de cumplir una amplia gama de misiones en futuros contextos de operaciones, desde el combate hasta las patrullas de largo alcance y las actividades de vigilancia. La EPC incluirá inicialmente dos variantes: una corbeta multipropósito de largo alcance y una multipropósito de combate completo, ambas maximizando innovaciones, sinergias y la interacción entre los tres principales diseñadores y constructores europeos de construcción naval citados: Naval Group, Fincantieri y Navantia. Al ser el primer sistema naval desarrollado tras el inicio de la guerra de Ucrania, la EPC podría presentar algunas características innovadoras, incluso en términos de integración de sistemas de combate. El proyecto se basa en un enfoque de diseño que debería favorecer la integración entre sistemas de diferentes empresas y países, y su éxito se medirá en última instancia por su capacidad para lograr un alto nivel de homogeneidad entre los sistemas de navegación y combate de las diferentes variantes nacionales. Algunas soluciones, como los sistemas de misiles, tienen más posibilidades de ser compartidas gracias a la posición consolidada del grupo inglés MBDA en el mercado europeo. Otras, como las relativas a radares y sensores, en las que varios de los países participantes cuentan con campeones industriales nacionales, requerirán un novedoso enfoque de cooperación. El éxito del proyecto EPC vendrá también por la evolución en la armonización de normas, lo que mejorará la interoperabilidad. No obstante, lo anterior, la complejidad del proyecto es grande, ya que sería la primera plataforma europea que cumpliría con los requerimientos y necesidades de tres o más países.

Imagen 5 – European Patrol Corvette (EPC). Fuente: Wikipedia, European Patrol Corvette

De la mano de la iniciativa EDINAF (Fundación Europea Digital Naval), el proyecto dTHOR busca establecer un marco digital común con reconocidos estándares abiertos de intercambio de datos y un análisis y modelización híbridos que combinen modelos físicos con los datos para mejorar la monitorización de la estructura del buque a través de la sensorización y el intercambio masivo de datos. El conocimiento del estado real de la estructura del barco en todo momento permitirá optimizar el mantenimiento asesorando a la tripulación sobre el desempeño real de la estructura durante todo el ciclo de vida.

En España, el programa naval en curso más relevante e innovador es el de las Fragatas F-110 de Navantia que incorpora novedades como su espacio multimisión, la integración de vehículos no tripulados de superficie y submarinos, la capacidad de instalación futura de DEW o su avanzado mástil integrado optimizado con un bajo RCS (índice de reflexión radar), que puede ser configurado con diferentes soluciones de sensores y antenas que dan soporte a una evolución del Sistema de Combate de Buques de la Armada (SCOMBA). La UTE PROTEC F-110 formada por Indra y Navantia tiene el objetivo de desarrollar y fabricar una serie de nuevos sensores que se alojarán en el mástil integrado (radar de defensa y sistemas de guerra electrónica o comunicaciones), así como nuevas funcionalidades y nueva infraestructura del SCOMBA. Los prototipos y nuevos desarrollos se instalarán en el Centro de Integración de sistemas en Tierra (CIST), situado en Cádiz, donde serán sometidos a integración y pruebas finales antes de su traslado e instalación a bordo de la fragata F-110.

El sistema IRST (Infrared Search and Tracking) de la F-110 consiste en una serie de sensores electrópticos que dota a la plataforma de un sistema capaz de detectar y seguir múltiples blancos de forma automática a partir de sus emisiones térmicas y que incorpora innovadores algoritmos de inteligencia artificial para mejorar la capacidad de detección de blancos.

En el aspecto energético, el programa de adquisición de submarinos S-80 incorpora un sistema de generación de energía innovador, independiente del aire, por medio de

células de combustible de hidrógeno (AIP) que lo dotará de capacidades tácticas sin precedentes al poder cargar sus baterías en inmersión a cotas profundas durante un periodo de varias semanas sin salir a superficie. El sistema AIP está diseñado para producir hidrógeno a partir de reformador de bioetanol.

Iniciativas como el proyecto Medusa 300 de la Dirección General de Armamento y Material (DGAM) pretenden desarrollar a nivel nacional componentes de los sistemas AIP que actualmente no se fabrican en España, en este caso concreto se desarrolla una pila de hidrógeno que completará al reformador de bioetanol que se está desarrollando para el S-80.

Más a largo plazo, e incidiendo en el tamaño de los buques de combate, en España el navío escolta que propone Navantia, junto con la División de Planes de la Armada, es el denominado Smart 8000. Con un tonelaje de entre 8.000 y 10.000 toneladas y 162 metros de eslora es un buque tipo destructor, con capacidades tanto para hacer frente a las amenazas convencionales más modernas, como para operar en conflictos en zona gris o guerra asimétrica. En él destaca un diseño de claras formas de baja firma, o stealth, sistema de lanzamiento vertical de misiles de 36 celdas, gran cubierta de popa para operar con aeronaves (helicópteros y UAV), sensores de última generación, etc. Desde el punto de vista de la innovación, el buque dispondrá de un sistema de combate de arquitectura abierta que estaría plenamente integrado en redes multidominio con otras unidades de las Fuerzas Armadas. En la parte delantera del puente incluye un DEW, y un sistema de defensa anti-misiles de última generación o los futuros EMRG (cañón tipo Riel electromagnético).

Por último, es reseñable destacar una nueva tendencia, cuyos primeros exponentes públicos son Portugal y Turquía, del desarrollo de plataformas tripuladas para UV. Basado en la plataforma L400 (de asalto anfibio o LHD diseñado por Navantia, similar al buque "Juan Carlos I", Turquía ha anunciado el desarrollo de una plataforma de características parecidas, pero para el despliegue de UV, en lugar de aviones y helicópteros tripulados como su antecesor. Y por su parte, la Marina de Portugal ha firmado con el grupo de construcción naval holandés Damen la construcción de un buque multipropósito de investigación oceanográfica con la capacidad de transportar y desplegar UAV, USV y UUV.

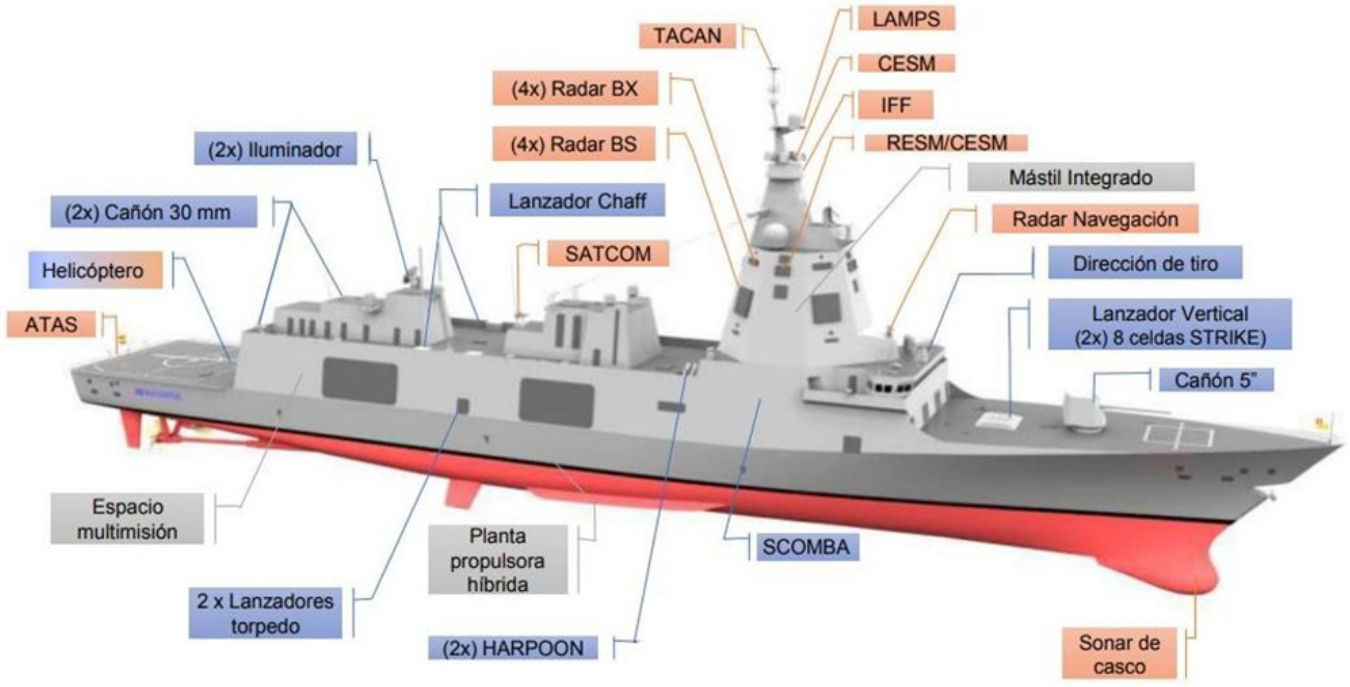


Imagen 6 – F-110 Armas y sensores. Fuente: ABC, Fragata F-110: así es el buque de guerra a cuyo corte de chapa ha asistido el presidente Sánchez, 06 abr 2022

Imagen 7 – Maqueta del Smart 8000 (Navantia). Fuente: Defensa.com (Julio Maíz), Smart 8000: el navío de escolta futuro de Navantia, 30 may 2023

2.3.3. Plataformas no Tripuladas

En cuanto a los vehículos autónomos, también se están desarrollando algunas iniciativas a nivel europeo entre las que destacan los siguientes.

M-SASV. Proyecto de vehículo de superficie semiautónomo que desarrollará un vehículo de tamaño medio con múltiples módulos de misión que permita operaciones no tripuladas, al tiempo que garantiza la posibilidad de recurrir al control tripulado cuando sea necesario.

SEAWINGS. Desarrollará una nueva clase de drones militares con fines de vigilancia. Dichos drones constituirán una novedad por ser capaces de volar por encima de la superficie del mar utilizando la acción de efecto suelo. Podrán operar tanto en el mar como en el aire, transportar grandes cargas, recorrer largas distancias, serán de bajo coste y no requerirán infraestructura ni vehículo de lanzamiento para el despegue y aterrizaje. Este proyecto está coordinado por LA PALMA RESEARCH CENTRE y participan entre otros la Universidad Politécnica de Madrid.

HYBRID. Tiene por objeto desarrollar un sistema no tripulado de despegue y aterrizaje vertical que pueda operar en una gran variedad de entornos y contra múltiples tipos de amenazas.

El rápido avance y la incesante proliferación de las minas marinas y los ataques de submarinos representan una amenaza potencial para las operaciones marítimas de la UE. Las medidas MCM y los sistemas ASW se consideran cruciales para permitir a la UE ejercer un control submarino adecuado. El proyecto PESCO **MAS MCM** pretende mejorar la seguridad marítima de la UE proporcionando a sus Estados miembros un conjunto diferenciado de tecnologías submarinas, de superficie y aéreas (semi) autónomas capaces de contrarrestar las minas marinas.

El proyecto **MIRACLE** tiene por objeto contribuir a la mejora de las misiones europeas MCM mediante la mejora de los principales componentes de la guerra contra las minas “stand-off”.

En el ámbito de los vehículos no tripulados, en España, las empresas Navantia, Saes y Perseo están desarrollando el denominado proyecto WISE, un submarino no tripulado capaz de llevar a cabo una amplia variedad de misiones.

Hay tres versiones contempladas: una versión para guerras de minas, otra de inteligencia ISR y la versión de merodeo naval que la convierten en un importante vector de ataque contra buques enemigos. El submarino, en su versión de pequeño tamaño, tiene una eslora de 2,3 metros, un peso de 80 kilogramos y es capaz de transportar una carga de hasta 40 kg. Además, tiene una autonomía de entre 50 y 70 millas, puede sumergirse hasta los 80 metros y alcanza velocidades de 15 nudos en superficie y de 10 nudos bajo el agua. Al no necesitar de tripulación, la embarcación es una opción más segura y económica para llevar a cabo, no solo misiones de defensa, sino también para su uso en aplicaciones civiles.

2.3.4. Armamento Convencional

En lo relacionado con armamento, empresas europeas como MBDA, el grupo noruego Kongsberg, Leonardo o el grupo español Escribano, están llamados a colaborar en el desarrollo de nuevos productos europeos. En concreto, respecto al desarrollo de armas hipersónicas y los correspondientes sistemas de defensa, el proyecto HYDEF se centra en la investigación y definición del concepto de un interceptor europeo ante amenazas hipersónicas tanto de misiles balísticos como de vehículos supersónicos garantizando la futura integración del sistema interceptador en una plataforma de combate naval. El consorcio está liderado por el grupo de ingeniería español Sener y la participación, entre otras, de las empresas españolas Escribano, GMV, Instalaza, y Navantia, así como del Instituto de Técnica Aeroespacial (INTA) del Ministerio de Defensa.

También MBDA desarrollará el interceptor HYDIS2 para proteger a Europa de misiles hipersónicos capaces de maniobrar a velocidades superiores a 6.174 km/h. El consorcio incluye 19 empresas y 30 proveedores de 14 países europeos.

Dadas las características de las plataformas navales actuales y la duración de su ciclo de vida, es esencial considerar la compatibilidad e interoperabilidad de las nuevas soluciones con los sistemas existentes. La integración de los nuevos sistemas con los legados debe considerarse un requisito esencial, más aún en un entorno como el europeo, con una gran diversidad de plataformas y sistemas, un amplio abanico de tiempos en servicio diferentes entre los Estados miembros y distintos programas e Iniciativas de modernización y mejora que se desarrollan en paralelo.

Imagen 8 – Maqueta del Submarino no tripulado WISE. Fuente: Infodefensa, ESPECIAL FEINDEF 2023, 22 may 2023

3. CONFLICTOS ACTUALES

Como ya se ha mencionado, hasta mediados de este siglo XXI se prevé un mundo multipolar en el que EEUU será el principal centro de poder junto a otros países, que como China, Rusia, India, Japón y la UE (Ref. 11) querrán formar parte de ese poderoso núcleo.

En el ámbito marítimo se dan muchos incidentes en aguas nacionales e internacionales donde los estados pretenden defender su mar territorial, de igual forma que en aguas internas, y garantizar la libertad de navegación por aguas internacionales tanto en rutas comerciales tradicionales como en nuevas posibles rutas.

Los incidentes más significativos han ocurrido y están ocurriendo en el Mar Oriental y en el Mar Meridional de China, en el Báltico y Mar Negro y en el Mar Rojo, con los ataques hutíes contra embarcaciones comerciales que transitan hasta el Canal de Suez (una de las rutas marítimas más transitadas del mundo se ha convertido, seguramente, en la más peligrosa). **La nueva Estrategia Militar de China, confiere una prioridad absoluta al entorno naval frente a la tradicional importancia dada al teatro terrestre**, ya que prima la protección de los intereses y derechos territoriales en el mar. Así, pretende desarrollar las capacidades marítimas para salvaguardar sus intereses de soberanía y derechos marítimos, y dar seguridad a la libertad de navegación fuera del territorio nacional para convertir a China en una potencia marítima.

Rusia está desplegando de forma creciente sistemas de tecnología avanzada como pudo ser visto en octubre y diciembre de 2015, cuando fuerzas rusas lanzaron misiles de crucero Kalibr, para atacar objetivos en Siria, desde buques en el mar Caspio y posteriormente desde un submarino clase Kilo diésel-eléctrico (SSK) en el mar Mediterráneo. Estos ataques demostraron que occidente no tiene el monopolio en este tipo de capacidades e indicó la flexibilidad existente con algunos sistemas de armas para poder ser instaladas en plataformas de submarinos nucleares de ataque o desplegadas en otro tipo de plataformas como las situadas en modernos SSK. En la guerra de Ucrania también se han empleado este tipo de misiles de crucero.

En los últimos años ha habido una reducción de la ventaja de occidente en las capacidades y tácticas de combate en la guerra convencional frente a otros como China y Rusia. Los misiles anti-buque de la US Navy tienen menor alcance que sistemas desarrollados por China, Rusia e India. Como resultado, Estados Unidos está llevando a cabo varias iniciativas de corto y largo plazo para corregir dicho desequilibrio. Estas incluyen un programa para desarrollar una versión anti-buque del misil de crucero de ataque a tierra Tomahawk (con un alcance de 1.600 km), además de una versión aire-superficie del misil antibuque de largo alcance actualmente en desarrollo.

La ciberguerra, es un dominio transversal al resto: aire, tierra, mar y espacio, y por tanto afecta también a la batalla naval. El aumento del nivel de digitalización de los sistemas y plataformas navales, así como el uso extensivo de las comunicaciones digitales en redes con múltiples sensores y sistemas de armas, abre una serie de vulnerabilidades en el ámbito digital que también necesita protección. Los sistemas de satélites militares y los Centros de Operaciones Marítimas también son y serán objetivo de ciberataques, interrumpiendo los datos recibidos y transmitidos que proporcionan ISR y C2 a las flotas en el mar. Quien sepa explotar estas vulnerabilidades en el enemigo y proteger las propias, tendrá una ventaja valiosa. El uso generalizado en el ámbito marítimo de sistemas no tripulados y modernos algoritmos de apoyo a la toma de decisiones, basados en inteligencia artificial y los protocolos de autoaprendizaje, abre un nuevo vector de ataque en el ámbito cibernético.

Este entorno actual requiere nuevos métodos y sistemas implicando, no sólo el necesario desarrollo e implantación de las nuevas soluciones tecnológicas, sino también el desarrollo de los procedimientos de operación asociados, así como el entrenamiento de las dotaciones.

4. CONTRIBUCIÓN DEL ENTORNO NAVAL A LA NUBE DE COMBATE

Una de las claves de los futuros conflictos en los que las operaciones multidominio serán predominantes, se basa en la denominada nube de combate, que se fundamenta en una premisa a priori sencilla: en esencia se trata de tener la información correcta, en el destino correcto, en el momento correcto y de forma segura. El objetivo principal es mejorar el poder militar mediante la superioridad de la información.

Para ello es esencial el diseño de una red de información descentralizada y resistente a la cibernética no sólo en el dominio marítimo, sino también en el aéreo, terrestre, espacial, cibernético y cognitivo utilizando tecnologías basadas en la nube que conectan los nodos de la red (usuarios: plataformas, unidades, centros de mando y control) en todos los dominios, permitiendo que la información fluya en tiempo real. La nube de combate debe convertirse así en una parte esencial de cualquier futuro sistema de combate.

En el ámbito marítimo, la nube de combate integrará tanto sistemas tripulados como no tripulados y utilizará los avances en baja observabilidad, las armas de precisión y las herramientas avanzadas de C2, asegurando que ninguna degradación puntual de la nube pueda paralizar las operaciones de combate. Tal esfuerzo presentará una oportunidad para crear capacidades de combate escalables y modulares, en lugar de obligar a las plataformas individuales u otros activos a asumir más y más tareas tácticas.

Las plataformas de combate marítimas de última generación, además de emplear el armamento operan como plataformas ISR. Con la fusión de datos y las capacidades de procesamiento de la nube, las plataformas tendrán también la capacidad de asumir una mayor parte del control local de las operaciones, mucho más allá de la ejecución descentralizada (control distribuido).

Algunos retos de la nube de combate son la amenaza de ciberataques electrónicos y su capacidad para funcionar en entornos electromagnéticos extremadamente restringidos, en los que las operaciones a menudo podrían degradarse o incluso negarse. Sin embargo, el reto más importante reside en la interdependencia de los usuarios de la nube que requerirá un nivel de interoperabilidad sin precedentes. Entre las fuerzas de defensa, tanto nacionales como internacionales, tradicionalmente las operaciones se han llevado a cabo en redes dispares y aisladas, lo que hace que el intercambio de datos y su uso a una escala y velocidad dirigida a cientos de objetivos sea considerablemente más difícil. Un ejemplo de ello es el Link-16, un sistema antiguo que, si bien permite las comunicaciones entre la mayoría de las plataformas, no puede dar cabida a la coordinación en tiempo real de la detección y los efectos contra una amenaza ágil, como la que pretende abordar MDO. La estandarización del dato y la filosofía del "dato único" son elementos clave para resolver este problema. La filosofía del dato único se basa en la introducción de la información una sola vez y en su reutilización en múltiples procesos, sin incurrir en posibles errores o en duplicidades. Es necesario alcanzar un compromiso de interoperabilidad que procure el "dato único" en un entorno colaborativo donde prime el intercambio de información según estándares y el equilibrio entre la necesidad de conocer y la responsabilidad de compartir. La importancia de disponer de un dato único no es otra que poder realizar análisis con resultados fiables y repetibles bajo unas determinadas condiciones y, en caso de fallo o sesgo, aspecto inherente a todo dato, poder revertirlo y trazarlo hasta su origen.

La aplicación de la nube de combate es especialmente importante en las operaciones marítimas multinacionales que se llevan a cabo, por ejemplo, en el marco de la OTAN o la UE, donde un buque insignia de una nación puede operar junto a diferentes buques de otras naciones. **La capacidad de los buques que operan conjuntamente para integrar datos e información de los diferentes sensores y sistemas de armas mejoraría enormemente la capacidad de decisión de los mandos**, al mismo tiempo que permitiría a cada buque desempeñar un papel específico dentro de una flota mayor, integrándose sin fisuras en un todo más amplio.

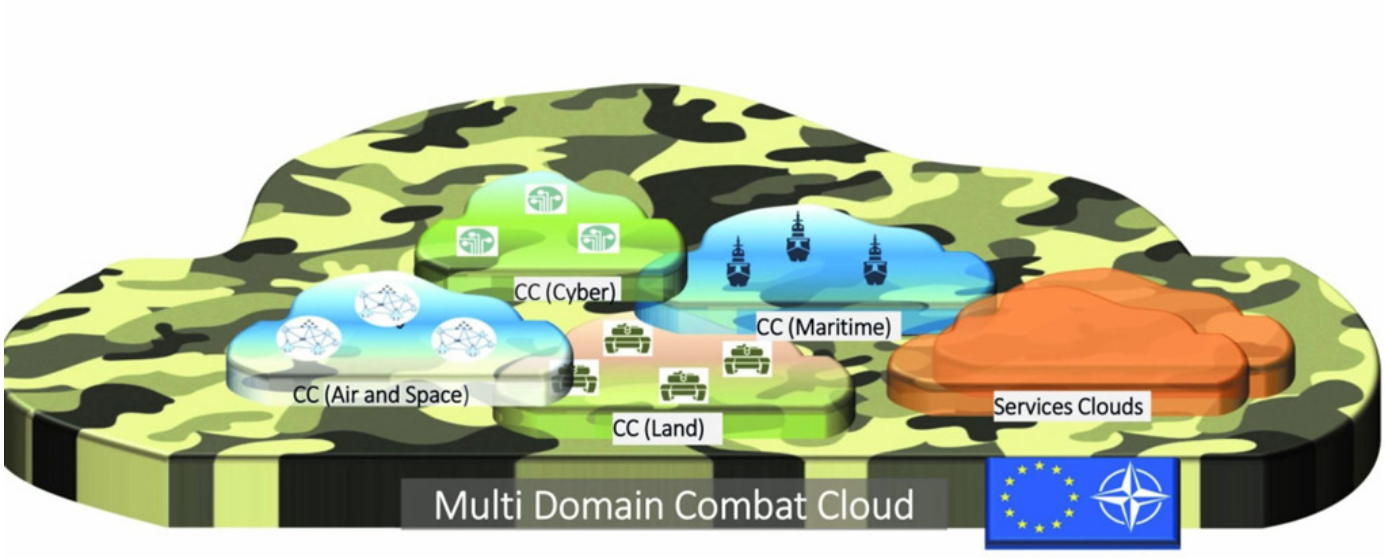


Imagen 9 – Multidomain Combat Cloud. Fuente: Revista ES&t, The Multi Domain Combat Cloud for networked operations management, 14 nov 2022

En 2021 el EDF incluyó en su convocatoria la EDINAF, cuyo objetivo es crear una arquitectura digital de referencia para buques que permita en el futuro la integración de una nube operativa naval conjunta. Con este fin, los socios del consorcio trabajarán para integrar una nube operativa naval conjunta en una nube operativa multidominio más amplia, permitiendo crear así en última instancia la próxima generación de buques inteligentes. Uno de los principales retos a los que se enfrentan las Marinas de Guerra y la industria a la hora de perseguir una integración efectiva es el tecnológico: los sistemas y sensores de combate naval contemporáneos producen grandes cantidades de datos que requieren grandes anchos de banda para poder ser compartidos en tiempo real por enlace de datos. Las soluciones a este problema pasan por la tecnología 5G, la adopción de nubes de combate y una arquitectura de IoT y BD adecuada para gestionar las enormes cantidades de datos que se generan en las operaciones militares, como es el caso, por ejemplo, de los sistemas no tripulados asignados a tareas de ISR. Además, es importante que los futuros sistemas se diseñen para una mayor autonomía con el objetivo de reducir el ancho de banda necesario para su control y también para que sean menos vulnerables a las interferencias.

El proyecto EDF denominado EDOCC (European Defence Operational Collaborative Cloud) tiene como objetivo proporcionar a la UE y los estados miembro una nube de combate multidominio, es decir, una plataforma virtual basada en tecnologías en la nube que aumente la interoperabilidad, eficiencia y resiliencia de las operaciones militares incluyendo las Plataformas Navales. El consorcio está liderado por Airbus Alemania y participan entre otros Navantia, GMV, Indra, Thales, MBDA y Leonardo. El proyecto estudiará, diseñará y validará conceptualmente la plataforma virtual y desarrollará la primera versión de un catálogo de servicios a la vez que identifica estándares y tecnologías apropiados para alto rendimiento e interoperabilidad. En el aspecto marítimo del proyecto, Navantia se encargará de garantizar la interoperabilidad de la solución desarrollada con las diversas plataformas navales.

En España, empresas como Navantia e Indra están impulsando la creación de una Nube de Combate Naval dotando a la Armada de un aumento significativo de la capacidad de la Fuerza Naval a nivel Estratégico, Operacional y Táctico, mediante la captura, el tratamiento y distribución de la información de forma ágil, descentralizada, segura y resiliente, consiguiendo disponer de conciencia situacional completa y única, y permitiendo mejorar de forma significativa el adiestramiento, planeamiento, dirección y ejecución de las operaciones navales, incluidas aquellas de contribución de la Fuerza Naval a operaciones multidominio, tanto nacionales como en coalición. Las principales características de esta nube de combate son:

- Aproximación realista, no reemplaza al CMS a bordo.
- Orientada a Servicios comunes. Despliegue ágil.
- Infraestructura Nube alojada en unidades navales.
- Tecnologías comerciales (COTS), infraestructura hiperconvergente (HCI), IA, Machine Learning (ML), BD, 5G, Realidad Virtual (VR).
- Soluciones para buques existentes y futuros.
- Interoperable, multidominio, multi-país.
- Coexistencia con Enlaces de Datos Tácticos actuales.
- Potenciación de la Industria Nacional/Exportación.
- Esfuerzo colaborativo entre la industria y Armada.
- Sinergias con Programas Europeos Nube: EDINAF, EDOCC y el futuro sistema aéreo de combate (FCAS).
- Un aspecto importante para el éxito de esta nueva Nube de Combate Naval es una evolución del SCOMBA que haga posible su integración nativa con ella. Esta evolución debería contemplar nuevas amenazas (más rápidas, más letales, más inteligentes y baratas), empleo de IA, ML, DL, BD, Realidad Aumentada (RA), RV, 5/6G y HCI, Arquitectura Orientada a Servicios (SOA), visión multidominio, concepto de operaciones (CONOPS), ciberseguridad, nuevas armas y sensores e integración masiva de vehículos no tripulados orgánicos y no orgánicos.

Para el desarrollo de los trabajos de la Nube de Combate Naval, Navantia tiene previsto construir el Centro de Excelencia para el desarrollo de 'Sistemas' (CBTS) en San Fernando.

Es importante destacar que las unidades navales pueden contribuir de una manera decisiva al despliegue de una nube táctica multidominio en operaciones en alta mar o litoral, incluyendo ayuda frente a catástrofes naturales. El 40% de la población mundial vive a menos de 100km de la costa, el 90% del comercio mundial es marítimo y en entorno marino hay numerosos conflictos fronterizos a veces provocados por una situación jurídica compleja, por tanto, es necesario resaltar la importancia de la participación de las unidades navales en nubes MDO y sus principales ventajas:

- Disponibilidad de espacio, peso, potencia, acondicionamiento y refrigeración (HVAC), comunicaciones, personal, etc. para ser potenciales servidores de Nube Multidominio.
- Disponibilidad de gran número de sensores orgánicos y no orgánicos.
- Alta movilidad, resiliencia y gran capacidad defensiva.
- Una doctrina históricamente muy ligada al concepto de "Multidominio".

Dado que todavía existen importantes retos para desarrollar la Nube de Combate Naval como son: la digitalización de las Fuerzas Armadas, la maduración tecnológica, la estandarización y el ordenamiento del ecosistema de nubes de combate; este desarrollo requerirá la colaboración entre numerosas empresas españolas y/o europeas capacitadas para abordar un número importante de tecnologías (habilitadoras, nube, de gestión de programas, ingeniería de sistemas y de operaciones navales).

5. APLICACIÓN DEL GEMELO DIGITAL EN CAPACIDADES NAVALES HACIA EL CONFLICTO MULTIDOMINIO

La capacidad de modelar y simular comportamientos cibernéticos y físicos en tiempo real de una manera operacionalmente relevante es crítica para apoyar las operaciones multidominio. Mediante los GD se alcanza la integración dinámica bidireccional entre un sistema virtual y uno físico, para lo que se requiere de modelos virtuales de alta fidelidad que reflejen adecuadamente los comportamientos del mundo real en el entorno virtual.

Un ejemplo de GD en el contexto marítimo de defensa podría ser una turbina de propulsión a bordo de un buque de combate con sensores digitales integrados, una réplica digital exacta de la turbina "viviendo" en la nube con una conexión totalmente automática de datos bidireccionales entre la turbina física y la virtual. Ejemplos de datos de la turbina física hacia la virtual podrían incluir los niveles actuales de combustible y las revoluciones por minuto del eje. Datos de la turbina virtual a la física podrían incluir órdenes para reducir la velocidad con el fin de conservar el combustible o una actualización de software que modifique el funcionamiento de los componentes físicos.
Dado que el GD implementa tecnologías innovadoras como son la IA, analítica de datos BD, fabricación aditiva, etc., la integración de los diferentes enfoques de GD es un claro reto para tener un modelo europeo compatible y que permita aprovechar al máximo los beneficios de la transformación digital mejorando la eficiencia y eficacia de las operaciones de combate y aumentando el retorno de la inversión en el ciclo de vida, ahorrando en costes de sostenimiento y operación.

5.1. Gemelos Digitales en el Ámbito Naval

En este apartado se describen someramente algunos ejemplos de GD navales en el ámbito de defensa que están en proceso de desarrollo actualmente.

La US Navy considera la transformación digital una de sus prioridades y ya utiliza GD para optimizar las modernizaciones y reparaciones de buques de la flota mejorando su disponibilidad y ahorrando tiempo y dinero. Así por ejemplo durante la ejecución de tareas de modernización del Sistema de Combate AEGIS el uso de su GD ha permitido acelerar el proceso de prueba de los cambios en el software y su implantación en la flota. Otro ejemplo destacable es el uso del GD de una turbina de gas de un buque militar en operación en el que hubo un problema con una de las turbinas de gas, y por medio de este gemelo digital se diagnosticó rápidamente el problema, se determinó cuál era el modo de fallo y se hizo llegar la pieza al buque sin tener que desplazar a un técnico hasta él. Además, la US Navy espera ampliar esta capacidad digital en el futuro yendo hacia un sistema de mantenimiento de buques más completo e integrado. No obstante, queda mucho trabajo por hacer para integrar diferentes GD y crear un entorno digital completo que pueda apoyar todo el proceso desde el diseño conceptual, elaborado por la propia Marina, el diseño de detalle de la industria y el mantenimiento posterior durante toda la vida útil de la clase de buque.

En España la Fragata F-110 será el primer programa de adquisición que incluye el desarrollo de un GD. Este sistema será una réplica virtual realimentada con los datos suministrados por una red de sensores distribuidos por el buque utilizando tecnologías como Cloud Computing, ML o el IoT. Estas tecnologías permitirán monitorizar el mantenimiento de las fragatas, e incluso algunas de sus operaciones, a miles de millas de distancia a través del GD desplegado en tierra.

El alcance del GD de las Fragatas F-110 incluye como principales funcionalidades:

- Optimizar el diseño y operación de los sistemas.
- Anticipar procesos de verificación y validación. Percepción y respuesta en tiempo real.
- Mantenimiento predictivo, basado en la condición.
- Modelado y simulación del funcionamiento de sistemas críticos.
- Apoyo a la toma de decisión.
- Identificación de deficiencias al comparar el sistema físico con sus modelos digitales.
- Soporte a la dotación con información actualizada.
- Almacenamiento y sincronización de datos e información entre las plataformas desplegadas.
- Gestión (generar, modificar y presentar) de la documentación operativa del buque.
- Interconexión con sistemas externos de información de carácter táctico, logístico, de información del personal embarcado (nivel de adiestramiento, económico/ financiero, salud, aptitudes, tareas asignadas, etc.)

Para la Armada, la prioridad en este Programa pionero de desarrollo de un GD de un buque completo, como consecuencia de las anteriores funcionalidades, se centra en la mejora del sostenimiento, adiestramiento y determinados aspectos de toma de decisiones operativas considerados alcanzables dentro del Programa de Adquisición, véase:

- Sostenimiento:
  - » Gestión de la configuración y visualización de la información de interés para la dotación.
  - » Capacidad de apoyo y reparación asistida (realidad virtual y aumentada, in situ o de forma remota).
  - » Apoyo en la gestión de sostenimiento (predicciones y recomendaciones de actuación por medio del uso de tecnologías de IA, BD e IoT).
  - » Impresión de piezas mediante tecnología 3DP (fabricación aditiva).

Imagen 10 – F110 – Gemelo Digital, Fuente: Periódico Expansión, Indra fabricará por 150 millones la antena digital del radar AESA de las Fragatas F-110, 12 dic 2019

- Toma de decisiones en operación, permitiendo predecir situaciones futuras y proporcionar recomendaciones de actuación.
  - » Sobre la configuración de equipos y sistemas para la optimización de firmas y maniobras para navegación segura.
  - » Acciones necesarias para estimar el grado de alistamiento y operatividad.
  - » Recomendar acciones para mejorar la eficiencia y el cumplimiento de la misión.
  - » Reacción táctica del buque ante situaciones determinadas.
  - » Reacción ante incidencias del tipo inundación, impacto e incendio.

Todas estas funcionalidades del GD de las F-110 obligan a disponer de una serie importante de capacidades técnicas que hacen de este desarrollo un reto tecnológico:

- Alta capacidad de cálculo, analítica avanzada y proceso gráfico a bordo.
- Almacenamiento y procesado de gran número de fuentes de datos a bordo.
- Desarrollo en tierra de asistentes a la operación, mantenimiento y entrenamiento con diferentes grados de automatización.

Para resolver este reto el programa incluye el despliegue de **tres plataformas digitales** que, para garantizar la unicidad y consistencia de los datos de cada uno de los GD, se mantendrán sincronizadas en tiempo útil:

- **Astillero:** en la que se registran todos los acontecimientos seleccionados en la vida constructiva de cada buque en particular y de la clase en general.
- **Defensa en tierra:** en la que se consolida y analiza la información de los cinco buques de la clase e interactúa con los sistemas existentes de la Armada.
- **A Bordo:** que alberga solamente la información del buque al que representa. Se encontrará embarcada en cada una de las unidades e interactuará directamente con los sistemas del buque.

6. CONCLUSIONES

En las últimas décadas se ha reducido la ventaja de occidente en las capacidades y tácticas de combate en la guerra convencional frente a otros protagonistas del escenario geopolítico como China y Rusia, siendo la estrategia militar de estos países dar mayor prioridad al entorno naval frente a la tradicional importancia dada al teatro terrestre.

El hecho de que la guerra naval toque prácticamente todos los dominios físicos de la guerra, además de las zonas litorales que son escenario de operaciones anfibias, hace del combate naval un caso de estudio ideal a la hora de examinar cómo la innovación tecnológica afecta a los sistemas de combate y a su integración eficaz como parte de un SoS en un enfoque multidominio.

Prueba de esto es que los sistemas de combate naval engloban todos aquellos elementos como sensores, actuadores, C2 y comunicación, etc. que contribuyen directamente a las operaciones ofensivas y/o defensivas (AAW, ASuW, ASW, guerra anti-minas (MW) abarcando desde misiles, torpedos, minas, cañones navales con munición guiada, helicópteros y aviones tripulados o no, hasta los sensores necesarios para la detección y la identificación de amenazas, y en un futuro no muy lejano, las DEW.

Sin duda, es la integración de los CMS naval, en un enfoque SoS, lo que representa el verdadero cambio de las reglas de juego en la lucha naval, siendo esta la clave para construir flotas más resistentes, versátiles y distribuidas que sean verdaderamente interoperables en un contexto multinacional y multidominio.

Esta evolución en la integración de sistemas solo será posible con el desarrollo y la implantación de nuevas tecnologías (IA, IoT, BD, blockchain, sistemas autónomos, etc.) que permitan que la nube de combate sea una realidad que otorgue al poder militar la necesaria superioridad de la información y en la toma de decisiones, es decir, que permita disponer de la información correcta, en el destino correcto, en el momento correcto y de forma segura.

Algunos retos de este enfoque SoS centrado en la nube de combate son la amenaza de ciberataques, la capacidad para mantener la operatividad en entornos electromagnéticos extremadamente restringidos, alcanzar la maduración tecnológica necesaria para un nivel de hiperconectividad e interoperabilidad sin precedentes, la digitalización de las Fuerzas Armadas y la estandarización y el ordenamiento del ecosistema de nubes de combate. Y la necesidad de la ciberdefensa obliga a la evolución de los sistemas C4ISR a sistemas C5ISR (mando, control, comunicaciones, computación y ciberdefensa).

Una consecuencia del mismo es la tendencia de las plataformas a integrar, CMS más sofisticados que sus predecesores (capaces de gestionar todos los sistemas y los datos entrantes y conectado a una red integrada). Esto permite garantizar su preparación en caso de conflicto con adversarios pares o casi-pares en un entorno multidominio, y equipados con un gran número de sensores, contramedidas y sistemas de armas de última generación que aumenten sus capacidades tanto ofensivas como defensivas.

Es también importante considerar que los diseños de los buques de guerra modernos deben tener en cuenta la futura evolución de la tecnología y de las necesidades operativas para alargar su vida útil, retrasando lo máximo posible su obsolescencia y reflexionando sobre las implicaciones en la dotación en términos de número y habilidades requeridas de cada miembro, así como el tipo de formación necesaria para operar dichas tecnologías avanzadas. Un planteamiento de este tipo requiere el desarrollo de sistemas abiertos y modulares que puedan someterse fácilmente a actualizaciones y mejoras para adaptarse a amenazas y requisitos operativos nuevos o cambiantes tanto en lo que respecta a la fase de desarrollo y diseño, como al marco contractual que sustenta un programa de adquisición. Y al mismo tiempo, del desarrollo de plataformas cada vez más completas y de mayores dimensiones que puedan albergar todos estos sistemas y equipamiento, y el desarrollo de vehículos no tripulados cada vez más complejos y con mayores funcionalidades.

Un elemento clave en el desarrollo de las capacidades navales en operaciones multidominio es el GD, cuyo desarrollo satisfactorio permitirá aprovechar al máximo los beneficios de la transformación digital mejorando la eficiencia y eficacia de las operaciones de combate multidominio y aumentando el retorno de la inversión en el ciclo de vida ahorrando en costes de sostenimiento y operación. Dado que este elemento incorpora tecnologías innovadoras críticas como la IA, analítica de datos, fabricación aditiva, etc., la integración de los diferentes enfoques o modelos de GD es un claro reto para tener un modelo de GD compatible entre naciones aliadas.

En todo este esfuerzo de las diferentes Marinas de Guerra e industrias europeas, la UE puede desempeñar un papel importante en el fomento de la cooperación entre sus Estados miembros a la hora de planificar el desarrollo y la adquisición de sistemas navales de combate de última generación. A corto plazo el programa EPC es uno de los proyectos más ambiciosos e importantes para comprobar la viabilidad de una cooperación eficaz dentro la UE.

Tras el análisis de la información presentada en este capítulo sobre capacidades navales, observamos gaps o dependencias tecnológicas de la UE frente a otros países en aspectos clave como el desarrollo de nuevas tecnologías en sistemas de armas (misiles hipersónicos y DEW). Se observa también falta de iniciativas de desarrollo de proyectos conjuntos de gran porte, análogas al proyecto de la EPC, en el área de C2 y comunicación, con proyectos similares al Overmatch de EEUU, y en el área de sistema de combate creando un CMS basado en los diferentes desarrollos existentes en Europa (SCOMBA – Navantia; TACTICOS – Naval Group; ATHENA – Leonardo, etc.) que fomente un enfoque SoS integrado e interoperable entre las diferentes unidades navales europeas y sirva de guía a la industria de Defensa (armas, sensores, etc.) en sus nuevos desarrollos. También es destacable la diferencia en prestaciones técnicas de algunos sistemas desarrollados en la UE frente a sus homólogos desarrollados en EEUU, como es el caso de los radares banda S de exploración aérea y su sistema para control y guiado de misiles anti-aéreos.

No obstante, hay que resaltar que existe una base industrial potente a nivel UE que cubre la mayor parte de las necesidades de Defensa y servirá, siempre que se aplique un enfoque común, para alcanzar o mantener las capacidades navales europeas al nivel de las grandes potencias mundiales en aspectos críticos como: nuevas tecnologías disruptivas (IA, IoT y BD, blockchain,

robótica y sistemas autónomos, tecnologías cuánticas, biotecnologías, etc.), nuevas tecnologías en sistemás de armas (armas hipersónicas, DEW), diseño y construcción naval, etc.

La principal dificultad que se debe superar a corto plazo es conseguir impulsar coordinadamente la base industrial europea, de modo que se satisfagan los intereses de todos los países miembros, fomentando en el marco de la UE colaboraciones, consorcios o incluso fusiones de empresas de diferentes países en las que se creen sinergias que permitan competir a nivel mundial. Para llevar esto adelante es fundamental una política de Defensa y Seguridad Europea común, en la que la soberanía Europea predomine sobre la de los estados miembros individuales, rompa con el proteccionismo tecnológico de los países miembros y que impulse y distribuya las inversiones en aquellas capacidades de interés estratégico común.

Centrando el análisis en la industria naval europea de Defensa, encontramos seis grandes astilleros como Navantia, Naval Group, Thyssenkrupp Marine Systems, BAE Systems, Fincantieri y Damen. Además de los anteriores, también se pueden destacar Karlskrona (astillero del grupo sueco SAAB), NVL (división militar del astillero alemán Lürssen), y otros, que cubren sobradamente las necesidades nacionales de construcción de buques militares de la UE. Muchas de estas empresas son estatales, o con alta participación estatal, por su carácter estratégico, y esto puede considerarse una oportunidad de cara a conseguir una mayor integración del sector industrial, dado que el hecho de ser estatal facilita poder llevar a cabo una reorganización de las capacidades de cada estado de modo que se mejore la eficacia y eficiencia de diseño y construcción naval con un enfoque europeo global. Además, en Europa existen un gran número de astilleros que, si bien no tienen entre sus principales productos buques militares, pueden apoyar y complementar a los grandes astilleros militares en tipos concretos de buques.

De lo contrario se corre el riesgo de tener muchos astilleros en Europa con baja carga de trabajo (inmersos en series cortas de buques para satisfacer la demanda nacional), multidisciplinares y probablemente deficitarios, que a largo plazo sean incapaces de competir internacionalmente y por tanto pierdan la ventaja tecnológica actual frente a astilleros de otros países con mejores situaciones financieras que les permitan seguir invirtiendo en I+D+i. Un enfoque interesante de reorganización podría ser la agrupación de astilleros para especializarse en tipos determinados de buques (portaaviones, fragatas, corbetas, patrulleros, submarinos, etc.) de modo que se pudiera compartir conocimiento, infraestructuras, mano de obra y oportunidades comerciales, afrontando series más grandes de buques, al tiempo que se mantienen las capacidades estratégicas de cada país, minimizando con ello redundancias.

REFERENCIAS

1. Congressional Research Service. (2024). Navy Shipboard Lasers: Background and Issues for Congress. Congressional Research Service (CRS) – Report R44175. https://sgp.fas.org/crs/weapons/R44175.pdf.

2. Brake M. et al (2023). Naval Combat Systems: Developments and Challenges. Istituto Affari Internationali (IAI). ISSN 2280-6164 https://www.iai.it/en/pubblicazioni/naval-combat-systems-developments-and-challenges.

3. Diario 20 Minutos. (2022, noviembre). Un enjambre de drones kamikaze navales con piezas canadienses y posible asesoría inglesa: así fue el ataque de Ucrania a la flota rusa. https://www.20minutos.es/noticia/5072948/0/asi-fue-el-ataque-de-ucrania-a-la-flota-rusa-con-drones-kamikaze-navales.

4. Forbes (2020, enero). China Has 'First-Strike' Capability To Melt U.S. Power Grid With Electromagnetic Pulse Weapon. https://www.forbes.com/sites/jamesconca/2020/06/25/china-develops-first-strike-capability-with-electromagnetic-pulse.

5. Breaking Defense (2022, abril). Bollinger Shipyards wins big with MCM USV production contract. https://breakingdefense.com/2022/04/bollinger-shipyards-wins-big-with-mcm-usv-production-contract/#:~:text=WASHINGTON%3A%20The%20Navy%20has%20awarded,vessel%20made%20by%20Textron%20Systems.

6. Hoja de datos UE. (2021). EPC - European Patrol Corvette. EUROPEAN DEFENCE FUND. https://defence-industry-space.ec.europa.eu/system/files/2022-07/Factsheet_EDF21_EPC.pdf.

7. Pons J. (2022). LA CORBETA de las cuatro banderas. Revista Española de Defensa. https://www.defensa.gob.es/Galerias/gabinete/red/2022/10/RED398.pdf.

8. Balfoort J. (2022). EUROPE, COOPERATING FOR A NAVAL AMBITION - The European Union's maritime security strategy, a tool for an integrated approach to the protection of European sea-related interests. Centre d'études stratégiques de la Marine - N°21. ISSN 2119-775X https://www.defense.gouv.fr/en/node/4487.

9. Argumosa J. (2017). Tendencias que afectarán a las Fuerzas Armadas 2050. INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS. https://www.ieee.es/Galerias/fichero/docs_opinion/2017/DIEEEO117-2017_FAS-2050_R.JesusArgumosa.pdf

BIOGRAFÍAS

ALBERTO DOMÍNGUEZ ABECIA

Ingeniero Naval por la Escuela Técnica Superior de Ingenieros Navales de la Universidad Politécnica de Madrid. Máster en Administración de Empresas por el Instituto de Empresa. Comenzó su carrera en el año 1999 y ha dedicado gran parte de su trayectoria profesional al análisis y seguimiento de proyectos de construcción naval, así como en el análisis de proyectos de explotación de buques civiles.

Asimismo, ha participado en el proyecto de diseño de un astillero de nuevas construcciones y reparaciones en Ecuador, y ha sido Secretario del Comité Técnico de Normalización AEN/CTN27 – Construcción Naval, de AENOR.

Es Jefe de Área de Sistemas de Plataformas Navales en Isdefe, y presta asistencia técnica en los Programas de obtención de las Fragatas F-110, Submarinos S-80, Buques de Acción Marítima y Flotilla Hidrográfica, en las correspondientes Oficinas de Programa de Jefatura de Sistemas Navales (JSNAV) de la Dirección General de Armamento y Material del (Ministerio de Defensa).

FERNANDO JAVIER SENENT GÓMEZ

Ingeniero Naval y Oceánico por Escuela Técnica Superior de Ingenieros Navales de la Universidad Politécnica de Madrid. Comenzó su carrera en el año 2003 y ha dedicado gran parte de su trayectoria profesional al desarrollo de proyectos navales, tanto militares como civiles, en el ámbito de las nuevas construcciones y ubicado en diversos países como España, India y Brasil. Con experiencia valorable en la mayoría de las fases de adquisición de programas multidisciplinares, desde el diseño conceptual hasta la producción, y con vocación profesional hacia la gestión de proyectos (certificado PMP 2003).

Tiene referencia profesional trabajando ya sea desde el lado del astillero constructor (contratista) como desde el lado del armador (contratante). Como consultor senior en el área de Sistemas de Plataformas Navales en la empresa Isdefe, presta asistencia técnica al Área de Plataforma del Programa de obtención de Fragatas F-110 en la Oficina de Programa de la Jefatura de Sistemas Navales (JSNAV) de la Dirección General de Armamento y Material del Ministerio de Defensa.


601

CAPÍTULO 5

Capacidades Aéreas ante el FCAS

Cesar Heras Menor de Gaspar

El concepto del Futuro Sistema de Combate Aéreo (Future Combat Air System conocido como FCAS), será la pieza clave para la definición del Combate Aéreo del futuro.

Este concepto FCAS ha de entenderse como la iteración de Sistemas de Sistemas, lo que engloba los medios aéreos que actualmente tienen las fuerzas aéreas, y las futuras plataformas y sistemas que existirán en el entorno de 2040. El objetivo de este concepto FCAS es potenciar y maximizar el combate colaborativo de los distintos elementos de las fuerzas aéreas que intervienen de forma relevante en el dominio aeroespacial.

El desarrollo de las capacidades relacionadas con el combate colaborativo será el punto de inflexión de las batallas aéreas del futuro, además, será lo que diferencie la futura superioridad en el enfrentamiento.

Los nuevos sistemas aéreos que se desarrollarán en las próximas décadas estarán orientados al trabajo colaborativo, apoyándose en las tecnologías que se encuentran en fase de maduración (como la IA, sistemas LO, nuevos tipos de armamento, etc.)., lo que va a implicar una adaptación de las Fuerzas Aéreas, las cuales deben definir su concepto FCAS.

Esta definición del FCAS a medio plazo, conllevará la implementación de nuevas capacidades a los sistemas actualmente operativos: Eurofighter, A-400, MRTT, C-295, RPAS y sustituto del F-18; los cuales deberán incorporar cierta capacidad de combate colaborativo, que a su vez deberá ser compatible con los futuros sistemas como el NGWS.

1. EVOLUCIÓN DEL COMBATE AÉREO HACIA EL CONFLICTO MULTIDOMINIO

Actualmente el combate aéreo está perfectamente estructurado y su ejecución se lleva a cabo por un conjunto de personas, organizadas de una forma determinada (roles predeterminados, jerarquía establecida, etc.), con un objetivo común: la ejecución de una misión. Se podría decir que, en el trabajo en equipo dentro del combate aéreo, cada miembro del grupo tiene una misión asignada, la cual ejecuta para poder conseguir el objetivo común.

La proliferación de cazas furtivos, los sistemas integrados de defensa aérea de nueva generación y los combates a mayor distancia y alejados del territorio nacional están dificultando conseguir y mantener la superioridad aérea. Todo apunta además a que el escenario futuro del combate aéreo integrará una combinación de aeronaves tripuladas y no tripuladas, manteniendo a los pilotos como jefe de la misión. Como se ha mencionado en el primer capítulo, las operaciones multidominio se caracterizarán por la capacidad de operar en diversos dominios de forma simultánea, con una coordinación y control distribuidos de manera ágil y rápida a través de estos.

Así, el futuro del poder aéreo combinará un gran número de aeronaves no tripuladas autónomas colaborativas, centradas en la ejecución de la misión, junto con los cazas, denominados de 6ª generación, tripulados por humanos. Un piloto en un caza necesitará de varios sistemas no tripulados para proporcionar profundidad de combate o vigilar el espacio de batalla que se avecina, evitar la detección, transmitir datos de sus sensores y, si es necesario, tomar decisiones que afecten a la misión. Esto no solo presenta un desafío en el diseño aeroespacial, sino que también requiere una gestión de la información del campo de batalla que actualmente se está desarrollando.

Es por ello, que la nueva forma de combatir en el dominio aéreo es el combate aéreo colaborativo, basado en los nuevos sistemas que están desarrollando las distintas naciones (como los casos del NGWS , NGNAD o GCAP), cuyo desarrollo marcarán la transformación de las fuerzas aéreas del futuro.

De igual forma que los aviones de combate, el resto de los sistemas que determinan el campo de batalla dentro del dominio aéreo (Aviones de transporte, sistemas C2 e información), están evolucionando también hacia un aspecto colaborativo, como son el desarrollo de programas del FMTC (Future Mid-size Tactical Cargo Aircraft.) o el JFEA (Joint Future European Airlifter), los cuales ya contemplan las operaciones colaborativas.

De este modo, las fuerzas aéreas se enfrentan al desarrollo de un nuevo concepto de combate aéreo, que supone a su vez un nuevo concepto de operación basado en la acción colaborativa entre distintos sistemas o plataformas actuales y de futuro, todo ello unido a la evolución tecnológica que permitirá poder desarrollar estas nuevas capacidades.

Pero ¿qué es el Combate Aéreo Colaborativo?

Para contestar esta pregunta, empezaremos por analizar las características del trabajo cooperativo y colaborativo, así como sus principales diferencias.

En el trabajo cooperativo, cada miembro del grupo tiene asignada una parte del trabajo de forma equitativa, siendo cada uno de ellos responsable de esa tarea específica, pero trabajando todos por llegar al mismo objetivo común. El tipo de liderazgo es tradicional, con un líder que estructura y supervisa tareas e hitos, tomando decisiones y dirigiendo las partes comunes. Podríamos decir que en este tipo de tareas se produce un aprendizaje individual de los componentes del grupo.

A diferencia, en el trabajo colaborativo, las tareas se realizan de forma grupal y no individual, compartiéndose conocimientos e ideas que enriquecen y desarrollan al grupo que gana también creatividad. El liderazgo es más informal, con las ventajas de lograr mayor eficacia y productividad, autogestión en las horas de trabajo, comunicación más fluida, con menos errores, mejor clima laboral que lleva a mayor motivación y sentido de pertenencia de los miembros del equipo.

En definitiva, es una modalidad de trabajo que basada en la filosofía de la interacción y que, como su nombre indica, implica trabajar en colaboración con otros individuos. En este enfoque, se crean sinergias y beneficios recíprocos entre los miembros del equipo. La clave principal del trabajo colaborativo es que todos los participantes se reúnen de manera conjunta, dinámica y descentralizada para alcanzar un objetivo común.

Establecidos estos conceptos y contestando nuestra pregunta, podemos decir que la diferencia más clara entre el combate aéreo cooperativo y el colaborativo radica en su nivel de interconexión y coordinación.

Mientras que, en el combate cooperativo, las aeronaves trabajan juntas como un equipo, la comunicación es directa entre ellas, lo que les permite compartir información sobre objetivos y amenazas, tales como formaciones de vuelo, ataques sincronizados y maniobras conjuntas, sin embargo, no necesariamente están completamente interconectadas. En el combate aéreo colaborativo, las aeronaves forman una red interconectada que distribuye datos en tiempo real, creándose una nube de información (nube de combate) que comparten datos sobre objetivos detectados, amenazas y rutas de vuelo, debiendo existir interfaces avanzadas entre hombre-máquina mejoradas y sistemas de visualización, teniendo como objetivo lograr una superioridad aérea conjunta mediante la colaboración efectiva de fuerzas conjunto-combinadas.

En resumen, mientras que el combate cooperativo se centra en la cooperación básica entre aeronaves, el combate colaborativo buscará una mayor interconexión y coordinación para maximizar la eficacia en el campo de batalla.

Dentro de los países aliados de la OTAN, se está elaborando una nueva doctrina que engloba las nuevas capacidades de los sistemas (Doctrina JADO, de sus siglas en inglés Joint All Domain Operations). Esta doctrina, engloba cómo afrontar de forma conjunta y simultanea la operación en los distintos dominios (terrestre, naval, aéreo, espacial y ciber) de forma simultánea.

Si bien, en cada dominio pueden desarrollarse acciones con efectos sobre el resto, para el dominio aéreo pueden hacerse las siguientes consideraciones:

- Una misión de defensa aérea representa una operación dentro del dominio aéreo.
- Una misión SEAD (Supresión de Defensas Aéreas Enemigas), supone una operación del dominio aéreo a ejecutar en el dominio terrestre.
- De igual forma si las defensas Áreas están situadas en un buque, o bien una misión anti-submarina (ASW), la operación del dominio aéreo se ejecuta dentro del dominio naval.
- Y, por último, si lo que queremos es destruir un centro de datos del enemigo, estaríamos realizando una operación aérea dentro del dominio ciber, dentro del plano físico de este.

Todo supone, definir adecuadamente las capacidades asociadas al Combate Aéreo Colaborativo, ya que afectarán a todos los dominios de la batalla.

Para poder definir estas capacidades, es necesario elaborar el concepto del Futuro Sistema de Combate Aéreo (FCAS por sus siglas en inglés), pieza clave para la definición del Combate Aéreo Colaborativo en el cual todos los sistemas que disponen las Fuerzas Armadas se ven afectados. En la siguiente figura se muestra cómo sería un esquema de colaboración FCAS:

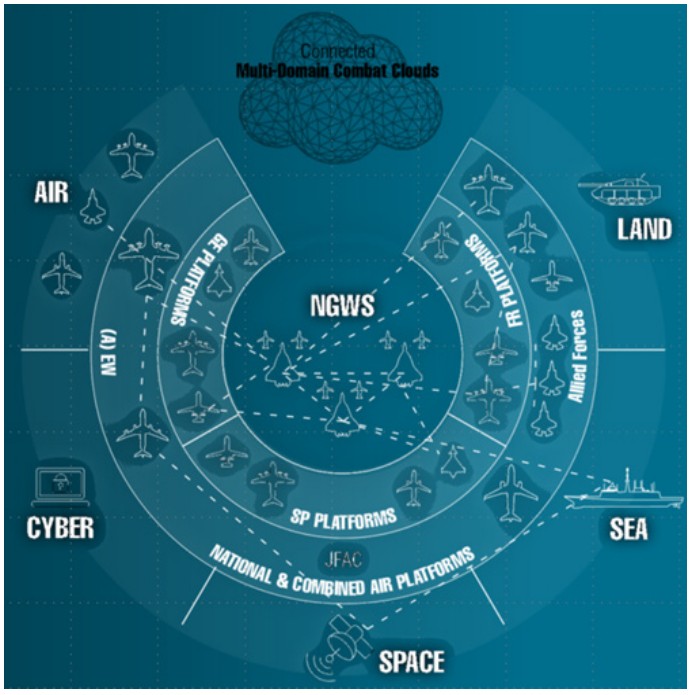


Ilustración 1: Representación FCAS (Futuro Sistema de Combate Aéreo)

El objetivo del concepto FCAS es potenciar y maximizar la operación colaborativa de los elementos de las fuerzas aéreas y otros que intervienen de forma relevante en el dominio aeroespacial.

En el ámbito europeo, este concepto engloba los sistemas de que disponemos actualmente Eurofighter, A-400, MRTT (Multi Role Tanker Transport), C-295, RPAS (Remotely Piloted Aircraft System) y sustituto del F-18, sistemas de mando y control, satélites para inteligencia, los cuales trabajarán de forma cooperativa, y los sistemas en desarrollo NGWS, Euromale, futuros RPAS o UAV, que lo harán de forma colaborativa. Esta forma de trabajar será la que determine las capacidades y necesidades derivadas de las futuras Nubes de Combate en cada dominio y la nube conjunta.

El concepto FCAS ha de entenderse como un Sistema de Sistemas (SoS), el cual engloba los medios aéreos que actualmente tienen las fuerzas aéreas, y las futuras plataformas aéreas que existirán en el entorno de 2040, y que no ha de confundirse con programas en curso, como el NGWS.

Algo importante que también definirá el combate aéreo colaborativo, será el factor de interoperabilidad. Los distintos sistemas que se están desarrollando dentro del ámbito de la OTAN, deberán poder ejecutar misiones de forma conjunta, por lo que los estándares de comunicación, gestión de datos y de información deberán ser comunes a todos, independientemente de las capacidades que, por separado, tengan cada uno de los sistemas.

Se trata de conseguir que, para cumplir la misión encomendada y alcanzar la superioridad en el enfrentamiento, se debe buscar la acción coordinada y eficiente de todos los recursos que participan e intervienen en el combate, en el dominio aeroespacial, de forma que el resultado vaya más allá de la mera suma de las capacidades de cada sistema.

El elemento diferenciador del combate aéreo colaborativo que permitirá maximizar la operación eficiente para tener éxito en los escenarios futuros será la nube de combate (CC por sus siglas en inglés, Combat Cloud). Este elemento del sistema permitirá compartir no solo información, sino los recursos de las diferentes plataformas incrementando la resiliencia y las capacidades del sistema completo.

En los programas que están actualmente en fase de estudio de concepto o desarrollo, como es el caso del NGWS, implica que las funciones que se le asignarán se realizarán como Sistema de sistemas (SoS), el cual está compuesto por los siguientes elementos, que tendrán cada uno una misión específica dentro de la misión del Sistema de sistemas:

- Avión de combate.
- Sistemas aéreos autónomos.
- Nube de Combate.

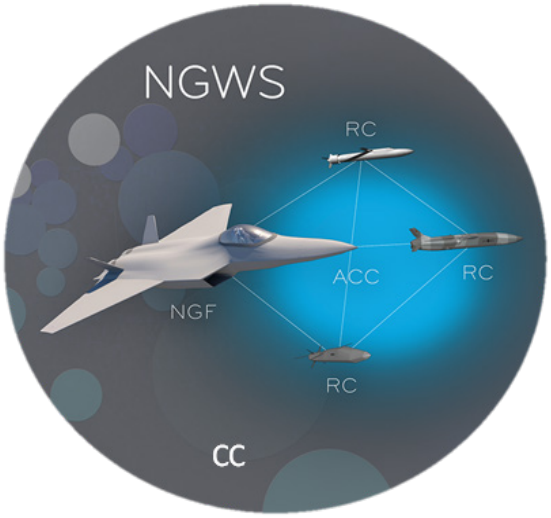


Ilustración 2: Representación gráfica de un Sistema de sistemas, Concepto del Programa NGWS

La ilustración anterior muestra el concepto de Sistema de sistemas que se está desarrollando en el programa NGWS. Se trata de un SoS que está formado por los tres elementos mencionados anteriormente, los cuales, desarrollaran las misiones encomendadas de forma colaborativa, siendo el primer sistema de armas de este tipo. Este futuro sistema impulsará el futuro concepto de operación FCAS.

El objetivo principal de todos los sistemas que participan en una misión aérea de combate (aviones de combate, transporte, no tripulados, C2, etc.) es reducir al máximo el denominado “Ritmo Operativo”, el cual permite debilitar las capacidades de combate del adversario.

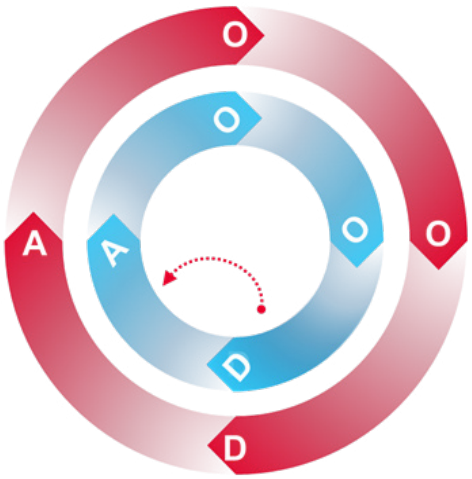


Ilustración 3: Representación del Ciclo OODA

El "Ritmo Operativo" es la ejecución del ciclo OODA (Observar, Predecir, Decidir y Actuar) y cuanto más rápido y preciso se ejecute, mejor se desarrollará el combate. Cuantas más veces se repita el ciclo azul de la ilustración, que representa las fuerzas propias, por cada ejecución del ciclo rojo (fuerzas adversarias), mayor ventaja operativa se dispondrá con respecto al enemigo.

En cualquier combate, la información del campo de batalla, lo que está ocurriendo, es algo necesario para el devenir de la misión, siendo un hecho diferenciador en cualquiera de los dominios. Este hecho se vuelve más restrictivo en el combate aéreo, ya que en numerosas ocasiones las comunicaciones se realizan entre los distintos equipos que forman las misiones lideradas por el Mission Commander, sin que el nivel operacional y estratégico puedan tener información durante la ejecución de la batalla. Hecho que será fundamental en el combate aéreo colaborativo (denominado FCAS), ya que permitirá la toma de decisiones de forma rápida y por todos los niveles.

Actualmente dentro del dominio aéreo, el Mission Commander realiza una ejecución de la misión de forma descentralizada al delegar en los subordinados la toma de decisiones para permitir flexibilidad, iniciativa y capacidad de respuesta en el cumplimiento de ésta. El concepto FCAS permitirá que el Mission Commander pueda participar de forma más activa dentro de la ejecución de una misión.

Para poder conseguir este objetivo, es necesario definir primero las nuevas capacidades que se quieren cubrir dentro del "BI-SC Capability Codes and Capability Statements" , establecer cuáles serán las que afecten a todos los dominios y posteriormente proceder a su implantación.

Evidentemente, estas capacidades se irán alcanzando de forma incremental, dependiendo de cómo evoluciona la tecnología, la disponibilidad económica y de las prioridades marcadas por las autoridades de planeamiento.

Aun así, tanto los países que están desarrollando el NGWS (España, Alemania, Francia), como el resto de los aliados de la OTAN (EE. UU, UK, Italia, etc.), están definiendo cuál es su concepto FCAS, lo que implicará cómo serán las futuras operaciones conjuntas entre los distintos aliados.

En el entorno 2040-2080, la nación que no tenga definidas y desarrolladas sus capacidades de Combate Aéreo Colaborativo no podrá ejecutar misiones con sus aliados, y por lo tanto verá disminuida su capacidad de superioridad en el enfrentamiento aéreo.

El nuevo FCAS deberá proporcionar unidad al ámbito y, a su vez, sinergia con el resto de ellos (terrestre, naval y ciber espacio; (como en la ilustración 1).

El poder aéreo ofrece la ventaja de encontrar, fijar y enfrentarse a las fuerzas de superficie del adversario en toda la profundidad del espacio de batalla. La sinergia de las capacidades de las fuerzas terrestres, navales y aéreas, que operen como una fuerza conjunta integrada, será lo que marque la diferencia en el éxito de la batalla.

El poder aéreo explota la naturaleza de la tercera dimensión. Las aeronaves son generalmente más rápidas que los vehículos de superficie y navales y, a menudo, pueden dirigirse directamente a un objetivo o destino, ya que, por definición, la elevación es inherente a las operaciones aéreas. Estos factores dan como resultado los tres atributos centrales del poder aéreo:

- **Velocidad.** La velocidad de las aeronaves permite proyectar el poder militar con rapidez y capacidad de respuesta y completar misiones rápidamente.

- **Alcance.** Alrededor del 70% de la superficie de la Tierra es agua, pero todo está cubierto por aire. Esto proporciona a las aeronaves un alcance inigualable, normalmente sin obstáculos por el terreno.

- **Altura.** La ventaja de la altura es una realidad militar perdurable. El poder aéreo ofrece un punto de vista incomparable; facilitar la observación y, por lo tanto, permitir las operaciones dentro de los dominios terrestre y marítimo.

El futuro combate aéreo contendrá la unión de cada uno de estos factores, pero en lugar de la acción de un grupo de aviones ejecutando cada uno su misión para el bien de una operación común se orientará a la ejecución de una operación de Sistema de sistemas, incluyendo el resto de los dominios (terrestre, naval y ciber).

Actualmente una operación aérea, se realiza de la siguiente forma:

1) Para cumplir con la misión asignada, la JTF (Joint Task Force) desarrolla un Concepto de Operaciones (CONOPS), proporciona la intención del comandante para la misión asignada y luego organiza las fuerzas asignadas en base al CONOPS.

Este CONOPS se desarrolla en un plan de operación (OPLAN), y el Comandante Supremo, designará un componente aéreo de fuerza conjunta, denominado comandante JFAC (Joint Force Air Component) para explotar las capacidades de las operaciones aéreas conjuntas.

2) Desde el comienzo de las operaciones, las fuerzas aéreas pueden perseguir objetivos estratégicos, operacionales o tácticos, en cualquier combinación, o los tres simultáneamente. Por lo tanto, es esencial que se tome un grado de unidad de esfuerzo que permita que los activos aéreos se concentren en el momento y lugar críticos para lograr resultados, maximizando la sinergia conjunta.

3) El control centralizado asigna la responsabilidad y la autoridad para planificar, dirigir y coordinar las capacidades aéreas a un solo mando y su estado mayor. A su vez, maximiza la eficacia operativa y evita la duplicación de esfuerzos.

4) Ejecución descentralizada. Es la delegación de la autoridad de ejecución a comandantes subordinados responsables y capaces para tomar decisiones en la escena que exploten oportunidades en situaciones complejas, cambiantes o fluidas.

5) La selección y mantenimiento del objetivo por parte del comandante es esencial, ya que cada operación militar debe tener un objetivo único, alcanzable y claramente definido que siga siendo el foco de la operación.

6) La legitimidad abarca las consideraciones legales, morales, políticas, diplomáticas y éticas que justifican las operaciones aéreas.

El futuro FCAS, deberá proporcionar eficiencia en cada uno de estos seis puntos, permitiendo reducir los ciclos OODA en el menor tiempo posible, y permitiendo al Comandante Supremo de la Fuerza Conjunta poder tomar decisiones en tiempo real, lo que hará que las misiones sean más rápidas, reduciendo el ciclo ATO “Air Asking Order”.

Un ATO es un medio por el cual el Comandante del Componente Aéreo de las Fuerzas Conjuntas (JFACC) controla las fuerzas aéreas dentro de un entorno de operaciones conjuntas. El ATO es un documento que enumera las salidas aéreas para un período fijo de 24 horas, con distintivos de llamada individuales, tipos de aeronaves y tipos de misión (por ejemplo, apoyo aéreo cercano o reabastecimiento de combustible aéreo).

La ATO es creada por un Centro de operaciones aéreas (AOC) que tiene mando y control para un teatro en particular. Más específicamente, la División de Planes de Combate del AOC es responsable de crear la ATO, así como la Orden de Control del Espacio Aéreo (ACO) asociada y la información detallada vinculada en las Instrucciones Especiales (SPINS).

La reducción del ciclo ATO será lo que diferencia la superioridad en el enfrentamiento en las futuras batallas.

Ilustración 4: Representación gráfica de un proceso COPD4

2. EJECUCIÓN DEL COMBATE COLABORATIVO

La forma de ejecución del Combate Aéreo Colaborativo ocasionará la definición de nuevas capacidades dentro de la fuerza aérea, y derivado de este hecho, se definirán nuevas capacidades que afecten a las operaciones multi-dominio.

La doctrina conjunta que se utiliza dentro de las operaciones aéreas en el entorno OTAN está definida por el documento "AJP 3.3 B Allied Joint Doctrine for Air and Space Operations". Esta doctrina engloba las amenazas y los sistemas de armas de los que actualmente dispone la OTAN, así como de los procesos (planeamiento, dirección y ejecución de la misión, etc.) a utilizar para ejecutar una operación aérea conjunta.

El poder aéreo, como se ha citado anteriormente, ofrece la ventaja de enfrentarse a las fuerzas de superficie del adversario en toda la profundidad del espacio de batalla, esto implica menores limitaciones físicas y espaciales que las impuestas a las fuerzas de superficie. Sin embargo, la sinergia de las capacidades de las fuerzas terrestres, navales y aéreas (multi-dominio), que operan como una fuerza conjunta integrada, puede ser definitoria en los casos en que un solo componente (ámbito) no pueda ser decisivo por sí mismo.

Desde el comienzo de una operación, las fuerzas aéreas perseguirán objetivos estratégicos, operativos o tácticos, o una combinación de los tres. Por lo tanto, es esencial disponer de un esfuerzo coordinado que permita que los sistemas aéreos se concentren en el momento y lugar críticos para lograr el objetivo de la misión, maximizando la sinergia conjunta. Dentro de una misión de combate aéreo se definen los siguientes principios:

- Unidad de Mando.
- Control centralizado.
- Ejecución descentralizada.
- Estrategia.
- Selección.
- Legitimidad.

Estos principios rigen una operación de combate aéreo, y definen como se ejecutarán las capacidades de la fuerza aérea en una operación conjunta dentro del marco de la OTAN.

El objetivo del combate aéreo sigue siendo lograr una victoria y luego quedar o permanecer fuera del alcance efectivo de un posible contraataque. Esto hace pensar que, si el objetivo final no ha cambiado, quizás la doctrina para llevar a cabo su consecución no deba cambiar.

La capacidad de llevar una gran cantidad de armas aire-aire de largo alcance, con múltiples opciones de búsqueda, será, casi con certeza, vital para el éxito en el futuro combate aéreo. Este compromiso, entre baja observabilidad y maniobrabilidad, es lo que en un futuro podría ser una de las causas de modificación de la ejecución de las misiones aéreas.

Actualmente, en los escenarios de operaciones, las ROE (Rules Of Engagement) son conservadoras, es decir, para poder abatir un objetivo aéreo se debe estar muy seguro y seguir estas reglas establecidas. Pongamos un ejemplo, supongamos que, para poder abatir un avión enemigo, las ROE indican que se ha de tener un contacto visual con el avión enemigo, y que se debe comprobar antes que se ha realizado una acción hostil (disparo de un misil). Bien, en esta situación, aunque el piloto tenga confirmación del radar de su avión, y de su sistema de defensa área terrestre de que es una amenaza, no podrá abatir al enemigo.

Con los futuros sistemas de combate aéreo, si son capaces de identificar visualmente al enemigo y comprobar que se ha realizado un disparo hacia su aeronave, estaremos ante la misma situación de confirmación de las ROE establecidas, pero no será necesario llegar al enfrentamiento visual.

En este ejemplo, será la tecnología la que permita decidir (por las pruebas aportadas) la forma de ejecutar una operación, lo que implicará un cambio en la ejecución de las misiones.

3. IMPACTO TECNOLÓGICO EN EL COMBATE AÉREO

Actualmente la cooperación científica y tecnológica entre los aliados de la OTAN y europeos es más necesaria que nunca para afrontar los retos de defensa y seguridad de hoy y de mañana. En la Cumbre de la OTAN del 2022, los distintos Jefes de Estado y de Gobierno se comprometieron a mantener la ventaja tecnológica de la Alianza.

La ciencia y la tecnología no son un objetivo en sí mismo, sino un habilitador clave fundamental en el desarrollo y consecución de capacidades militares. El desarrollo

científico-tecnológico no solo fomenta la prosperidad de la sociedad, sino que también protege la soberanía de nuestra democracia.

Las naciones deben aumentar las inversiones en I+D relacionadas con la ciencia y la tecnología, no solo en I+D militar, sino también en universidades y laboratorios civiles, así como actualizar los enfoques para el desarrollo y fortalecer la colaboración civil-militar. Por ello, no sólo es necesario compartir entre los aliados las capacidades militares de cada nación, si no que, para poder alcanzar el desarrollo tecnológico que nos permita cubrir las necesidades conjuntas futuras, será necesario abordar el desarrollo de tecnologías de forma coordinada.

Con respecto a las futuras tecnologías que apoyaran las capacidades operativas y, por ende, serán un habilitador que nos permitan alcanzar los objetivos del combate aéreo del futuro, se encuentran las descritas a continuación.

3.1. Realidad Aumentada para Futuros "cockpit"

Actualmente la carga mental a la que se ve sometido un piloto de combate es muy alta, el propio hecho físico de soportar las distintas fuerzas de la gravedad, junto al estrés del enfrentamiento, supone un gran hándicap para un combate aéreo. Estas acciones se dan por hecho cuando se opera un avión de combate debido al entrenamiento que recibe el piloto, y poder así centrarse en el manejo de los sensores y la gestión del armamento para poder ejecutar la misión encomendada.

Los nuevos sistemas de combate aéreo multiplicarán la carga mental del piloto, lo que implicará mayor gestión tanto de la aeronave como de los sistemas que tiene asociados. Es por ello por lo que las tecnologías a madurar deben facilitar al piloto de combate que pueda realizar la misión, de forma eficiente, presentando la información oportuna en tiempo y forma.

Las tecnologías a este respecto están evolucionando en sistemas de realidad aumentada, asignando acciones que se ejecutarán desde el casco de los propios pilotos, movimientos oculares, visión externa fuera de la cabina, y presentación de la información en el propio casco.

De igual forma los sistemas de transporte táctico, sistemas de apoyo MRTT y AEW&C (Airborne Early Warning and Control) están desarrollando conceptos de consolas de operación y sistemas de comunicaciones enfocados a misiones colaborativas, las cuales aportarán datos específicos para ejecutar la misión conjunta.

3.2. Control de Sistemas Autónomos

Es evidente que el futuro de la aviación pasa por el desarrollo de sistemas autónomos, los cuales poco a poco irán asumiendo misiones que actualmente ejecutan aeronaves tripuladas. El dilema de estos sistemas es incluir en el "loop" de ejecución las decisiones humanas y que, además, sean capaces de tomar decisiones (ejecución de una táctica determinada ante una situación inesperada) por sí mismos.

La propia definición del concepto que se elabora dentro del programa NGWS implica la gestión de un Sistema de sistemas, formados por sistemas remotos que operarán junto al avión de combate para completar la misión. Estos sistemas no tripulados deberán disponer de la suficiente autonomía de vuelo y capacidad de toma de decisión para responder adecuadamente a los cometidos que le otorgue su caja "jefe de misión".

En cuanto a la autonomía de vuelo, cada elemento debe conocer en todo momento su posición, la del resto de sistemas, así como la posición de su jefe de misión, todo ello en entornos altamente denegados, por lo que el desarrollo tecnológico se debe enfocar en mantener las comunicaciones en este tipo de entornos y en desarrollar el concepto de MUT (Manned-Unmanned Teaming).

Este concepto de MUT no contiene únicamente la capacidad de vuelo en formación con otras aeronaves, como se suele decir en el ámbito de desarrollo de aeronaves no tripuladas, el hecho de volar adecuadamente es algo que se presupone, el MUT deberá tomar decisiones en función de las tácticas a aplicar en la misión y de la evolución de esta. Para ilustrar con un ejemplo, el MUT debe hacer lo mismo que dos pilotos que llevan volando juntos durante muchas horas, es decir no hace falta hablar por la radio, ambos conocen las tácticas a ejecutar en función de cómo evolucione la misión.

Este nuevo concepto MUT abarcará la operación de sistemas tripulados y no tripulados de forma colaborativa. Los sistemas no tripulados inteligentes, modulares y conectados por una red distribuida de inteligencia actuarán como multiplicadores de fuerza para la aeronave tripulada, mejorando las capacidades del equipo y manteniendo al piloto fuera de peligro, mientras aún tiene el control.

3.3. Inteligencia Artificial

Es evidente que el desarrollo de la Inteligencia Artificial (IA) está evolucionando muy rápidamente, y que sin duda será un habilitador de tecnologías en cualquier ámbito y el aéreo no será una excepción.

La utilización de la IA para facilitar la toma de decisiones al piloto será un hecho diferenciador para la futura operación del combate aéreo, si bien el concepto de "man in the loop" siempre estará encima de la mesa.

> El empleo de la IA en el ámbito aéreo presenta un reto importante, ya que debe ser entrenada para poder aportar decisiones que aporten valor en la gestión de un sistema de armas,

lo que será un hándicap a la hora de implementar el desarrollo de la IA.

Para poder alimentar esta IA, será necesario almacenar todo tipo de misiones en todos los sistemas (aviones de combate, transporte, apoyo, etc.). Esta información será la que determine la capacidad de la IA y su poder en el futuro. Como ejemplo, podemos desarrollar de forma conjunta con otras naciones sistemas basados en IA, pero cada uno entrenará estos sistemas con los datos que disponga, lo que será el elemento diferenciador de una nación u otra, aunque el desarrollo de la IA sea el mismo.

Así mismo, planteará vulnerabilidades que actualmente no se contemplan, como el posible acceso por parte del adversario a los algoritmos de entrenamiento de la IA, que permitirá literalmente engañar al sistema. Ello requerirá importantes medidas de seguridad en la implementación de estos algoritmos para garantizar el éxito en las operaciones.

3.4. Sistemas Distribuidos

El concepto de sistemas distribuidos, enfocado a los sensores y subsistemas de armamento que incorporarán los futuros sistemas de combate aéreo, consiste en la gestión compartida de estos recursos.

En el caso de los sensores, se trata de un conjunto de sensores interconectados en una o varias plataformas, actuando como una red organizada, aprovechando los servicios activos y pasivos de cada uno y obteniendo una capacidad mayor de operación con un dato mucho más fiable. Para poder conseguir la madurez tecnológica suficiente, se ha de profundizar en los conceptos de sensores activos y pasivos, distribuidos y colaborativos, así como en la mejora de la calidad de los datos del sensor y en la operación en entornos denegados.

En el caso del armamento, el concepto es utilizar todas las armas disponibles, gestionando cual es la mejor opción para el objetivo que se ha fijado, estableciendo prioridades de uso y probabilidades de aciertos.

3.5. Conectividad

La conectividad es uno de los temas más importantes dentro del combate aéreo del futuro. La necesidad de enviar, recibir y gestionar una gran cantidad de datos será un hecho obligatorio en este tipo de sistemas, sin olvidarse de que estas comunicaciones se han de realizar en entornos altamente denegados sobre sistemas de tecnología de baja observabilidad.

Los sistemas de comunicación de cercanía entre las distintas plataformas tendrán un papel fundamental, ya que, entre otros, la denominada COP (Common Operational Picture), tendrá que ser distribuida y alimentada constantemente para poder gestionar los distintos "assets" que intervienen en el combate.
Como tecnología disruptiva, se deben madurar las denominadas comunicaciones de oportunidad, radares para enviar información, sistemas IRS (Infra red System) que también se pueden utilizar para este propósito, etc.

3.6. Sistemas de Baja Observabilidad

Para el combate aéreo del futuro, el no ser visto será un habilitador que permitirá establecer la superioridad en el enfrentamiento. Aunque no será el único factor, esta tecnología marcará durante los primeros años de vida de un sistema de combate una ventaja significativa.

La baja observabilidad se ha en entender en todo su significado, es decir materiales que tienen una baja RCS (Radar Cross-Section), sistemas de propulsión que disminuyen la firma IR (Infra Red), y sistemas de comunicaciones de baja emisión.

Aparte de los materiales empleados en la construcción de una plataforma, la forma será la que determine su condición bajo observable y, como durante su vida operativa no se puede cambiar la forma de la misma, sus características de baja observabilidad estarán supeditas a la evolución de los sensores de detección.

Una vez localizadas las tecnologías principales que afectarán al futuro combate aéreo, hay que identificar los retos tanto de la industria como del Ministerio de Defensa para poder conseguir las futuras capacidades.

Retos de la industria

- **Certificación de los nuevos sistemas:**
  - Las bases de certificación de los sistemas actualmente están basadas en la certificación de cada plataforma por separado. Los Sistemas de sistemas que vuelan de forma colaborativa y que, además, el comportamiento de uno afecta al otro, no han sido certificados aún, lo que supondrá un reto importante para las industrias, ya que habrá que demostrar que la seguridad de vuelo se mantiene durante la operación.
  - La inclusión de la Nube de Combate dentro de los sistemas aéreos también será un gran reto con respecto a la aeronavegabilidad, ya que, en un SoS colaborativo los sistemas no tripulados y tripulados ejecutaran maniobras de forma coordinada cuyas órdenes y datos de posición viajaran a través de esta Nube de Combate. Aún está por determinar cómo afectará esto a la aeronavegabilidad de los sistemas implicados.
  - Certificación de algoritmos de IA dentro de las aeronaves. Hoy por hoy no se ha identificado la referencia sobre la que se debe certificar un algoritmo de IA. Este hecho es también un gran reto para las autoridades de aeronavegabilidad.
- Poder tomar las decisiones adecuadas durante un combate aéreo a nivel estratégico es importante, ya que durante la batalla se producen circunstancias que obligarán a cambiar decisiones en este ámbito. Asegurar las comunicaciones a este nivel en entornos denegados supone un gran reto tecnológico, el cual necesita ser resuelto. Otra alternativa es poder operar sin comunicaciones activas durante ciertos periodos, con sistemas no tripulados y tripulados, porque ambos tengan la capacidad de actuar en estos ámbitos de operación.
- Los sistemas de combate aéreo del futuro necesitarán actualizaciones constantes, durante todo su ciclo de vida, por tanto, se deben diseñar para que las actualizaciones no supongan un coste elevado de integración, y hacerse por bloques que permitan implementaciones parciales de nuevos servicios y capacidades.
- Un factor muy importante es el coste de las operaciones, de nada sirve tener un sistema de armas muy potente y novedoso, si el coste de operación no es viable, por lo que se deben diseñar estos aprovechando economías de escala entre los distintos usuarios, así como impulsar sistemas de simulación y adiestramiento que permitan operaciones de alta fidelidad.

Retos del Ministerio de Defensa

- Las autoridades de aeronavegabilidad se deben preparar para los nuevos retos, la certificación de Sistemas de sistemas, que además dispondrán de IA. Deben establecerse las bases de certificación a seguir por parte de los fabricantes de sistemas, considerando que nunca anteriormente se han abordado este tipo de certificaciones.
- Se debe facilitar el manejo de la información clasificada, ya que, el combate aéreo del futuro permitirá que la planificación, ejecución y posterior análisis de una operación se realice en tiempo real, así como la información de la situación del armamento, horas de vuelo que le quedan al sistema, en tiempo real con los sistemas logísticos, lo que implicará que la infraestructura de red debe ser clasificada, eficiente y robusta.
- Los centros de experimentación de los que actualmente dispone el Ejército del Aire y del Espacio deben orientarse a la generación de nuevas capacidades con las herramientas de simulación operativa, desarrollando nuevos conceptos, estableciendo los requisitos para que la industria los elabore, y posteriormente validándolos en los laboratorios.

4. IMPACTO EN LA FORMACIÓN Y ENSEÑANZA

Los nuevos medios de combate aéreo contribuirán a la superioridad de una misión incorporando múltiples plataformas y sistemas, hasta el punto de exigir una nueva definición de las misiones, con un impacto importante en la forma de cómo se deben entrenar los jefes de misión, pilotos e incluso personal de apoyo en tierra.

El piloto del futuro debe volcar sus esfuerzos durante la misión, en la gestión de los diferentes sistemas y subsistemas que tiene asignados, analizando la información que le proporciona cada uno de ellos para conseguir el objetivo de la misión. Por ello, la gestión de la información que le llega es algo de vital importancia:

- El piloto, únicamente debe tener la información relevante, en el momento adecuado.
- La forma de presentar la información debe ser la adecuada para que el piloto pueda gestionar de forma eficiente la misma y tomar las decisiones en tiempo real.
- El piloto debe recibir propuestas en base a la experiencia acumulada en misiones anteriores por los sistemas (gestión de la IA).

Es por ello por lo que, en el entrenamiento del futuro combate aéreo, la información que recibe el piloto tendrá un papel muy importante. Las necesidades principales identificadas para este entrenamiento y enseñanza de los futuros sistemas de combate aéreo deben contener:

- Servicios de Formación.
- Simuladores virtuales de los nuevos sistemas y de conceptos operativos.
- Interoperabilidad de sistemas.
- Estandarización de la formación.

4.1. Servicios de Formación

Debido a la complejidad de los nuevos sistemas, será necesario establecer un sistema de gestión de formación y adiestramiento modular que gestione todas las actividades de entrenamiento realizadas desde el más básico hasta los ejercicios globales conjuntos.

Para poder generar escenarios de alta complejidad, es necesario disponer de fuentes fiables de los datos a simular, por lo que cobra mucha importancia la creación de los denominados modelos de ingeniería de cada uno de los sistemas y subsistemas que formarán parte del combate aéreo. Actualmente, no existen todos los modelos de los sistemas y plataformas que están operativos, pero en las nuevas generaciones de sistemas permitirán simular y reflejar el campo de batalla.

Estos modelos de ingeniería consentirán realizar simulaciones de posibles modernizaciones, incorporación de nuevos sistemas a la operación FCAS, así como de analizar posibles cambios de cualquier ámbito: ejecución de la misión, entrenamiento, implementación de sistemas o algoritmos logísticos, etc.

4.2. Simuladores Virtuales de los Nuevos Sistemas y de Conceptos Operativos

Si bien los simuladores de los sistemas están enfocados para realizar el entrenamiento de los pilotos, el nuevo combate aéreo, va a necesitar que se cuente con simuladores a nivel operacional, que faciliten la validación de conceptos, lo que mejorará la evolución de los sistemas de sistemas dentro del combate.

Estos simuladores van a permitir que se simulen misiones complejas a nivel Sistema de sistemas, no únicamente de la plataforma, permitiendo tanto identificar “gaps” operativos que derivaran en nuevas capacidades, como la validación de modelos de integración de los distintos componentes y sistemas que actúan en el campo de batalla. Esto está muy relacionado con el desarrollo de los modelos de ingeniería comentados en el punto anterior.

Las nuevas capacidades de simulación deben permitir la generación de entornos sintéticos, la interacción con sensores simulados y la integración con el entorno del piloto, así como de simular las capacidades de decisión del “Joint Force Commander”.

4.3. Interoperabilidad de los Sistemas

Otro de los aspectos importantes dentro de la formación será la simulación de la interconexión de los distintos dispositivos de entrenamiento. Es necesario que exista una interoperabilidad entre todos los aliados para poder realizar entrenamientos conjuntos, para definir misiones complejas en la que intervienen muchos SoS.

La interconexión de los dispositivos de entrenamiento es la línea de base para realizar el entrenamiento futuro de todas las tripulaciones. Además, por exigencias de interoperabilidad, esta interconexión debería extenderse a un entorno internacional incluyendo, al menos en un primer paso, a otras naciones europeas.

4.4. Estandarización de la Formación

El uso de un modelo común de programas de formación optimizaría el diseño del sistema junto con la posibilidad de crear una base de datos de escenarios de formación comunes o, estableciendo centros de formación internacional altamente estandarizados que cubra desde las necesidades básicas de formación hasta la "formación compleja".

Tradicionalmente, la ejecución del entrenamiento militar ha estado basado en recursos puramente militares, pero algunas naciones están modificando este aspecto, introduciendo recursos civiles en su modelo de entrenamiento, tanto en simulador como en entrenamiento de vuelo.

Con el fin de optimizar los recursos, se podría establecer una escuela de formación integral con sistemas de formación dedicados e instructores civiles contratados para los cursos de formación básicos completos. Ya que, los pilotos son un recurso altamente especializado, el beneficio real de este modelo es que las naciones podrían dedicar a sus pilotos a misiones operativas dentro de sus escuadrones operativos, en lugar de dedicarlos a la instrucción (como se hace actualmente), optimizando el vuelo de los pilotos militares y permitirles aprovechar al máximo su experiencia operativa.

Más allá de todo lo mencionado anteriormente, no hay que olvidar el coste derivado de la formación y adiestramiento, la operación de los nuevos sistemas, como ha ocurrido en el pasado, supondrá un mayor coste por hora de vuelo, por lo que cuanto mayor sea la capacidad de simulación (alta fidelidad) en el entrenamiento de los sistemas, el coste de la operación de estos se verá reducido. Los nuevos entrenadores utilizarán sistemas reales y entidades simuladas y controladas por IA, involucrando a muchos actores y permitiendo una gestión real del campo de batalla.

En términos generales, es necesario profundizar en el estudio de los requisitos para asegurar una definición común del alcance y su impacto en el área de adiestramiento y enseñanza, definiendo las necesidades de las fuerzas aéreas, junto con las capacidades que puede aportar la industria. Los retos principales que se plantean son los siguientes:

- **Tecnológicos.** Existen claros desafíos en cuanto a la tecnología necesaria para hacer frente a las necesidades de formación de las futuras tripulaciones, maduración de la IA, análisis de big-data, realidad virtual y aumentada.
- **Colaboración con las fuerzas aéreas y la industria.** La entrada en servicio de los nuevos sistemas supondrá un reto en términos de recursos tanto humanos como de material para garantizar un nivel adecuado de adiestramiento.
- **La seguridad.** A pesar de que existe mucha experiencia en la implementación de seguridad física en los sistemas e instalaciones de entrenamiento, un desafío importante es garantizar la seguridad de los datos y la información. El sistema de entrenamiento de los nuevos sistemas deberá incluir potencialmente participantes con diferentes niveles de autorización para acceder a los datos y la información cuando opere en ejercicios multinacionales.

Sobre este aspecto, será necesario incluir escenarios de adiestramiento que incorporen ciberataques, ya que este campo tomará mucha relevancia en los enfrentamientos del futuro, y los pilotos/gestores del campo de batalla dentro del futuro combate aéreo se deberán enfrentar y entrenar este tipo de escenarios.

5. NUEVO CONCEPTO DE APOYO LOGÍSTICO

El combate aéreo del futuro deberá permitir una gestión del sostenimiento en tiempo real, es decir, cuando el sistema está regresando o ha regresado a su base, éste debe haber indicado qué necesidades de sostenimiento va a demandar, identificando antes de llegar a la base las tereas a realizar para su puesta a punto en una nueva misión y en todo el ámbito de la operación, no solo la operación de las distintas aeronaves, sino, incluyendo el armamento utilizado para su reposición.

Durante una operación, los sistemas disminuyen su rendimiento debido a problemas de degradación y obsolescencia. La necesidad de extender la vida operativa de los sistemas de armas para reducir la carga de mantenimiento y aumentar la disponibilidad de la flota requiere el desarrollo de soluciones para garantizar un buen rendimiento durante todo el ciclo de vida. Estas soluciones se basan en tecnologías relativas al concepto de mantenimiento predictivo, orientadas a la predicción de fallos y la optimización de las actividades de mantenimiento.

La incorporación de tecnologías que permitan implementar estrategias de mantenimiento predictivo supondría un gran salto en la gestión de los sistemas logísticos del futuro. Las tecnologías por desarrollar sobre estos sistemas se deben enfocar principalmente en:

- Desarrollo de sensores capaces de recopilar suficientes datos durante la operación del sistema.
- Análisis de big-data generado por sistemas de armas.
- Desarrollo de algoritmos predictivos mediante IA capaces de predecir con precisión la vida útil remanente del sistema.

El mantenimiento predictivo se debe abordar tanto desde el punto de vista del sistema que está en vuelo, como desde el punto de vista de los sistemas de apoyo en tierra y todo el soporte necesario para realizar dicho mantenimiento. Las áreas de mejora que se implementarán en este concepto son las siguientes:

- **Reducción de la huella logística:** el mantenimiento predictivo debe brindar visibilidad de las tareas de mantenimiento que se realizarán durante un despliegue de acuerdo con los perfiles de la misión.
- **Aumentar la disponibilidad operativa de la flota:** mejora de la eficiencia en las operaciones de mantenimiento, evitando demoras y cancelaciones. El mantenimiento predictivo estimará las horas de vuelo útiles restantes hasta que se requiera una acción de reparación y se reduzcan las fallas inesperadas, lo que aumenta la utilización del equipo.
- **Capacidades de mejorar la planificación de flotas:** proporcionará recomendaciones sobre configuraciones de plataforma específicas adecuadas para cada tipo de misión.

La comunicación en tiempo real de los sistemas aéreos con los sistemas de soporte en tierra facilitará:

- Demanda predictiva de proveedores: repuestos disponibles a tiempo.
- Optimización de stock: minimización de almacenes.
- Cadena de suministro más eficiente: reducción de picos de demanda y periodos de indisponibilidad de piezas.
- Disminución de los costes de los equipos: ahorro de costes en tiempo de inactividad.
- Reducción de las reparaciones realizadas antes del fallo en base a las predicciones, pudiendo ser éstas menos costosas que después del propio fallo.

El uso de tecnología basada en algoritmos de aprendizaje de IA conseguirá que los ordenadores de abordo realicen el análisis de una gran cantidad de datos sin procesar y puedan descubrir patrones o predicciones en cuanto necesidades de mantenimiento. La IA posibilitará el análisis predictivo para eventualmente apoyar en el proceso de toma de decisiones y la actualización en tiempo real de los procedimientos de aislamiento de fallos o la simulación automatizada de los mismos.

Otra tecnología que ayudará el desarrollo de este concepto de sostenimiento será la aplicación del big-data. Se trata de una tecnología relacionada con el procesamiento, análisis y gestión de un gran volumen de datos mediante técnicas no convencionales. Los datos pueden ser generados por máquinas (es decir, sensores, registros de servidores) o recibidos a través de proveedores de servicios web.

La incorporación de gemelos digitales proporcionará el conocimiento exacto del estado físico y la capacidad de prever lo que sucederá en el futuro del sistema, mejorando la eficiencia del sostenimiento.

Las comunicaciones inalámbricas y seguras para descarga de datos de aeronaves serán aplicables para el ámbito de los sistemas de apoyo en tierra y también para el mantenimiento predictivo. El uso de comunicaciones inalámbricas admitiría una descarga más rápida de datos para su análisis en tierra con un menor impacto en la operación y mejores condiciones para la tripulación.

Los sensores inteligentes posibilitan una recopilación más precisa y automatizada de datos ambientales con menos ruido. Estos dispositivos se utilizan para mecanismos de monitoreo y control en una amplia variedad de entornos, incluidas las redes inteligentes, el reconocimiento del campo de batalla, la exploración y una gran cantidad de aplicaciones.

Los sistemas de apoyo en tierra engloban disciplinas como la gestión de datos, las actividades a desarrollar en este ámbito serán:

- Reducción de la fase de respuesta.
- Aumentar la disponibilidad de la flota y reducir la cantidad de GSS (Ground Support Systems) a utilizar.

Para garantizar que el sistema de apoyo en tierra se optimice correctamente, hay algunas tecnologías relevantes que se deben tener en cuenta, como en el caso de la realidad

aumentada. Esta tecnología consiste básicamente en la visión del mundo real físico con imágenes superpuestas generadas por computadora, cambiando la percepción de la realidad. Esencialmente, mejora la percepción física (vista, oído, tacto) al agregar capas de información digital sobre el mundo real. En el ámbito de los sistemas de apoyo en tierra, esta tecnología es aplicable para las actividades de mantenimiento en tierra.

Por último y pensando en el diseño del concepto FCAS, será necesario que la fase de soporte en servicio comience en la etapa temprana de diseño para garantizar que se cumplan los requisitos en este campo. Las actividades de soporte en servicio asociadas a la fase de diseño no deben ceñirse a las consideraciones tradicionales, sino a un diseño activo de la arquitectura de servicios.

En consecuencia, se deben abordar varios requisitos de soporte en servicio para las plataformas y se deben tener en cuenta como cualquier otro requisito de diseño. Cuanto más tarde se consideren esas capacidades, más difícil será implementarlas en el futuro, reduciendo la eficiencia y el coste de operación del sistema.

6. SISTEMAS AÉREOS BASADOS EN COMBATE COLABORATIVO

Tal y como se ha indicado, el combate colaborativo será el punto de inflexión de las batallas aéreas del futuro, además la evolución de esta capacidad será la que diferencie la superioridad en el enfrentamiento. Es por ello, que todas las potencias mundiales se están preparando, desarrollando conceptos y sistemas aéreos orientados al Combate Aéreo Colaborativo en el entorno 2040. Una muestra de estos núcleos vertebrales son los siguientes sistemas:

- Alemania-España-Francia: Programa NGWS.
- EE. UU.: Programa de la USAF, Next Generation Air Dominance (NGAD).
- Reino Unido-Italia-Japón: Programa Global Combat Air Programme (GCAP-Tempest)
- China: Programas de desarrollo J28 (+GJ20).
- Rusia: Programas de desarrollo SU57/75 + MIG 41 + S70.

Todos estos desarrollos tienen en común, el concepto Sistema de Sistemas. Todos están formados por un caza, sistemas autónomos (drones, RPAS, Remote Carries, UAV, etc.) y una Nube de Combate que capacita al sistema para implementar el Combate Aéreo Colaborativo.

El factor diferencial de un sistema u otro será sin duda la Nube de Combate (Combat Cloud), y su capacidad de resiliencia en entornos denegados, así como el concepto de empleo. Si bien todos los sistemas tienen en común que serán los primeros en ejecutar misiones de forma colaborativa, las capacidades de cada uno de ellos están orientas a distintas misiones:

- El concepto de sistema NGAD está más orientado a misiones estratégicas ya que define un caza muy bajo observable con gran capacidad de portar armamento, lo que implica misiones aire-suelo.
- El concepto chino y ruso, está más orientado a misiones aire-aire.
- El concepto NGWS y GCAP está más orientado a misiones mixtas.

Viendo el panorama internacional en el desarrollo de estos sistemas, en el momento de redactar este libro son conceptos salvo en el caso de EE. UU, en el ámbito europeo (incluyendo a UK) parece complicado desarrollar dos sistemas con capacidades similares ya que el coste de este desarrollo será muy elevado. Esto puede llevar, una vez que se finalicen los desarrollos conceptuales de los programas NGWS y GCAP y que las naciones participantes determinen sus requisitos, a la reconfiguración del esquema industrial en el desarrollo de los sistemas, con la aparición de nuevas alianzas entre naciones que actualmente están en programas distintos.

El concepto Futuro Sistema de Combate Aéreo no es algo que se implementará de la noche a la mañana, lo que implica, que hasta la llegada de los sistemas que ejecutarán misiones de forma colaborativa, hay que desarrollar las capacidades de combate cooperativo en el medio plazo, en el entorno del 2030-35.

Este desarrollo del FCAS a medio plazo, conllevará la implementación de nuevas capacidades a los sistemas actualmente operativos: Eurofighter, A-400, MRTT, C-295, RPAS y sustituto del F-18. Estos sistemas deberán incorporar esta capacidad de combate cooperativo, que a su vez deberá ser compatible con los futuros sistemas NGWS, FCTM o UAV.

Las siguientes figuras muestran los desarrollos de los distintos conceptos que están actualmente en curso dentro de las principales potencias mundiales:

Next-Generation Weapon System (NGWS) en FCAS (Future Combat Air System)

Proyecto de un sistema de armas de nueva generación entre Alemania, España y Francia.
El sistema estará formado por cazas de sexta generación, Sistemas autónomos denominados *Remote Carriers* y una Nube de Combate.

Global Combat Air Programme (GCAP-Tempest)

Proyecto de un nuevo caza de sexta generación entre Reino Unido, Italia y Japón.

F-X Project

Proyecto de un nuevo caza de sexta generación por parte de Japón.

MIG-41 (PAK-DP) Project

Proyecto para el desarrollo de un avión interceptor furtivo pesado por parte de Rusia.

ADF Project

Proyecto de caza de quinta generación por parte de Taiwan.

Next Generation Air Domiance (NGAD)

Proyecto de un sistema de armas de nueva generación de estados Unidos. Se trata de un Sistema de Sistemas orientado al Mando y Control Aéreo para el dominio del combate aéreo del futuro.
El sistema formado por distintos *assets* (Una aeronave *Command Fighter* aeronaves no tripuladas y una nube de Combate).

PCA Project

Proyecto dedicado al estudio de la posible sustitución del F-15 y F-22 por parte de Estados Unidos (USAF).

F/A – XX Concept

Proyecto dedicado al estudio de la posible sustitución del F-18 Super Hornet por parte de Estados Unidos (NAVY).

J–XX Project

Proyecto de desarrollo de un caza de sexta generación por parte de China.

7. CONCLUSIONES

El concepto FCAS ha de entenderse como la iteración de Sistemas de Sistemas, lo que engloba los medios aéreos que actualmente tienen las fuerzas aéreas, y las futuras plataformas y sistemas que existirán en el entorno de 2040. El objetivo de este concepto FCAS (Future Combat Air System) es potenciar y maximizar la operación colaborativa de los elementos de las fuerzas aéreas que intervienen de forma relevante en el dominio aeroespacial.

Es necesario desarrollar este Concepto FCAS el cual permitirá la transición del combate cooperativo al combate colaborativo, así como establecer los "road-maps" de adaptación de los sistemas actuales del Ejercito del Aire y del Espacio.

A medio plazo, todo ello conllevará la implementación de nuevas capacidades a los sistemas actualmente operativos: Eurofighter, A-400, MRTT, C-295, RPAS y sustituto del F-18; los cuales deberán incorporar cierta capacidad de combate colaborativo, que a su vez deberá ser compatible con los futuros sistemas como el NGWS (Next Generation Weapon System).

Los nuevos sistemas aéreos que se desarrollarán en las próximas décadas estarán orientados al trabajo colaborativo, apoyándose en las tecnologías que se encuentran en fase de maduración como la Inteligencia Artificial, lo que hace necesario recopilar los datos necesarios actuales para alimentar los algoritmos que se desarrollen en el futuro.

La evolución del concepto FCAS desarrollará herramientas de simulación operativa que permitirán incorporar futuros sistemas a este entorno, asi como, desarrollar nuevos conceptos operativos que permitirán adaptarse a las futuras batallas aéreas.

BIBLIOGRAFÍA

1. NATO, (2023). “Bi-SC Capability Codes and Capability Statements”. USA.

2. NATO, (2021) “CD&E Handbook”. Norfolk, Virginia, USA.

3. Ministerio de Defensa, (2018). “PDC-01 Doctrina para el empleo de las FAS”. Catalogo General de Publicaciones Oficiales. [publicacionesoficiales.boe.es]. Madrid, España.

4. NATO STANDARDIZATION OFFICE (NSO), (2016), “Standard AJP-3.3 Allied Joint Doctrine for Air and Space Operations”. Edition B Version 1.USA.

5. NATO STANDARDIZATION OFFICE (NSO), (2021). “Standard AJP-3.9 Allied Joint Doctrine for Joint Targeting”. Edition B Version 1.USA.

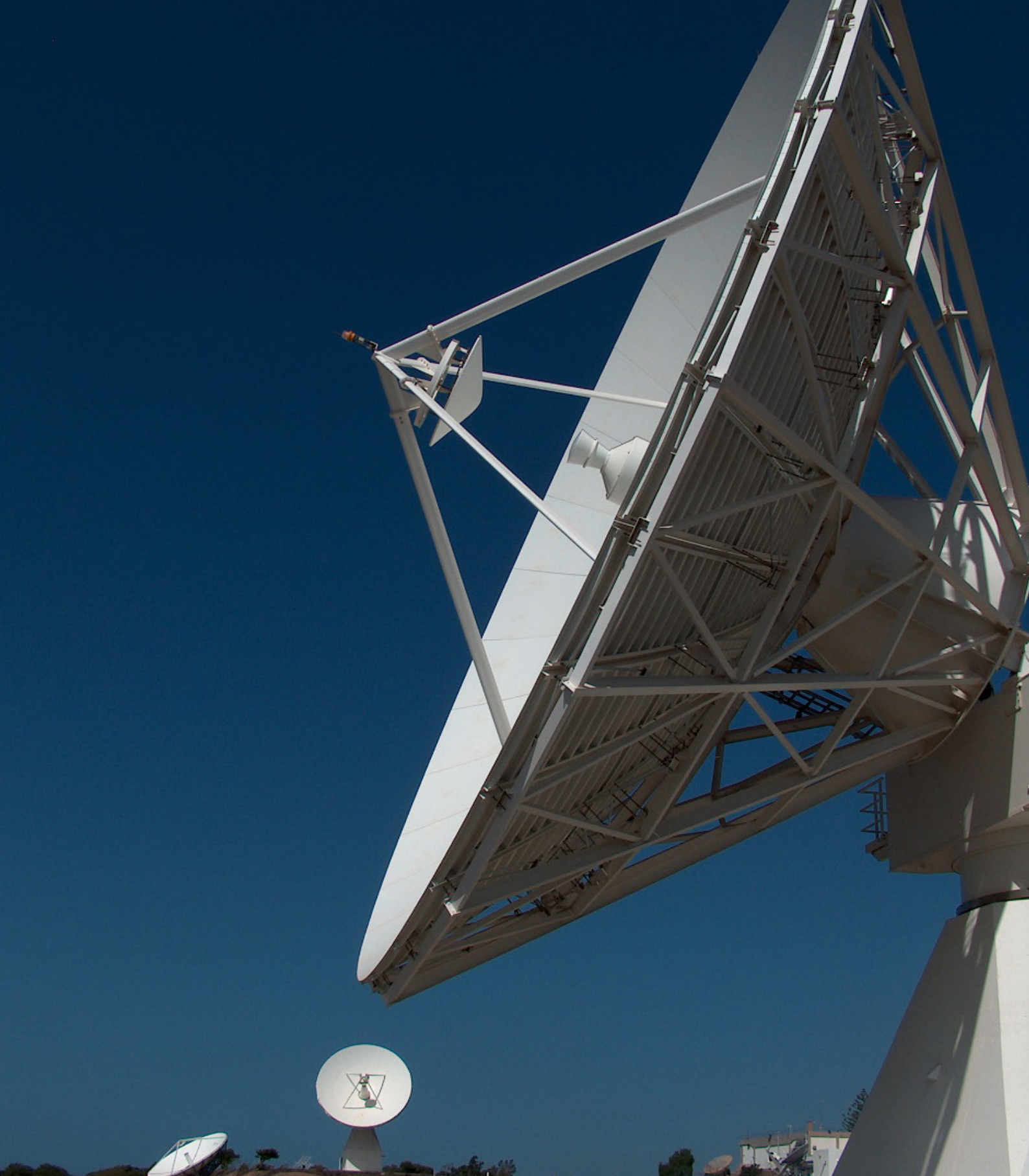
6. NATO STANDARDIZATION OFFICE (NSO), (2021). “Standard AJP-3.20 Allied Joint Doctrine for Cyberspace Operations”. Edition A Version 1.USA.

BIOGRAFÍAS

CÉSAR HERAS MENOR DE GÁSPAR

Ingeniero de sistemas en la empresa Ingeniería de Sistemas para la Defensa de España (ISDEFE) prestando actualmente asistencia técnica en la Oficina de Programa Next Generation Weapon System (NGWS) dentro del entorno de un Future Combat Air System (FCAS), especialmente en los ámbitos del caza de sexta generación y sistemas remotos. Anteriormente, prestó asistencia técnica en la Dirección General de Armamento y Material (DGAM) en los ámbitos del planeamiento de la obtención de armamento y material, en el desarrollo de sistemas RPAS (Remotely Piloted Aircraft System) y en la gestión de grandes programas de defensa.

Antes de unirse a ISDEFE, César trabajó como ingeniero de sistemas en HoneyWell, Amper Programas en los programas de sistemas de aviónica y comunicaciones.



CAPÍTULO 6

Capacidades Espaciales

Isaac Domínguez Santos

Muchas actividades habituales en nuestra sociedad actual están basadas en el espacio. En la vida diaria se recurre a sistemas y servicios espaciales en ámbitos como las telecomunicaciones, la navegación, la predicción meteorológica o el conocimiento del territorio. Esos mismos servicios son necesarios y muchas veces críticos en el ámbito militar. Nuestras fuerzas armadas precisan disponer de unas capacidades en telecomunicaciones, observación de la Tierra y navegación. Además, una vez que el espacio se convierte en dominio por sí mismo como lo son el marítimo, aéreo y terrestre, es preciso también dotarse de las capacidades necesarias de mando y control para operar en el entorno espacial y para garantizar la propia soberanía y la utilización del mismo de la que dependen otras capacidades críticas como las mencionadas. La propia naturaleza espacial y los niveles de inversión requeridos hacen de la cooperación internacional una herramienta obligatoria para dotarse de las capacidades requeridas. El dinamismo del sector espacial requiere de un constante esfuerzo innovador y estar especialmente atentos a nuevos enfoques de la actividad y sobre todo al surgimiento de tecnologías disruptivas.

1. CAPACIDADES ESPACIALES

1.1. Comunicaciones por Satélite

Inicio de las capacidades de comunicación por satélite militares

Esta primera parte de las capacidades espaciales, las comunicaciones por satélite, tendrá un enfoque cronológico. La razón es doble. Por un lado, poner de relieve una actividad en la que nuestro país fue uno de los primeros en disponer de estas capacidades propias, y por otro, entender cómo se llegó al modelo de adquisición de la capacidad mediante la colaboración público-privada, modelo que sigue en la actualidad para las capacidades de comunicación y que se ha replicado para las capacidades de observación de la Tierra por satélite.

En septiembre de 1992 se lanza el satélite HISPASAT 1A y en julio del 1993 el satélite 1B. Ambos satélites, junto a las misiones comerciales del servicio fijo y de difusión por satélite incorporaban una carga gubernamental en banda X. Los dos satélites compartían una misma posición orbital (30ºW) y las cargas gubernamentales tenían las mismas frecuencias, pues estaban concebidas para servir una de redundancia de la otra.

En aquel momento solo tres países de la OTAN disponían de capacidad en banda X propia y adicional a las capacidades comunes que proporcionaba el sistema NATO IV de OTAN. Estos países eran Estados Unidos, Reino unido con su sistema SKYNET y Francia con el sistema SYRACUSE. El antiguo bloque soviético también disponía de esta capacidad.

Las capacidades que ofrecían los satélites HISPASAT en banda X eran tres transpondedores que permitían la comunicación en un haz fijo de 5º de apertura sobre el área de interés geoestratégico de España comprendido entre el mar del Norte y cabo Blanco (Mauritania) de norte a sur y desde las Azores a Asia Menor de Oeste a Este, un segundo haz de las mismas características, pero orientable y un haz global de 19º a través de una antena de baja ganancia cubriendo toda la superficie visible de la Tierra. Las operaciones del satélite y las estaciones de seguimiento eran competencia de la empresa HISPASAT y se realizaban desde sus instalaciones de Arganda del Rey.

Con los satélites en órbita y en estado operativo, era preciso dotar al Ministerio de Defensa de un segmento terreno de usuario. Para ello se había diseñado el programa SECOMSAT que contemplaba terminales de anclaje en Torrejón de Ardoz, Bermeja (Valdilecha) y Tenerife, terminales embarcados navales, terminales tácticos y terminales manpack. No obstante, las dificultades financieras del momento, estamos en plena crisis tras las conmemoraciones de 1992, retrasaron el despliegue previsto. Otro acontecimiento vino a modificar de nuevo los planes. España, por primera vez en muchos años, desplegaba tropas en el exterior, concretamente en los Balcanes, y la comunicación por satélite era la única alternativa razonable para dar servicio al despliegue. Por ello se puso en marcha un plan urgente de dotación de capacidades en diciembre de 1992 denominado CICSAT (Capacidad Inicial de Comunicaciones por Satélite).

Evolución hasta las capacidades actuales

Una vez resuelta la emergencia de dotar de comunicaciones al despliegue en los Balcanes, se fue dotando a las FAS progresivamente de más terminales de comunicaciones dentro del plan previsto en el programa SECOMSAT. También se desarrollaron en España, fruto de la colaboración de la industria y la universidad, componentes específicos como antenas, transceptores, amplificadores, conversores, etc., permitiendo disponer de un producto de muy alto contenido nacional.

Los requisitos de la segunda generación de comunicaciones militares llevaron a la necesidad de disponer de satélites dedicados en lugar de compartir plataforma con otras misiones civiles y a la necesidad de disponer de dos satélites con sus respectivos segmentos terrenos de control para dos posiciones orbitales. Además del reto técnico, apareció un importante reto financiero.

La solución propuesta fue recurrir a la colaboración público-privada. Se creó la sociedad HISDESAT SA participada por la industria nacional: HISPASAT con un 43%, EADS CASA, hoy Airbus Defense & Space con el 15 %, INDRA con el 7% y SENER con el 5%. Por parte del Ministerio de Defensa la sociedad INSA, hoy ISDEFE, ostentaba el 30% de las acciones. A su vez se creó en EE.UU. la sociedad XTAR LLC participada en 55,5% por Space System Loral y en un 44,5% por la propia HISDESAT. Esta estructura societaria permitió la adquisición y puesta en servicio de dos satélites. HISDESAT adquirió el satélite SPAINSAT que se lanzó a su posición orbital 30ºW el 11 de marzo de 2006. Por su parte XTAR LLC puso en órbita en la posición 29ºE el satélite XTAR-EUR el 12 de febrero de 2005. Estos dos satélites constituyen la base del actual sistema español de comunicaciones por satélite descrito en los siguientes apartados.

Sistema Español de comunicaciones por satélite. Segmento espacial

El sistema Español de Comunicaciones por Satélite está constituido por dos satélites:

El satélite SPAINSAT operado por la sociedad HISDESAT localizado en la posición orbital 30ºW dispone de capacidad en banda X y en banda Ka. Su configuración de transpondedores se adapta a los requerimientos de las FAS españolas, aunque con una capacidad adicional para su posible uso compartido por otros países aliados.

El satélite XTAR-EUR operado por la empresa XTAR está en la posición 29ºE. Tiene una configuración genérica de transpondedores en banda X para prestar servicios de capacidad comercializable a gobiernos aliados, aunque en caso de fallo del satélite SPAINSAT se puede reconfigurar para replicar la configuración específica para las FAS españolas de este satélite.

El satélite SPAINSAT en 30ºW consta de :

1) Cinco transpondedores operacionales en banda X para uso por las FAS españolas. Estos transpondedores están en la banda de 7900 MHz a 8400 MHz en subida y 7250 MHz a 7750 MHz en bajada. La transmisión en subida se hace en polarización circular a derechas, mientras que en bajada se hace en polarización circular a izquierdas. Estos transpondedores no hacen reuso de frecuencias en polarizaciones ortogonales.

2) Cuatro transpondedores de uso general de 72 MHz de ancho de banda cada uno en las mismas bandas. Cada par de estos transpondedores reúsan las mismas frecuencias en polarizaciones ortogonales (circular a derechas y circular a izquierdas).

3) Un transpondedor en la banda Ka militar con un ancho de banda de 36 Mhz, subida en la banda de 30 a 32 GHz y bajada en la banda de 20,2 a 21,2 GHz.

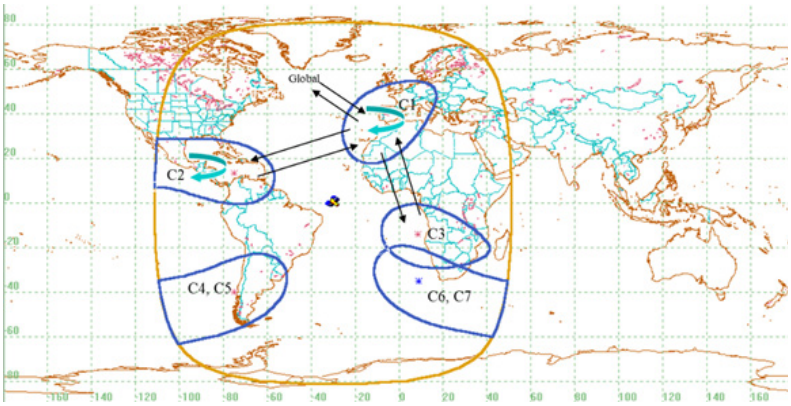


Figura 5.6.1.1: Cobertura del satélite SPAINSAT

La figura 5.6.1.1 representa las coberturas del satélite SPAINSAT y una configuración posible de sus haces.

Las antenas de que está dotado el satélite permiten activar los siguientes haces:

- Un haz fijo de 4,5º centrado sobre la península Ibérica. Haz C1
- Dos haces orientables de 4,5º. Haces C2 y C3
- Un haz global (19º) sobre toda la superficie visible desde el satélite. Haz G1
- Un haz en banda Ka centrado sobre la península Ibérica
- Un haz orientable en banda Ka
- Cuatro haces orientables de 4,5º para los servicios adicionales. Haces C4, C5, C6 y C7
- Un haz global (19º) para los servicios adicionales. Haz G2. Los haces G1 y G2 se solapan sobre la cobertura global del satélite (superficie visible de la Tierra), aunque sobre canales radioeléctricos diferentes.

La interconexión de haces permite una gran flexibilidad en las operaciones y puede configurarse a través de comandos desde las estaciones de control. Los haces se apuntan mediante el movimiento mecánico de las antenas que son paraboloides conformados. A esta capacidad se une la ofrecida por la antena IRMA desarrollada por la industria nacional. Esta antena de recepción a bordo del satélite, a diferencia de los paraboloides conformados, es una antena de elementos activos que puede configurar su diagrama de radiación por la combinación de fases de sus elementos. Ello permite hacer barridos para detectar transmisiones interferentes desde tierra y, una vez geolocalizada, generar un nulo de recepción que anule la interferencia.

El satélite XTAR-EUR en 29ºE monta doce transpondedores operacionales en banda X de 72 MHz de ancho de banda cada uno para uso genérico. Estos transpondedores están en la banda de 7900 MHz a 8400 MHz en subida y 7250 MHz a 7750 MHz en bajada. Se recurre al reúso de frecuencias con polarizaciones ortogonales (circular a derechas y circular a izquierdas). De esta manera dos transpondedores comparten frecuencias, pero usan

polarizaciones ortogonales, duplicando de este modo la capacidad. Esta característica fue novedosa en su momento ya que típicamente se usaba una sola polarización de subida y su contraria de bajada. Cualquiera de esos doce transpondedores puede ser asignado a uno de los 4 haces orientables de 4,5º de los que dispone el satélite.

Este satélite incorpora en su carga útil un conjunto de conmutadores y actuadores controlables remotamente que permiten replicar parte de la configuración de la carga útil del satélite SPAINSAT en caso de fallo de este. Como línea general, la explotación de la capacidad del satélite XTAR-EUR está orientada para ser comercializada entre organismos gubernamentales de países aliados, pero en caso de fallo del SPAINSAT se "condenarían" tres transpondedores de 72 MHz más 12 MHz de un cuarto transpondedor para replicar la capacidad de SPAINSAT asignada a las FAS españolas y ponerla a disposición de estas en un periodo mínimo de tiempo.

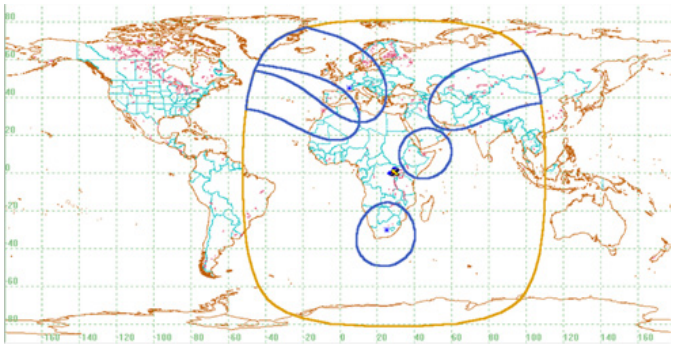


Figura 5.6.1.2: Cobertura del satélite XTAR-EUR

La figura 5.6.1.2 representa la huella del satélite XTAR-EUR en la que se representa una configuración genérica de sus cuatro haces.

Segmento de Control

El segmento terreno de control del sistema español de comunicaciones gubernamentales por satélite está distribuido entre España (península y Canarias) y Norteamérica. Las estaciones de seguimiento están todas en territorio nacional, ya que desde cualquier punto del territorio español se puede tener acceso tanto al satélite SPAINSAT como al satélite XTAR-EUR. A su vez, y por razones fundamentalmente de redundancia, está distribuido entre Arganda del Rey (Madrid) y Maspalomas en la isla de Gran Canaria. En el continente americano se dispone de Centros de control principal y de respaldo operados por XTAR ubicados en Pensilvania (EE. UU.) y Otawa (Canadá).

Figura 5.6.1.3: Estaciones Terrenas XTAR-EUR y SPAINSAT en Maspalomas

La figura 5.6.1.3 Muestra el aspecto de la estación de 15 m en banda S/X en Maspalomas para el control de SPAINSAT y las estaciones de 6,3 m en banda X apuntando cada una a uno de los satélites.

Segmento Usuario

La utilización de las capacidades proporcionadas por el sistema satelital depende de un adecuado segmento terreno de usuario, El segmento terreno de usuario está compuesto por los terminales fijos, móviles o transportables destinados a establecer comunicaciones entre los usuarios del sistema en todos los escenarios operativos previstos. También incluyen los elementos de monitorización y ayuda a la explotación de las capacidades, como supervisión del espectro y el enlace, asignación de portadoras o control de la antena activa anti-interferencias IRMA embarcada en el SPAINSAT.

Cabe destacar el importante papel de la industria española en el despliegue y suministro continuo a las FAS de todos los elementos del segmento terreno. Ello permite, no solo disponer de un parque de terminales con amplias capacidades operativas, sino que ha posicionado a la industria española en un papel de liderazgo en este tipo de sistemas a nivel internacional.

Los componentes del segmento usuario se clasifican en tres grupos:

1) Elementos de control y ayuda a la explotación: monitorización de enlaces, supervisión de espectro y control de la antena IRMA.

2) Estaciones de anclaje, que incluye las estaciones fijas de acceso al satélite y el interfaz con los sistemas de comunicaciones militares y redes de comunicaciones terrestres en general. El Ministerio de Defensa Español ubica estas instalaciones en dependencias del Ejército del Aire y del Espacio (EA) y la Armada en Torrejón de Ardoz y Valdilecha, respectivamente.

3) Los terminales de usuario permiten el acceso al sistema de satélites, no solo a los usuarios directos, sino que además proporcionan el interfaz de comunicaciones terrestres en el punto de despliegue, de tal manera que recogen todas las comunicaciones en un área determinada y actúan como punto de acceso a las redes globales. Existe una gran variedad de terminales: terminales fijos, terminales de despliegue rápido, terminales transportables “Satcom at the Quick Halt” o “Satcom on the Move” que mantienen comunicación en movimiento. Terminales en maleta “Manpack”, terminales navales, aeronáuticos y terminales especiales en helicóptero o submarino.

El reemplazo de los SPAINSAT y XTAR-EUR

Los satélites SPAINSAT y XTAR-EUR están apurando sus últimos años de vida útil. Como se comentó anteriormente, fueron lanzados en 2006 y 2005 respectivamente con una vida útil nominal de 15 años. La adecuada gestión orbital de ambos satélites y la fiabilidad de sus componentes están permitiendo alargar esta vida útil. En la fecha de redacción de estas líneas, la nueva generación de satélites SPAINSAT NG I y SPAINSAT NG II están en una fase avanzada de diseño y construcción. El satélite SPINSAT NG I ocupará la posición orbital de 29ºE (actual posición de XTAR-EUR). Está previsto su lanzamiento en el año 2024 mediante lanzadores reutilizables Falcon 9 de la empresa norteamericana SpaceX.Por su parte, el satélite SPAINSAT NG II se llevará a la posición orbital 30ºW también por un lanzador Falcon 9 de SpaceX a lo largo del año 2025.

Esta nueva generación de satélites amplía las capacidades de los actuales en banda X y Ka militar por un factor de 16. Además, incorporan la banda UHF de la que no se disponía.

Dado que sus posiciones orbitales son similares a los actuales SPAINSAT y XTAR-EUR, la huella global combinada es la misma, posibilitando la comunicación desde cualquier punto del territorio nacional con un punto entre los meridianos 110ºW y 110ºE aproximadamente. Entre la capacidades mejoradas y añadidas destacamos las siguientes:

1) En la banda X:

- Las antenas activas a bordo SARA, (evolución de las actuales IRMA, también de desarrollo español,

Figura 5.6.1.4 terminales de usuarios. Imagen cedida por AICOX Soluciones S.A

permiten optimizar las capacidades de geolocalización y cancelación de interferencias mediante técnicas de "beamhopping", "beamforming" y "nulling".

- Permite configurar 16 áreas de cobertura mediante haces orientables y dos áreas de cobertura globales.

2) En la banda Ka Militar: incorpora capacidad bidireccional a través de seis haces orientables más una cobertura global, y mediante un procesado digital a bordo, permite la interconexión de las bandas X y Ka militar proporcionando un altísimo nivel de flexibilidad.

3) En la banda UHF: hace posible una cobertura global.

4) Junto a las capacidades de transmisión, los nuevos satélites basados en la plataforma EUROSTAR NEO de Airbus, incorporan refuerzos y protecciones contra fenómenos nucleares en la atmosfera.

Además de atender las necesidades operativas de las FAS, los nuevos satélites pueden proporcionar capacidad a otros países aliados en el marco de acuerdos bilaterales y a organismos multinacionales y europeos. En particular, las características de los satélites SPAINSAT NG les hacen adecuados para ser parte del paquete de capacidades NATO y contribuir a las iniciativas de las agencias EDA, EUSPA y de la CE como GOVSATCOM.

Asociado al lanzamiento de los satélites SPAINSAT NG está el despliegue de nuevos sistemas del segmento de control y de usuario que permitan tanto el control como la utilización de las nuevas bandas y capacidades. Son necesarias estaciones de anclaje adicionales, especialmente en las bandas Ka militar y UHF y nuevos centros de seguimiento y control. Al centro de Maspalomas antes descrito se unirá un nuevo centro en Hoyo de Manzanares.

El parque de terminales actual a disposición de las FAS es plenamente compatible con los nuevos satélites, pero la eficiente utilización de las nuevas capacidades requiere la dotación de más terminales en las bandas Ka y UHF, así como terminales multibanda. La industria española ya dispone de este tipo de desarrollos, lo cual contribuirá a reforzar la posición de liderazgo industrial de nuestro país en estos sistemas.

Capacidades compartidas e interoperabilidad

El modelo de adquisición de capacidades en comunicaciones por satélite descrito está basado en los sistemas propios, adquiridos a través de un innovador modelo de partenariado público privado, que dota a las FAS españolas de las capacidades descritas del sistema SPAINSAT/XTAR-EUR y su continuación con los SPAINSAT NG.

Este modelo se complementa a través de oportunidades de colaboración internacional entre las que destaca la participación en el paquete de capacidades OTAN (CP. 9A0130 SATCOM), En este aspecto, el papel de España no se limita solo a ser usuario de las capacidades puestas a disposición de los países miembros, sino que el propio operador español HISDESAT podría contribuir poniendo a disposición capacidades nacionales. Para ello, los satélites que van a reemplazar a los SPAINSAT y XTAR-EUR disponen de características que los hacen compatibles con los requisitos NATO. Frecuencias, posiciones, anchos de banda y parámetros radioeléctricos, así como los requisitos HANE para eventos nucleares en la atmósfera, que hacen de los nuevos SPAINSAT NG una plataforma adecuada para aportar al paquete de capacidades NATO.

También España está tomando una posición de liderazgo en el programa GOVSATCOM de la EDA, que pretende poner a disposición de los países europeos unas capacidades comunes de comunicación por satélite. Tanto el Ministerio de Defensa como la industria española y el propio operador HISDESAT son actores muy activos en las fases de requisitos y preparación de programa GOVSATCOM. Recientemente se ha asignado al INTA el papel de Autoridad Nacional Competente GOVSATCOM para la coordinación del uso de estas capacidades.

Finalmente, existen memorandos de entendimiento (MoU) o colaboraciones bilaterales con otros países con el objeto de promover el uso conjunto de capacidades. Ejemplos de estas colaboraciones son los MoUs con Noruega, Polonia y distintos países iberoamericanos.

1.2. Observación de la Tierra

Las capacidades de observación de la Tierra de las FAS han estado basadas en el programa de los satélites ópticos HELIOS. Es un programa en el que participan Francia, Bélgica, Italia, Grecia y España. El HELIOS II es la continuación del HELIOS I compuesto por dos satélites ópticos.

En paralelo a esta capacidad, a mediados de la década de los 2000 se puso en marcha el programa PNOTS (Plan Nacional de Observación de la Tierra por Satélite). Este programa, fruto de la colaboración de los Ministerios de Defensa y de Industria, Energía y Turismo preveía la construcción y puesta

en servicio de dos satélites: El PAZ con tecnología de radar de apertura sintética (SAR) y el INGENIO con tecnología óptica.

Este ambicioso programa permitiría a España poder ser el primer país europeo en disponer de un sistema dual óptico y radar para uso civil y militar. Además, posibilitaría en la continuación de la participación en el programa internacional MUSSIS (Multinational Space-based Imaging System for Surveillance, Reconnaissance and Observation), continuador de los programas HELIOS, pasar de ser un país receptor de capacidades a contribuir a las capacidades ofrecidas a los miembros del programa.

Los planes se truncaron parcialmente con la pérdida del satélite INGENIO por un fallo en el lanzador VEGA ocurrido durante su lanzamiento del 17 de noviembre de 2020 desde Kourou en la Guayana Francesa. Por el contrario, sí había resultado exitoso el lanzamiento del satélite PAZ por un lanzador Falcon 9 de SpaceX desde la base aérea Vandenberg en California (EE.UU.) en febrero de 2018.

Así pues, tras las vicisitudes del programa PNOTS, en la actualidad las capacidades españolas en Observación de la Tierra están basadas en el satélite Radar PAZ y en la participación española en los programas HELIOS II y componente óptica (CSO) de MUSSIS. Estas capacidades se amplían con imágenes de los satélites alemanes TerraSAR-X y TanDEM-X, gemelos del PAZ y cuyas órbitas similares les permiten funcionalidades de constelación con mejora de los tiempos de revisita y productos multisensor, y con datos puntuales procedentes de suministradores comerciales.

El satélite PAZ ha seguido un modelo de adquisición similar al de los satélites de comunicaciones. Es propiedad de la empresa HISDESAT con participaciones de la industria española y el Ministerio de Defensa a través de su empresa ISDEFE. El suministro de las imágenes del satélite se realiza a través de un contrato marco con HISDESAT.

El segmento terreno de observación de la Tierra es propiedad del Ministerio de Defensa. La estación principal de seguimiento de control y recepción de imágenes es propiedad del INTA y se encuentra en el CEIT (Centro Espacial de INTA en Torrejón) campus de Torrejón de Ardoz. Esta capacidad está redundada desde el CEC (Centro Espacial de Canarias), también de INTA, que en caso de necesidad puede asumir desde alguna de sus antenas la transmisión y la recepción, tanto en la banda S como X propias del satélite. El procesado de las imágenes, desde su recepción en el CEIT hasta su uso en productos de inteligencia se lleva a cabo también en un centro del Ministerio de Defensa, en este caso el CESAEROB (Centro de Sistemas Aeroespaciales de Observación) del Ejército del Aire y del Espacio.

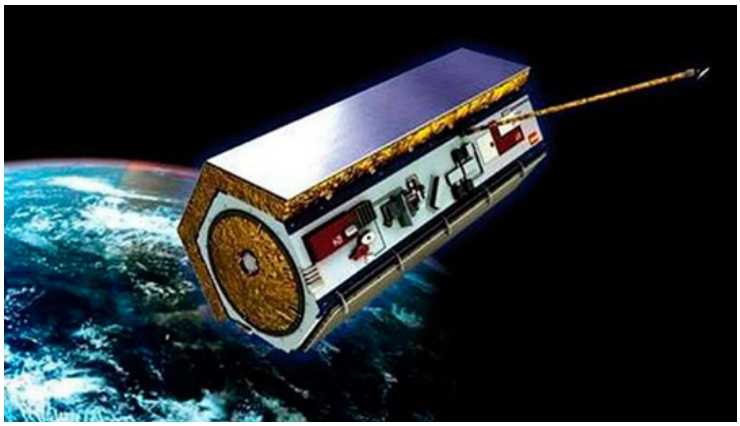


Figura 5.6.2.1: Representación artística del satélite PAZ. Fuente HISDESAT

El satélite PAZ

El satélite PAZ es un satélite de observación con un sensor radar de apertura sintética, lo cual le dota de capacidades de observación todo tiempo con independencia de la cobertura de nubes y la iluminación natural por el sol, ya que la imagen se crea mediante el proceso de señales radioeléctricas en banda X emitidas por el propio satélite que rebotan en los objetivos sobre la superficie de la Tierra.
PAZ está en una órbita heliosíncrona a 514 km de altitud con un periodo de rotación de aproximadamente 95 minutos. Con esta órbita, y en las latitudes del territorio nacional, incluida Canarias (latitudes por encima de 28º Norte o Sur), se consigue tener una revisita en menos 35 horas. En general, cualquier punto de la superficie terrestre puede ser revisitado en un tiempo inferior a 70 horas.

Órbita	Síncrona con el Sol
Órbitas/día	15,18
Periodo de repetición	11 días
Altura nominal en el ecuador	514 km
Inclinación	97,44º
Hora del nodo ascendente	18:00 ± 0,25h (hora local)

Tabla 5.6.2.1: Características de la órbita de PAZ

El satélite PAZ puede operar en distintos modos con mayor o menor resolución, desde los modos tipo “Spotlight” con resoluciones de hasta 25 cm, hasta los modos tipo “ScanSAR” que, con resoluciones menores, permiten barridos de hasta 200 km de amplitud. La siguiente tabla muestra los distintos modos en los que, con un tamaño de escena determinado, se consiguen distintas resoluciones.

MODO	RESOLUCIÓN ESPACIAL (ACIMUT X RANGO)	TAMAÑO DE ESCENA (ACIMUT X RANGO)
WideScanSAR	≤ 39 m x [1.75 – 3.18] m (SSC)	208 Km x [273 … 196] Km
ScanSAR	≤ 18 m x 6 m	100 km x 100 km
Stripmap-single	≤ 3 m x 3 m	30 km (rango)
Stripmap-dual	≤ 6 m x 6 m	15 km (rango)
Spotlight-single	1 m x 1 m	10 km x 10 km
Spotlight-dual	2 m x 2 m	10 km x 10 km
HR Spotlight-single	< 1 m x 1 m	5 km x 5 km
HR Spotlight-dual	< 2 m x 2 m	5 km x 5 km
Staring Spotlight	0.25 m x 0.59 m (SSC)	[2.7..3.6] km x [9.. 4.6] km

Tabla 5.6.2.2: Modos de operación de PAZ

Estas características técnicas permiten múltiples aplicaciones a las FAS tales como vigilancia de cualquier punto de la superficie terrestre, generación de productos de inteligencia, simulación para operaciones Militares (MilOps), cartografía de alta resolución, monitorización de desastres naturales y evaluación de daños, control fronterizo, etc.

Situación futura

Tras el fallido lanzamiento del satélite INGENIO, la capacidad óptica de observación de la Tierra se está logrando a través del CSO de MUSSIS. Asimismo, el satélite PAZ cumplió en febrero de 2023 cinco años en órbita, que es su vida útil nominal. La precisión de inyección orbital lograda por el lanzador Falcon 9 ha permitido un sustancial ahorro de combustible en el posicionamiento en la órbita definitiva, lo que, unido a la fiabilidad de los componentes, permite estimar su vida útil en 5 años más, al menos hasta el 2028. Con los plazos que se manejan en los sistemas espaciales se están contemplando dos actuaciones paralelas: definición del PAZ2 para reemplazar al PAZ al final de su vida útil y definición de un nuevo satélite óptico que pueda aportar las capacidades, mejoradas al estado del arte actual, previstas para el malogrado INGENIO. La culminación de estas actuaciones permitirá retomar los planes de disponer de capacidad propia, tanto con sensores ópticos como con sensores radar, y poder convertir a España, no solo en país usuario de las capacidades europeas, sino en país contribuyente a esas capacidades.

1.3. Sistemas de Navegación y Posicionamiento por Satélite

La capacidad de posicionamiento por satélite de las FAS se ha cubierto hasta ahora a través del sistema GPS del Departamento de Defensa de los EE.UU. Además de la capacidad de uso general civil, las FAS están utilizando la denominada PPS o Servicio de Posicionamiento Preciso para uso militar. Este servicio se usa en el marco de un acuerdo de uso operacional suscrito por todos los países de la OTAN por el que el Gobierno de los EE.UU. permite el acceso a estas capacidades a sus países aliados. Este acuerdo está en vigor, con sucesivas extensiones, desde 1994.

Por otro lado, España ha participado desde su inicio en los años 2000 en el desarrollo del sistema GALILEO de la Comisión Europea que tiene como objetivo principal lograr la independencia de los países europeos en las capacidades de Navegación y Posicionamiento por Satélite. Para el despliegue y operación de los sistemas Galileo la Unión Europea creó la GSA (GNSS Agency), que posteriormente se ha convertido en la EUSPA (Agencia de la Unión Europea para el Programa Espacial), asumiendo competencias, además de navegación, en comunicaciones (GOVSATCOM) y observación de la Tierra (COPERNICUS). Hay que resaltar en el desarrollo de Galileo el papel de la ESA (Agencia Espacial Europea), que es un organismo internacional no dependiente de la Unión Europea, constituido por 22 países europeos y Canadá como estado asociado, y que es el organismo con la experiencia y capacidades técnicas relevantes para la actividad espacial en Europa.

En la actualidad el Sistema Galileo, que se describe más adelante, está operativo en todos sus servicios. España ha seguido apostando por el despliegue del sistema y en el apoyo a la industria nacional para el desarrollo de todo tipo de capacidades, desde el diseño de terminales y módulos, hasta el desarrollo de múltiples aplicaciones. También se ha apostado por albergar infraestructuras. Nuestro país hospeda:

1) El centro de servicios GNSS ubicado en las instalaciones del INTA en el campus de Torrejón. Este centro es el principal interfaz de apoyo a los usuarios en todos los servicios prestados por el sistema.

2) Uno de los centros redundados de Monitorización de Seguridad Galileo (GSMC) ubicado en las instalaciones del INTA en el Campus La Marañosa (San Martín de la Vega – Madrid). Este centro es redundante del situado en la localidad francesa de Saint Germain en Laye. El centro se trasladó a La Marañosa en 2019 tras la salida del Reino Unido de la Unión Europea dejando de ser, por tanto, un país miembro del sistema Galileo.

3) El Centro Espacial de Canarias en Maspalomas, también instalación del INTA, alberga las estaciones terrenas y un centro de control del sistema MEOLUT de salvamento y rescate por satélite del sistema Galileo. Estas instalaciones se operan conjuntamente, ya que complementan el servicio, con el sistema COSPAS-SARSAT embarcado en satélites de órbita baja.

Dentro de los servicios Galileo, es de particular relevancia para las FAS españolas el denominado Servicio Público Regulado (PRS), que está destinado exclusivamente a aplicaciones gubernamentales, incluidas las de Defensa. Este servicio ofrece prestaciones mejoradas de precisión, seguridad, integridad, robustez y disponibilidad. El acceso al mismo está restringido. Para que la industria nacional pudiera optar a desarrollos en módulos de seguridad del mismo y para coordinar el despliegue de las infraestructuras de soporte y el acceso de usurarios cualificados, el Sistema Galileo prevé el establecimiento de autoridades competentes nacionales en PRS, por sus siglas en ingles CPA (“Compentent PRS Authority”). En España esta autoridad la ostenta el INTA desde 2012.

Se está desplegando una importante actividad en proyectos piloto que permitan avanzar en la incorporación de las capacidades proporcionadas por los servicios PRS de Galileo a la operativa de las FAS de manera compatible y solapada con el uso del GPS en virtud de los acuerdos con los EE.UU.; acuerdos que, por otro lado, incorporan la reciprocidad en facilitar el uso del PRS por dicha nación. Los proyectos piloto permiten, por un lado, validar determinados servicios y por otro, familiarizar a los usuarios en el nuevo sistema.

El establecimiento de requisitos de uso en plataformas y sistemas de armas, la colaboración con terceros países, no europeos, que puedan usar España como punto de acceso al servicio PRS, la capacitación de los usuarios y la reducción de costes al disminuir el uso de las capacidades GPS, están entre los objetivos prioritarios en esta fase inicial de consolidación de las capacidades Galileo. Todo ello sin olvidar fomentar las posibilidades de la industria nacional para proporcionar terminales, módulos y aplicaciones en los mercados europeos y globales.

El sistema Galileo

El segmento espacial de Galileo está constituido por una constelación de 30 satélites en órbitas de media altitud (MEO “Medium Earth Orbit”) a 23.222 km de altitud. Es una constelación tipo Walker 56:24/3/1, Es decir, 24 satélites en 3 planos inclinados a 56º, que abarcan los 360 grados alrededor del ecuador. A ellos se suman 6 satélites de repuesto, dos por plano orbital, hasta completar los 30 satélites de la constelación. Esta característica proporciona mejor cobertura en zonas polares que el GPS. Uno de los proyectos piloto desarrollados en España ha sido la validación de esta mejor de cobertura obteniendo posiciones en altas latitudes durante las campañas antárticas.

Los satélites están equipados con relojes atómicos con precisiones mejores que 1 ns en 24 horas. La transmisión de las señales de navegación son en la banda L (0,96 GHz – 1,61 GHZ) compatibles con el sistema GPS.

Las distintas estaciones, centros de control y otros centros que constituyen el segmento terreno de Galileo están distribuidos por todo el planeta, pero siempre en territorios dependientes de naciones europeas (Europa y territorios ultramarinos).

Sus elementos principales son:

1) Seis estaciones de Seguimiento Telemetría y Telecomando ubicadas en Reunión (FR) Papeete (FR), Noumea (FR), Redu (BE), Kourou (FR) y Kiruna (SE)

2) Cinco estaciones de subida de datos de navegación, ubicadas en Svalvard (NO), Reunión (FR) Papeete (FR), Noumea (FR) y Kourou (FR)

3) Dos centros de control con funciones asignadas y capacidad de redundarse uno a otro. GCC-I en Fucino (IT) y GCC-D en Oberpfapfenhoffen (DE)

4) Dos centros de monitorización de seguridad e interfaz con las CPAs en La Marañosa, San Martín de la Vega (ES) y en St. Germain en Laye (FR)

5) Un centro de servicios Galileo, GSC en Torrejón de Ardoz (ES)

6) Un centro de referencia geodésica

7) Un centro de referencia de tiempo

8) 15 sensores de señal GSS en territorios bajo soberanía europea.

El sistema Galileo puede proporcionar los siguientes servicios a través de las diferentes señales de navegación que maneja:

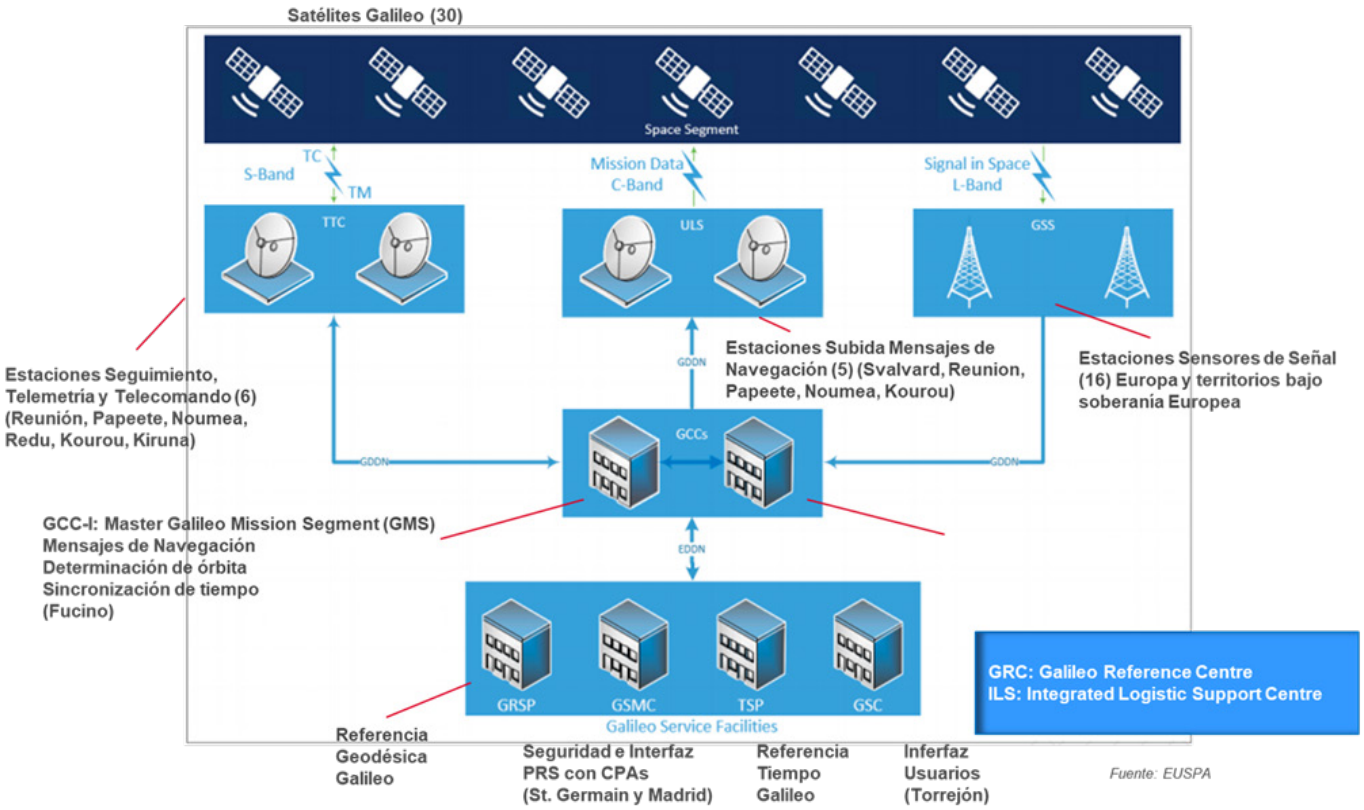


Figura 5.6.4.1: Arquitectura del segmento terreno GALILEO. Fuente EUSPA

Open Service (Os) **Servicio Abierto**	Acceso libre a servicio de posicionamiento, navegación y tiempo
Public Regulated Service (Prs) **Servicio Público Regulado**	Servicio encriptado diseñado para mayor robustez y disponibilidad, destinado a usuarios autorizados por los gobiernos
Search & Rescue Service (Sar) **Servicio de Búsqueda Y Salvamento** **Sar Forward & Return Link**	Contribución a COSPAS-SARSAT. Asistencia a la localización de gente en peligro y confirmación de recepción de alerta.
Os-Navigation Message Authentication (Os-Nma) **Os Autenticado**	Extensión del Servicio OS mediante la autenticación del mensaje de Navegación
High Accuracy Service (Has) **Servicio de Alta Precisión**	Servicio basado la provisión de datos de valor añadido y correcciones de alta precisión a través de una señal adicional. Acceso libre.
Commercial Authentication Service (Cas)	Servicio de acceso autenticado basado en el uso de señales con códigos encriptados. De pago.

Tabla 5.6.3.1: Servicios GALILEO

El Servicio Público Regulado (PRS)

Las señales de los satélites de navegación (GNSS) son muy débiles y están sujetas a perturbaciones. Estas perturbaciones pueden ser interferencias no intencionadas (no voluntarias ni predecibles) procedentes de fuentes diversas como comunicaciones móviles, enlaces de microondas, señales de TV, Wifi/WiMax, etc. Pero también pueden sufrir interferencias intencionadas o "jamming". El jamming crea la imposibilidad de adquisición de señal o la adquisición de manera tan degradada que tiene impacto severo en la precisión de la localización. Además, puede ser generado por dispositivos de bajo coste, relativamente fácil adquisición o fabricación y dificultad de localización si son de baja potencia. Otra técnica, aún más peligrosa es la suplantación mediante señales falsas o "Spoofing", Mediante la transmisión de señales falsas adecuadamente procesadas se puede generar en los receptores falsas medidas de posición, velocidad o tiempo sin conocimiento por parte del usuario. Son técnicas muy complejas y elaboradas que pueden llevar a la captura de vehículos por fuerzas hostiles a través del "engaño" de sus sistemas de navegación.

El servicio Público Regulado (PRS) surge de la necesidad de garantizar la autenticidad y continuidad de la señal de navegación, que los sistemas GNSS, salvo la señal militar del GPS no pueden garantizar. Es un servicio robusto y de acceso controlado para aplicaciones gubernamentales que requieren un alto nivel de continuidad y seguridad.

El PRS proporciona datos de posición – velocidad – Tiempo (PVT) autenticados, está protegido contra interferencias de todo tipo y contra modificaciones intencionadas de la señal. Es un servicio independiente y operativo de alta continuidad, especialmente en periodos de crisis o cuando otros servicios pueden estar degradados y que permite la restricción de su uso en áreas geográficas concretas, a receptores o grupos de usuarios determinados y con limitaciones temporales, pudiendo denegar el servicio a receptores o grupos de usuarios definidos en lugares y tiempos configurables. Finalmente, y al ser Galileo un sistema perteneciente a la Unión Europea está diseñado para permitir no compartir datos sensibles de una nación con otras naciones, garantizando la soberanía individual dentro de la Unión.

La protección frente a jamming se lleva a cabo mediante técnicas de diversidad de frecuencas y modulaciones de espectro ensanchado (Modulación BOC "Binary Offset Carrier"). Las capacidades de protección frente a spoofing se consiguen con autenticación y cifrado de códigos PRN y de mensajes de navegación. También se mejora la relación señal ruido para mejorar la disponibilidad de las señales respecto a otros servicios del sistema Galileo.

Las características antes descritas del servicio requieren establecer una comunicación entre los centros de control de Galileo o los puntos de contacto de los participantes (POC-P) y los terminales, adicionales a las propias señales de navegación. Esta comunicación se requiere, entre otras razones operativas, para la inicialización de terminales e intercambio de claves, las peticiones y autorizaciones del servicio o el reporte de incidentes, pudiéndose establecer a través de los propios satélites Galileo que incorporan el denominado Canal Primario: Un canal de comunicaciones entre los centros de control, los POC-P y los terminales en campo.

El Canal Primario, sin embargo, tiene una serie de limitaciones e inconvenientes derivados de un bajo ancho de banda disponible, la unidireccionalidad del canal y la necesidad de intercambiar información entre POC-P de países e infraestructuras comunes para hacer llegar datos hasta los propios terminales del país. Además, a medida que se aumenta el número de terminales o se hace necesario gestionar grupos amplios, se ralentizan los tiempos para la primera posición adquirida (TTFF) y se requiere mantener los terminales encendidos mucho tiempo hasta adquirir claves e información de seguridad. Si bien estas limitaciones irán desapareciendo progresivamente a medida que las nuevas generaciones de satélites Galileo reemplacen a los actualmente en operación, el uso eficiente de las capacidades PRS requiere en la actualidad por parte de los participantes del despliegue de un canal de comunicaciones alternativo entre los POC-P y los terminales de cada participante. Es el denominado Canal Secundario.

En España, la autoridad competente CPA está desarrollando junto con la industria nacional esta capacidad. La comunicación con los receptores se puede llevar a cabo a través de redes tácticas como TETRA, TETRAPOL, HF o redes LTE o VSAT. Con el establecimiento de este canal bidireccional se logra un menor tiempo de arranque de los receptores, un mayor ancho de banda para el intercambio de datos, el direccionamiento individual de los terminales y la posibilidad de aumentación GNSS para la reducción de los tiempos de posicionamiento. Entre las ventajas de disponer de un Canal Secundario Nacional está también el mantenimiento de la soberanía en la gestión de los sistemas propios.

La figura 5.6.3.2 muestra el esquema de comunicación entre los terminales y los centros Galileo, bien a través del Canal Primario, bien a través del Canal Secundario.

Proyectos Piloto

El despliegue inicial del Canal Secundario Español llevado a cabo por la CPA residente en el INTA ha sido clave para realizar los primeros proyectos piloto, ya que incorpora, junto con una cadena acreditada nominal, una cadena de preproducción y validación operacional. En este entorno se han podido llevar a cabo proyectos tendentes a validar a nivel de usuario final el servicio. Destacamos entre estos proyectos las medidas de líneas base cartográficas, la cartografía Antártica, el empleo del sistema Galileo en cartas náuticas, el estudio de precisión y estabilidad de señales de tiempo, la evaluación de sistema para usos SAR, la evaluación de la señal en entornos multibandas o demostradores muy innovadoras de arquitecturas distribuidas de terminales PRS que permiten mantener en ubicaciones seguras los módulos de seguridad sin necesidad de integrarlos en los terminales, entre otros.

1.4. Sistemas de Vigilancia Espacial

Las amenazas para la Defensa Nacional se pueden materializar en diversos entornos. A los tradicionales espacios terrestre, marítimo y aéreo hay que añadir el ciberespacio y el espacio ultraterrestre. Aunque podemos

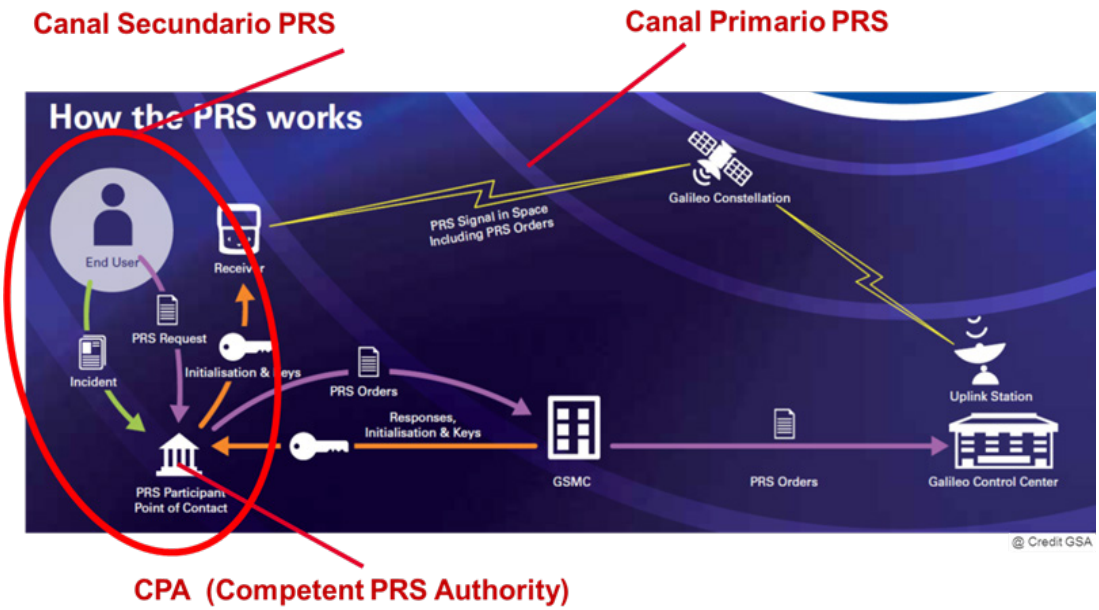


Figura 5.6.3.2 Canal secundario. Fuente EUSPA

considerar el espacio aéreo y el ultraterrestre como un continuo, no cabe duda de que el espacio ultraterrestre, con sus propias leyes físicas distintas de las que rigen la dinámica en la atmósfera, presenta unas peculiaridades que requieren de una estructura de mando y control, unos medios y unas capacidades adecuadas para operar en dicho entorno.

Los servicios que utilizan el espacio son de uso común en la vida diaria de los ciudadanos. Las telecomunicaciones, la navegación, la predicción meteorológica, la observación de territorio, por citar solo alguna de las aplicaciones que la ciudadanía usa a diario, están basadas en sistemas y plataformas espaciales. También, desde el punto de vista militar, el espacio proporciona capacidades y servicios únicos y esenciales, multiplicadores de fuerza y, a la vez, críticos para el análisis de la situación, la realización de operaciones o la alerta temprana de amenazas desde el propio espacio (misiles de largo alcance) o desde los espacios aéreo, terrestre y marítimo. Elementos hostiles en el espacio pueden, desde denegar servicios en el uso pacífico del espacio, hasta generar en sí mismos amenazas contra el territorio por obtención ilegitima de inteligencia o interferencia a los sistemas civiles y militares propios, tanto en el espacio como en los demás entornos. Tampoco debemos olvidar la vigilancia de amenazas naturales como son los objetos que pueden impactar contra la superficie terrestre y los fenómenos de clima espacial, fundamentalmente de origen solar que pueden generar eventos catastróficos sobre los demás sistemas eléctricos y electrónicos y suponer una amenaza para las vidas y los bienes de la ciudadanía. Por todo lo anterior, las naciones han tenido que tomar medidas y dotarse de capacidades para asegurarse la libertad de acción en el espacio ultraterrestre.

En España, el Ejército del Aire ha pasado a llamarse Ejército del Aire y del Espacio y la fuerza a llamarse Fuerza Aeroespacial. La orden del Ministerio de Defensa DEF/264/2023 de 16 de marzo por la que desarrolla la organización básica del Ejército del Aire y del Espacio añade a los tradicionales Mando Aéreo de Combate, Mando Aéreo General y Mando Aéreo de Canarias, el Mando del Espacio que tiene como cometido principal “la preparación de sus unidades, así como la dirección, planeamiento, organización y coordinación de las funciones que posibiliten la vigilancia, control y operación en el espacio”.

Dado que el espacio ultraterrestre, junto con el ciberespacio, es un entorno global y sin fronteras por definición, la colaboración internacional es fundamental para abordar los problemas y amenazas que en el se desarrollan. En 2014, la Unión Europea estableció un marco común para el apoyo a las actividades de vigilancia y seguimiento espacial (Space Surveillance and Tracking – SST). En este marco, España es miembro activo y coordinador de un consorcio de países: EUSST, formado por España, Francia, Alemania, Italia, Portugal, Polonia y Rumanía, que ha desplegado capacidades operativas para proporcionar de manera ininterrumpida servicios de prevención de colisiones en el espacio, análisis de reentradas y fragmentaciones a otros usuarios. Este papel de liderazgo ha permitido que la industria nacional sea también líder en Europa en cuanto a soluciones tecnológicas y desarrollos para estos fines.

El Centro de Operaciones de Vigilancia Espacial (COVE)

Por su parte, el Ejército del Aire y del Espacio creó en 2019 el Centro de Operaciones de Vigilancia Espacial (COVE). Sus instalaciones están ubicadas en la Base Aérea de Torrejón de Ardoz (Madrid) y opera el radar escalable de altas prestaciones (S3TSR) en la Base Aérea de Morón (Sevilla). Este radar puede considerarse un de los principales logros del I+D+i español, desarrollado por la industria nacional con el apoyo de la administración española.

Figura 5.6.4.1 Radar S3TSR en la Base Aérea de Morón. Fuente desconocida

Las capacidades que aporta este radar se complementan con sistemas civiles y militares de otros países miembros del consorcio EUSST, a través de los denominados SpOC (Space Operation Centers) generalmente civiles, y particularmente, con el S3TOC (Centro Español de Vigilancia y Seguimiento Espacial) inicialmente coordinado por el CDTI, del Ministerio de Ciencia e Innovación, y en la actualidad por la Agencia Estatal Agencia Española del Espacio. A través de estos centros, se tiene

acceso a otros sensores para la observación del espacio, tanto radáricos como ópticos. Cabe destacar que España es una de las principales potencias mundiales en puntos de observación astronómica y telescopios que aportan una información de alto valor para los fines de la vigilancia espacial.

El COVE tiene asignados por el Ejército del Aire y del Espacio los cometidos pertinentes, entre los que se encuentran:

- Vigilar, controlar y catalogar los objetos que orbitan la tierra. Detección, identificación y caracterización de objetos espaciales.
- El análisis de amenazas que afecten a capacidades espaciales propias y activación de mecanismos de protección. Alertas sobre esas amenazas.
- Apoyo a operaciones en todo lo relacionado con amenazas provenientes del espacio. Alertas de sobrevuelos de satélites con capacidades de observación sobre zonas de operaciones.
- Predicciones de clima espacial y afectación al espectro radioeléctrico
- Apoyo al lanzamiento de vehículos. Coordinación de vehículos suborbitales o en tránsito y seguimiento de maniobras de re-entrada.
- Fomentar la coordinación con otros centros de vigilancia y operaciones espaciales, estandarización de taxonomías y datos espaciales para facilitar el intercambio y órgano consultor, en general, de todo aquello relacionado con la vigilancia y seguimiento espacial.

2. SOLUCIONES Y RETOS TECNOLÓGICOS ESPACIALES

2.1. Procesado a Bordo, Interconexión de Haces y Antenas Activas

Tradicionalmente los satélites eran simples repetidores ubicados en una posición tan privilegiada como puede ser una órbita geoestacionaria con visibilidad sobre un tercio de la superficie terrestre. La señal se transmite desde una estación terrena modulando una señal en una determinada frecuencia. El satélite recibe esa portadora, la cambia a la frecuencia asignada al canal de bajada, la amplifica y la retransmite.

Este uso convencional tiene sus limitaciones e ineficiencias. Por un lado, la frecuencia utilizada para la subida o para la bajada de la señal es única para toda el área de cobertura que dibuja sobre la superficie terrestre la intersección del haz de la antena de transmisión o recepción. El espectro es un recurso escaso y por lo tanto la estrategia del repetidor limita la capacidad o ancho de banda útil.

Por otro lado, esta estrategia es ineficiente energéticamente. La energía es también un recurso limitado a bordo de un satélite. Para que la señal llegue a Tierra con un nivel suficiente debe ser amplificada con una potencia determinada. Esa potencia se distribuye en toda la cobertura de ese haz de comunicaciones, mientras que la señal va dirigida a un punto determinado de la Tierra donde está la estación de recepción. Es decir, se pierde mucha energía en toda la superficie terrestre donde no queremos comunicar necesariamente en ese momento. Cabe recordar que las comunicaciones por satélite son un radioenlace con un vano de más de 36000 km. y que hay que cumplir los balances del enlace. A menor potencia transmitida mayor tiene que ser el tamaño de las antenas de recepción. Difuminar la señal en decenas de miles de km2 hará que la densidad de potencia que llega a nuestro receptor sea pequeña y para captar la suficiente energía para demodular la señal serán precisas antenas terrestres de gran diámetro. Las aplicaciones tácticas, satcom on the move, manpack, navales o de despliegue rápido requieren terminales lo más reducidos posibles.

Una de las estrategias a seguir para soslayar las anteriores limitaciones o ineficiencias es recurrir a sistemas de comunicación multihaz. Para cubrir una determinada área, por ejemplo, un continente, con un satélite se puede diseñar una antena con una parábola conformada que dibuje un haz más o menos adaptado a la geografía del continente, o por el contario se puede diseñar una antena, basada en parábolas o en elementos radiantes activos que cubra el continente mediante múltiples haces más pequeños. En este segundo caso, la energía transmitida se concentra sobre un haz mucho menor, por lo que a la superficie de la tierra llega una densidad de energía más alta y la misma frecuencia se pude reutilizar en distintos haces sin que se generen interferencias. De esta manera multiplicamos el ancho de banda o la capacidad del propio satélite.

Llegados a este punto, hay que introducir un nuevo factor. Solo los terminales bajo un mismo haz serán capaces de comunicar entre ellos. Para hacer posible la comunicación

entre terminales que están en distintos haces es preciso llevar a cabo una interconexión entre haces en el propio satélite evitando el retraso inasumible que significaría hacer dos saltos para llevar a cabo la conmutación en tierra.

La interconexión entre haces puede ser estática, bien de manera permanente mediante conexiones fijas o bien conmutable desde tierra a través de telecomandos. Esto permite definir distintas áreas de cobertura, reconfigurar el satélite dependiendo de las necesidades asignando capacidad a una determinada zona o teatro de operaciones, lo cual, combinado con haces móviles permite una gran flexibilidad operativa. Esta estrategia es la seguida, por ejemplo, en la mayor parte de la capacidad de los actuales satélites españoles SPAISAT/XTAR que dividen la cobertura en haces orientables mediante comando y con conexiones estáticas entre ellos.

Un paso más es tener procesado a bordo. En vez de que el satélite actúe como un repetidor podemos hacer que funcione como un rúter. Ante una señal que le llega de la Tierra, el satélite no se limita a amplificarla, cambiarla de frecuencia y retransmitirla, sino que analiza las cabeceras de los paquetes de datos que transporta y redirecciona la señal hacia el haz donde está el terminal al que va dirigido el paquete de información. Estamos ante una interconexión dinámica de haces. Aunque ello no difiere en exceso de la tarea que todos conocemos de un rúter de internet, hay que realizarlo a 36000 km y en un entorno agresivo como es el espacio, con muy bajo porcentaje de errores. Y lo más importante, el nivel de fiabilidad tiene que ser mucho mayor que la conmutación en Tierra, pues un fallo en el sistema anularía la práctica totalidad el satélite. Este tipo de sistemas requieren de repetidores "regenerativos"; no amplifican y retransmiten la señal, sino que, como paso previo a la conmutación o enrutado, tienen que demodular el contenido y una vez asignado el paquete de datos al haz de salida hay que volver a modular antes de su amplificación. Por ello el equipamiento a bordo se complica por incorporar capacidades de recepción, amplificación de bajo ruido, demodulación, enrutado, modulación y amplificación de potencia. Cada vez son más comunes los satélites que incorporan procesado a bordo. En bandas de frecuencia altas (Ka, Ka militar) es la estrategia más habitual para permitir el reúso de frecuencia y optimizar la potencia disponible en un sistema que opera sobre centenares de haces.

Un satélite de comunicaciones gubernamentales de altas prestaciones que incorpora procesado a bordo se complementa con antenas activas. Las antenas activas, a diferencia de los paraboloides, configuran el haz radiante mediante la combinación de distintos elementos activos. Mediante la combinación de la potencia y fase de cada uno de los elementos se pueden definir distintas formas de haz, no solo para orientar la señal a un determinado teatro de operaciones, sino para geolocalizar señales, reforzar la transmisión en un punto o generar nulos que eliminen interferencias.

Capacidades Española y Europeas

Las antenas activas han sido objeto de diversos programas de desarrollo en el marco de la Agencia Espacial Europea, en particular a través de los programas de telecomunicaciones avanzadas ARTES ("Advanced Research in Telecomunication System"). España ha sido uno de sus grandes impulsores a través de la financiación de estos programas por el CDTI.

Fruto de la participación en los programas europeos y el esfuerzo inversor en I+D+i, España dispone desde hace años de estas capacidades. El satélite SPAINSAT, actualmente en órbita, incorporara una antena desarrollada por el INTA y CASA Espacio, actualmente AIRBUS DS en su sede de Madrid. La antena denominada IRMA opera en banda X y está basada en tecnología de "arrays" combinados en fase. Esa antena es de solo recepción y permite generar hasta cuatro haces configurando su forma o generando patrones de recepción con estrategias de geolocalización de transmisiones y anulación de interferencias.

La evolución de estas antenas ha llevado al desarrollo, fundamentalmente con tecnologías de resonador dieléctrico (DRA – Dielectric Resonator Antennas") de una nueva generación de antenas. AIRBUS ha desarrollado la antena para el satélite de observación astronómica de la ESA GAIA o la antena ELSA para Eutelsat Quantum, entre otras.

Dentro de las capacidades de Defensa, los satélites SPAINSAT NG incorporan las antenas SARA, también desarrollada por AIRBUS DS. Esta antena, basada también en tecnología DRA, supone un avance importante respecto a la anterior generación IRMA al incorporar capacidades de reconfiguración, tanto en la recepción como en transmisión, y manejar simultáneamente hasta 16 haces, 8 por polarización. La gran capacidad de generación de haces permite, además de las funcionalidades comunes de estas antenas de localización y anulación de interferencias, desarrollar estrategias de salto de haz o "beam hopping"; lo que permite atender simultáneamente a distintos terminales en movimiento (navales, aeronáuticos o terrestres) mediante conmutación dinámica o atender a la vez a varias zonas operacionales.

2.2. Comunicaciones Cuánticas

Necesidad de comunicaciones cuánticas

En primer lugar, antes de hablar de mecánica cuántica y de las soluciones tecnológicas basadas en ella, hay que hacer un ejercicio de abstracción y no intentar aplicar los conocimientos intuitivos que tenemos derivados de la mecánica clásica tratando de buscar una explicación a por qué algo ocurre de tal o cual manera.

La aparición de capacidades de computación cuántica supone una amenaza a la seguridad de las comunicaciones tal como las entendemos en la actualidad. Muchos de los protocolos críticos para las comunicaciones se basan en unas funcionalidades criptográficas como son la encriptación de clave pública, la firma digital y el intercambio de claves. En la actualidad esas funcionalidades se desarrollan a partir de algoritmos de intercambio de clave como el Diffie-Hellman, los criptosistemas RSA o de curva elíptica. La seguridad de estos algoritmos radica en la dificultad de resolución de problemas matemáticos como la factorización de grandes números enteros o logaritmos discretos. La aparición de algoritmos que pueden ejecutarse sobre plataformas cuánticas, como por ejemplo el algoritmo de Shor, pueden resolver esos problemas matemáticos complejos y romper la criptografía de una manera rápida y fácil de ejecutarse en computadoras cuánticas con los suficientes cúbits. Con el actual ritmo de evolución de las capacidades de computación cuántica, se estima que en el entorno de 2030 un ordenador cuántico sería capaz de romper un sistema criptográfico RSA de 2000 bits. Eso sí, el coste de esa computadora rondaría los mil millones de dólares. Algo caro, pero al alcance de instituciones públicas y algunas privadas.

Llamamos criptografía post-cuántica a una serie de algoritmos capaces de resistir a un ataque criptográfico por una computadora cuántica. La mayor parte de los sistemas asimétricos (clave pública) no lo superaría. Sin embargo, los sistemas criptográficos simétricos actuales como los sistemas criptográficos de bloques AES, incluidas las funciones hash, sí son robustos frente a un ataque con computación cuántica. Los sistemas simétricos son aquellos basados en el conocimiento de una clave única por todas las partes de una comunicación, por lo que su seguridad radica en una adecuada generación y distribución de claves. Es aquí donde la criptografía cuántica y el satélite se convierten en herramientas básicas para lograr esa criptografía robusta.

Principios de la criptografía cuántica

Para logar el objetivo de la criptografía cuántica de proporcionar comunicaciones seguras, se hace uso de principios y teoremas de la mecánica cuántica por los cuales el emisor y el receptor de un sistema de comunicaciones pueden acordar una clave común sin intercambiarla físicamente o a través de un canal preexistente y con la seguridad de que únicamente ellos conocen la clave. Los principios en los que se basa la criptografía cuántica son:

1) Polarización de los fotones como estado cuántico. Un fotón individual puede ser polarizado en un determinado plano.

2) Principio de incertidumbre de Heisenberg: dos propiedades relacionas de una partícula no pueden conocerse simultáneamente con precisión, pues la medida de una altera necesariamente la otra y viceversa.

3) Teorema de no clonación (Wootters y Zurek) que establece que es imposible crear una copia exacta de un estado cuántico escogido al azar de una partícula individual. No podemos clonar el spin, la polarización u otros estados cuánticos.

En un canal de comunicaciones cuánticas entre un emisor y un receptor, la mera presencia de un observador, que quiera medir estados cuánticos de los fotones intercambiados, alteraría esos estados y sería detectado, pudiendo los legítimos intervinientes optar por abortar la comunicación e iniciarla de nuevo hasta estar seguros de su integridad.

Distribución cuántica de claves (QKD – "Quantum key distribution")

La distribución cuántica de claves aprovecha los principios de la mecánica cuántica para simultáneamente generar y hacer llegar la clave de manera segura a ambos extremos de un canal de comunicaciones. Para ello hace uso de protocolos basados en el intercambio de fotones con determinados estados cuánticos, como por ejemplo la polarización. Existen distintos tipos de protocolos QKD: Protocolos de variable discreta: BB84, B92, SSP (Seis estados) o SARG04; protocolos de partículas entrelazadas como el protocolo de Eckert que hace uso de dos partes de un sistema cuántico en el que dos partículas entrelazadas, aunque estén separadas físicamente grandes distancias, alteran simultáneamente sus estados y protocolos de variable continua.

Experiencias cuánticas conocidas

Uno de los experimentos cuánticos más conocidos es el satélite chino Micius. A través de este satélite se distribuyeron claves entre la Academia de Ciencias Austriaca y la Academia de Ciencias China separadas 7600 km. Además, se incluyó un enlace de fibra entre la estación terrena en China y la sede de la academia. Con las claves intercambiadas se mantuvo una videoconferencia a través de un canal VPN con una duración de 90 minutos. Con este satélite también se comprobó el intercambio de claves con un protocolo de partículas entrelazadas a 1200 km y se vio que los estados entrelazados se mantenían con esa separación entre partículas.

Comunicaciones cuánticas en Europa

La Comisión Europea estableció en 2018 la iniciativa "Quantum Flagship" para la financiación de las tecnologías cuánticas. Europa ha tomado conciencia de la importancia de este tipo de tecnologías para no perder la carrera por la supremacía cuántica con los otros dos grandes actores: Estados Unidos y China. El Reino Unido, una vez fuera de la Unión Europea, también es un actor de relevancia en estas tecnologías.

Dentro del "Quantum Flagship" se enmarca la iniciativa EuroQCI o Iniciativa de Infraestructuras de Comunicación Cuántica Europea con el objetivo de desplegar una infraestructura de comunicación cuántica segura que abarcará toda la Unión Europea, incluyendo sus territorios ultraperiféricos. La iniciativa se desarrolla en colaboración con la Agencia Espacial Europea (ESA) para su diseño, desarrollo y despliegue. El EuroQCI consistirá en un segmento terrestre basado en enlaces de fibra óptica para unir nodos estratégicos y con topología transfronteriza. También dispondrá de un segmento espacial basado en satélites. Esta infraestructura será parte integrante del sistema de comunicaciones seguras basado en satélites que también está desarrollando la Unión Europea denominado IRIS2.

El EuroQCI hará uso de tecnologías innovadoras de comunicación cuánticas desarrolladas en el marco general del "Quantum Flagship" financiadas por la propia UE. Un pilar fundamental es la participación de la industria europea y pymes para garantizar que los componentes críticos sean europeos y minimizar la dependencia de terceros, en tecnologías tan sensibles como son la ciberseguridad o todo lo relacionado con las tecnologías cuánticas.

Iniciativas en España

Dentro de la iniciativa global europea EuroQCI, un grupo de entidades españolas lideradas por HISPASAT y entre las que destacan empresas líderes en tecnología, comunicaciones, sector bancario, así como instituciones científicas, universitarias y de la Defensa, están definiendo una misión consistente en el uso de satélites geoestacionarios para la distribución de claves cuánticas. Los satélites geoestacionarios permiten una amplia área de cobertura para la distribución de claves, pero por el contrario tienen que superar los efectos provocados por las grandes distancias de transmisión en la órbita geoestacionaria a 36.000 km.

El proyecto Caramuel, que así se denomina esta iniciativa, incluye una carga útil embarcada en un satélite geoestacionario compuesta por un telescopio de alta precisión, una fuente de fotones capaz de hacer transmisiones a tierra fotón a fotón para preservar las propiedades cuánticas y la electrónica asociada. El segmento terreno se compone de un centro de control y estaciones ópticas de usuario formadas por telescopios y receptores criogenizados para detectar fotones individuales. Los usuarios críticos de Caramuel dispondrán de su propio telescopio, mientras que otros usuarios comerciales podrán tener acceso a la red, a través de enlaces terrestres al nodo más próximo, reduciendo así el coste de la instalación y creando de esta manera una red global.

2.3. Nuevas Constelaciones de Satélites de Comunicaciones en Órbitas Bajas y Medias

Una constelación de satélites es un grupo de satélites que trabajan juntos como un sistema único. Por lo general, el objetivo de las constelaciones es proporcionar una cobertura conjunta muy amplia o una disponibilidad permanente de las capacidades que proporcionaría un satélite individual.

Los satélites pueden estar ubicados en distintos tipos de órbitas. Nos referimos a satélites geoestacionarios cuando están en una órbita situada a unos 36000 km sobre el Ecuador y que tiene como particularidad que la velocidad angular es coincidente con la de rotación de la tierra. Por ello, para un observador en la superficie terrestre el satélite está aparentemente fijo en una determinada elevación y azimut.

Por otro lado, los satélites de órbita baja ("Low Earth Orbit" LEO) orbitan a altura de unos pocos cientos de kilómetros sobre la superficie de la Tierra. Un observador en un punto dado vería el satélite aparecer por el horizonte, moverse con una velocidad sobre el cielo durante 10-15 minutos y desaparecer por el otro lado del horizonte. Al cabo de unos 90 minutos lo volvería a ver durante otros 10 minutos o menos y posiblemente no lo vuelva a ver hasta el día siguiente, debido a la geometría del problema. Ello se debe a la diferencia entre la velocidad angular del satélite comparada con la velocidad de rotación de la Tierra. Un satélite LEO podría proporcionar unos 30-40 minutos de servicio de comunicaciones al día.

Sin embargo, si ponemos en órbita un número determinado de satélites en planos orbitales y posiciones dentro de esos planos calculados adecuadamente podremos asegurar que en la práctica totalidad de la Tierra siempre hay uno o varios satélites visibles. Si además esos satélites pueden comunicarse entre ellos a modo de nodos de una red, una constelación adecuadamente diseñada puede proporcionar comunicaciones entre dos puntos de la superficie terrestre durante todo el tiempo. Para poder ofrecer estos servicios, una constelación LEO precisa de centenares de satélites. La constelación Starlink, que ha pasado a ser la más conocida por su relevante papel en proporcionar comunicaciones al gobierno de Ucrania en pleno conflicto con Rusia tiene en órbita más de 4000 satélites en la actualidad y prevé llegar hasta los 11000 en órbitas entre 550 y 1325 km de altitud. A partir de un número del orden centenar de satélites con órbitas adecuadamente seleccionadas, como hace la constelación OneWeb comercializada por Eutelsat, se pueden conseguir también buenas capacidades de comunicaciones globales.

Existen otro tipo de órbitas, las denominadas órbitas medias terrestres ("Medium Earth Orbit" – MEO). Estas órbitas están a alturas ente 15000 y 25000 kilómetros. Estas órbitas son las que ocupan, por ejemplo, los satélites de navegación GPS o GALILEO. Al estar la órbita más alta, el periodo de ésta es menor y el satélite está más tiempo visible sobre el horizonte. Ello permite cubrir la superficie de la Tierra con visibilidad permanente a uno o varios satélites con constelaciones con un menor número de satélites. Por ejemplo, GPS es una constelación de 24 satélites en órbitas de 20.189 km y es posible desde la mayor parte de la superficie terrestre (salvo regiones polares) ver permanentemente al menos tres satélites. GPS o la europea GALILEO son constelaciones denominadas Walker, citadas anteriormente, con tres planos inclinados 55º (56º GALILEO) y sus satélites distribuidos regularmente en fase en esos planos.

Si comparamos el número de satélites necesarios para tener comunicaciones globales con sistemas LEO o MEO con una constelación basada en satélites geoestacionarios, comprobamos que ésta ofrece una cobertura prácticamente global (salvo regiones polares) con solo ¡3 satélites!.

¿Por qué recurrir entonces a constelaciones de decenas, cientos o miles de satélites LEO o MEO? La latencia es el motivo por el que se recurre a órbitas más bajas. Pero también está el coste de poner un objeto en órbita, mucho menor en una órbita baja que en una geoestacionaria a 36000 km. Además, los satélites en órbita baja pueden ser más pequeños y se puede distribuir la carga de comunicaciones entre ellos, resultando que una constelación de centenares de satélites en órbita baja puede tener un coste de puesta en órbita del orden de un geoestacionario y puede proporcionar mucho más ancho de banda con un retardo mucho menor, y en cualquier caso asumible en la mayor parte de las comunicaciones. Otra de las ventajas, no menor, es la fiabilidad de la red. El fallo de un satélite geoestacionario es catastrófico, compromete la constelación y su reposición es muy cara. El fallo de uno, diez o cincuenta satélites de una constelación como Starlink o OneWeb puede ser desde irrelevante hasta llegar a suponer alguna diminución en las capacidades del sistema y siempre su reposición es un porcentaje pequeño del coste de la propia constelación. Un solo lanzamiento puede reponer decenas de satélites.

IRIS2

Las constelaciones de satélites pueden ser desplegadas para los distintos usos que proporciona el espacio: navegación, observación de la Tierra y comunicaciones. Dentro de las constelaciones de comunicaciones podemos diferenciar entre las constelaciones para radiodifusión (Sirius, XM Radio), las dedicadas a servicios telefónicos o comunicaciones bidireccionales como Globalstar, Iridium o las que ofrecen conectividad e internet como la citada Starlink, OneWeb, o Iridium NEXT. También últimamente están surgiendo redes para aplicaciones de banda estrecha diseñadas para "Internet de las Cosas" (IoT) que pueden usar mini y microsatélites muy baratos y compatibles con dispositivos terrestres existentes. Son ejemplos de este tipo de redes de datos Spire o HiperGlobal o la iniciativa española Sateliot compatible con dispositivos terrestres 5G.

Ante este despliegue de iniciativas comerciales que abarcan desde la participación de grandes actores aeroespaciales (Airbus, Thales), grandes tecnológicas como SpaceX o Amazon, hasta starts-ups como la mencionada Staeliot española, la Unión Europea ha propuesto un ambicioso

programa denominado IRIS2: “Infrastructure for Resileince, Interconectivity and Security by Satellite”. La iniciativa IRIS2 tiene como objetivos principales asegurar el acceso global a comunicaciones gubernamentales seguras por satélite para cualquier tipo de acciones de los gobiernos en vigilancia, acción exterior, gestión de crisis o protección de las propias infraestructuras, así como permitir la provisión de servicios comerciales por parte del sector privado para disponer de comunicaciones de gran ancho de banda y conectividad global eliminando zonas muertas o sin acceso. Para ello se hace uso de infraestructura existente y nuevos despliegues, También se integran en esta infraestructura otros activos estratégicos europeos como las comunicaciones gubernamentales por satélite geoestacionario GOVSATCOM o las comunicaciones seguras con encriptación cuántica de la iniciativa EuroQCI.

Uno de los elementos a desplegar será una constelación de satélites de órbita baja que ofrezca una cobertura casi global, y en todo caso, en cualquier punto del territorio continental de la Unión Europea y regiones ultraperiféricas, sin ningún tipo de vacío de cobertura. Otro punto importante es la independencia operativa y tecnológica de la Unión Europea. Los sistemas a desplegar contarán con tecnologías propias y todas las infraestructuras estratégicas, particularmente las estaciones y centros de control estarán ubicados en territorio continental europeo. Las políticas europeas están también destinadas a la creación de un tejido industrial altamente competitivo y a la participación de iniciativas privadas en el despliegue de las capacidades. IRIS2 prevé tres tipos de servicios:

1) Los denominados “HardGov” son servicios restringidos a usuarios gubernamentales autorizados basados en infraestructuras gubernamentales y que requieren un grado muy alto de seguridad.

2) Los servicios “LightGov”, también reservados a usuarios gubernamentales, pero que hacen uso de infraestructuras compartidas o infraestructuras comerciales.

3) Servicios comerciales. Son servicios destinados a usuarios comerciales que se pueden beneficiar de las infraestructuras públicas compartidas o de las propias infraestructuras comerciales.

La planificación inicial de la red IRIS2 y su interrelación con otras infraestructuras estratégicas de la Unión Europea como GOVSATCOM o EuroQCI prevé que IRIS2 entre en fase de explotación en 2027 y se pueda declarar la completa operatividad en 2028.

2.4. Las Constelaciones de Pequeños Satélites para Aplicaciones de Observación de la Tierra e “Internet de las Cosas”

Asociamos la calidad de un sistema de observación de la Tierra por satélite con la resolución de las imágenes que proporciona; sin embargo, este no es el único parámetro a tener en cuenta. Dependiendo de las aplicaciones, la calidad radiométrica, la resolución espectral, la precisión de la localización o los tiempos de revisita pueden ser elementos determinantes.

A medida que las aplicaciones de observación de la Tierra buscan otros productos o, por exponerlo de otra manera, los requisitos de inteligencia van más allá de tener imágenes de muy alta resolución y se busca, por ejemplo, mayor revisita o detección de determinados parámetros distintos a las imágenes masivas, se produce una convergencia entre estos requisitos y los requisitos de sistemas comerciales. Así, los sistemas de observación de la Tierra se ponen al alcance, no solo ya de los Estados y otros grandes actores, sino de iniciativas comerciales más modestas, “start-ups” y modelos de negocio del denominado “New Space”.

Si un sistema, bien comercial, bien de inteligencia requiere un refresco continuo de imágenes, más que una imagen de alta resolución, si prima la revista sobre la resolución, en lugar de un sistema de una o dos grandes plataformas espaciales, la solución, quizá, esté en una constelación de pequeños satélites, proporcionando imágenes más pequeñas, optimizadas para ciertos parámetros a detectar, pero actualizadas frecuentemente.

Los sistemas se simplifican aún más si los parámetros a detectar son captados por sensores en tierra y retransmitidos a la plataforma espacial para su retransmisión a un servidor central utilizando técnicas de Internet de las cosas (IoT). En estos casos, si bien “observamos” el territorio y mapeamos parámetros distribuidos geográficamente, estamos ante constelaciones realmente de comunicación de datos que prescinden de grandes ópticas o sistemas de procesado y transmisión, por lo que las constelaciones de satélites se simplifican y las capacidades pueden ser albergadas en micro o nanosatélites.

Todos estos sistemas en los que convergen requisitos de inteligencia y requisitos comerciales se despliegan con una aproximación conjunta de tecnologías espaciales y de tecnologías de la información. Es importante la plataforma espacial, pero es tan importante el proceso del

dato que simplifique la citada plataforma, su transmisión y la generación del producto comercial o de inteligencia. También destacan estos sistemas por una orientación al servicio más que al producto, aprovechándose precisamente de esta convergencia entre espacio y tecnologías de la información. Esa aproximación está al alcance de start-ups, pero también la abordan los grandes actores que compaginan los sistemas convencionales con despliegues de constelaciones de pequeños satélites con un "espíritu de start-up" e ideas del "New Space". Consecuencia de ello es la proliferación de propuestas de todo tipo, pero también el altísimo porcentaje de propuestas que se quedan en el papel o se abandonan en fases iniciales del despliegue.

Junto a iniciativas como Plantet Labs o las propuestas de grandes empresas como Airbus que combinan los grandes sistemas convencionales con colaboraciones con empresas más pequeñas e instituciones de enseñanza, surgen en España varias de iniciativas tanto en observación con IoT (Fossa Systems, Sateliot, Alén Space). También existen iniciativas públicas en colaboración entre España, Portugal y Brasil como es la red Atlántica consistente en una constelación de pequeños satélites de observación de la Tierra para aplicaciones medioambientales como la detección y monitorización de incendios forestales y que es parte del PERTE Aeroespacial español.

2.5. El Acceso al Espacio desde España

Una de las capacidades, aún incipientes en España, es el acceso al espacio con medios propios. Por acceso al espacio entendemos el conjunto de capacidades de lanzador y base de lanzamiento con sus sistemas auxiliares (radares, sistemas optrónicos, trayectográficos, estaciones de seguimiento y control, etc).

Sí se han desarrollado capacidades precursoras como lo fueron en las décadas de 1980 y 1990 los lanzamientos de misiles suborbitales INTA-100, 200 y 300 desde la base de El Arenosillo en Huelva. Como continuación de estos programas se planteó a finales del siglo pasado el desarrollo de un lanzador de pequeños satélites denominado Capricornio que finalmente no se concluyó. En dicho programa participaba la industria aeroespacial, electrónica y de explosivos y materiales energéticos líderes en sus campos en España en aquellos momentos.

Finalmente, más de dos décadas después, ha sido la iniciativa privada la que está punto de aportar esta capacidad. La empresa española PLDSpace con sede en Elche e instalaciones de ensayo en Teruel está desarrollando los lanzadores Miura-1 y Miura-5. El primero es un cohete suborbital, mientras que el segundo podrá llevar nano y microsatélites a órbita. Ambos están basados en tecnología de combustible líquido y son vectores reutilizables.

Desde el punto de vista de la base de lanzamiento, hay que tener en cuenta las particularidades geográficas del territorio nacional. Salvo en caso de usar vehículos lanzadores reutilizables en los que se puede controlar la recuperación de las distintas etapas y que no caigan componentes incontrolados a la superficie terrestre, es preciso, por lo general, volar sobre el mar o sobre territorio despoblado y de soberanía propia en las fases iniciales del vuelo. Las órbitas de interés suelen ser ecuatoriales inclinadas o cuasi-polares (heliosíncronas). En el primer caso habría que lanzar hacia el Este, de lo contrario la rotación de la Tierra añadiría un plus de energía necesaria para la inyección en órbita. En el segundo caso se puede lanzar al norte o al sur.

Con las restricciones geográficas y orbitales, desde territorio nacional serían posible lanzar en órbitas cuasi polares desde las Islas Canarias. Desde el sur del archipiélago existe un corredor totalmente marino comprendido entre el Archipiélago de Cabo Verde al oeste y Senegal al este. La costa sur de la Península Ibérica tendría limitaciones de ángulos de lanzamientos para no sobrevolar Marruecos. El resto del territorio no permite esquivar zonas pobladas salvo lanzamientos al oeste desde la fachada Atlántica que son altamente ineficientes. Teniendo en cuenta estas consideraciones, al mismo tiempo que se planteaba el desarrollo del lanzador Capricornio, se iniciaron los estudios para construir una base de lanzamiento. Se escogieron ubicaciones en la costa suroeste de la isla de Gran Canaria y en la costa sur de la isla de El Hierro. Fue en esta última ubicación donde se empezaron a realizar los trabajos previos que finalmente se cancelaron por problemas presupuestarios, sociales y medioambientales.

La única experiencia de lanzamiento de un satélite desde territorio nacional fue el lanzamiento en 1997 del satélite MINISAT-01. Se lanzó desde un lanzador Pegasus-XL adosado a la panza de un avión Lockheed L-1011 que despegó desde la Base Aérea de Gando. Este satélite tenía una órbita ecuatorial inclinada, por lo que para evitar sobrevolar el continente africano se lanzó hacia el oeste, hacia el Atlántico. En este caso, la potencia de lanzador y el peso reducido del satélite permitieron aportar el extra de energía necesario.

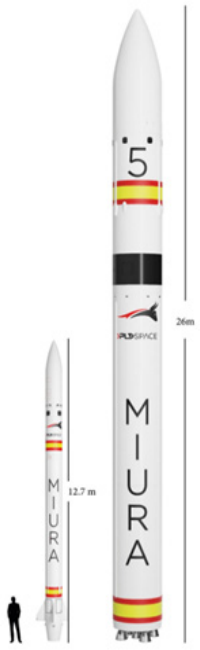


Figura 5.7.1: vehículos lanzadores de PLD Space Miura-1 y Miura-5. Fuente PLDSpace

En la costa de Huelva están ubicadas las instalaciones del INTA de El Arenosillo, desde donde se han lanzado cohetes suborbitales y se llevan a cabo rutinariamente todo tipo de ensayos de misiles y armamento para las FAS nacionales y de otros países europeos. Para estas misiones el centro cuenta con capacidades de seguimiento y trayectografía. Esta ubicación permite ciertos vuelos limitados por la proximidad de la costa norte de Marruecos.

Para lanzamientos de grandes satélites y satélites geoestacionarios se recurre siempre a lanzamientos comerciales. España participa en el lanzador Arianne y en la Base Espacial de Guayana, en Kourou (Guayana Francesa) que son las capacidades comunes de los países europeos con una fuerte componente francesa. También Italia dispone de un lanzador, el Vega que opera desde la Guayana Francesa. Sin embargo, es frecuente recurrir a lanzadores comerciales norteamericanos, o con anterioridad al actual conflicto de Ucrania, a lanzadores rusos o ucranianos desde bases rusas.

2.6. Plataformas de Gran Altitud (HAP) en la Estratosfera como Solución Tecnológica Complementaria

Durante la primera mitad del año 2023 empezaron a publicarse en la prensa diversos incidentes protagonizados por vehículos de origen desconocido en la estratosfera. Globos o artefactos voladores a gran altura surcaron los cielos de Estados Unidos y en algunos casos fueron derribados por aviones caza ante lo incierto de la amenaza. Posteriores análisis atribuyeron lo avistamientos a misiones de observación de China o a globos liberados por aficionados a la aerostación.

Por encima de 14 km o 50.000 pies, zona donde se desarrolla la práctica totalidad el tráfico aéreo convencional, y hasta los 30 km de altitud, se extiende una zona escasamente explotada para la actividad aeronáutica. Esta zona tiene un indudable interés para el despliegue de sistemas de observación o comunicaciones por cubrir un nicho intermedio entre los satélites y los drones o vehículos tripulados que operan a altitudes mucho más bajas.

Altitudes entre los 14 y 30 km pueden proporcionar áreas de cobertura de una extensión significativa, menor que la de un satélite en órbita, sin duda, pero mucho mayor que la de cualquier otra plataforma aérea en la troposfera. Por otro lado, en comunicaciones, donde la latencia pasa a ser un parámetro clave en ciertas aplicaciones, las plataformas estratosféricas la reducen significativamente al disminuir el tiempo de propagación de las señales respecto a una carga en un satélite LEO, MEO y sobre todo GEO donde el retardo llega a fracciones significativas del segundo.

El acceso a la estratosfera es órdenes de magnitud más barato en términos energéticos que la puesta en órbita de un satélite. No obstante, el entorno tiene sus dificultades derivadas de las características físicas de la zona como baja presión, baja temperatura e intensa radiación.

El acceso a esta parte de la atmósfera se logra a través de tres tipos de vehículos, cada uno de ellos con unas características que los hacen más adecuados para determinados tipos de misión.

- Vehículos de ala fija. La sustentación se logra, como en un avión, mediante el uso de la propulsión para generar empuje aerodinámico.
- Globos aerostáticos. Usan gases más ligeros que el aire para lograr la sustentación por flotación.
- Dirigibles. La sustentación es principalmente por flotabilidad, aunque incorpora propulsión mediante motores eléctricos que combinados con superficies de control aerodinámico permiten un grado de maniobrabilidad importante.

Los globos y los dirigibles son más ligeros que el aire y se denominan LTA ("Lighter tan Air") por sus siglas en inglés.

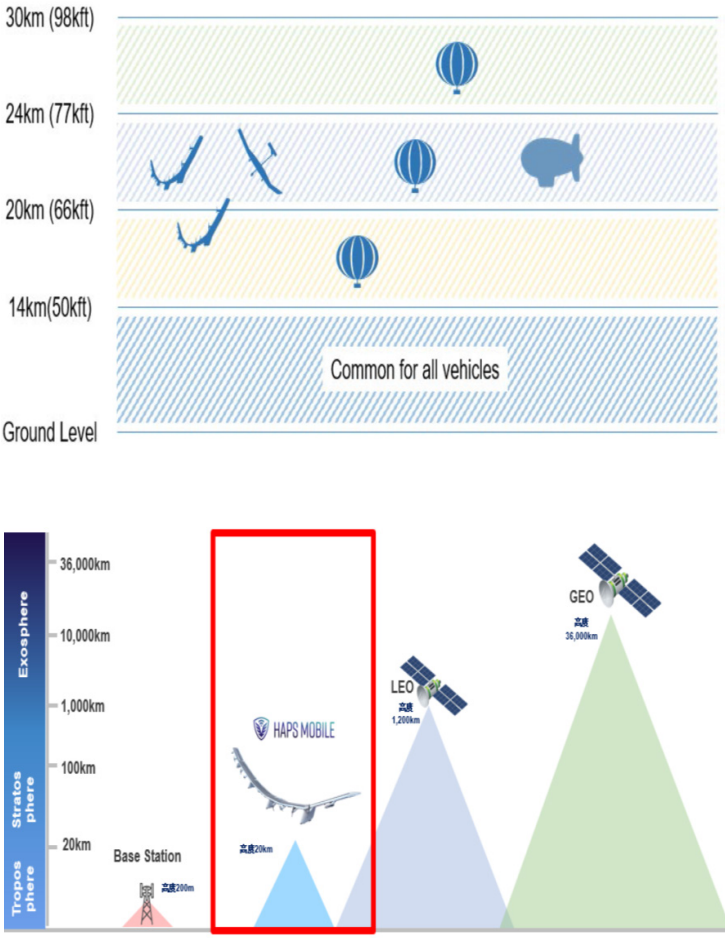


Figura 5.7.6.1: Altitudes de operación de HAPS y comparación de coberturas. Fuente HAPS Alliance

Las aplicaciones principales de estos sistemas son muy variadas, y en general, se solapan con las aplicaciones de satélites de observación y comunicaciones, cubriendo un espacio intermedio entre éstos y las redes terrestres de comunicación o los sistemas de aviones no tripulados (UAS) o vehículos aéreos tripulados para observación. Podemos citar los siguientes campos de aplicación que se benefician de las plataformas estratosféricas: observación de la Tierra, extensión de la conectividad de redes, gestión de catástrofes, defensa y seguridad, control marítimo, vigilancia de fronteras y espacios naturales, infraestructuras críticas, topografía y gestión del territorio, etc.

Por otro lado, el acceso a la estratosfera, siendo menos exigente energéticamente que el acceso a la órbita terrestre, tiene importantes desafíos para afrontar las bajas temperaturas, la alta radiación cósmica o la presencia de ozono que vuelven el entorno altamente agresivo. El despliegue de sistemas operativos requiere de desarrollos en aspectos tales como: inteligencia artificial y "machine learning", nuevos materiales, baterías y fuentes de energía solar, miniaturización e instrumentación, control de tráfico aéreo y regulación, modelos atmosféricos y de vientos muy precisos, polímeros y materiales de alta resistencia mecánica y barreras a la radiación, entre otros.

Iniciativas europeas y españolas

Las principales empresas involucradas en el desarrollo, construcción, despliegue u operación de plataformas estratosféricas, subsistemas o componentes se encuentran asociadas en la organización HAPS Alliance. Esta organización promueve el acceso a la estratosfera desde todos los ámbitos: científico y tecnológico, industrial o regulatorio. Predominan las empresas de EE.UU., si bien Europa está también ampliamente representada.

La Unión Europea, dentro de la Cooperación Estructurada Permanente (PESCO) en materia de Defensa, gestiona la línea "European High Atmosphere Airship Platfom". En este marco se ha puesto en marcha el denominado proyecto EuroHAPS, seleccionado dentro del Fondo Europeo de Defensa (EDF), cuya finalidad es el desarrollo de demostradores para mejorar las capacidades de inteligencia, vigilancia y reconocimiento (ISR). El proyecto desarrollará tres demostradores tecnológicos sobre plataformas más ligeras que el aire (LTA – "Lighter tan Air"). Estas plataformas serán: un dirigible estratégico, un dirigible híbrido y un sistema autónomo de globos estratosféricos. Embarcarán cuatro misiones ISR: LIDAR 3D, inteligencia de comunicaciones infrarrojas, inteligencia de señal y telecomunicaciones. Algunas de estas misiones nunca han sido desarrolladas en Europa. El consorcio del proyecto agrupa a varias empresas y está liderado por Thales. INTA, SENER, Thales España y pymes ostentan la representación española. Se ha seleccionado como uno de los lugares de pruebas la isla de Fuerteventura donde el Gobierno Autónomo Canario está invirtiendo en una infraestructura llamada Stratoport como base terrestre de operación de este tipo de plataformas.

3. CONCLUSIONES

España dispone de unas capacidades espaciales consolidadas en telecomunicaciones por satélite. No en vano, fue uno de los primeros países en dotarse de un sistema propio de comunicaciones por satélite específicamente para uso gubernamental. El uso intensivo del sistema y su evolución han conducido a que nuestro país disponga de una flota propia de satélites a través de HISDESAT y un modelo de participación público-privada.

En Observación de la Tierra nuestras FAS también disponen de capacidades propias gracias al satélite de radar de apertura sintética PAZ replicando el modelo de colaboración público privado de HISDESAT. También nuestro país hace un uso intensivo de capacidades compartidas con organismos internacionales a los que pertenece o directamente a través de acuerdos específicos con países aliados de nuestro entorno principalmente para las capacidades óticas.

En Navegación se está en la fase de despliegue de las capacidades PRS del sistema Europeo Galileo, donde España está entre los principales actores, tanto en el despliegue de las capacidades propias como en el soporte al sistema global albergando importantes infraestructuras.

También en una fase de despliegue están las capacidades de vigilancia espacial donde el Ejército del Aire y del Espacio ha creado un mando específico (Mando Espacial) y un centro de vigilancia espacial (COVE) muy alineado con los esfuerzos nacionales y europeos en la definición y despliegue de las capacidades SST.

La necesidad de consolidar las capacidades y avanzar en los despliegues requiere de un importante esfuerzo propio y de cooperación internacional, así como de una continua actividad innovadora y de prospectiva. El sector espacial es muy dinámico y en constate evolución. Hay multitud de iniciativas, tanto de instituciones como del sector privado con propuestas innovadoras y de tecnologías disruptivas. El procesado a bordo de satélites, las comunicaciones cuánticas, los servicios basados en constelaciones de satélites o el uso de la estratosfera, entre otros, plantean constantemente nuevos retos que hay que afrontar a través de una constante innovación y una necesaria cooperación internacional a nivel europeo y global.

REFERENCIAS

1. Montes Palacio, M. (2023). Historia del Programa Espacial Español. Ed. YO me publico

2. Dirección General de Armamento y Material (2015). Plan Director de Sistemas Espaciales.

3. Plataforma Aeroespacial Española (2010). Armonización de las Actividades del Sector Espacial Español en Comunicaciones y Cargas de Pago de RF para el Segmento Espacio

4. Gil, D., Claverie, A. et al (2017) Towards Disruptions in Earth Observation? New Earth Observation Systems and Markets Evolution. Acta Astronáutica 137.

5. HISDESAT S.A. (2023). Diversas publicaciones electrónicas y folletos comerciales. www.hisdesat.es

6. Boletín Oficial del Estado. Ministerio de Defensa. Orden DEF/264/2023 de 16 de marzo, por la que se desarrolla la organización básica del Ejército del Aire y del Espacio.

7. Planets Labs, Pbc. (2022). Planet Imagery Product Specification. www.planet.com.

8. Delgado Nevado, J., García Muñoz, L.E. (Tutor) (2021). Comunicaciones Cuánticas (Trabajo Fin de Grado). Universidad Carlos III de Madrid

9. Comisión Europea (2023). La iniciativa de Infraestructura de Comunicación Cuántica Europea (EuroQCI).

10. Comisión Europea. Comisariado de Industria de Defensa y Espacio. (2023). IRIS2: The New EU Secure Satellite Constellation. Infrastructure for Resilience, Interconnctivity and Security by Satellite.

11. Haps Alliance. (2022). Driving the Potential of the Stratpsphere.

12. Payload Aerospace, S.L. (PLD Space). (2023). Diversas publicaciones electrónicas y folletos comerciales. www.pldspace.com.

BIOGRAFÍAS

ISAAC DOMÍNGUEZ SANTOS

Director de Espacio y Centros Tecnológicos
ISDEFE.
Nacimiento: 1968 Grajal de Campos (León)

Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid (1992)

Desde 1993 ha desarrollado su carrera profesional en Ingeniería y Servicios Aeroespaciales, S.A. (INSA), actualmente Ingeniería de Sistemas para la Defensa de España, S.A. (ISDEFE) en temas relacionados con las comunicaciones, el espacio y la defensa. En la actualidad es director de Espacio y Centros Tecnológicos en ISDEFE.

Entre sus responsabilidades actuales está la gestión de la actividad de ISDEFE en el sector espacial para la Agencia Espacial Europea, el Instituto Nacional de Técnica Aeroespacial (INTA), y otras instituciones relacionadas con el espacio, así como la asistencia a los centros tecnológicos de la Defensa.

Colabora en distintos másteres y cursos de verano relacionados con las comunicaciones y el espacio y otras instituciones dedicadas a la divulgación. Ha sido distinguido con la Cruz al Mérito Aeronáutico.

CAPÍTULO 7

Capacidades del Ciberespacio

Benito Fernández García
Daniel Benavente López
Salvador Llopis

Este capítulo trata de poner en relevancia las capacidades de la UE en el ciberespacio, realizando un análisis sobre este nuevo dominio operativo reconocido tanto en UE como en OTAN. Para ello se profundiza en sus principales características diferenciadoras y amenazas asociadas, destacando su papel en las Operaciones Multidominio y sus potenciales efectos.

Por otra parte, se analiza la situación actual de la UE en relación a las políticas e iniciativas sobre ciberdefensa y ciberseguridad que se están llevando a cabo, resaltando los principales actores e instrumentos que tienen especial relevancia. Siguiendo esta línea, también se realiza una identificación y clasificación de las principales capacidades actuales de la UE en materia “Ciber”, junto con las tendencias a futuro, considerando primordial la continuación de su desarrollo y evolución.

1. CIBERESPACIO EN EL MULTIDOMINIO

1.1. ¿Qué es el Ciberespacio?

El ciberespacio ha cobrado una gran importancia en los últimos tiempos. Tanto los servicios prestados por la Administración como los productos desarrollados por la industria se apoyan en elementos digitales para poder ser empleados por la sociedad. Además, el ciberespacio interconecta no solo los propios procesos internos de cada organización, sino que también, de manera global, las diferentes entidades con los que se relaciona, viéndose involucrados por completo la sociedad en su conjunto: usuarios, empresas, gobierno, sectores, ciudadanos, etc., y de ahí la creciente importancia que está tomando dentro de la UE, tanto la protección como el adecuado desarrollo y evolución del ciberespacio.

Generalmente se concibe el espacio como un conjunto de redes y elementos digitales interconectados o relacionados (sin necesidad de estar conectados físicamente) entre sí en el que se genera, maneja o transforma información (en ocasiones crítica y relevante) sobre la base de unos procesos de Tecnologías de la Información y las Comunicaciones (TIC) propios de los Sistemas de Información. No obstante, cada organización dentro del ámbito de su competencia y responsabilidad matiza esta idea general añadiendo y ampliando la definición para que se ajuste mejor y sea más precisa a su propio contexto.

Desde un punto de vista militar, el ciberespacio ha sido declarado un dominio operativo, al igual que los dominios terrestre, marítimo, aéreo y espacial. La OTAN lo define como "el dominio global compuesto por todos los sistemas interconectados de comunicación, tecnología de la información y otros sistemas electrónicos, redes y sus datos, incluidos los que están separados o son independientes, que procesan, almacenan o transmiten datos". A nivel nacional, en el Concepto de Ciberdefensa del JEMAD (2018), se define el ciberespacio como un entorno global y dinámico, en constante evolución y lleno de amenazas, que pueden afectar no solo a los sistemas del Ministerio de Defensa, sino también a las infraestructuras críticas de España. En el ámbito de la UE, también se categoriza el ciberespacio como un dominio operativo, donde las misiones y las operaciones militares de la UE son cada vez más dependientes de un acceso ininterrumpido seguro que requiere capacidades robustas y resilientes. La visión militar y estrategia del ciberespacio como dominio de las operaciones adoptada en 2021 establece las condiciones marco y describe los fines, formas y medios necesarios para la utilización del ciberespacio como un dominio de las operaciones en apoyo a la Política Común de Seguridad y Defensa (PCSD) de la UE.

Establecer las fronteras virtuales para limitar el campo de acción y el área de interés de una organización en el ciberespacio es un desafío, así como evaluar los efectos en cadena dentro del mismo. Este hecho es clave cuando las acciones tienen un componente militar o se enmarcan en una Operación. Debe establecerse una definición inequívoca del ciberespacio de interés en cuestión.

1.2. Amenazas en el Ciberespacio como Dominio Operativo

Actualmente, en la UE se reconocen cinco dominios operativos: tierra, mar, aire, espacio y ciberespacio. En 2016, en la Cumbre de Varsovia, la OTAN también reconoció el ciberespacio como un nuevo dominio de operaciones, al igual que la UE había hecho en su marco de política de ciberdefensa del año 2014. Particularmente en España también se ha reconocido, existiendo una unidad militar con competencias en este campo denominada Mando Conjunto del Ciberespacio.

Una de las características más diferenciadoras, frente al resto de dominios operativos, es que el ciberespacio comprende un ámbito creado íntegramente por la humanidad. Las reglas que lo rigen lo convierten en un dominio diferente, complejo para ejecutar operaciones en él y donde existen nuevos factores a incluir en el planeamiento y ejecución de una Operación. Podemos citar a modo ilustrativo como factores diferenciadores frente a otros dominios: la gran velocidad en la materialización de las acciones (milisegundos), el menor control sobre alcances indeseados por efectos cadena, la complejidad en la detección, la amplia gama de vulnerabilidades y vectores de ataque potenciales, el poco coste de acceso a herramientas de alto impacto por parte de adversarios, caducidad en la efectividad de las medidas de protección, la falta de supervisión y regulación sobre capacidades del adversario, la dificultad en la atribución, el marco legal heterogéneo y en muchos casos difuso, etc.

El ciberespacio es un dominio donde existe una gran asimetría entre el defensor y el atacante, ya que este último puede producir altos impactos con recursos limitados.

Es decir, el coste de desarrollar la capacidad para producir ataques significativos es muy inferior al coste de desarrollar la capacidad de defender el ciberespacio propio. Esto se debe a que el atacante sólo tiene que encontrar y explotar una vulnerabilidad, mientras que el defensor tiene que proteger y controlar una inmensa superficie de exposición conformada por elementos digitales cada vez más interconectados y expuestos, los cuales tienen numerosas vulnerabilidades, tanto derivadas del propio proceso de fabricación de elementos, como de la propia configuración y mantenimiento de éstos, que debe realizarse por personal especializado el cual, hoy en día, es escaso.

Este contexto es el caldo de cultivo ideal para que florezcan grupos que actúen por interés propio atacando a organizaciones legítimas. La diversidad de estos grupos que, o bien usan el ciberespacio como camino para producir efectos en el mundo real o bien atacan los propios activos digitales, es muy amplia. Dependiendo de su capacidad, interés y objetivos se clasifican en varias categorías que se detallan a continuación.

Los más peligrosos son los actores que actúan como grupos “esponsorizados” por gobiernos o directamente con vínculos a gobiernos. Éstos disponen de unidades o grupos altamente especializados en distintas disciplinas que se centran en la obtención y análisis de información de otros gobiernos, así como en la ejecución de ciberataques capaces de afectar a servicios esenciales de naciones adversarias. Estos ataques pueden centrarse en los sistemas militares, pero también en las infraestructuras críticas de un país, que pueden desestabilizar el clima social o incluso crear terror al afectar a infraestructuras como la electricidad, el agua, los hospitales, las comunicaciones, entre otras.

Además de los grupos “esponsorizados”, existen también grupos organizados criminales independientes que actúan impulsados por sus propios intereses, en muchos casos económicos. Estos grupos pueden, en ocasiones, colaborar con naciones para ayudarles a alcanzar sus objetivos. También pueden actuar como mercenarios y ofrecer sus servicios al mejor postor, destacando el espionaje industrial como una de sus actividades más lucrativas, donde su objetivo es robar secretos y patentes valiosas. Un ejemplo reciente de este tipo de actividades se dio durante la pandemia del COVID19, con un incremento de ataques a la industria farmacéutica.

Otras categorías de grupos en el ciberespacio son aquellos con capacidades más limitadas, enfocados en llevar a cabo acciones ilícitas menos complejas, como extorsiones, chantajes, sustracción de datos, suplantación de identidades personales, obtención de información privilegiada y robo de activos digitales, entre otros.

En el ámbito del terrorismo, también encontramos actores peligrosos que buscan causar daño específico, no solo en el ciberespacio sino también con consecuencias físicas, relacionadas con un mensaje e ideología concretos. Utilizan el ciberespacio y ciberataques como vehículos para lograr sus objetivos, incluyendo labores de propaganda, captación y radicalización, así como recaudación de fondos. Cerca de estos grupos se encuentran las guerrillas o milicias que, sin representar una nación, aspiran a controlar un estado y pueden llevar a cabo acciones ofensivas de diversas índoles.

La organización americana MITRE ha hecho un gran esfuerzo por identificar, analizar, centralizar y compartir información de los diferentes grupos , convirtiéndose en una referencia global para su identificación y referencia. Además, detallan las técnicas, tácticas y procedimientos que dichos grupos utilizan basándose en el modelo MITRE ATT&CK , convertido en estándar de facto de la industria de ciberseguridad.

En otro frente, nos encontramos con el hacktivismo, una rama del activismo social radical que lleva a cabo sus acciones en el ciberespacio. Su principal objetivo es propagar mensajes de manera ilegítima en medios digitales, incitando a través de redes sociales a cometer actos de desórdenes sociales o delictivos, e incluso organizando ataques de denegación de servicio contra servicios en línea. Este tipo de amenaza representa un riesgo importante para la imagen de gobiernos y organizaciones, y se ha establecido como un desafío que debe ser abordado con seriedad.

Por último, no debemos subestimar a los llamados insiders, es decir, personal que pertenece a las propias organizaciones y que puede causar daño desde dentro. Estos actores pueden actuar motivados por diferentes razones, como el descontento, el soborno, el chantaje o la búsqueda de notoriedad. En ciertos ámbitos, su impacto puede ser significativo, sirvan de ejemplo los casos ocurridos en el gobierno americano con personal militar que ha publicado información clasificada.

A continuación, y a modo ilustrativo, se relacionan las diferentes categorías de amenazas, objetivos perseguidos, impactos y sus contramedidas como apoyo a la mayor comprensión del lector:

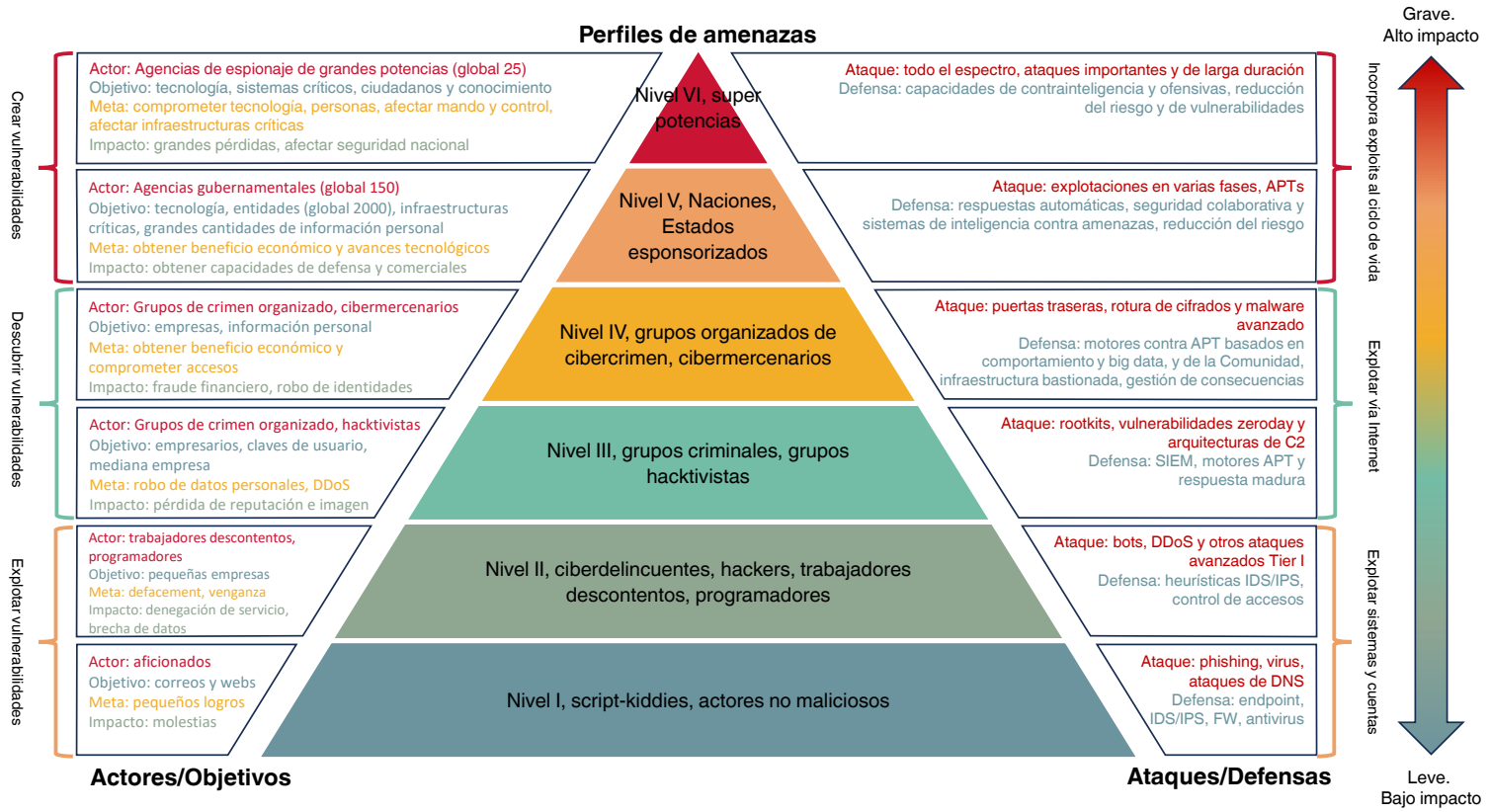


Figura 1 – Categorización de amenazas en el ciberespacio.
FUENTE: Sinitsin, O. (s.f.). The Pyramid of Pain in the SolarWinds Cyber Attack. Dynamite Analytics. https://dynamite.ai/pyramid-pain-solarwinds-cyber-attack/

La UE, a través de sus diferentes entidades y organizaciones, implementa iniciativas para contrarrestar la amenaza en todos sus niveles. Para otras amenazas, entidades como la Europol disponen de competencias en la lucha contra el cibercrimen. Además, la UE cuenta con una amplia variedad de agencias e instituciones que ofrecen líneas de acción más transversales, capaces de abordar amenazas de diversa naturaleza de menor impacto. Un ejemplo de ello puede verse en agencias como ENISA, en el que su trabajo para fomentar la fabricación y empleo de productos TIC más robustos y con menos vulnerabilidades disminuye las posibilidades de éxito de los grupos atacantes. A lo largo del capítulo, se profundizará en el ecosistema europeo y las líneas de acción más relevantes en este campo de la ciberseguridad y ciberdefensa.

1.3. Papel del Ciberespacio en el Multidominio y Zona Gris. Efectos

Hemos visto en apartados anteriores cómo el ciberespacio es un ámbito más donde se desarrollan las Operaciones; no obstante, tiene otra peculiaridad importante que es su transversalidad (junto con el cognitivo) con el resto de los ámbitos (tierra, mar, aeroespacial). Dicha transversalidad implica que los potenciales efectos de acciones maliciosas que se reproduzcan en él podrían afectar o amplificarse en el resto de los dominios. En el ciberespacio, no solamente se aloja la información y los datos relativos a la ciberseguridad, sino también servicios TIC en los que se apoyan diferentes capacidades militares como, por ejemplo, los Sistemas de Mando y Control Militar. Éstos poseen información relevante para cualquiera de las acciones que se llevan a cabo en cualquier dominio y, si ésta es comprometida o manipulada, las consecuencias podrían afectar directamente al éxito de la operación.

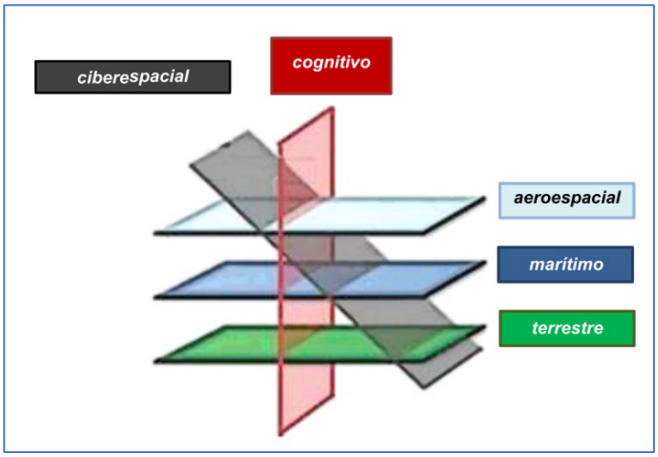


Figura 2 – Ámbitos de la operación
FUENTE: Centro Conjunto de Desarrollo de Conceptos (2018). PDC-01 (A) Doctrina para el empleo de las FAS. Ministerio de Defensa de España.

En la actualidad, las amenazas están evolucionando y volviéndose más complejas y sofisticadas. Diferentes países, incluyendo España, así como organizaciones como la OTAN y la UE, están trabajando en el desarrollo del concepto de Operaciones Multidominio. Este enfoque se caracteriza por la complejidad del entorno operativo tecnológico, globalizado y cambiante, que exige una respuesta ágil y veloz frente al oponente. La conectividad también es crucial para llevar a cabo este tipo de enfrentamientos.

El espectro de los conflictos se extiende desde situaciones de paz hasta el combate de alta intensidad, pasando por una zona intermedia, conocida como Zona Gris. A nivel nacional se define como "la zona del espectro de los conflictos donde predominan las actuaciones situadas al margen del principio de buena fe entre estados que pese a alterar notablemente la paz no cruzan los umbrales que permitirían o exigirían una respuesta armada. En esta zona se emplean acciones híbridas, mezclando simultáneamente medios convencionales y no convencionales, y en la que intervienen actores estatales y no estatales, cuyos intereses no son siempre evidentes".

A menudo, existen acciones en el ciberespacio que se ejecutan como alternativa a otros medios más letales o simplemente por ser nuevas oportunidades de generar crisis a Estados por debajo del umbral de un conflicto militar, pero con efectos significativos a nivel estado y con repercusión a nivel UE. Algunos ejemplos son las intervenciones en la opinión con falsos bulos o deep-fakes en procesos electorales o ciberataques a instituciones claves durante una pandemia.

Por tanto, el papel de las operaciones en el ciberespacio es importante tanto en las Operaciones Multidominio como en las acciones ejecutadas en la Zona Gris. Es decir, las actividades maliciosas en este dominio se pueden dar en todo el espectro de los conflictos, desed tiempo de paz a guerra.

Figura 3 – Espectro de los conflictos
FUENTE: Centro Conjunto de Desarrollo de Conceptos (2018). PDC-01 (A) Doctrina para el empleo de las FAS. Ministerio de Defensa de España.

Actualmente en la guerra entre Rusia y Ucrania se ha podido observar el uso del ciberespacio en todo el espectro. En las fases iniciales principalmente se observaron acciones en la citada Zona Gris, y en fases posteriores se han observado acciones de operaciones en todos los ámbitos.

Dada la numerosa información existente sobre la guerra entre Rusia y Ucrania en fuentes abiertas y siendo tan ilustrativo para el objetivo perseguido en este apartado, se exponen a continuación algunos hechos documentados que explican efectos conseguidos al operar en el ciberespacio.

1.3.1. Efectos en el Ciberespacio en el Conflicto entre Rusia y Ucrania

Desde el inicio de la guerra, se han materializado ciberataques de distinto tipo y efecto, pero no es algo nuevo ni han sido exclusivos de este conflicto. Por ejemplo, desde antes de 2014, año del conflicto de Crimea y Dombás, ya se pudieron identificar ciberataques dentro de la Zona Gris que causaron efectos en infraestructuras críticas de sectores relacionados con la energía o las comunicaciones, que posteriormente continuaron en el tiempo.

Sin embargo, a partir del 24 de febrero de 2022 cuando la guerra se inició, se observa cómo se empiezan a intensificar los ciberataques contra Ucrania de forma alarmante,

destacando tanto el ataque a Viasat para interrumpir las comunicaciones vía satélite como los enfocados de nuevo en las infraestructuras críticas para dejar al país sin los servicios clave. Se deduce, por tanto, que los ciberataques se han utilizado de forma activa y constante como un arma más.

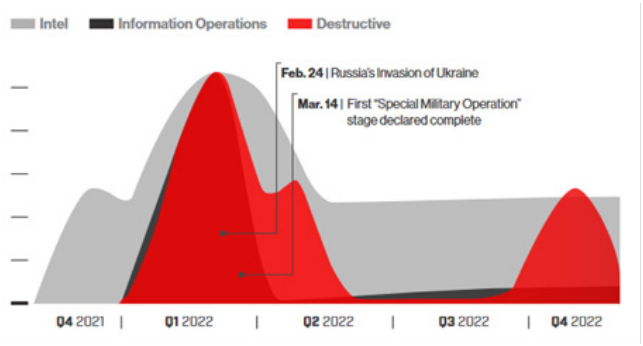


Figura 4 –Actividad operativa de Rusia contra Ucrania en 2022
FUENTE: Crowdstrike (2023). 2023 Crowdstrike Global Threat Report. https://www.crowdstrike.com/resources/reports/crowdstrike-2023-global-threat-report/

Otro punto relevante que se ha podido identificar es la coordinación entre los ciberataques y los ataques en el resto de los ámbitos. Por ejemplo, un hecho destacable es que, tras lanzar varios ciberataques a ciertas infraestructuras, posteriormente se han realizado bombardeos en ellas, lo cual lleva a deducir que existe una relación directa y coordinada entre ambos tipos de acción ofensiva, con el objetivo de causar mayores impactos. Sin embargo, esta forma de actuar tampoco es nueva, y ya se identificó en 2008 en el conflicto de Georgia.

Con relación a los actores que ejecutan estos ciberataques, a pesar de que su atribución suele ser compleja, se puede atisbar que, además de los grupos "esponsorizados", detrás de su ejecución se encuentran grupos APT (Advanced Persistent Threat) específicos. Se trata de equipos totalmente organizados con elevadas capacidades y cualificación, dedicados a perpetrar el ciberataque en todas sus fases.

Por el contrario, no solamente los propios grupos con posibles vínculos a gobiernos han realizado estas acciones. Existen actores que han sido muy relevantes, los hacktivistas que, llamados o animados incluso por los propios gobiernos, han participado en apoyo de ambos bandos, estimándose en más de 200 grupos en total involucrados. En esta línea, un punto destacable es la creación del IT Army de Ucrania, cuyo gobierno realiza un llamamiento internacional para apoyo en el ciberespacio, obteniendo una respuesta masiva que llegó a ser de hasta 300.000 personas, coordinadas a través de distintas redes sociales.

Otro tipo de acciones a tener en cuenta han sido las relativas a la obtención de información de fuentes abiertas u OSINT (Open Source Intelligence), así como las operaciones de influencia a través del ciberespacio, especialmente en redes sociales, que han jugado un papel muy relevante para influir en la perspectiva de la población de los distintos países sobre el conflicto y lo que estaba ocurriendo en él.

Las capacidades de ataque e inteligencia en el ciberespacio han jugado un papel relevante, pero también se ha dado importancia a la defensa. Ucrania ha tomado acciones clave para resistir de manera eficiente los ciberataques, gracias a la preparación previa en todos los sectores y la cooperación entre el ámbito civil y militar, basándose en lecciones aprendidas de conflictos anteriores. La protección de sistemas y la capacidad de reacción conjunta, junto con la necesaria flexibilidad en cada caso, han sido determinantes.

Esto ha permitido mitigar los efectos de las ciberamenazas y degradar las capacidades del adversario para operar en el ciberespacio. La defensa y la seguridad de las redes y servicios esenciales han sido fundamentales en este conflicto, así como una coordinación bien definida entre todos los actores implicados en la realización de operaciones en el ciberespacio.

Un punto relevante que destacar es cómo ha cobrado importancia el uso de la tecnología civil en refuerzo de las operaciones militares. La telefonía móvil y el acceso a Internet han sido activos fundamentales bajo control y mantenimiento, con preparación previa y el uso de telecomunicaciones y servicios complementarios a través de constelaciones satelitales de baja órbita u otras. Otro punto a subrayar ha sido la migración de tecnología local a la nube de grandes proveedores, evitando la pérdida de información ante ataques.

Todo esto forma parte de la "guerra hibrida" en la que se utilizan toda clase de medios y procedimientos, como la fuerza convencional, la insurgencia, el terrorismo, la migración, los recursos naturales e incluso otros más sofisticados aprovechando el empleo de las últimas tecnologías, donde el gran protagonista son las operaciones en el ciberespacio.

En consecuencia, la defensa permanente del ciberespacio es una exigencia y requiere del fomento y desarrollo de unas capacidades en ciberseguridad y ciberdefensa.

Conjugar adecuadamente política, inversión y legislación es clave para controlar y gestionar los riesgos en el ciberespacio.

Aunque el adversario se beneficie de no seguir reglas ni leyes, los Gobiernos, particularmente la UE, pueden y deben aprovechar la "unidad de acción" para obtener su ventaja.

1.3.2. Ciberseguridad y Ciberdefensa. Tipos de Operaciones en el Ciberespacio

El ciberespacio se explota cada vez más con fines políticos e ideológicos. Las amenazas híbridas combinan campañas de desinformación con ciberataques dirigidos a la infraestructura, procesos económicos e instituciones democráticas. Estas acciones pueden causar daños físicos, acceder ilegalmente a datos personales, robar secretos industriales o de Estado, sembrar la desconfianza y debilitar la cohesión social. Todas estas actividades erosionan la confianza de los ciudadanos en sus instituciones y gobiernos y pueden ralentizar el adecuado desarrollo de la sociedad europea.

Los productos digitales se lanzan al mercado con vulnerabilidades, lo que aumenta aún más la superficie de ataque. La industria y empresas de diferentes sectores de la UE están cada vez más digitalizadas y conectadas a través de Internet, llegando a conectar cada vez más infraestructuras críticas que tradicionalmente estaban aisladas. Entre estas últimas se encuentran las plataformas militares y los sistemas de armas.

Los términos de ciberseguridad y ciberdefensa se utilizan generalmente para referirse a la misma idea, y se aplican al mundo civil y militar respectivamente. Ambos términos tienen conceptualmente muchas similitudes al compartir productos, habilidades, técnicas, formación, infraestructuras TIC, etc., diferenciándose en la finalidad, alcance y ámbito de empleo.

La ciberseguridad tiene como finalidad proteger los Sistemas TIC propios, dotándoles de resiliencia y capacidad de recuperación ante desastres e incidentes garantizando unos servicios usables y confiables. Cuando nos referimos a ciberdefensa se introduce la idea de producir efectos en un adversario de tal manera que neutralice su acción o potencial acción sobre los sistemas propios. Por esta razón, el ciberespacio involucrado en la ciberdefensa se extiende no solo a elementos propios, sino que abarca elementos de terceros o incluso del adversario y se le denomina en términos militares área de interés y área operativa. Para los objetivos que persigue este cuaderno, ambos términos se usarán indistintamente sin entrar en su finalidad diferente. A nivel nacional existe un documento publicado por el Ministerio de Defensa para el lector que requiera más detalle sobre la definición de estos conceptos.

Las actividades para protegernos en el ciberespacio se dividen en cuatro grupos fundamentales. El primero son las "acciones de soporte", que habilitan nuestros Sistemas de Información para poder gestionar las crisis e incidentes de ciberseguridad. En segundo lugar, se encuentran las "acciones de Defensa", destinadas a proteger nuestros activos digitales y detectar actividad maliciosa. El siguiente grupo son las "acciones de Inteligencia, Vigilancia y Reconocimiento", que obtienen información relevante para neutralizar las potenciales amenazas. Por último, tenemos las "acciones de Ataque", como aquéllas destinadas a contrarrestar las acciones del adversario mediante la destrucción, disrupción, degradación del ciberespacio del adversario. La doctrina española está alineada con la doctrina de la OTAN y, para poder profundizar en estos temas, existe la publicación AJP 3-20 "Allied Joint Doctrine for Cyberspace Operations". Los esfuerzos de la UE en el ámbito militar (ciberdefensa) se centran en fomentar y potenciar las capacidades de los Estados miembros, proponiendo actividades de colaboración conjunta. En el ámbito civil (ciberseguridad) la UE y en especial la Comisión Europea está siendo muy activa, generando normas y regulaciones que deben aplicarse o transponerse en cada Estado miembro.

Con el panorama de amenazas descrito en apartados anteriores y dado el contexto geopolítico actual tan complicado y tensionado en torno al uso del ciberespacio, se observa un creciente número de países que están estableciendo "fronteras digitales" en cuanto al acceso a tecnología relevante o en la aceptación de una determinada regulación. El camino y el modo para establecer dichas fronteras pueden impactar en derechos fundamentales como la libertad y la democracia, que son los valores fundamentales de la UE. Ésta, como elemento unificador, tiene por delante un trabajo descomunal para armonizar, crear y potenciar unas capacidades comunes relativas a ciberseguridad y ciberdefensa, sin menoscabar la soberanía de sus miembros. En los últimos tiempos la UE ha creado un ecosistema en donde numerosas entidades trabajan persiguiendo un fin común. En el próximo apartado lo veremos en más detalle.

2. SITUACIÓN ACTUAL EN LA UNIÓN EUROPEA: INICIATIVAS DE CIBERDEFENSA Y CIBERSEGURIDAD

2.1. Principales Entidades Europeas Involucradas

Europa aspira a capacitar a las empresas y a las personas para un futuro digital sostenible, más próspero y centrado en el ser humano. Para ello, ha creado una hoja de ruta en la que se marcan unos objetivos para el 2030. Esta hoja de ruta se

conoce como “Europe’s Digital Decade” y sirve de “brújula digital” hacia donde orientar esfuerzos. Básicamente, se apoya en cuatro pilares: primero, la digitalización de los servicios públicos para mejorar su eficiencia y accesibilidad; segundo, la transformación digital de las empresas, impulsando la innovación y la competitividad en el mercado europeo; tercero, el desarrollo de infraestructuras TIC seguras y de vanguardia para fortalecer nuestra posición en el ciberespacio; por último, pero no menos importante, potenciar la capacitación de los ciudadanos europeos, tanto en su rol de usuarios como en el ámbito profesional. Esta aspiración traerá múltiples beneficios, pero sin duda este aumento y potenciación del ciberespacio europeo está muy presente en la consecución de los fines de la Agenda Digital Europea. Así, se entiende el protagonismo de proteger el espacio digital mediante una capacidad de ciberseguridad que evolucione al ritmo de estos nuevos cambios tecnológicos para que sea eficaz.

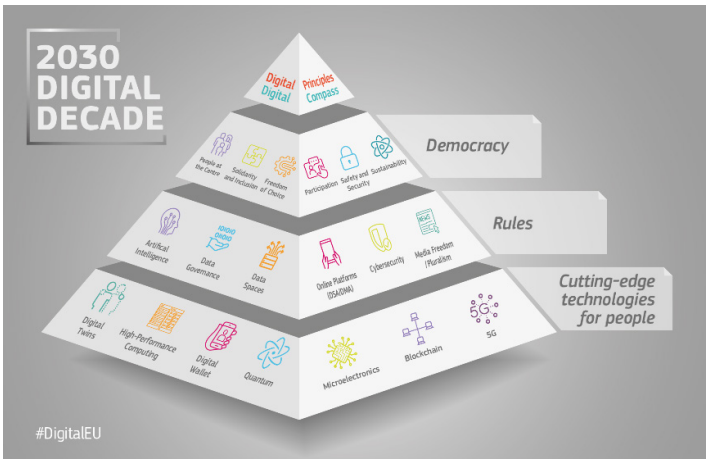


Figura 5 – Brújula digital para el 2030 en UE
FUENTE: European Commision (s.f.). Europe’s Digital Decade. Unión Europea. https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade

Para todo ello, se han ido creando una serie de organismos y entidades europeas a las que se les han ido asignando funciones y competencias, que conforman ya los cimientos para cumplir con los objetivos previstos. Se identifican a continuación las principales entidades con una breve descripción de sus funciones y cometidos. La colaboración e intercambio de información entre las entidades principales se realiza de manera regular.

- **ENISA.** Creada en 2004. La Agencia de la Unión Europea para la Ciberseguridad (ENISA) contribuye a la política de seguridad de la información de la UE, mejora la fiabilidad de los productos, servicios y procesos de TIC mediante programas de certificación, coopera con los Estados miembros y con los organismos de la UE y ayuda a Europa a prepararse para los desafíos futuros en esta materia. Mediante el intercambio de conocimientos, la creación de capacidades y la sensibilización, la Agencia coopera con las principales partes interesadas en fortalecer la confianza en la economía conectada, impulsar la resiliencia de las infraestructuras de la Unión y, por último, proteger a la sociedad y a la ciudadanía europea de las amenazas digitales. La UE, con el mandato “Cybersecurity Act”, ha reforzado su papel renombrándola como la Agencia de la UE para la ciberseguridad aunque manteniendo sus siglas originales.

- **CERT-EU.** Se creó en 2011. El CERT-EU está formado por un equipo de expertos en seguridad informática. Como todo Equipo de Respuesta ante Emergencias Informáticas (CERT son sus siglas en inglés) se encarga de recopilar, gestionar, analizar y compartir información con las instituciones, los órganos y las agencias de la UE sobre amenazas, vulnerabilidades e incidentes relacionados con infraestructuras TIC no clasificadas. También coordina las respuestas a incidentes dentro de su comunidad, constituida por más de 80 entidades relacionadas o integradas en el ecosistema de la UE incluyendo instituciones y agencias europeas, proporcionando servicios especializados como análisis forense digital, primera respuesta ante incidentes, ciberinteligencia y asesoramiento técnico. Pertenece a diversos foros internacionales como FIRST, EGC y Trusted Introducer para relacionarse con otros CERTs/CSIRTs, y además se destacan los acuerdos existentes tanto con OTAN desde el 2016 con el suyo propio, denominado NCIRC, para compartir información técnica como con ENISA.

- **EUROPOL.** Desde 2010 es agencia oficial de la UE, con sede en La Haya (Países Bajos). Tiene la misión de asistir a los Estados miembros en la prevención y la lucha contra toda forma grave y organizada de delincuencia, ciberdelincuencia y terrorismo a escala internacional. Europol colabora asimismo con numerosos Estados asociados no pertenecientes a la UE y organizaciones internacionales. Dispone de una dirección operativa específica para combatir el cibercrimen denominada EC3 (European Cyber Crime Center), en el que entre otros servicios se destacan los relacionados con el forense informático y productos de ciberinteligencia que comparten con CERTs/CSIRTs y entidades con las que tienen acuerdos.

- **ECCC.** El Centro Europeo de Competencia en Ciberseguridad (ECCC) que, junto a la Red de Centros de Coordinación Nacionales, es el nuevo sistema europeo para el apoyo a la innovación y a la política industrial en materia de ciberseguridad. El centro inaugurado en 2023 en Bucarest (Rumania), desarrollará e implementará una agenda común para el desarrollo

tecnológico junto a los Estados miembros, la industria y la comunidad tecnológica. El Centro y la Red tomarán decisiones estratégicas de inversión y reunirán recursos de la UE, los Estados miembros y, de manera indirecta, de la industria para mejorar y fortalecer la capacitación tecnológica e industrial en esta materia. El Centro tendrá un papel destacado en el cumplimiento de los objetivos de ciberseguridad de los programas Europa Digital y Horizonte Europa.

- **Comisión Europea:** Elabora e implanta las políticas de la UE en materia de ciberseguridad y sociedad digital principalmente a través de la Dirección General de Redes de Comunicación, Contenido y Tecnologías (CONNECT) y la Dirección General de Industria de Defensa y Espacio (DEFIS) que dirige las actividades de la Comisión Europea en esos ámbitos y entre otras actividades, se encarga de mantener la competitividad y la innovación de la industria europea de defensa garantizando la evolución de una base tecnológica e industrial de la defensa europea. DEFIS gestiona el Fondo Europeo de Defensa establecido durante el periodo 2021-2027 y publica anualmente un programa de trabajo que incluye ciberdefensa como una categoría destacada de las acciones.

- **Servicio Europeo de Acción Exterior (SEAE):** Es el servicio diplomático de la UE y se encarga de la política exterior de la Unión. El Estado Mayor de la Unión Europea (EUMS) bajo la autoridad del Comité Militar de la Unión Europea (EUMC) realiza, entre otras funciones, el asesoramiento de las misiones y operaciones militares de la Política Común de Seguridad y Defensa.

La Figura 6 describe las relaciones de los actores principales en la UE con distintas responsabilidades. A este respecto cabe mencionar que existe un memorándum de entendimiento para la cooperación entre la EDA, ENISA, CERT-EU y el EC3 de Europol. Además, la EDA actúa de interfaz en materia de Defensa con la Comisión Europea, manteniendo estrechos lazos con el EUMS, en relación con las políticas europeas de ciberseguridad y otras iniciativas.

La cantidad y profundidad de todas estas iniciativas demuestran el gran esfuerzo que está poniendo la UE en sentar unos sólidos cimientos para el proceso de transformación digital en la que está inmersa para la presente década. Una vez realizada la normativa es momento para la implementación en los próximos años. A continuación, se describen brevemente las políticas más destacadas en ciberseguridad y ciberdefensa:

- La Estrategia de Ciberseguridad de la UE, presentada el 16 de diciembre de 2020, bajo el nombre The EU's Cybersecurity Strategy for the Digital Decade, sienta las bases para reforzar la resiliencia colectiva europea contra las ciberamenazas y garantizar que ciudadanos y empresas puedan beneficiarse plenamente de unos servicios y herramientas digitales fiables y de confianza, tanto del sector público como del privado. Se pone especial énfasis en los operadores de infraestructuras críticas como la banca, sanidad, transporte y energía. Esta estrategia refuerza el liderazgo de la UE en el campo del ciberespacio, ya que da pie a desarrollar

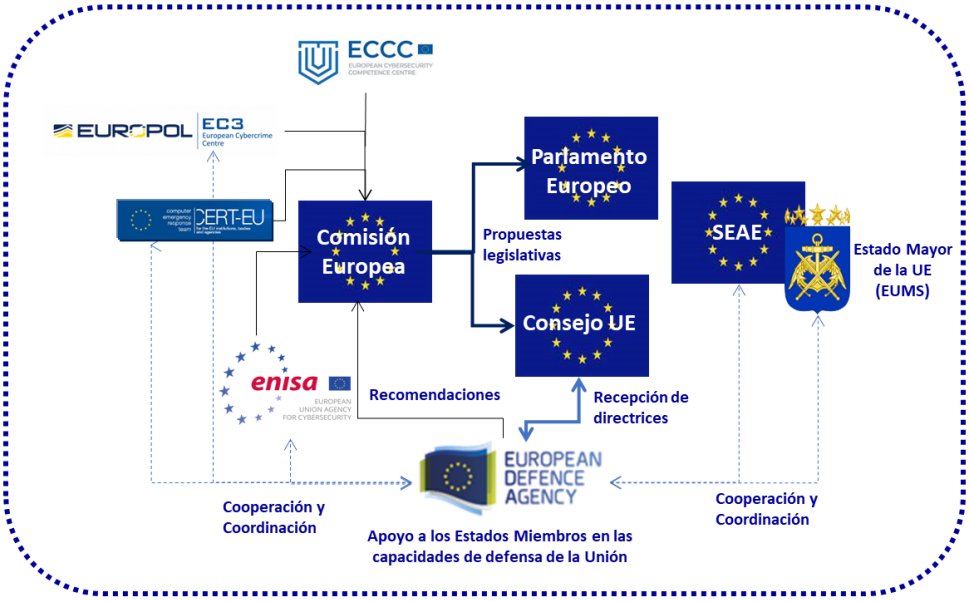


Figura 6 – Identificación de actores en la UE con indicación de sus relaciones - FUENTE PROPIA

normas, acuerdos y proyectos innovadores que pongan a la UE a la vanguardia y le doten de suficiente soberanía en el ámbito tecnológico. Dicha soberanía o autonomía estratégica podría entenderse como la necesaria reducción de dependencias exteriores que aseguren la disponibilidad tecnológica europea propia. Dicha estrategia consta de tres ámbitos de acción:

1. Resiliencia, soberanía tecnológica y liderazgo.
2. Desarrollo de capacidades operativas en relación con la prevención, disuasión y respuesta ante ciberamenazas.
3. Cooperación para impulsar un ciberespacio global y abierto.

- El Marco Político Europeo sobre Ciberdefensa, desarrollado en 2014 y actualizado en 2018, denominado "EU Cyber Defence Policy Framework" (CDPF), surge como respuesta a la declaración del ciberespacio como ámbito de las operaciones. Su objetivo fue identificar, conjugar y enmarcar los aspectos que tuvieran relación con la ciberdefensa brindando apoyo a la ejecución de la Política Común de Seguridad y Defensa en el ámbito del ciberespacio.

  Este documento identifica las áreas prioritarias de actuación en ciberdefensa, definiendo los principales actores involucrados y sus funciones, respetando las responsabilidades y competencias respectivas de cada uno de los Estados miembros, así como el marco institucional de la UE y su autonomía en la toma de decisiones. Las seis áreas prioritarias identificadas son:

  1. Apoyar el desarrollo de capacidades de ciberdefensa en cada uno de los Estados miembros y actuar juntos a través de la coordinación y cooperación.
  2. Potenciar la seguridad y protección de los Sistemas de Telecomunicaciones e Información (CIS) utilizados por la UE para llevar a cabo la PCSD.
  3. Promover la cooperación entre entidades civiles y militares.
  4. Desarrollar y aumentar la inversión en I+D para disminuir la dependencia tecnológica.
  5. Mejorar la formación, adiestramiento y capacitación a través de ejercicios.
  6. Ampliar y fortalecer las relaciones y acuerdos con terceros.

A pesar de que el Marco Político no se encuentra en vigor, los autores han decidido incluir un breve resumen para resaltar que la ciberdefensa ha tenido su marco propio desde 2014 como resultado de la publicación de la primera Estrategia Europea de Ciberseguridad del 2013.

- La Comunicación Conjunta de la Comisión Europea sobre la Política Europea de Ciberdefensa, emitida el 10 de noviembre de 2022, bajo el título EU Policy on Cyber Defence, representa una declaración de intenciones acerca de la postura europea en materia de ciberdefensa. Esta política se fundamenta en los avances y consideraciones reflejadas en publicaciones como la Estrategia de Ciberseguridad de la UE, la Brújula Estratégica para la Seguridad y Defensa (Strategic Compass for Security and Defence), la revisión de prioridades y las conclusiones identificadas y expresadas en diversas publicaciones posteriores al 2018 acerca de la postura en ciberseguridad de la UE y su abanico de respuestas ante ciberataques.

  Con el fin de mejorar la capacidad de prevenir, detectar, defender, recuperarse y disuadir los ciberataques dirigidos contra la UE y sus Estados miembros, esta política establece las siguientes líneas de acción:

  1. Actuar juntos para fortalecer las capacidades de ciberdefensa.
  2. Robustecer y proteger el ecosistema tecnológico existente dentro de la UE.
  3. Invertir en desarrollar capacidades de ciberdefensa.
  4. Asociarse para abordar retos comunes.

Se observa que existe un común denominador en los documentos referenciados que actúa como hilo conductor entre ambos a lo largo del tiempo. Este común denominador se sustenta en la cooperación y colaboración de los diferentes actores, el aumento de la inversión en investigación y desarrollo, y potenciar la protección de las redes existentes.

2.2. Situación Actual a Nivel Estratégico en Ciberseguridad y Ciberdefensa dentro la Unión Europea

Tomaremos como referencia para el análisis dos de las iniciativas más importantes en el área de capacidad de los Estados miembros. La primera de ellas es la Cooperación Estructurada Permanente (PESCO) mientras que la segunda será el Fondo Europeo de Defensa (EDF) y su programa

precursor EDIDP (Programa de Desarrollo Industrial de la Defensa Europea), para dar constancia de todos los proyectos y actividades que se están llevando a cabo actualmente. Ambas contribuyen a dar una visión más general de los retos tecnológicos y grandes áreas que se están abordando tanto por los gobiernos como por la Industria. Estas iniciativas se sirven de la Estrategia de Ciberseguridad de la UE y de la Política de Ciberdefensa de la UE como elementos que refuerzan y acompañan la implementación durante estos próximos años con el fin de contrarrestar las potenciales ciberamenazas y atender a los desafíos.

2.2.1. La Cooperación Estructurada Permanente en Defensa (Pesco)

La Cooperación Estructurada Permanente en defensa es un mecanismo por el cual los Estados miembros declaran su interés en cooperar en áreas de interés estratégico en defensa, siendo la ciberdefensa uno de ellos. La EDA y el SEAE/EUMS conforman la secretaría de PESCO con los cometidos de consolidar y asesorar las propuestas de proyectos desde la perspectiva de capacidad y de la operativa, realizar el asesoramiento anual de cumplimento de los compromisos PESCO por parte de los Estados miembros, apoyar la implementación de los proyectos mediante solicitud y asegurar de que no existe una duplicación innecesaria de esfuerzos con otras iniciativas similares.

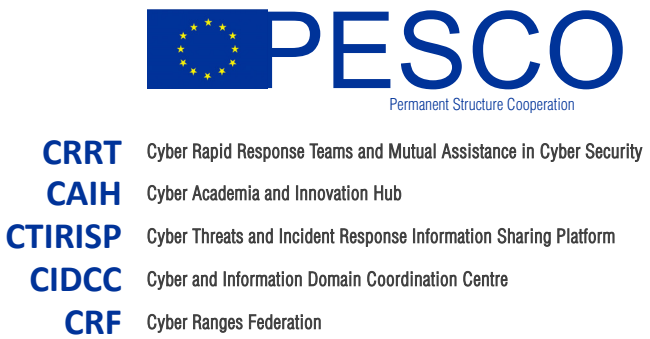


Figura 7 – Proyectos PESCO en el área de Ciberdefensa
FUENTE: Permanent Structured Cooperation (s.f.). European Union. https://www.pesco.europa.eu/

Al momento de escribir este libro hay en curso cinco proyectos PESCO en el área de Ciberdefensa: Equipos de Respuesta Rápida en Ciberdefensa (CRRT), Academia de Ciberdefensa y Hub de Innovación (CAIH), Plataforma de intercambio de información sobre ciberamenazas y respuesta a incidentes (CTIRISP), Centro de Coordinación del dominio Ciber y de la Información (CIDCC), Federación de campos de maniobras virtuales o "Cyber Ranges" (CRF).

Otros proyectos PESCO de capacidad también contemplan la ciberdefensa como parte inherente del proyecto, consolidando la cooperación en defensa entre los Estados miembros. PESCO se basa en ejemplos previos de cooperación y busca establecer un nivel de ambición más alto para mejorar y cohesionar el panorama de capacidades militares europeo. Este marco permite una cooperación progresiva en defensa, reflejando el apoyo al desarrollo colaborativo de capacidades, que junto con los medios proporcionan un sólido respaldo a las operaciones y misiones de la PCSD.

PESCO complementa otras dos importantes iniciativas: El Fondo Europeo de Defensa (EDF) que se abordará a continuación y la Revisión Anual Coordinada en Defensa (CARD) que apoya los esfuerzos de los Estados miembros para identificar las oportunidades de nuevas colaboraciones. La coherencia entre estas iniciativas y PESCO, junto con la orientación hacia las prioridades de capacidades en la UE, es clave para mantener la efectividad en el desarrollo de las capacidades en asuntos de Defensa europeos. Se busca reforzar un conjunto de fuerzas de amplio espectro capaz de operar en diversas operaciones y misiones. El nuevo Plan de Desarrollo de Capacidades (CDP) de la UE aprobado en noviembre de 2023 contribuye a impulsar estos objetivos.

2.2.2. El Fondo Europeo de Defensa

El Fondo Europeo de Defensa, como el principal instrumento de financiación gestionado por la Comisión Europea actualmente, trata de abordar el problema relacionado con la baja cooperación existente aún en la UE. El gasto en equipamiento de forma colaborativa en la UE apenas alcanza el 18% de un nivel de ambición establecido en el 35%. Asimismo, el gasto total en investigación y desarrollo tecnológico de forma colaborativa es del 7,3 % en contraposición con un nivel de ambición del 20%. El EDF busca fomentar la colaboración entre los Estados miembros, superar la fragmentación y mejorar la competitividad y la soberanía tecnológica de la industria europea de defensa. La ciberdefensa es una categoría principal de las acciones a desarrollar dentro del programa de trabajo anual del Fondo y, por tanto, se han financiado hasta el 2023 varios proyectos entre los que se destacan:

PROGRAMA DE FINANCIACIÓN: EDIDP 2019-2020		
Referencia	**Topic**	**Proyecto Seleccionado**
CSAMN: Conciencia situacional de Ciberdefensa y capacidades de defensa, redes de defensa y tecnologías para comunicación segura e intercambio de información.	Conjunto software para habilitar la conciencia situacional de ciberdefensa en tiempo real para la toma de decisiones en defensa.	ECYSAP
	Solución software para habilitar la búsqueda de amenazas y la respuesta ante incidentes en vivo, basada en una inteligencia compartida de ciberamenazas.	PANDORA
	Conjunto de herramientas de ciberdefensa interconectadas y de fácil despliegue para uso en defensa.	CYBER4DE
PROGRAMA DE FINANCIACIÓN: EDF 2021		
Referencia	**Topic**	**Proyecto Seleccionado**
EDF-2021-CYBER-R: Inteligencia de ciberamenazas y mejora de capacidades operacionales de ciberdefensa.	EDF-2021-CYBER-R-CDAI: Mejorando la ciberdefensa y la gestión de incidentes con la Inteligencia Artificial.	Ainception EU-GUARDIAN
EDF-2021-CYBER-D: Capacidad mejorada para ejercicios y entrenamiento en ciberdefensa.	EDF-2021-CYBER-D-IECTE: Eficiencia mejorada de los entrenamientos y ejercicios de ciberdefensa.	ACTING
PROGRAMA DE FINANCIACIÓN: EDF 2022		
Referencia	**Topic**	**Proyecto Seleccionado**
Ciberdefensa	EDF-2022-RA-CYBER-CSACE: Adaptando la conciencia situacional de ciberdefensa para entornos computacionales evolutivos.	NEWSROOM
	EDF-2022-DA-CYBER-CIWT: Conjunto de herramientas de guerra cibernética y de la información.	EUCINF
	EDF-2022-DA-CYBER-CSIR: Ciberseguridad y sistemas para la mejora de la resiliencia.	FACT
PROGRAMA DE FINANCIACIÓN: EDF 2023		
Referencia	**Topic**	**Proyecto Seleccionado**
Ciberdefensa	EDF-2023-RA-SI-CYBER-ASPT: Automatización de PENTESTING de seguridad.	*Selección de proyectos prevista para 2024.*
	EDF-2023-DA-CYBER-CSA: Conciencia situacional de ciberdefensa.	
	EDF-2023-DA-CYBER-DAAI: Agente de Inteligencia Artificial autónomo y desplegable.	

Tabla 1. Descripción de los proyectos de ciberdefensa del EDIDP (2019-2020) y EDF (2021-2023)

3. CAPACIDADES ACTUALES EN LA UE

Actualmente, dominar el ciberespacio permite tener una capacidad de influencia sin precedentes. Actores apoyados por Estados y grupos criminales lo están usando para realizar ciberataques, campañas de desinformación, o incluso enfoques híbridos donde se opera en varios dominios para interferir en los objetivos de la UE o producir daños sobre ellos. Por ello, **la UE actualmente dispone de capacidades para hacer frente a estas amenazas, pero es necesario fortalecerlas y evolucionarlas, lo que no ocurrirá de manera inmediata.** El desarrollo de una capacidad requiere abordar diferentes aspectos entre los que se encuentran: generar doctrina, definir una organización, mantener un liderazgo, incorporar personal con la capacitación y formación adecuadas, disponer de unas infraestructuras sólidas y contar con el respaldo de una base tecnológica, capacidad industrial, y un presupuesto adecuado.

La situación actual de la UE en relación con el desarrollo de capacidades puede clasificarse en 6 categorías, según el criterio y la experiencia de los autores:

Capacidad 1: Orientación y apoyo para el desarrollo de capacidades locales en cada Estado miembro.

Ayudar a cada Estado miembro en el desarrollo de sus propias capacidades hace que el conjunto de la UE sea más fuerte y resiliente, manteniendo al mismo tiempo su propia capacidad de decisión en las prioridades, características y alcance. Dentro de este ámbito los países desarrollan e implantan servicios de ciberseguridad que incluyen la monitorización de redes, herramientas de protección y detección de ciberamenazas, plataformas de "ciberinteligencia" y alerta temprana, laboratorios de investigación forense y análisis de malware, gestión de incidentes de ciberseguridad, gestión de crisis y recuperación ante desastres, entre otros muchos. Todos estos servicios suelen realizarse a través de los CERTs/CSIRTs y Centros de Operaciones de Seguridad coordinados por las entidades nacionales de cada país.

La EDA a través de su línea de acción denominada CARD, comentada en el apartado anterior, proporciona una oportunidad para que haya un diálogo con los Estados miembros sobre los planes de fuerza de cada país en el desarrollo de sus capacidades, evaluando su nivel de madurez y la viabilidad de futuros apoyos. Otras actividades principales incluidas son:

- Consultoría especializada: ENISA apoya a los países a través de la publicación de numerosos estudios, herramientas, seminarios y documentación especializada en cuanto a ciberseguridad generada por la propia Agencia.
- Servicio de prospección y observatorio tecnológico: EDA elabora planes de acción relativos a Tecnologías Emergentes y Disruptivas (EDT) aplicables a la ciberseguridad y ciberdefensa e informa a los Estados miembros para apoyarles en sus estrategias.
- Apoyo a la Innovación de los Estados miembros: la ECCC que, junto con los centros de coordinación por cada país (Network of National Coordination Centres – NCCs) actualmente en desarrollo, están conformando una comunidad europea. Dicha comunidad tiene como principal objetivo innovar en materia ciberseguridad, y posicionar a la industria europea en un referente en esta área.

Capacidad 2: Diseño y evolución de capacidades en ciberdefensa en la UE.

El propósito de esta capacidad es identificar necesidades, realizar una prospección tecnológica adecuada y estudiar la viabilidad y beneficio de iniciar investigaciones o proyectos de desarrollo. La EDA juega un papel fundamental en esta área, basándose en las prioridades establecidas a través del CDP, el nivel de desarrollo y madurez de cada capacidad obtenido del CARD y las conclusiones derivadas de un análisis de carencias. Actividades principales incluidas:

- Gestión de investigación y coordinación de I+D+i: la EDA dispone de unos grupos especializados en investigación y tecnología denominados CapTechs, encargados de evolucionar las capacidades en base a las necesidades identificadas. Uno de estos CapTech se enfoca exclusivamente en temas de ciberdefensa, llevando a cabo prospección tecnológica, identificación de carencias y ejecución de programas conjuntos de investigación.
- Desarrollo de nuevos proyectos: la iniciativa PESCO es la más relevante con sus más de 60 proyectos en diferentes áreas. Cabe mencionar el área denominada "Cyber/C4ISR", exclusiva para proyectos con un alto componente "ciber", como los ya comentados en el apartado 2.2.1 sobre PESCO.

Capacidad 3: Planeamiento y ejecución de operaciones en el ciberespacio.

En esta capacidad se engloban las actividades necesarias para llevar a cabo misiones u operaciones específicas propias de un contexto militar o para proporcionar servicios de ciberseguridad, definidos en un catálogo ofrecido por alguna entidad europea, en el marco de sus competencias, dentro del contexto más civil.

Servicios y actividades principales existentes:

- **Proyección de la fuerza en el dominio del ciberespacio:** el SEAE es el encargado de llevar a cabo la acción externa de la UE. Bajo su organización existen y se coordinan varias entidades para llevar a cabo la misión y cumplir con los objetivos de ésta. Existe un tipo de misión orientado a la seguridad, defensa y gestión de crisis, en donde se incluyen las ejecutadas en el ámbito operativo del ciberespacio. En este contexto, la resiliencia y la interoperabilidad son claves, aquí la UE se apoyará y reutilizará los principios, procesos y estándares que se están implementando en la OTAN, como la iniciativa FMN (Federated Mission Networking), capacidad destinada a apoyar el mando, el control y la toma de decisiones en operaciones futuras mediante un mejor intercambio de información en redes federadas de misión. Las capacidades para las misiones y operaciones del CSDP son proporcionadas por los países integrantes para una determinada misión, por lo que el planeamiento y la coordinación de las mismas es vital para cumplir con los objetivos de estas.

- **Resiliencia e interoperabilidad:** potenciar las infraestructuras de los Estados miembros y garantizar la adecuada integración de estas, principalmente para su empleo dentro de una misión. Actualmente la UE apuesta por modelos federados como FMN y el desarrollo de redes de mando y control seguras y resilientes.

- **Servicios de ciberseguridad:** los Centros de Operaciones de Seguridad y los Equipos de Respuesta a Incidentes (CERT/CSIRT) juegan un papel fundamental para esta función. Los primeros administran y operan las herramientas de ciberseguridad implantadas en las redes y los segundos proporcionan servicios de ciberdefensa relacionados principalmente con la gestión de incidencias de seguridad CIS. Como Threat Hunting, Forense digital, análisis de malware, intercambio de ciberinteligencia, etc... Se establece una red operacional denominada MICNET compuesta por los diferentes milCERT de los Estados miembros para proporcionar principalmente los servicios protección de las redes y también para apoyar en la capacidad de ciberdefensa a aquellas redes que se desplieguen bajo el paraguas de la PCSD para una misión.

- **Autoprotección frente a ciberamenazas:** las instituciones, los órganos y las agencias de la UE se benefician de los servicios ofrecidos por el CERT-EU. Ofrece diversos servicios específicos destinados a prevenir, detectar, mitigar y responder a los ciberataques de mafias, grupos organizados y hacktivistas. Apoya a todas las instituciones, órganos y agencias de la UE, compartiendo información sobre amenazas y vulnerabilidades que puedan afectar a la infraestructura de TIC de la UE y proporcionando medidas de protección o mitigación.

- **Lucha contra el cibercrimen:** Europol lidera la lucha contra el cibercrimen, abordando delitos como estafas, extorsión, abusos y explotación infantil online, venta ilegal de información, robo de datos y terrorismo que ocurre en el ciberespacio. El EC3, desde su creación en 2013, es el centro de referencia en esta capacidad y dispone de tres capacidades principales:

  1. Forense e investigación digital: recogida y análisis de pruebas digitales, atribución y desarrollo de informes técnicos periciales de apoyo a fiscalía.

  2. Ciberinteligencia: generación y compartición de información existente en el ciberespacio a través de sus investigaciones o adquiridas por técnicas de explotación de fuentes abiertas con CERT públicos/privados.

  3. Coordinación de operaciones internacionales en donde se necesite el soporte de diversas fuerzas y cuerpos de seguridad del estado (FCSE) según el ámbito de jurisdicción que aplique en los elementos digitales objeto de estudio. Cabe destacar su grupo "Joint Cybercrime Action Taskforce (J-CAT)", con más de 140 operaciones completadas desde su año de creación en 2014, como la desarticulación de mercado de venta de drogas en la Dark Web, arresto de bandas y grupos de extorsión a empresas que operan infraestructuras críticas, arrestos por realizar fraudes con criptomonedas, neutralización de redes botnet usadas para atacar a terceros (ej: EMOTET), y muchas otras.

Capacidad 4: Desarrollo normativo y reglamentación.

Esta capacidad se enfoca en el desarrollo y establecimiento de normas y regulaciones relacionadas con la ciberseguridad en la UE.

- **Certificación de la Ciberseguridad:** tras la ampliación de competencias de ENISA a raíz de la publicación de la norma "CyberSecurity Act", ésta agencia desempeñará un papel clave en la creación y mantenimiento del marco europeo de certificación de la Ciberseguridad. El alcance de la certificación abarcará productos, servicios y procesos, y beneficiará a la industria europea al "inducir" la compra de productos certificados. De esta manera, las empresas aumentaran su mercado pasando de ámbitos locales al ámbito europeo. Además, Europa pone foco en la cadena de suministro, que representa un riesgo cuando no está suficientemente controlada y busca mayor independencia tecnológica de terceros. Para la

adecuada implementación de la citada norma se creó el European Cybersecurity Certification Group (ECCG) que trabaja en estrecha colaboración con ENISA.

- **Desarrollo Legislativo:** dado que las amenazas a la Ciberseguridad son casi siempre transfronterizas, un ciberataque contra las infraestructuras críticas de un país puede afectar al conjunto de la UE. Cada país de la UE necesita contar con organismos gubernamentales fuertes que supervisen la Ciberseguridad en su territorio y colaboren con sus homólogos de otros Estados miembros compartiendo información. No obstante, deben existir unos principios homogéneos y comunes a toda Europa, que posteriormente serán transpuestos a la normativa legal de cada país miembro tras un periodo de adaptación.

- **Desarrollo de buenas prácticas:** a través de las publicaciones de sus numerosas agencias e instituciones, se promueven desde acciones de concienciación y buen uso del ciberespacio para la sociedad hasta documentación dirigida a empresas y organizaciones.

Capacidad 5: Formación y Adiestramiento.

- **Capacidad formativa:** dentro de esta capacidad, se cuenta con una oferta formativa importante proporcionada por la Escuela Europea de Seguridad y Defensa (en inglés, ESDC). Esta escuela dispone de un plan de estudios específico para ciberseguridad. El objetivo de este plan es abordar la formación en ciberseguridad y Defensa y ofertarlo al personal civil y militar, incluyendo los requisitos relativos a la PSCD en toda la formación. La temática incluye los ámbitos de la ciberseguridad y ciberdefensa, la ciberdelincuencia, la seguridad de la información en red, y las relaciones exteriores. Dispone de una plataforma denominada "Cyber Education, Training, Evaluation and Exercise (ETEE)", donde se han celebrado numerosos cursos con apoyo de diversas entidades de los Estados miembros. La ESDC trabaja estrechamente con diversas entidades de la UE, como EDA, EUROPOL, CEPOL, ECTEG, ENISA, CERT-EU y "EU Hybrid Centre of Excellence", para que la capacidad sea más eficaz y de calidad.

- **Desarrollo y ejecución de ciberejercicios:** en esta capacidad, se llevan a cabo diversos ciberejercicios con diferentes objetivos de adiestramiento dirigidos a distintas audiencias. Por su relevancia se destacan dos: Cyber Europe organizado por ENISA para entrenar habilidades y procedimientos propios del plano técnico y operativo, y Cyber Phalanx organizado por la EDA para entrenar habilidades y procedimientos propios a nivel estratégico como operacional. Además, algunas entidades europeas y Estados miembros participan en otros ciberejercicios que permiten generar confianza y compartir información sobre el uso de herramientas, plataformas y procedimientos. En este último punto se destacan la participación en ejercicios de la OTAN como Cyber Coalition y Locked Shields.

Capacidad 6: Cooperación.

La cooperación en ciberseguridad se lleva a cabo mediante diversas iniciativas y acuerdos que promueven el trabajo conjunto entre diferentes actores. A continuación, se presentan algunos ejemplos representativos por cada categoría:

- **Desarrollo de compromisos y acuerdos:**

  1. La existencia de conferencias periódicas como la "EU Cyber Commanders Conference" , en donde se pone en común estrategias seguidas en cada Estado miembro en su lucha contra incidentes relevantes. En caso necesario, este foro puede usar la red CyCLONE (EU Cyber Crises Liasion Organization Network) para la gestión de crisis en donde la cooperación militar y civil es esencial.

  2. Cooperación con la industria tecnológica: la UE busca aprovechar las sinergias existentes entre las iniciativas y desarrollos para el sector civil y el militar, apostando e incentivando tecnologías de uso "dual". Además, bajo la iniciativa "EU Defence Innovation Scheme (EUDIS)" de la Comisión Europea y el Hub de Innovación en Defensa de la EDA (HEDI), se apoya el emprendimiento y la innovación principalmente de PYMES para aumentar la independencia tecnológica en el futuro.

  3. Cooperación entre la OTAN y la UE: existen intercambios de información a muchos niveles (ciberamenazas, técnicas y herramientas, e incluso diseños de sistemas para aplicar estándares como FMN). También existen acuerdos de cooperación para formación, adiestramiento y ejercicios, como el reflejado en el Acuerdo Técnico de colaboración entre el NCIRC-OTAN y CERT-EU, firmado el 10 de febrero de 2016. El marco de cooperación se rige por la Declaración Conjunta OTAN-UE y la determinación de un conjunto de propuestas de actividades comunes a ambas organizaciones.

  4. Intercambio de información en diversos ámbitos, como son los relativos a ciberamenazas, formación, o diseño e implementación de Sistemas CIS específicos dentro de los marcos existentes de interoperabilidad.

- **Posicionamiento geoestratégico en Ciberseguridad:** partenariado con terceros (ej: USA) y organizaciones clave (ej: UN), cuyo objetivo es reforzar la capacidad de la UE para actuar como proveedor de seguridad mundial, prevenir conflictos y reforzar la seguridad internacional. El nivel de ambición se encuentra reflejado en la Brújula Estratégica de la UE del año 2022.

- **Apoyo de profesionales especializados:** muchos Estados miembros están trabajando para disponer de un conjunto de profesionales con conocimientos especializados en Ciberseguridad, que puedan ser activados e integrados puntualmente y temporalmente en unidades gubernamentales para hacer frente a crisis en el ciberespacio, conformando así una "ciber-reserva". La UE bajo el nombre de "EU Cyber Solidarity Act" está regulando actualmente todos los aspectos que rodean esta iniciativa y con la ayuda de ENISA, está desarrollando proyectos piloto para validar esta capacidad.

4. CAPACIDADES FUTURAS EN LA UE. TENDENCIAS

La Brújula Estratégica publicada por la UE en 2022 establece las prioridades para mejorar las capacidades en un horizonte temporal hasta el 2030. A continuación, se destacan las propuestas relacionadas con la ciberseguridad y ciberdefensa:

- Creación de una Capacidad de Despliegue Rápido de la UE con hasta 5.000 militares para abordar diferentes tipos de crisis.

- Reforzamiento de los despliegues tanto en misiones civiles como militares, mejorando los procesos de activación, los tipos de actuación y garantizando una mayor solidaridad financiera.

- Impulso de sus capacidades de análisis de inteligencia en este ámbito.

- Desarrollo de Equipos de Respuesta contra amenazas híbridas.

- Continuo desarrollo del conjunto de instrumentos de "ciberdiplomacia" y actualización de la Política de Ciberdefensa de la UE para estar mejor preparada y responder mejor ante los ciberataques.

- Actuación ante la amenaza de campañas de desinformación a través del desarrollo de un conjunto de instrumentos contra la manipulación de información y la injerencia por parte de agentes extranjeros.

- Facilitación de la comunicación y el intercambio de información entre los Estados miembros para apoyar los objetivos nacionales y alinearlos con los intereses de la UE como conjunto.

- Ofrecimiento de incentivos para fomentar la participación de los Estados miembros en proyectos colaborativos de desarrollo de capacidades y para que inviertan conjuntamente en elementos de apoyo estratégicos y capacidades de nueva generación para operar en los ámbitos terrestre, marítimo, aéreo, espacial y cibernético.

- Impulso de la innovación tecnológica en el ámbito de la defensa para subsanar las carencias estratégicas y reducir las dependencias tecnológicas e industriales.

- Refuerzo de la cooperación con socios estratégicos como la OTAN, las Naciones Unidas y los socios regionales, como la OSCE, la Unión Africana y la ASEAN.

- Desarrollo de asociaciones bilaterales más adaptadas con países afines y socios estratégicos como Estados Unidos, Canadá, Noruega, el Reino Unido y Japón, entre otros.

- Establecimiento de asociaciones adaptadas en los Balcanes Occidentales, la vecindad oriental y meridional, África, Asia y América Latina, mediante el refuerzo del diálogo y la cooperación, el fomento de la participación en misiones y operaciones de la PCSD y el apoyo al desarrollo de capacidades.

Por otra parte, y con una visión a más largo plazo, la hoja de ruta de la UE se verá influenciada por la evolución de las tecnologías emergentes y disruptivas (EDT en inglés). Actualmente, tecnologías como Blockchain, Inteligencia Artificial, Computación Cuántica, 5G o Gemelo Digital ofrecen grandes oportunidades para el desarrollo y la evolución de las capacidades de la UE. Además, no hay que olvidar que los adversarios también potenciarán sus capacidades con estas tecnologías, por lo que la UE debe ser más rápida y efectiva en su adopción si quiere mantener el liderazgo. Estos hechos generarán tanto oportunidades como nuevas amenazas para la ciberdefensa, que se sumarán a las ya existentes y deberán gestionarse para evitar futuros riesgos. A modo de ejemplo se describe a continuación las perspectivas de los proyectos a abordar en los próximos años a través del Fondo Europeo de Defensa (MAP 2023):

CATEGORÍA DE ACCIÓN: CIBERDEFENSA		
Área	**Topic**	**Resultados esperados 2021-2027**
Operaciones de Ciberdefensa	• Selección de talentos en ciberseguridad • Blockchain para la Identificación Amigo-Enemigo (Identification Friend or Foe, IFF) • Tecnologías de Ciberdefensa disruptivas • Soluciones de Ciberdefensa integradas en sistemas de armas o ciberseguridad y resiliencia de vehículos autónomos en operaciones militares. • Entrenamiento y ejercicios de ciberdefensa • Desarrollo para operaciones informativas defensivas de la información	Creación de dos líneas principales de acción colaborativa persistentes que contribuyan al desarrollo de herramientas europeas comunes y/o interoperables para: • Operaciones de ciberdefensa y gestión de incidentes • Guerra de la información, operaciones defensivas y medidas preventivas • Resiliencia de los sistemas ciber-físicos
Conciencia Situacional en Ciberdefensa	Podría preverse la evolución de las herramientas de intercambio de información sobre la base de los requisitos nacionales, incluidos los sistemas de coordinación ante incidentes con funcionalidades para oportunidades a escala de la UE	

Tabla 2. Perspectiva Multianual indicativa del Fondo Europeo de Defensa (2021-2027).

La evolución de la ciberdefensa va unida a la mejora de las infraestructuras digitales. Por ejemplo, las redes 5G ofrecerán una escalada en posibles aplicaciones tecnológicas, gracias a tener redes más rápidas, de baja latencia interconectando un alto número de dispositivos, pero también podrán suponer una proliferación de distintos tipos de ciberataques de los que será necesario defenderse. La Inteligencia Artificial abrirá oportunidades de nuevos desarrollos e incluso formas de actuación en el mundo digital, y redundará en el aumento de la seguridad de los sistemas, pero también podrá utilizarse para desarrollar y realizar ciberataques de forma más inmediata y sencilla. La criptografía post-cuántica también supondrá un gran avance en la protección de los datos gracias a un cifrado mucho más robusto, pero a su vez los ordenadores cuánticos harán posiblemente que los algoritmos de cifrado actuales dejen de proporcionar una protección adecuada.

La revolución tecnológica es imparable para las Fuerzas Armadas en Europa y el reto es abordar los elementos esenciales de esa transformación digital en tiempo y adaptado a las necesidades. La ciberdefensa se apoya en una infraestructura digital en continua evolución, incluyendo el uso de computación en la nube y redes de comunicaciones inalámbricas 5G/6G. La construcción del ecosistema de telecomunicaciones se basa en el apoyo a las Operaciones Multidominio, lo que implica disponer de una red única de transporte de la información interoperable y segura para poder sincronizar efectos en todos los dominios operacionales.

Ante este desafío, la ciberdefensa es habilitadora de la protección de las redes y sistemas de información, de la conservación de su disponibilidad, confidencialidad e integridad con vistas a apoyarse en la Inteligencia Artificial para nuevas funcionalidades y explorar los desafíos tecnológicos que supondrán el cambiar un modelo tradicional de ciberseguridad basado en el perímetro de la red a otro de defensa en profundidad con la inclusión en los diseños de los nuevos sistemas de los enfoques denominados centrados en los datos o “data-centric” y de confianza cero o “zero-trust”. Al final, es un balance entre oportunidad y riesgo a asumir en las medidas de seguridad y control objeto de la ciberdefensa y ciberseguridad, lo que incluye una especial relación con los sistemas telemáticos y las señales electromagnéticas.

5. ANÁLISIS Y CONCLUSIONES

El presente capítulo expone la relevancia de la ciberseguridad y ciberdefensa en la Unión Europea a través de las políticas e iniciativas lanzadas principalmente por la Comisión Europea y con la aportación de varios actores.

Quizás uno de los retos más urgentes sea abordar la implementación de todas las iniciativas y políticas de forma gradual y coherente con los recursos de los Estados miembros y los propios de la Unión Europea. Se deduce sobre todo, del "Cyber Solidarity Act", la necesidad de que los ámbitos civil y militar trabajen conjuntamente en situaciones de crisis o de incidentes a gran escala (Cyber Emergency Mechanism) junto a las necesidades de formación (Cyber Skills Academy), que son de interés para las Fuerzas Armadas en Europa.

A raíz de la publicación de las nuevas prioridades de desarrollo de capacidades militares en la UE en noviembre de 2023 se identifican dos áreas prioritarias de ciberdefensa: (i) obtener "capacidades de operaciones de ciberdefensa de espectro completo", centrada en garantizar la resiliencia del ciberespacio propio, la mitigación de los riesgos y la protección de las redes de misión frente a una gama completa de ciberamenazas, y (ii) la necesidad de conseguir una "ventaja en la guerra cibernética y en la preparación" ante un potencial adversario. Estas capacidades son esenciales para coordinar y gestionar las operaciones en el ciberespacio, realizar la evaluación de daños, priorizar los activos de ciberdefensa clave, gestionar los riesgos y compartir información para garantizar la sincronización e integración de actividades tanto civiles como militares. Todo ello permitirá una defensa eficaz y garantizará un sólido conocimiento de la situación en ciberdefensa, en el que la UE se encuentra invirtiendo actualmente y desde años atrás, dada la magnitud del desafío tecnológico a la hora de disponer de una plataforma de apoyo a la decisión y una componente fundamental de gestión del ciberespacio dentro de un sistema de mando y control integrado para las misiones y operaciones dirigidas por la UE en el marco de la PCSD.

En relación con las áreas claves para los próximos años, la primera se centrará en el desarrollo de capacidades de ciberdefensa ágiles y adaptables, abordando la convergencia de la Ciberdefensa con la Guerra Electromagnética, especialmente en el nivel táctico. La mejora de la resiliencia se obtendrá a través de la adopción de recomendaciones de carácter voluntario en el ámbito militar para aumentar la ciberseguridad de las redes, inspirándose en la Directiva Europea sobre la Seguridad de la Información y las Redes, conocida como "Network and Information Security Directive" (NIS2), cuya transposición al ordenamiento jurídico de los Estados miembros tendrá lugar en 2024. La mejora en la ciberseguridad también abordará la interoperabilidad y estándares en tecnologías duales. En cuanto a la segunda área prioritaria, la investigación y la innovación para las capacidades de Ciberdefensa serán claves para mantenerse al día de posibles evoluciones en la defensa de los sistemas militares impulsados principalmente por las tecnologías disruptivas emergentes y, por tanto, se deberán adoptar las decisiones relativas a la inversión a medio y largo plazo en aquellas tecnologías más prometedoras. Las tecnologías de ciberdefensa de última generación darán lugar a la creación de prototipos y experimentación conducentes a disminuir los riesgos de un producto final capaz de desplegarse rápidamente en apoyo a operaciones. Estas capacidades permitirán crear un ecosistema seguro para las Operaciones Multidominio. La conectividad por diseño del Multidominio es una tendencia a largo plazo en el área de capacidad militar en el horizonte 2040+, junto a otras como la lucha por la superioridad cognitiva o el dominio en el espectro electromagnético. El aumento de la preparación será reforzado a través de un programa conjunto de formación, entrenamiento y ejercicios de ciberdefensa a nivel europeo.

A lo largo del texto, se puede apreciar que el impulso continuo y sostenido de adoptar un marco regulatorio de una extensión sin precedentes en materia de ciberseguridad, unido a la búsqueda de las mejores capacidades posibles de ciberdefensa a nivel europeo, serán determinantes para el cumplimento de las misiones y operaciones en el marco de la PCSD, cuya hoja de ruta marca la Brújula Estratégica del 2022 y que permite afirmar que la UE dispone en la actualidad de unos cimientos sólidos para liderar este campo científico-tecnológico fundamental para el desarrollo de una sociedad digital y moderna.

El desarrollo y evolución de las capacidades "Ciber" es considerado por la UE como primordial y será un impulsor para su consolidación como actor relevante en un mundo cada vez más tecnológico.


HACKED

REFERENCIAS

1. Centro Conjunto de Desarrollo de Conceptos (2020). PDC-00 Glosario de terminología de uso conjunto. Ministerio de Defensa de España.

2. Centro Conjunto de Desarrollo de Conceptos (2018). PDC-01 (A) Doctrina para el empleo de las FAS. Ministerio de Defensa de España.

3. Centro Conjunto de Desarrollo de Conceptos (2018). Concepto de Ciberdefensa. Ministerio de Defensa de España.

4. Council of the European Union (2018). EU Cyber Defence Policy Framework (2018 update). European Union. https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf

5. European Commision (2020). The EU's Cybersecurity Strategy for the Digital Decade. European Union. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

6. European Union Military Staff (2021). European Union Military Vision and Strategy on Cyberspace as a Domain of Operations. European Union. https://www.statewatch.org/media/2879/eu-eeas-military-vision-cyberspace-2021-706-rev4.pdf

7. European Commission (2022). EU Policy on Cyber Defence. European Union. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2022:49:FIN

8. Council of the European Union (2022). A Strategic Compass for Security and Defence. European Union. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

9. Parliament and Council of the European Union (2022). DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). European Union. https://eur-lex.europa.eu/eli/dir/2022/2555

10. European Defence Agency (2023). The 2023 EU Capability Development Priorities. European Union. https://eda.europa.eu/publications-and-data/brochures/the-2023-eu-capability-development-priorities

11. European Defence Agency and Isdefe (2023). Enhancing EU Military Capabilities beyond 2040. Main findings from the 2023 Long-Term Assessment of the Capability Development Plan. European Union. https://eda.europa.eu/docs/default-source/eda-publications/enhancing-eu-military-capabilities-beyond-2040.pdf

12. North Atlantic Treaty Organization (2020). Allied Joint Publication-3.20. Allied Joint Doctrine for Cyberspace Operations. NATO Standarization Office (NSO). https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320

13. Khmelova, I. Yurchenko, O. y Hutyk, D. (2022). Cyber, artillery, propaganda. Comprehensive Analysis of Russian Warfare Dimensions. State Service of Special Communications and Information Protection of Ukraine. https://nsarchive.gwu.edu/sites/default/files/documents/rr9q9n-glu5j/2023-01-17-Ukraine-ESCU-Cyber-Artiller-Propaganda-Comprehensive-Analysis-of-Russian-Warfare-Dimensions-ESCU.pdf

14. European Commision (s.f.). Europe's Digital Decade. Unión Europea. https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade

15. European Union Agency for Cybersecurity (s.f.). European Union. https://www.enisa.europa.eu

16. European Defence Agency (s.f.). European Union. https://eda.europa.eu/

17. CERT-EU. Directorate-General for Digital Services of the European Commission (s.f.). European Union https://cert.europa.eu/

18. European Union Agency for Law Enforcement Cooperation (s.f.). European Union. https://www.europol.europa.eu/

19. European Cybersecurity Competence Centre and Network (s.f.). European Union. https://cybersecurity-centre.europa.eu/index_en

20. Permanent Structured Cooperation (s.f.). European Union. https://www.pesco.europa.eu/

21. European Cyber Situational Awareness Platform (s.f.). European Union. https://www.ecysap.eu/

22. Cyber Defence Platform for Real-time Threat Hunting, Incident Response and Information Sharing (s.f.). European Union. https://www.pandora-edidp.eu/

23. Cyber Rapid Response Toolbox for Defence Use (s.f.). European Union. https://www.cyber4de.eu/

24. AI Framework for improving Cyber Defence Operations (s.f.). European Union. https://www.ainception.eu/

25. European Framework and proofs-of-concept for the intelligent automation of Cyber Defence Incident management (s.f.). European Union. https://www.eu-guardian.eu/

26. Advanced European platform and network of Cybersecurity training and exercises centres (s.f.). European Union. https://acting-project.eu/

27. European Defence Found (s.f.). European Union. https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf_en

28. European Security and Defence College (s.f.) European Union. https://esdc.europa.eu/category/news/cyber-etee/

29. Evento CIBER combinado (CYBERCO / MIC / FIC-MICNET) (octubre de 2023). Presidencia Española. Consejo de la Unión Europea. https://spanish-presidency.consilium.europa.eu/es/eventos/evento-ciber-combinado-cyberco-mic-fic-micnet/

30. MITRE. ATT&CK. https://attack.mitre.org/

31. Sinitsin, O. (s.f.). The Pyramid of Pain in the SolarWinds Cyber Attack. Dynamite Analytics. https://dynamite.ai/pyramid-pain-solarwinds-cyber-attack/

32. Crowdstrike (2023). 2023 Crowdstrike Global Threat Report. https://www.crowdstrike.com/resources/reports/crowdstrike-2023-global-threat-report/

BIOGRAFÍAS

BENITO FERNÁNDEZ GARCÍA

Jefe del Área de Ciberdefensa de Isdefe.

Es Licenciado en Informática por la Universidad de Granada. Enfocó su carrera profesional a la Seguridad de la Información, recorriendo con Isdefe su largo camino como profesional casi en su totalidad. Como Jefe de Área en Ciberdefensa gestiona el área, coordina a su personal, dirige los proyectos asignados y asesora a las organizaciones de su ámbito a obtener, desarrollar y potenciar sus capacidades en ciberdefensa, así como le apoya con personal adiestrado en su puesta en operación.

Durante toda su carrera, ha tenido la oportunidad de ocupar distintos puestos y realizar trabajos de ingeniería de diversa índole, en clientes del ámbito nacional, como el Mando Conjunto del Ciberespacio, y del internacional, como el Mando Aliado de Transformación de OTAN (ACT / NATO) y el Centro de Excelencia de Ciberdefensa (CCDCOE / NATO).

Dentro de las actividades realizadas, se encuentra la auditoría de seguridad, diseño y ejecución de ejercicios de Ciberdefensa, desarrollo de normativa y gestión de oficinas de programa. Además, ha participado como ponente en diferentes foros, conferencias y grupos de trabajo, organizados tanto por entidades nacionales como por la OTAN.

Dentro de las certificaciones de seguridad y de gestión de proyectos que posee, se encuentran la Habilitación de Director de Seguridad del Ministerio del Interior, PRINCE2, CISSP y CISA. Le fue otorgada la Cruz del Mérito Aeronáutico con Distintivo Blanco del Ministerio de Defensa.

DANIEL BENAVENTE LÓPEZ

Coordinador Área de Ciberdefensa de Isdefe.

Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid, ha dedicado su carrera al mundo de la Ciberdefensa y la Ciberseguridad, desarrollándose casi en su totalidad en Isdefe mediante la ejecución de proyectos del Sector Público, con especial dedicación al Ministerio de Defensa.

Centrado en actividades relacionadas con la consultoría y la gestión de proyectos, desarrolladas para organizaciones de ámbitos nacionales (como el Mando Conjunto del Ciberespacio) e internacionales (como OTAN y UE), ha ocupado distintos puestos como ingeniero, ejerciendo actualmente la función de Coordinador (Área de Ciberdefensa de Isdefe). Enfocado en la definición y el desarrollo de capacidades de Ciberdefensa, se ha especializado además en las áreas de análisis y gestión de riesgos, gobierno y normativa de seguridad, diseño de arquitecturas de sistemas, gestión de I+D+i y prospectiva tecnológica.

Es autor / coautor de varios estudios y publicaciones, algunos realizados en el marco del Centro de Excelencia de Ciberdefensa (NATO CCDCOE), participando en grupos de trabajo internacionales (UE) y como ponente en distintos foros y actividades docentes, incluyendo el ámbito universitario.

Consciente de la relevancia de la formación continua en esta profesión, posee distintas titulaciones y certificaciones, donde destacan la Habilitación de Director de Seguridad del Ministerio del Interior, Máster en Dirección y Administración de Empresas (MBA), PMP, CISSP y CISA, entre otros. Fue condecorado con la Cruz del Mérito Militar con Distintivo Blanco del Ministerio de Defensa.

SALVADOR LLOPIS

Salvador Llopis ocupa los cargos de segundo jefe de la Unidad de Superioridad de la Información y Oficial de Proyecto de Telecomunicaciones y Sistemas de Información (CIS) dentro del Directorado de Capacidades, Armamento y Planificación de la Agencia Europea de Defensa (EDA) en Bruselas. Es responsable del programa de capacidad militar en C4ISTAR que incluye, entre otras, el área de desarrollo de sistemas de Mando y Control. Dirige el Equipo de Proyecto CIS – un grupo de trabajo compuesto por expertos de los 27 Estados Miembros de la Unión Europea. Asimismo, dirige y coordina las actividades del grupo de trabajo europeo sobre seguridad centrada en los datos y las arquitecturas de confianza cero. Es oficial de Transmisiones del Ejército de Tierra y componente de la LIV promoción de la Academia General Militar. Es Académico de la Academia de las Ciencias y las Artes Militares. Es Doctor en Telecomunicaciones por la Universitat Politecnica de Valencia. Es autor de varias publicaciones científicas y miembro del consejo editorial de la revista Journal of Defence and Security Technologies.


VAMTAC
ET 119463

CAPÍTULO 8

El Reto Industrial

Yolanda Jaén González
Rocío Mora Picazo
Sergio Vicente López

La historia reciente ha puesto de relieve que, para poder tener autonomía en la toma de decisiones de cara a resolver un conflicto o una crisis sanitaria, ha de poseer una industria capaz de acometer el suministro de los sistemas y bienes necesarios. De lo contrario, todas las medidas vendrán condicionadas por terceros, poniendo en riesgo la independencia en la toma de decisiones y la capacidad de respuesta ante una crisis. En el caso de la defensa este factor es aún más crítico.

Para poder llevar a cabo cualquier planeamiento futuro de las capacidades operativas necesarias o para adoptar y definir políticas y estrategias nacionales, la industria ha de ser un elemento a considerar desde el comienzo, ya que puede ser un factor diferenciador.

Este capítulo realiza un análisis de los diferentes aspectos de la industria de defensa a tener en cuenta de cara a obtener una visión clara y precisa del escenario actual y poder así informar políticas y estrategias.

1. CARACTERIZACIÓN DEL SECTOR INDUSTRIAL DE LA DEFENSA

La Base Industrial y Tecnológica de la Defensa (BITD) comprende las entidades gubernamentales y del sector privado involucradas en la investigación, desarrollo, diseño, producción, entrega y mantenimiento de sistemas y tecnologías militares. Estas entidades proporcionan a las Fuerzas Armadas (FAS) los equipos y sistemas que les son necesarios para la consecución de sus objetivos y cumplimiento de sus compromisos.

El sector industrial de defensa cuenta con unas características propias que se han de analizar para saber cómo pueden impactar en el contexto actual tanto desde el punto de vista estratégico, como del operativo.

Algunas de estas características que pueden tener un impacto mayor, y se considera adecuado analizar en más detalle, son las expuestas a continuación.

1.1. Un Sector Vinculado a la Soberanía Nacional

La existencia de una industria de defensa competitiva y con un alto nivel de capacidades tecnológicas es imprescindible para la soberanía nacional. En caso contrario, no existe la posibilidad de garantizar la seguridad y la defensa del territorio de forma autónoma cuando, para disponer de las plataformas y los sistemas necesarios, se depende en exceso de desarrollos tecnológicos procedentes de terceros países. Por este motivo, la estrategia industrial de defensa debe ocupar un lugar clave dentro de las políticas de un país, para poder cumplir la visión y objetivos de seguridad y soberanía nacional establecidos. Cabe añadir que el factor presupuestario con el que se doten estas políticas es crucial para su puesta en marcha.

La vinculación con la soberanía nacional implica que, en un porcentaje elevado de los desarrollos, el cliente final sea único, ya que los programas o proyectos se realizan para cubrir necesidades específicas de un Estado, salvo que sea un programa de cooperación que beneficie a varios Estados. Esta característica del mercado de defensa, junto a sus bajos volúmenes de producción en comparación con los del mercado civil, generan una alta competencia entre las empresas. Esto obliga a las empresas a ser altamente competitivas y a tener altas capacidades tecnológicas e industriales si quieren no sólo suministrar a sus países de origen sino también a terceros. Además, la competitividad es mayor al ser, por su criticidad, un sector fuertemente intervenido y regulado, lo que supone una gran barrera de entrada. Las exportaciones son indispensables para mantener una industria fuerte y capaz, más en el escenario actual en el que se está definiendo el mapa industrial de defensa europeo.

Este es un reto mayúsculo ya que, a pesar de la intención de crear una Europa de la Defensa, este deseo se encuentra con una barrera clara y difícilmente salvable. Los países consideran un factor clave el peso y poder que se ejerce en el escenario europeo e internacional a través de sus industrias de defensa, consiguiendo no solo supremacía tecnológica sino un mayor peso político. Por lo tanto, los países tienden a desarrollar políticas proteccionistas para garantizar el suministro de los sistemas que consideran críticos para proteger las áreas y capacidades de su industria nacional dedicada a la defensa. Esto dificulta el acceso de otras empresas no nacionales a sus mercados de defensa, así como el desarrollo de programas colaborativos. También genera un escenario complejo de cara a definir un mercado de defensa europeo justo y equilibrado, en el que no predomine ningún país de forma contundente sobre otro y se favorezca un reparto de capacidades de alto valor añadido entre los diferentes países. Así, se hace indispensable establecer, a nivel europeo, los mecanismos necesarios que permitan y garanticen alcanzar este equilibrio, ya que es la única forma de, por un lado, propiciar que los países tengan una predisposición positiva a cooperar y, por otro lado, posicionar a la industria de defensa europea en el mercado internacional. De esta forma Europa podrá alcanzar su deseada soberanía estratégica sin que los países dejen de lado su soberanía nacional individual.

1.2. Jerarquización y Fragmentación de la BITD Europea

Dos de las características más representativas del sector industrial de defensa a nivel europeo son tanto su jerarquización como su fragmentación, ambas ligadas entre sí. En tanto a la jerarquización, existe sólo un reducido número de empresas capaces de generar productos propios con capacidades y tecnologías punteras. Son estas las que ejercen la labor de tracción sobre el resto de las empresas, que actúan como sus suministradoras y/o colaboradoras, y las que poseen mayor capacidad de exportación. Estas empresas son las principales contratistas de los ministerios de defensa de cada país y, por lo tanto, se encuentran en la cúspide de la pirámide.

La fragmentación en la BITD europea supone una debilidad comparativa frente al resto de competidores. Como ejemplo contrapuesto se encuentra el caso estadounidense donde existen unas empresas con un tamaño sumamente mayor, con una gran capacidad industrial, muy especializada, que revierte en un menor número de sistemas operativos diferentes, lo que evita problemas de interoperabilidad.

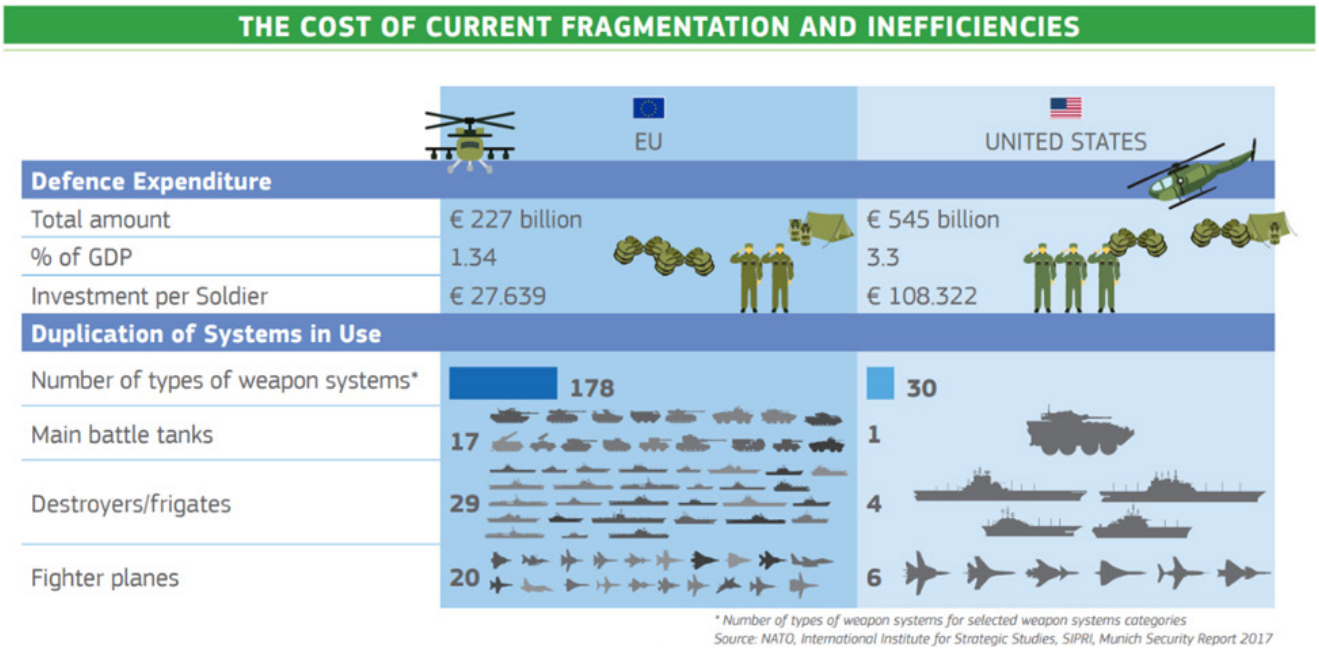


Figura 1. Coste de la actual fragmentación e ineficiencias. Datos del 2017 - Fuente: European Defence Fund Factsheet - Comisión Europea 2019.

La BITD tiene una gran dependencia del efecto tractor generado por los contratistas principales. Esto puede generar un potencial problema ya que gran parte de las capacidades residen en PYMES y MIDCAPS. Dentro de las cadenas de suministro es reseñable el número de PYMES y MIDCAPS que tienen un papel importante por aportar capacidades esenciales, además de la industria auxiliar que suministra equipos, componentes y servicios. Por eso es indispensable asegurar una herramienta que fomente la elección por parte de las empresas contratistas principales de PYMES y MIDCAPS nacionales y europeas en los programas de los que son adjudicatarias, siempre y cuando puedan cumplir con los requisitos demandados, sobre todo en los sistemas/equipos considerados críticos y/o estratégicos. Estas empresas son la base sobre la que se sustenta el aseguramiento de la cadena de suministro, así como la creación de una base industrial de defensa capaz y competitiva.

1.3. Estructura Empresarial: Consorcios y Empresas Tractoras

El impulso de la Europa de la Defensa está generando un entorno en el que se fomentan progresivamente los proyectos colaborativos entre empresas europeas, poniendo de relieve la importancia de que los países posicionen estratégicamente a sus empresas.

De cara al posicionamiento de las empresas en estos proyectos, es importante no sólo las capacidades industriales de las mismas, sino también su tamaño, ya que ello redundará en poder ocupar una posición preponderante y que el resultado de su participación derive en un mayor valor añadido.

Además, como se puede observar en la figura 2, el peso a nivel mundial de la industria de defensa europea es reducido en comparación con el de Estados Unidos, la principal potencia mundial que engloba más de la mitad de las ventas de defensa, seguido por China, cuya tendencia es alcista en su pugna por obtener el liderazgo como potencia.

Dentro de la industria europea, el Reino Unido lidera a nivel de ventas, mientras que, entre los Estados miembros de la Unión Europea, destaca Francia, seguido por Italia. Un aspecto destacable del mapa empresarial europeo es el liderazgo claro de una o dos empresas por país, lo que está ligado al concepto de campeón nacional.

Con el objetivo de conseguir un mejor posicionamiento de la industria europea de forma global, existen una serie de movimientos que se han ido produciendo en los últimos años.

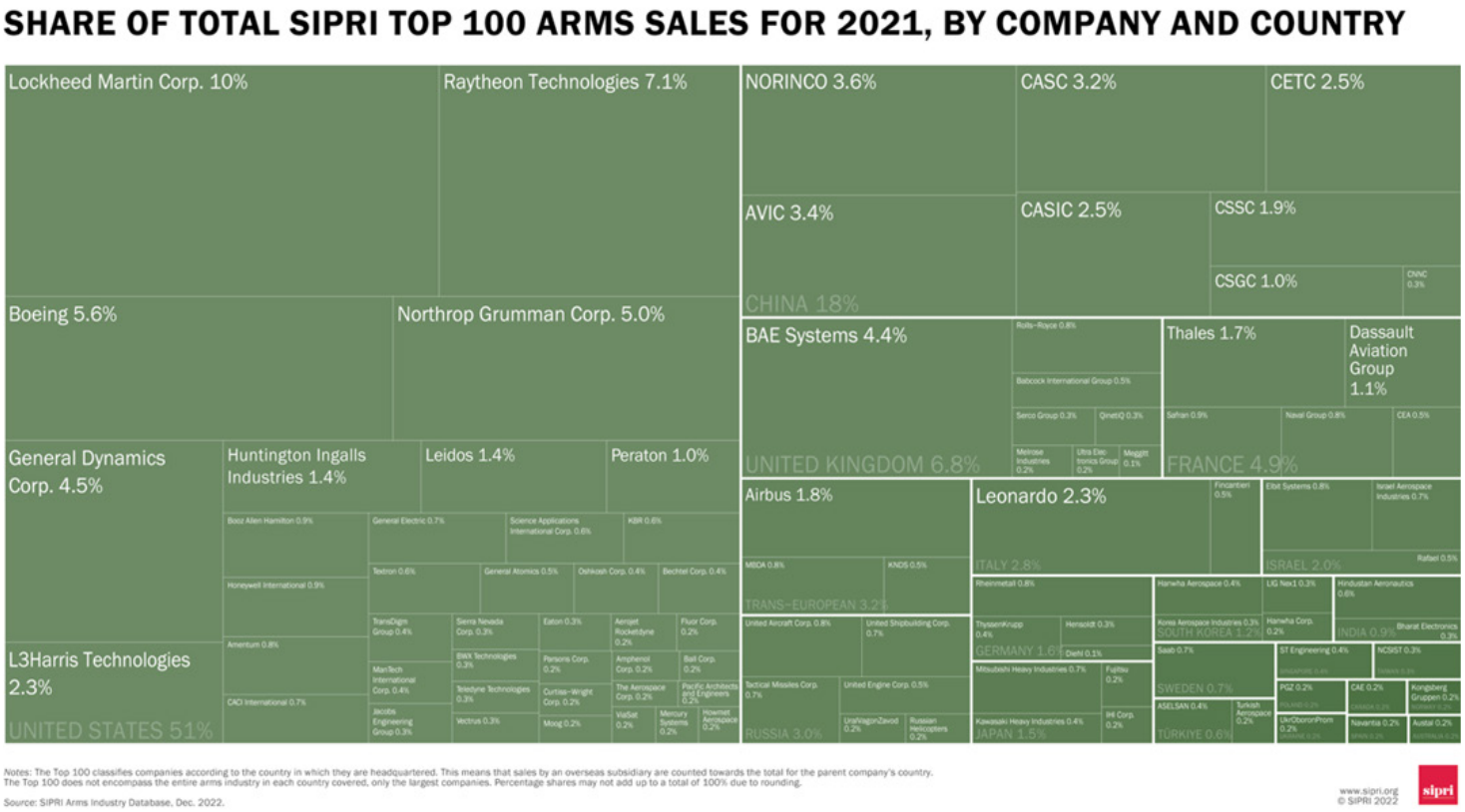


Figura 2. Porcentaje del total de las 100 mayores ventas de armas del SIPRI para 2021, por empresa y país Fuente: SIPRI Arms Industry Database 2021

El primero de ellos son los movimientos de agrupación empresarial en torno a consorcios o empresas líderes (prime). Durante las últimas décadas se han producido en el sector varios movimientos de agrupación empresarial como en el caso de Airbus en el sector aeronáutico o de MBDA en el subsector misiles. Existe también un movimiento que aspira a una Airbus naval cuyo piloto puede ser la formación del consorcio creado para el programa europeo de la European Patrol Corvette (EPC), donde participa Naviris, la empresa creada a partes iguales entre Naval Group y Fincantieri, junto a la española Navantia. Mediante la creación de estos consorcios, se busca tanto incrementar el tamaño de las empresas como complementar sus capacidades fomentando las transferencias de tecnología y conocimiento entre ellas.

Además de estos movimientos de consolidación por subsectores, otro planteamiento estratégico que se está dando, en este caso a nivel país, es la creación de empresas que cubran el papel de campeón nacional o consorcio nacional. Este fenómeno consiste en la ejecución, a nivel estratégico, de movimientos, decisiones y planteamientos que desembocan en la existencia de una empresa que actúa como campeón nacional en un determinado subsector y en torno a la cual se pueden producir fusiones o concentraciones de programas, siendo uno de los objetivos su fortalecimiento tanto a nivel económico como de capacidades. Una de las ventajas de esta política es la creación de empresas cada vez más grandes y potentes que tengan una posición de mayor peso de cara a los programas colaborativos europeos. Por ejemplo, en el sector naval en Alemania hay una agrupación de astilleros militares, en Francia el Estado dirige la estructura de empresas en el sector y los papeles que se potencian en las mismas en base a capacidades, y en Reino Unido se reparte carga de forma estratégica entre los astilleros. En este sentido, hay que señalar que los programas colaborativos son habituales en plataformas aéreas, misiles y espacio; menos en plataformas navales y excepcionales en las terrestres.

Ya en clave nacional cabe destacar que el posicionamiento que puedan alcanzar las empresas de la BITD nacional supone, desde el punto de vista estratégico, un reto; y la vía que se elija para afrontarlo tendrá repercusión tanto en las capacidades industriales que se tengan a nivel nacional como en las capacidades con las que se dote a las FAS, considerando a la industria como una capacidad operativa más de las FAS.

Las políticas nacionales y las medidas adoptadas para potenciar las capacidades tecnológicas e industriales de la industria española de defensa tienen efecto en el posicionamiento, tanto europeo como global, que puedan llegar alcanzar. El objetivo ha de ser el de disponer, en cada subsector o línea de producto, de empresas con capacidades en el estado del arte y competitivas, ayudando a que esas empresas ocupen posiciones fuertes en los consorcios y a que su participación sea de alto valor añadido. En este aspecto, se parte con el hándicap de poseer una BITD de pequeño tamaño, comparativamente hablando, frente a sus competidores europeos. Este factor puede ser mitigado a través de la creación de consorcios, donde puedan aunarse esfuerzos y conjugar capacidades para lograr un mejor posicionamiento en el mercado internacional al hacer un frente común. Esto repercutiría positivamente tanto en su papel en los proyectos colaborativos europeos como en el retorno que se logre a nivel nacional en distintos aspectos: económicos, empleo cualificado, capacidades industriales de la industria y su aplicabilidad a las FAS.

1.4. Proyectos Complejos de Alto Componente Tecnológico

Los proyectos de defensa suelen demandar un alto componente tecnológico, y su aplicabilidad en entorno hostiles y sus desarrollos no aplicables en otros ámbitos ocasionan largos proyectos de investigación y desarrollo. Estos proyectos necesitan amortizar los costes de desarrollo en un número elevado de unidades, de tal forma que uniendo este efecto con los derivados de la curva de aprendizaje y la economía de escala se pueda presentar un coste unitario asumible.

Las características implícitas en los programas de defensa están relacionadas con la planificación operativa. Y la deseable existencia de un compromiso entre las necesidades de las FAS de un país y los desarrollos propios de las industrias nacionales, repercute tanto en el nivel tecnológico de las industrias y de sus cadenas de suministro como en otros aspectos que afectan a la sociedad, por ejemplo, el empleo o la formación.

Para ligar de forma adecuada este hecho resulta imprescindible contar con una estrategia que aborde las capacidades y tecnologías consideradas prioritarias de cara a la inversión, tal y como establece la recientemente aprobada Estrategia Industrial de Defensa (EID 2023), ya que permite orientar las políticas hacia los programas que desarrollen dichas capacidades a la vez que se realiza una gestión presupuestaria eficiente.

En ocasiones, la amplia longitud de los citados periodos de desarrollo de tecnologías, además de afectar a las necesidades operativas, puede implicar, en ocasiones, unos sobrecostes. Existen diferentes iniciativas que ayudan a paliar alguno de los impedimentos que se encuentran a la hora de desarrollar tecnologías a nivel nacional como los elevados costes de desarrollo, la estandarización e interoperabilidad, la adecuación a las necesidades de los ejércitos y la reducción del coste de las compras y el sostenimiento, disminuyendo la pendiente de la curva de aprendizaje.

Un claro ejemplo de estas medidas es el Programa Foreign Comparative Testing (FCT [1]), del Departamento de Defensa de Estados Unidos. Este programa consiste en la adquisición de tecnologías desarrolladas a nivel mundial con un grado de madurez (TRL, Technology Readiness Level) elevado para probarlas y evaluarlas de cara a su implementación futura, ayudando a la toma de decisiones y a la definición de requisitos en los futuros programas de adquisición. Este programa acelera la adquisición de capacidades eludiendo el ciclo de desarrollo al permitir probar y evaluar tecnologías extranjeras ya maduras. Otra opción sería el lanzamiento de programas de desarrollo de capacidades transversales a diferentes programas que permitan el desarrollo de capacidades tecnológicas e industriales de forma progresiva y constante en el tiempo, eludiendo periodos de ausencia de inversión y por lo tanto de desarrollo, que tantas veces imposibilita poder contar con sistemas probados y que cumplan las necesidades operativas en los plazos necesarios.

2. CAMBIO DE PARADIGMA: LAS TECNOLOGÍAS DISRUPTIVAS, LOS DESARROLLOS DUALES Y SU IMPACTO EN LA INDUSTRIA

Los avances tecnológicos realizados en los últimos años están inmersos en la revolución 4.0 que tiene como característica central la digitalización de la industria, lo que plantea unos retos y necesidades que han de ser abordados tanto para mejorar la organización de la industria de defensa como el planeamiento militar.

También se debe tener en cuenta el cambio de paradigma empresarial acontecido. Tradicionalmente muchos de los avances tecnológicos se iniciaban en el sector de defensa mediante programas de I+D e inversiones estatales para más tarde ir fluyendo hacia el sector civil. Sin embargo, en la actualidad se está viviendo el efecto contrario, los desarrollos tecnológicos se crean y desarrollan antes en el sector civil, generando una situación que debe ser analizada en el sector de defensa para tratar de obtener las tecnologías necesarias de la forma más eficiente posible.

1. https://ac.cto.mil/pe/fct/

La innovación, y los avances en tecnologías emergentes y disruptivas, son un factor importante para garantizar la efectividad operativa de las FAS. La industria de defensa debe, por un lado, incorporar la innovación a sus sistemas aprovechando los diversos usos y aplicaciones que genera y, por otro lado, planificar en el largo plazo las inversiones necesarias para poder asegurar una BITD competitiva y resiliente.

Como ejemplo de este enfoque en innovación para el sector de la defensa, se encuentra la Instrucción sobre la innovación en defensa en el Ministerio de Defensa francés [1] que establece el marco organizativo general de la política de innovación del Ministerio y que sitúa el foco tanto en la innovación planificada, basada en estudios operativos o técnico-operativos y estudios de investigación y tecnología, como en la innovación abierta, apoyándose en los desarrollos externos al ámbito de la defensa.

A continuación, se detallan algunos de los retos que presenta el impacto en la industria de defensa de las tecnologías disruptivas y los desarrollos duales.

2.1. Retos Generales

2.1.1. Reto para el Planeamiento Militar

En ocasiones existe un delicado equilibrio entre las necesidades operativas y las de la industria. Desde el punto de vista operativo, la prioridad es contar con los mejores equipos y sistemas posibles tanto desde el punto de vista tecnológico como desde el de la interoperabilidad, que reviertan en una mayor eficacia en las operaciones. Sin embargo, estas necesidades a veces se encuentran con dificultades desde el punto de vista tecnológico-industrial.

La primera es el horizonte temporal, ya que, aun existiendo necesidad operativa de disponer de una tecnología, los tiempos de desarrollo de la tecnología en la BITD nacional son largos y pueden no estar acompasados con la industria. También afectaría a esta falta de encaje temporal aspectos económicos como la congelación de inversiones o reducciones en el gasto, factor a tener en cuenta a pesar de que nos encontremos actualmente en un ciclo expansivo de inversión. Estas restricciones presupuestarias, unido al coste de los desarrollos, podrían suponer un impacto en la viabilidad de estos programas de investigación y desarrollo, lo que puede repercutir en una disminución a futuro de las capacidades de las FAS de disponer de tecnologías de vanguardia.

La segunda son las tecnologías. Las tecnologías emergentes son altamente cambiantes, por lo que debe existir una visión común entre las FAS y la industria sobre qué tecnologías serán necesarias con el objetivo de definir una estrategia común, ya que, en caso contrario, puede darse que los desarrollos e inversiones de la industria difieran de las necesidades de las FAS. Este hecho también está influenciado por la pérdida de liderazgo en el desarrollo de la industria de defensa en favor de las empresas del sector civil.

Cabe señalar que muchos países, empezando por los más poderosos, se plantean contar con los mejores equipos y sistemas, siempre que “se lo puedan permitir”, aludiendo así al delicado equilibrio que hemos señalado anteriormente.

2.1.2. Liderazgo Tecnológico del Sector Civil

En cuanto al desarrollo de las nuevas tecnologías, es el sector civil quien tiene la iniciativa por lo que, desde el punto de vista de la industria de defensa, la aproximación más eficiente, y por razones de necesidad, es servirse de las capacidades tecnológicas que se están desarrollando en el sector civil.

Dada esta situación, el enfoque de la industria de defensa hacia la absorción de estas capacidades, debería girar en torno a las siguientes actuaciones con el fin de mejorar la eficiencia:

En primer lugar, se debería minimizar la inversión en programas de I+D en tecnologías emergentes y disruptivas (EDT) de forma solitaria, ya que ocasiona un mayor gasto en un entorno de recursos limitados y en un horizonte temporal en el que los grandes tiempos de desarrollo de estas tecnologías podría ocasionar que, en el momento en el que estén listas para su implantación, ya sean tecnologías obsoletas en el mercado.

Por otro lado, el liderazgo tecnológico del sector civil acentúa una dependencia de terceros que supone una vulnerabilidad en términos de autonomía estratégica. Más aún, considerando que las empresas que cuentan con el estado del arte de estas tecnologías pertenecen en gran medida a países con un control férreo de su tecnología, como es el caso de EEUU, o países acechados por la sospecha de espionaje, como China. Una forma de minimizar esta vulnerabilidad es el desarrollo nacional que, desde el punto de vista de seguridad, es una opción

superior. Este hecho se acentúa en ámbitos especialmente críticos como el de la ciberseguridad. La garantía y confianza de los sistemas autónomos y de apoyo a la decisión basados en tecnologías como la Inteligencia Artificial (IA), puede ser, en algunos casos, difícil de asegurar si se depende de tecnologías de terceros.

En cuanto a la preferencia por los desarrollos nacionales, hay que establecer un equilibrio entre las necesidades operativas y el tiempo que en ocasiones implica este desarrollo, ya que no siempre se dispone de la capacidad. Contar con soluciones intermedias mediante adquisiciones a terceros permite dar respuesta a la operatividad, aunque crea una vulnerabilidad temporal la dependencia de terceros.

Por último, el hecho de que la vanguardia tecnológica en el desarrollo se concentre en las empresas del sector civil y la necesidad por parte del sector industrial de defensa de absorber estos desarrollos, plantea un reto en cuanto al nivel que se debe fijar en los objetivos de capacidades militares en los programas. Uno de los aspectos críticos desde el punto de vista operativo es el tiempo que transcurre desde que surge una necesidad tecnológica, hasta que esta se concreta. Por ello es necesario realizar estudios y análisis sobre la ambición que se tiene en cuanto al nivel tecnológico para evitar sobre especificaciones, ya que en muchas circunstancias no será necesario aplicar el último nivel tecnológico desarrollado en el sector civil para las aplicaciones de defensa. Este incremento en las especificaciones supone un aumento de costes y plazos que puede dar lugar a problemas de interoperabilidad, además de suponer un factor de estrés tanto para la industria como para la cadena de suministro, ambos eslabones necesarios para proveer las últimas tecnologías necesarias para los desarrollos.

Igualmente, hay que considerar las limitaciones operativas que pudieran imponerse a equipos de origen extranjero para su utilización en caso de conflicto.

2.1.3. Empresas Duales

La realidad empresarial muestra que la mayoría de la industria del sector defensa está compuesta por empresas duales, hecho que puede resultar beneficioso a la hora de crear sinergias, trasladando avances tecnológicos desde el ámbito civil al de la defensa, no sólo entre empresas sino dentro de las mismas.

Además, las empresas duales pueden paliar ciertas casuísticas que afectan al sector defensa como el caso anteriormente mencionado de la dependencia de los presupuestos nacionales, que ocasiona que, en periodos de disminución de la demanda o de reducción presupuestaria, se produzcan pérdidas a nivel de infraestructura o de personal. Este fenómeno se produce cuando se da una pérdida de perfiles muy técnicos para determinados programas, por la falta de continuidad de los mismos, que en momentos de intensificación de la demanda o presupuestos es hartamente difícil recuperar.

Otra problemática que considerar es el volumen de pedidos típicos de los programas de defensa. Frente a contratos provenientes del sector civil, los volúmenes de defensa son, en numerosos casos, como por ejemplo en capacidades tecnológicas, significativamente menores, lo que implica que la producción y la cadena de suministro relegan a los programas de defensa a una posición trasera al sector civil.

2.2. Retos Particulares de la EDT

Las EDT como son la IA (sometida ya, a finales de 2023, a los primeros estadios de regulación por la UE), Internet de las cosas (IoT) y Big Data, robótica y sistemas autónomos, tecnologías cuánticas, biotecnologías, armas hipersónicas, tecnologías espaciales, nuevos materiales y blockchain, permiten un mejor abordaje de los retos actuales y futuros, como son la interconexión entre múltiples plataformas en entornos colaborativos, la energía dirigida y sus aplicaciones en defensa o el domino del ciberespacio.

La implantación de estas tecnologías dentro del ciclo inversor plantea una serie de retos sobre cómo abordar su desarrollo propiciando un marco para el análisis de cuáles de ellas son más críticas. Algunos de ellos son:

2.2.1. Introducción de Nuevas Amenazas

Las EDT tienen el potencial de introducir amenazas nuevas e impredecibles que los sistemas de defensa tradicionales pueden no estar equipados para manejar. Los contratistas de defensa deben ser ágiles y adaptables para responder rápidamente a las nuevas amenazas, lo que requiere una inversión significativa en investigación y desarrollo. Sin embargo, estas inversiones son caras, y los contratistas deben saber equilibrar la necesidad de innovación con los costes de la inversión.

2.2.2. Reforzar la Integridad en el Ámbito de Ciberseguridad

La hiperconectividad habilitada por las nuevas tecnologías significa un flujo de información y datos sin parangón en la historia de la humanidad, lo que supone un reto de seguridad para la industria en general y para la de defensa en particular, ya que la criticidad de la información que se maneja es mucho mayor. Un comportamiento rutinario es que los usuarios otrora confiables de una red se conecten desde distintos dispositivos en entornos como la nube, lo que abre una puerta a los cibercriminales para acceder a estos datos. Esto ha generado unas medidas correctivas que se conocen como Zero Trust Security o estrategia de confianza cero, que establece unas capas de control del usuario, dispositivos y acceso bajo un paraguas de mejora continua. Este modelo de seguridad está basado en la premisa de que no se confía ni se permite acceder a los activos a ningún usuario hasta que haya sido validado como entidad legítima y autorizada.

Otra tendencia en las EDT es el extendido uso de software comercial off-the-shelf (COTS) y sistemas operativos de código abierto, principalmente por su bajo coste. Esto conlleva problemas de seguridad, ya que los sistemas de código abierto, cuya naturaleza es la de la contribución comunitaria, podrían estar plagados de vulnerabilidades o puertas traseras que se podrían implantar en el código base.

2.2.3. Obsolescencia

Con la tecnología avanzando a un ritmo exponencial, es cada vez más difícil mantenerse al día con los últimos desarrollos. Esto puede ocasionar que en ciertos casos cuando se disponga de cierto desarrollo, ya se encuentre obsoleto. Este riesgo hay que tenerlo en cuenta a la hora de diseñar las estrategias de desarrollo y de planeamiento de capacidades, y es por ello, que las sinergias creadas con el sector civil, que puede ayudar a reducir los tiempos, son un aliado para combatirlo, si bien habrá que tener en cuenta el tipo de sistemas.

2.2.4. Competencias y Habilidades del Personal

La aplicación de estas tecnologías tiene un componente personal indiscutible. En la actualidad, el sector de defensa se enfrenta a una situación compleja en cuanto a la atracción y retención del talento. La implementación de dichas tecnologías y el impulso de programas y proyectos donde se desarrollen productos y tecnologías de valor añadido puede suponer un mayor atractivo, tanto profesional como en condiciones que redunden en una potenciación de los perfiles técnicos y de trabajos de valor añadido. Existen además necesidades tanto de personal para desarrollar las capacidades como de formación y entrenamiento al usuario final.

Un punto crítico asimismo es la necesidad de que estos conocimientos y habilidades perduren y sobrevivan a la duración de los programas, tanto para su aplicación en el ciclo de vida como para su utilización en otros desarrollos. También hay que considerar la necesidad del mantenimiento del conocimiento, ya que la formación del usuario en las nuevas aplicaciones y desarrollos no debe ir en detrimento de la utilización de otras aplicaciones o versiones anteriores que se mantengan en uso.

3. LA INDUSTRIA COMO FACTOR CLAVE PARA LA AUTONOMÍA ESTRATÉGICA

El actual entorno internacional ha puesto de manifiesto la creciente relevancia de las cuestiones relacionadas con la autonomía estratégica, tanto a nivel nacional como europeo. Se entiende por autonomía estratégica la capacidad de un actor de actuar de forma autónoma, sin depender de otros países, en ámbitos políticos de importancia estratégica [2], como es la defensa.

Tanto la crisis del Covid-19, como la guerra de Ucrania han sacado a relucir riesgos y vulnerabilidades de la industria de defensa, mostrando la fragilidad de las cadenas de suministro y la creciente dependencia en productos críticos de terceros estados no europeos.

En los últimos años se han desarrollado numerosas iniciativas para abordar la mitigación de las excesivas dependencias europeas del exterior. No sin razón, la autonomía estratégica abierta es uno de los pilares de la Presidencia española del Consejo de la Unión Europea. Este matiz de apertura supone que el objetivo principal se encuentra en garantizar la capacidad de hacer frente a las crisis en solitario si es necesario, pero sin descartar la cooperación siempre que sea posible. No se puede olvidar que Europa también forma parte de la Alianza Atlántica y mantiene estrechos lazos de cooperación con el resto de sus miembros, especialmente Estados Unidos.

Algunas de estas iniciativas tienen su foco en la cadena de suministro de la industria de defensa, puesto que es indispensable mantener control sobre la misma para poder asegurar la provisión de sistemas y otros medios imprescindibles a las FAS para la correcta consecución de sus objetivos.

3.1. Cadenas de Suministro Seguras y Sostenibles

Para garantizar el desarrollo y mantenimiento de capacidades críticas para la defensa y la seguridad nacional se requieren cadenas de suministro robustas, resilientes y seguras.

Las cadenas de suministro son cada vez más globales e interconectadas, lo que da lugar a numerosas dependencias y vulnerabilidades. La crisis del Covid-19 ya subrayó la dependencia de suministradores externos y la fragilidad de las cadenas de suministro globales.

La reciente Estrategia Industrial Europea de Defensa (EDIS) y el Programa Europeo de la Industria de Defensa (EDIP) incluye un conjunto de medidas para reforzar la industria de defensa y mejorar la seguridad de suministro europea. Cabe resaltar la importancia que cobra la seguridad de las cadenas de suministro de componentes críticos para la defensa en ambas iniciativas, dedicándole el EDIP un capítulo que detalla acciones enfocadas a la preparación, explorando adquisiciones anticipadas o certificaciones cruzadas; a la vigilancia y monitorización de las cadenas de suministro, contemplando mapeos de las cadenas de suministro e indicadores de alerta temprana; y a la prevención y mitigación de crisis de suministro, mediante, por ejemplo, priorización de pedidos de defensa, así como otras disposiciones para declarar estados de crisis de suministro.

El Plan de Acción para la Producción de la Defensa de la OTAN también contempla acciones dirigidas a proteger las cadenas de suministro de la Alianza, abordando desde componentes de microelectrónica a municiones.

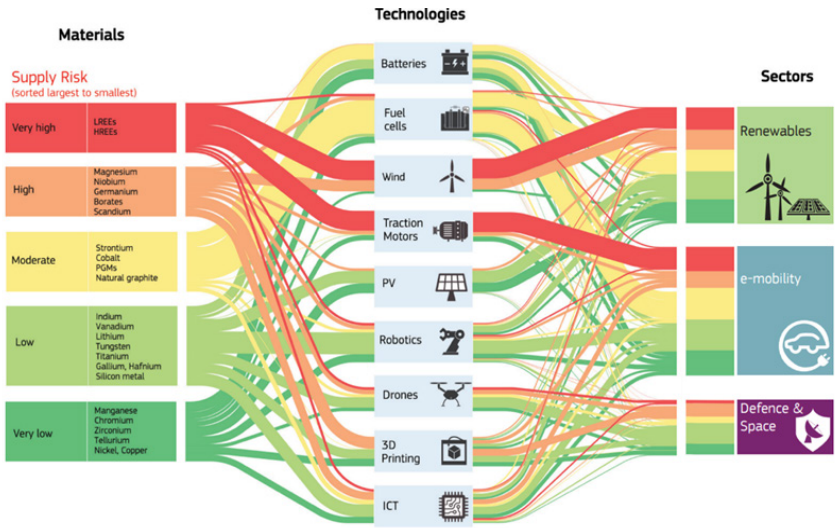


Figura 3.Representación semicuantitativa de los flujos de materias primas y sus riesgos actuales de suministro a las nueve tecnologías y tres sectores seleccionados. Fuente: EU Joint Research Centre. 2020. "Critical Raw Materials for Strategic Technologies and Sectors".

3.1.1. Reto para el Planeamiento Militar

El camino hacia una economía descarbonizada y los procesos de digitalización están incrementando la competencia por materias primas, materiales industriales y microelectrónica, y están creando una mayor dependencia de las regiones geográficas que suministran estas materias y tecnologías.

La UE ya predice que materias primas como por ejemplo el litio, necesario para la fabricación de baterías, están ganando cada vez más importancia por su criticidad para la transición de combustibles fósiles a energías limpias. En 2022, la UE estimó que, para cumplir con los compromisos climáticos adquiridos en 2050, y teniendo en cuenta únicamente los sectores de energías renovables y e-movilidad, necesitaría hasta 60 veces más litio y 15 veces más cobalto en comparación con los niveles actuales [3]. Las recientes iniciativas de aumento de la producción en sistemas de defensa también incrementan necesariamente la demanda de materias primas críticas (CRM, por sus siglas en inglés). La dependencia de Europa en CRM es muy elevada, llegando incluso a la dependencia total en tierras raras. Y no sólo hay que tener en cuenta la dependencia de países que poseen las reservas, sino también de qué países poseen las fases de minado, refinería o procesamiento. Así, la dependencia se agrava al tener en cuenta el predominante papel de China como único suministrador en la mayoría de las CRM.

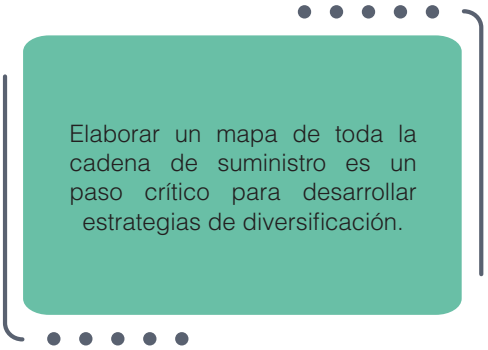
El avance de las EDT también influirá en los niveles de demanda de diferentes materias primas, al estar muchas de estas tecnologías en bajos niveles de madurez tecnológica (TRL) no hay certeza de que la oferta pueda mantenerse a la altura de la demanda.

En la figura 3 se puede apreciar cómo la mayoría de los materiales necesarios para desarrollar EDT fluyen hacia sectores civiles como el de las energías renovables y la movilidad eléctrica. Esto se encuentra estrechamente relacionado con el bajo volumen de los pedidos de defensa mencionado anteriormente, la descarbonización y la aceleración de innovaciones tecnológicas por parte del sector civil complican el aseguramiento de ciertos componentes críticos tanto en tiempo como en disponibilidad.

El aumento de la producción de municiones como respuesta al conflicto en Ucrania también han disparado la demanda de materiales energéticos, especialmente altos explosivos y propelentes, que representan un eslabón fundamental de la cadena de valor en la producción de municiones. La escasez o cuellos de botella de estos elementos están considerados uno de los riesgos más críticos para la producción de municiones. La continuación de los esfuerzos por aumentar la producción de capacidades de defensa, bien sean consumibles o sistemas más complejos, resultará inevitablemente en tensiones en los suministros de materias primas críticas y otros productos esenciales como la microelectrónica.

3.1.2. La Necesidad de Identificar la Cadena de Suministro

Para poder asegurar las cadenas de suministro y su resiliencia, éstas deben estar correctamente identificadas, trazadas y evaluadas, lo cual implica conocer los suministradores no sólo Tier 1 a 3, sino también al resto de niveles. La pérdida de capacidades incluso en los niveles más bajos de la cadena de suministro puede conllevar implicaciones negativas para los productos finales si no son controladas adecuadamente.



Al identificar posibles vulnerabilidades y fuentes alternativas de suministro, se puede desarrollar una cadena de suministro más sólida y eficiente que pueda resistir mejor las interrupciones y suministrar los bienes y servicios necesarios para la defensa.

3.1.3. El Papel de las Pymes y Start-Ups

La BITD se caracteriza por la presencia de numerosas PYMEs dentro de las cadenas de suministro que aportan capacidades esenciales y contribuyen de manera muy relevante a la innovación y al desarrollo de tecnologías de vanguardia. Sin embargo, ante una crisis, las PYMEs deben enfrentarse a mayores problemas de liquidez para poder mantener su actividad, lo que las hace más vulnerables.

Estas empresas están también más expuestas a inversiones de agentes estatales o no estatales con intereses que no están necesariamente alineados con la seguridad nacional; las inversiones extranjeras directas (IED), que suelen estar relacionadas con el crecimiento de las empresas y el acceso a nuevas tecnologías, pueden, especialmente en el caso de fusiones y adquisiciones, suponer un riesgo por la consecuente externalización de puestos de trabajo, pérdida de control sobre las cadenas de suministro, pérdida de control sobre el proceso de toma de decisiones, o transferencias de tecnología. Esto es especialmente relevante en el caso de start-ups tecnológicas en ámbitos altamente innovadores.

Uno de los mecanismos más efectivos para prevenir los riesgos asociados con las IED en las PYMEs y start-ups es la realización de una revisión exhaustiva de la inversión antes de aprobarla, la cual incluye una evaluación de los posibles riesgos asociados con la inversión, la tecnología y propiedad intelectual de la empresa, y el posible impacto en la seguridad nacional.

3.1.4. La Importancia de Asegurar los Sistemas Heredados

Otro aspecto relevante relacionado con la pérdida de capacidades es el abandono de la importancia de los conocidos como legacy systems o sistemas heredados. Los sistemas heredados son sistemas antiguos que siguen siendo utilizados por el usuario y no se quiere o no se pueden reemplazar o actualizar de forma sencilla. Se trata de sistemas con capacidades consolidadas que dan buenos resultados y que podrían paliar problemas de interoperabilidad en casos de crisis.

En la actual carrera tecnológica, con el objetivo de obtener sistemas en el estado del arte cada vez más innovadores, estas capacidades tienden a perderse por no ser consideradas críticas o esenciales. El foco en las EDT también actúa en detrimento de estos sistemas, cuyas capacidades tienden a perderse por no dar continuidad a los perfiles específicos que se necesitan. Además, la inversión o adquisición de las empresas que crean estos sistemas heredados no suelen estar controladas, por no ser altamente innovadoras ni estar en el foco de atención. Sin embargo, el mantenimiento de las capacidades que permiten la fabricación de estos sistemas con elevada tasa de respuesta ante situaciones de crisis resulta esencial para evitar una pérdida de capacidad de reacción.

3.1.5. La Problemática de la Certificación

Tanto la dualidad de los suministradores de defensa, como la implementación de tecnologías civiles en sistemas de defensa suponen un reto con respecto a los robustos procesos de certificación de productos de defensa.

A medida que el sector civil, no acostumbrado a estos estrictos requisitos de seguridad, toma la delantera, los criterios comerciales prevalecen sobre los de seguridad en el diseño tanto de hardware como de software. Esto dificulta los procesos de certificación y puede comprometer la cadena de suministro, especialmente en la prestación de servicios esenciales o críticos.

Por otro lado, y en general, estos procesos de certificación, que conllevan largos periodos de tiempo, suponen también un reto ante situaciones de disrupciones de las cadenas de suministro, por la imposibilidad de certificar nuevos proveedores de manera rápida y eficaz para evitar retrasos o cuellos de botella, o, ante situaciones de cierres de fronteras, como es el ejemplo de la crisis del Covid-19, el impedimento de envío de pedidos que debían ser certificados por clientes extranjeros en las instalaciones del fabricante o el cliente.

Si bien la criticidad de equipos y sistemas del sector hacen necesario que exista un mayor control de la calidad y seguridad de los productos, estas circunstancias restan flexibilidad ante un incremento de la capacidad productiva.

Table 1: Inventory Replacement Times for Key Systems

	Number transferred to Ukraine	Production rate (year)	Manufacturing lead time (months)	Production time (months)	Total time to rebuild (months)
155 mm ammunition (recent rate)	1,074,000	93,000	Inventory rebuild not possible because of U.S. training requirements		
155 mm ammunition (surge rate)	1,074,000	240,000	12–18	44	59 (5 years)
155 mm precision munition—Excalibur (recent rate)	5,200	1,000	22	56	84 (7 years)
155 mm precision munition—Excalibur (surge rate)	5,200	2,400	22	23	48 (4 years)
Javelin (recent rate)	8,500	1,000	24	12	149 (~8 years)
Javelin (surge rate)	8,500	2,100	24	12	56 (~5.5 years)
HIMARS (recent rate)	20	20	26	12	37 (3 years)
HIMARS (surge rate)	20	72+	26	5	30 (2.5 years)
GMLRS (recent rate)	"Thousands"	5,000	17+	?	?
GMLRS (surge rate)	"Thousands"	10,000+	17+	?	?
Stinger (recent rate)	1,600	100?	24+	192	216 (18 years)
Stinger (historical rate)	1,600	350?	24+	55	79 (6.5 years)

Color Key

- **Unlikely to rebuild inventories within five years**
- **Inventory replacement within five years at low risk**
- **Rebuilding timeline unclear but substantial risk of low inventories and long replacement cycles**

Source: Author's analysis based on multiple sources.

CSIS | INTERNATIONAL SECURITY PROGRAM

Figura 4. Tiempos de reposición del inventario de sistemas clave del Departamento de Defensa de EEUU Fuente: Cancian, Mark. 2023. "Rebuilding U.S. Inventories: Six Critical Systems" CSIS.

3.2. Retos Industriales ante los Aumentos de Producción y Reservas de Capacidades

Durante las últimas décadas, el planeamiento en Europa ha estado centrado en operaciones de estabilización, mantenimiento de la paz, o lucha contra el terrorismo. El estallido de una guerra de alta intensidad en Europa ha puesto de relieve una serie de retos como la necesidad de aumentar rápidamente los stocks de ciertas capacidades, como la munición, o la necesidad de contar con reservas de capacidades estratégicas.

Desde el punto de vista industrial, el aumento de la producción conlleva a su vez desafíos como la necesidad de gestionar a los proveedores con volúmenes de demanda que no habían sido previstos, problemas en habilitar o crear la infraestructura necesaria para un aumento considerable de la producción, así como la adquisición y retención del personal necesario para llevarlo a cabo.

A modo ilustrativo, la tabla anterior refleja los tiempos de reposición necesarios para reponer los sistemas clave transferidos desde EEUU a Ucrania. La producción "recent" se refiere a los niveles financiados en los últimos años, mientras que la producción "surge" refleja los índices más altos allí donde el Departamento de Defensa ha manifestado que aumentaría la producción. El plazo de fabricación ("manufacturing lead time") considera el periodo que transcurre entre la firma de un contrato y la llegada del primer artículo, el cual suele ser un intervalo de dos años, variable según el sistema. El tiempo de producción ("production time") se refiere al tiempo que se tardaría en producir todo el inventario necesario, y el tiempo total de reconstrucción ("total time to rebuild") incluye tanto el plazo de fabricación como el de producción. Un aspecto interesante a destacar es el hecho de que la producción aplicada a la reposición de inventarios de munición de 155mm debe tener en cuenta las necesidades de entrenamiento de tiro de las FAS [4].

Con el fin de mantener una reserva de capacidades, se pueden valorar opciones como el almacenamiento de stock o el mantenimiento de una línea de producción "ever-warm". Esto conlleva una planificación logística, financiera, e incluso legal que debe ser evaluada para balancear los costes y los beneficios. Por ejemplo, el mantenimiento de una línea de producción "ever-warm", la cual se mantendría continuamente latente y se activaría bajo demanda, requeriría una colaboración público-privada para poder mantenerse activa aún sin volumen de demanda, o mayor certidumbre para poder acometer tal inversión. Este tipo de líneas de producción serían de gran utilidad para los sistemas de defensa considerados como críticos a la hora de afrontar una crisis. El almacenamiento de stock también implica cuestiones logísticas a evaluar, como la mencionada habilitación de la infraestructura. En el caso de las municiones, por ejemplo, los polvorines están altamente regulados [5], lo cual complica el establecimiento de nuevos polvorines.

Otra problemática asociada al aumento de la producción pueden ser las pruebas de los sistemas. Ya se han registrado retrasos en instalaciones de pruebas, lo cual puede exacerbarse en el caso de un aumento drástico de la producción, resultando contraproducente al incurrir en retrasos de cualquier manera.

Por último, hay que valorar la capacidad financiera de los países, ya que un incremento de la producción puede incurrir en elevados costes que exija una planificación a medio y largo plazo que establezca unos objetivos y dote del respaldo financiero necesario.

3.3. La Importancia de la Estandardización e Interoperabilidad

3.3.1. La Estandardización como Medio para Lograr la Interoperabilidad

Como se ha mencionado anteriormente, la fragmentación de la industria de defensa resulta en un elevado número de sistemas de defensa –como se puede apreciar en la Figura 1, la UE tiene alrededor de 178 sistemas de armas distintos, mientras que EEUU cuenta con 30-. Esto revierte en vulnerabilidades como la que se ha visto durante el conflicto de Ucrania, que ha demostrado la criticidad de la interoperabilidad y estandardización de sistemas de defensa como los de artillería y municiones –dentro de los envíos de material a Ucrania se han contabilizado casi una decena de sistemas de artillería con el mismo calibre, pero ninguno intercambiable.

3.3.2. La Interoperabilidad y las Adquisiciones Conjuntas

La estandardización e interoperabilidad también es relevante a la hora de las iniciativas de compras e inversiones conjuntas lanzadas a raíz de la Declaración de Versalles (2022), que estableció la Ley de adquisición común (EDIRPA, por sus siglas en inglés) para 2022-2024, un instrumento a corto plazo para reforzar las capacidades industriales europeas de defensa mediante la adquisición conjunta por parte de los Estados miembros de la UE, y el futuro Programa Europeo de Inversión en Defensa (EDIP, por sus siglas en inglés).

La interoperabilidad es importante para estas iniciativas puesto que los proyectos conjuntos de adquisición de defensa a menudo involucran la integración de sistemas y equipos de diferentes países. Si estos sistemas no pueden trabajar juntos de manera efectiva, se corre el riesgo de incompatibilidades técnicas que pueden obstaculizar la operatividad y la eficacia de las fuerzas armadas. Por lo tanto, la interoperabilidad debe ser una consideración clave en la planificación y ejecución de proyectos de adquisición conjunta.

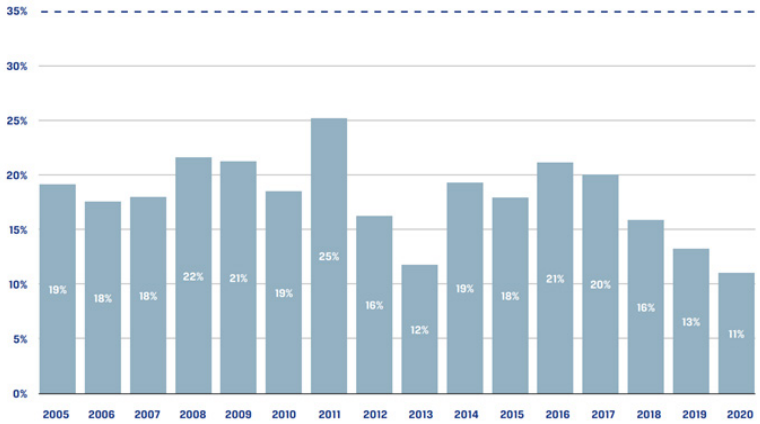


Figura 5. Adquisición colaborativa europea de equipos de defensa en porcentaje de la adquisición total de equipos de defensa (European Defence Agency, 2020. "Defence Data 2019-2020")

3.3.3. Estándares y EDT

El desarrollo, ratificación y promulgación de estándares debe estar alineado con el ritmo de la rápida innovación del sector privado, sobre todo en el desarrollo de EDT. Esto es especialmente relevante si se tiene en cuenta el extendido uso de COTS y software de fuentes abiertas, mencionado anteriormente.

Es altamente recomendable potenciar la creación de procesos de aprobación de suministradores que incorporen diversos estándares establecidos. En el caso de ciberseguridad, por ejemplo, al afectar los ciberataques a todas las fases del ciclo de vida del producto, todos los actores deberían implementar estándares tecnológicos a prueba de hackeos a lo largo de toda la cadena de suministro para hacer el ecosistema industrial más seguro.

4. CONCLUSIONES

LA INDUSTRIA COMO PILAR DE DEFENSA

El sector industrial de la defensa es un sector altamente vinculado a la soberanía nacional y por tanto se encuentra fuertemente intervenido y regulado, lo cual genera alta competencia entre las empresas y fomenta políticas proteccionistas por parte de los Estados.

Además, a nivel europeo la BITD está fragmentada y jerarquizada, además de estar centrada en los países más grandes, lo cual revierte en ineficiencias y una debilidad comparativa frente a competidores como los Estados Unidos, que cuentan con un sector más homogéneo.

A raíz de la situación geopolítica actual, se está impulsando el desarrollo de proyectos colaborativos de investigación y desarrollo de capacidades. Con el objetivo de alcanzar un posicionamiento ventajoso en la denominada Europa de la Defensa, se han venido produciendo, hace ya años, movimientos tanto de agrupación de empresas en torno a consorcios, como de fomento de creación de campeones nacionales que obtengan mayor peso en los programas colaborativos.

Un sector de estas características exige contar con una estrategia industrial de defensa que defina las capacidades y tecnologías consideradas prioritarias de manera que las industrias puedan realizar inversiones más eficientes.

El papel del Ministerio de Defensa dentro de la Administración es la de aplicación de la política de Defensa determinada por el Gobierno y la gestión de la Administración militar. La política de Defensa establecida por la Directiva de Defensa Nacional (DDN) de 2020 indica, como directrices de actuación, el fortalecimiento de la industria de defensa nacional y el desarrollo de una BITD europea. Estos objetivos se describen como prioritarios, así como el aseguramiento de que los sistemas empleados por las FAS se encuentran en la vanguardia tecnológica. Como se describe en la DDN, la industria está ligada a las capacidades de las FAS y por tanto disponer de una BITD competitiva repercute directamente en las mismas.

Además, se puede considerar a la industria como un pilar dentro de las políticas de defensa por su contribución a la autonomía estratégica y por su aportación a la Europa de la Defensa. De forma adicional, la inversión en industria de defensa aporta beneficios como:

- Potencia el desarrollo industrial y tecnológico de las empresas al tratarse de un sector muy competitivo, lo que implica que hay que alcanzar estándares elevados para participar.
- Genera un empleo de calidad, con personal altamente cualificado y con una productividad por encima de la media nacional.
- Se obtiene un alto retorno económico de las inversiones realizadas, tanto por las inversiones nacionales como por las exportaciones, ya que es un sector donde el volumen de exportaciones unido a los programas cooperativos supone el 80% de la facturación.
- Constituye un elemento de cohesión, ya que la BITD se encuentra repartida por el territorio nacional.

LA IMPORTANCIA DE LAS EDT EN EL ESCENARIO ACTUAL

La implantación de las EDT en la industria de defensa para su uso posterior en las operaciones militares supone una serie de retos importantes desde el punto de vista industrial. El primer aspecto sería que debe existir una visión compartida entre los gobiernos y las empresas sobre las capacidades en las que se debe focalizar el desarrollo, ya que la investigación y el desarrollo de estas tecnologías suponen unos costes y tiempos muy elevados, y por lo tanto un reto para la industria. Por ello, un objetivo es realizar una gestión eficaz, balanceando los niveles de innovación y la agilidad de las empresas para cubrir las demandas operativas con la eficiencia en el uso de las inversiones.

Otro aspecto a tener en cuenta es la seguridad. A medida que la tecnología avanza, lo hacen también las amenazas cibernéticas. Por ello la industria de defensa debe mantenerse a la vanguardia en términos de ciberseguridad, con políticas como la de Zero Trust y focalizando la atención en los riesgos que supone aspectos como el uso de software COTS.

Todas estas necesidades no podrán ser cubiertas sin una industria capaz de afrontar estos retos y para ello se necesita además de una inversión y gestión acordes, un conocimiento técnico que es necesario captar, formar y mantener para que pueda producirse el desarrollo de estas tecnologías y su posterior traslado al escenario de operaciones. Esto está siendo un problema en la actualidad en el sector de defensa, por lo que la continuidad en las inversiones que suponga un marco estable para las empresas ayudará a potenciar, consolidar y retener estos perfiles.

LA IMPORTANCIA DE LA AUTONOMÍA ESTRATÉGICA EN MATERIA DE DEFENSA

La voluntad europea y española de asegurar autonomía estratégica en sus sectores claves, como la defensa, parte de la necesidad de los Estados de poder dar una respuesta sin dependencias de terceros a las crisis multidimensionales a las que se enfrentan. Esto es, tener autonomía de acción y autonomía de decisión ante la globalización e interrelación de las cadenas de suministro mundiales.

En los últimos años se han desarrollado numerosas iniciativas para fortalecer la industria de defensa europea, la creación de la Cooperación Estructurada Permanente (PESCO), los Fondos Europeos de Defensa (EDF), el Fondo Europeo para la Paz (EPF), o las recientes Ley de Adquisición Común (EDIRPA) y Reglamento de Apoyo a la Producción de Municiones (ASAP), y el Programa Europeo de la Industria de Defensa (EDIP). Sin embargo, abordar los retos anteriormente mencionados -asegurar las cadenas de suministro desde las materias primas hasta los productos finales, fomentar la certificación, estandardización e interoperabilidad, o vigilar las consecuencias de la inversión directa extranjera- resulta crucial para poder afianzar un sector industrial de la defensa seguro y resiliente.

Como ejemplos de la importancia de la autonomía estratégica, encontramos los retos industriales que ha planteado la guerra en Ucrania como el repentino aumento de la demanda de producción de munición, que plantea serios problemas en las cadenas de producción, la problemática de la interoperabilidad de los sistemas de armas, o el planteamiento de establecer reservas de capacidades estratégicas para hacer frente a futuras crisis.

¿QUÉ DEBEN HACER EUROPA Y ESPAÑA EN ESTE CONTEXTO?

A nivel nacional, el primer paso a acometer y que ha sido altamente demandado tanto por la industria como por las FAS es asegurar un escenario de estabilidad presupuestaria que permita realizar planificaciones a medio y largo plazo y a la BITD contar con un horizonte donde las reglas del juego estén definidas. Este escenario está en vías de instauración con la intención de alcanzar una inversión en defensa del 2% del PIB para el año 2029 en virtud de los compromisos alcanzados con la OTAN, tal y como señala la Estrategia Industrial de Defensa (EID) 2023.

La EID es la respuesta del Ministerio de Defensa hacia muchos de los retos y desafíos ilustrados en este apartado industrial. A partir de los objetivos que fija la EID: incremento de la autonomía estratégica en materia de defensa, contribución a la Europa de la Defensa y consolidación de una BITD competitiva y sostenible, se definen diez ejes de aplicación con sus líneas de acción correspondientes.

Los dos primeros ejes giran en torno a las denominadas Capacidades Industriales Estratégicas para la Defensa (CIED) y cómo establecer políticas para su potenciación y desarrollo en los programas de Armamento y Material, factor que contribuye a lograr aumentar la autonomía estratégica.

El tercer eje propone como herramienta para el desarrollo de las CIED el lanzamiento de programas transversales multiplataforma que incluyan a distintos subsectores dentro del sector defensa. Para lograr este objetivo, el cuarto eje argumenta que es crucial la creación de consorcios y alianzas tanto a nivel nacional como europeo, con el propósito de asentar a la industria de defensa como un pilar en las políticas de Defensa y Seguridad en Europa. Todas estas medidas ofrecen beneficios indudables a nivel nacional, como se refleja en el quinto eje, suponiendo un instrumento vertebrador y de crecimiento a nivel territorial.

El sexto eje afronta el reto digital y de las nuevas tecnologías, mientras que el séptimo eje aborda la problemática de atraer y retener talento, y cómo un sector puntero en tecnología y desarrollos puede servir de polo de atracción de talento al tiempo que promueve y difunde la cultura de defensa.

Para finalizar, los últimos tres ejes recogen acciones a nivel de gestión para lograr una implementación más efectiva de todas las políticas y medidas propuestas. Ello requiere la colaboración entre los organismos gubernamentales, una propuesta hacia el exterior conjunta y coordinada, y un diálogo constante y fructífero con la industria y principales actores del sector.

Una vez se cuenta con estabilidad presupuestaria, España debe ser un actor protagonista en la construcción de la Europa de la Defensa, basándose en la estrategia industrial difundida, en la que se establecen las capacidades que se consideran estratégicas en cada subsector, fomentando la potenciación de consorcios y uniones que hagan más competitiva a nuestra industria en el entorno europeo. La industria española de la defensa debe poder dotar a las FAS de los sistemas y equipos que les son necesarios, logrando una posición destacable en los programas europeos e incrementando el volumen de las exportaciones.

Así como para España es fundamental el posicionamiento de su industria en el panorama europeo, para el continente es primordial el fortalecimiento de una industria robusta y acorde a los objetivos establecidos en las políticas de la Unión, que permita tanto de disponer de las capacidades necesarias para cumplir con las operaciones de defensa y seguridad como de reducir en el máximo de lo posible las dependencias externas de otros actores relevantes en el panorama internacional y que pueda llegar a comprometer la soberanía de los estados europeos.

El fortalecimiento de la UE es también el fortalecimiento del pilar europeo de la OTAN. La autonomía estratégica abierta que España ha tenido como prioridad durante su presidencia del Consejo de la UE ratifica esta noción. Europa, y España, deben ser conscientes de sus necesidades operacionales estratégicas, así como de sus carencias y limitaciones, para poder definir qué capacidades deben desarrollar nacionalmente, cuáles en cooperación con otros Estados Miembros europeos, y cuáles adquirir directamente a terceros estados, de la Alianza Atlántica o externos a la misma.

REFERENCIAS

[1]. Instruction n° 2067/ARM/CAB/CC6 relative à l'innovation de défense au sein du ministère des armées. Du 07 mai 2020.

[2]. European Union Parliament Briefing (2022) "EU strategic autonomy 2013-2023: From concept to capacity".

[3]. Servicio de Investigación del Parlamento Europeo (2023) Briefing: "Securing Europe's supply of critical raw materials".

[4] Servicio de Investigación del Parlamento Europeo (2023) Briefing: "Securing Europe's supply of critical raw materials".

[5] Real Decreto 130/2017, de 24 de febrero, por el que se aprueba el Reglamento de Explosivos.

BIOGRAFÍAS

YOLANDA JAÉN GONZÁLEZ

Es licenciada en Física Aplicada por la Universidad Autónoma de Madrid (UAM), posee un M.B.A. Industrial por la E.O.I. y ha cursado un Programa de Desarrollo Directivo (PDD) en ESADE. Tiene más de 20 años de experiencia en el sector de la defensa, especialmente en el ámbito de la cooperación y estrategia industrial. Su vida laboral la inició en 1999 en la Gerencia de Cooperación Industrial - ISDEFE participando en la gestión y negociación de la cooperación industrial de los principales programas de adquisición del MINISDEF. Desde 2009 desempeña la coordinación de los contratos no solo con el MINISDEF sino con otros Gobiernos y Organismos internacionales (Ministerio de Defensa del Perú, Agencia Europea de Defensa, DGDEFIS, etc.) relativos al análisis de capacidades industriales de las empresas del sector de defensa, definición de estrategias y políticas industriales, gestión de la participación industrial en programas, etc. Desde 2022 es la Jefa del Área de Gestión Industrial de Isdefe liderando los proyectos relacionados con el conocimiento y gestión industrial del sector de la defensa.

ROCÍO MORA PICAZO

Es consultora en Isdefe y Máster en Estudios Estratégicos y Seguridad Internacional por la Universidad de Granada. Es también diplomada en Altos Estudios de la Defensa Nacional por el Centro Superior de Estudios de la Defensa Nacional (CESEDEN).

Durante los últimos cuatro años ha trabajado para la Dirección General de Armamento y Material del Ministerio de Defensa, en particular para la Subdirección General de Inspección, Regulación y Estrategia Industrial de Defensa, la Agencia Europea de Defensa y la Comisión Europea en materia de estrategia industrial de defensa, particularmente en análisis industriales y de mercado de la defensa y en aseguramiento de las cadenas de suministro.

Previamente, trabajó para el Departamento de Operaciones de Paz de Naciones Unidas, en la Oficina de Estado de Derecho e Instituciones de Seguridad, y para el Consejo de Europa.

.

SERGIO VICENTE LÓPEZ

Es ingeniero naval y oceánico por la Universidad Politécnica de Madrid. Gran parte de su vida profesional ha estado ligada al ámbito de la defensa y seguridad. Se unió a Isdefe en junio de 2014, en el Área de Cooperación Industrial para participar en la gestión industrial de los programas navales. En noviembre de 2014, pasó a trabajar para la Armada en la Jefatura de Apoyo Logístico, concretamente en la Oficina de Certificación de Submarinos, donde colaboró en la implantación y desarrollo de este programa de seguridad para la plataforma y la dotación, que es una adaptación del programa Subsafe de la marina americana desde hace más de 60 años, con la cual tuvo la oportunidad de formarse y trabajar estrechamente con el objetivo de aplicar la experiencia y los conocimientos adquiridos en el mismo.

En mayo de 2022 volvió a involucrarse en lo relacionado con la gestión industrial, uniéndose al equipo de apoyo técnico para la subdirección de INREID de la DGAM, donde ha estado vinculado principalmente a la parte de Estrategia Industrial de Defensa y al conocimiento industrial. Relacionado con el mundo de la Defensa también, tuvo la oportunidad de formar parte de la VII promoción del curso de Defensa Nacional para jóvenes impartido en el CESEDEN.

Además, tiene un gran interés por la gestión de proyectos donde posee certificaciones como el PMP, Prince 2 o PM2.


0806 / 52 EBK
14.687
8.904
2.653
85-12-54-20
YU-Qi-p0-AW
651.32
667.43
286
70
YU 07/26
193.94
14.687
152 68

RETOS DE FUTURO Y CONCLUSIONES

Si se presta atención a la evolución de los presupuestos de defensa en el mundo, y particularmente los europeos, puede observarse un cambio de tendencia en los últimos años, con un progresivo incremento. En la raíz de las causas podemos intuir la creciente competencia por los recursos naturales y el control de los medios de producción y suministro de bienes y servicios, lo cual está generando tensiones en diversas regiones del mundo. Particularmente, grandes economías en desarrollo como China, caracterizadas por una demanda constante de recursos para mantener sus índices de crecimiento económico, están provocando una alteración en los estándares tradicionales que han venido rigiendo el orden internacional en las últimas décadas.

La velocidad sin precedentes a la que se están produciendo los avances tecnológicos no hace sino potenciar esta competencia por los recursos de una manera rápida y, en muchos casos, impredecible. En efecto, estos avances tecnológicos están permitiendo que actores estatales y no estatales se esfuercen por consolidar su posición en este nuevo escenario mediante métodos muy diferentes a los que tradicionalmente se habían venido empleando.

Así, donde antes el conflicto armado era la herramienta política principal cuando la diplomacia fallaba ante una crisis de seguridad entre naciones, actualmente vemos que se trata de un elemento más dentro de toda una combinación de estrategias y técnicas (políticas, económicas, comerciales, demográficas o sociales) en favor de los intereses de un estado o país.

Cada vez más, la dicotomía tradicional entre guerra y paz se convierte en un estado de competencia continuo donde existe una "zona gris" que se amplía continuamente, en la que la forma de actuar puede llegar a ser altamente imprevisible. Por otra parte, en este nuevo entorno geoestratégico, las normas y estructuras tradicionales en materia de orden internacional, incluyendo organizaciones como la ONU, la UE o la OTAN y convenios y acuerdos como los asociados al derecho internacional humanitario, se encuentran con dificultades para responder a la complejidad y la incertidumbre del escenario mundial contemporáneo.

En todo este contexto, es crucial que las Fuerzas Armadas de los países desarrollados estén en condiciones de adaptarse e incluso de repensar el papel más apropiado que deben asumir para garantizar el desempeño adecuado de sus cometidos. Esto implica entender la evolución del escenario geoestratégico e interiorizar el rápido avance tecnológico en la organización y, particularmente, en las capacidades militares.

Esta adaptación trae consigo la redefinición de estrategias, doctrinas y organización, así como la modernización de los medios y recursos para aprovechar de manera adecuada las nuevas tecnologías. Todos estos cambios deben abordarse tanto desde un punto de vista estructural como conceptual.

El presente cuaderno muestra un estado general de las capacidades militares en el ámbito europeo frente a las de otros países y cuáles son los retos principales que se identifican para las Fuerzas Armadas, con el fin de posicionar adecuadamente a la UE en el nuevo escenario geoestratégico global. Como consecuencia de este trabajo, los principales desafíos a los que se enfrenta la UE se pueden catalogar en cuatro grandes grupos.

Diferentes perspectivas de la amenaza por parte de los países europeos. Existe claramente una falta de concepción de amenaza común a nivel europeo, con inquietudes de seguridad diferentes y manteniendo todavía muchas amenazas "no compartidas" entre los estados europeos.

Procesos de planeamiento desincronizados. Se puede ver cómo, aunque la amenaza fuese común, los procesos de planeamiento de identificación y priorización de las capacidades necesarias para enfrentarla se encuentran desincronizados entre los países europeos. Y no solo se trata de acompasarlos temporalmente, sino de dimensionar y armonizar los niveles de esfuerzo, los criterios y procesos de aprobación y viabilidad financiera, así como el acuerdo para una estrategia común de desarrollo de capacidades que podría incluso pasar por asumir una especialización por estados o conjuntos de estados en el desarrollo de sistemas militares.

La industria de defensa. La industria desempeña un papel cada vez más relevante en el desarrollo de los sistemas militares. Por un lado, debe continuar proveyendo el armamento y materiales necesarios de forma que se mantenga una autonomía estratégica nacional y europea, pero por otro, se enfrenta al complicado desafío del componente dual de las nuevas tecnologías digitales. Esta dualidad trae nuevos competidores y nuevas reglas de mercado a las que el sector de la defensa no se encuentra acostumbrado.

No debe perderse de vista que el desarrollo tecnológico asociado a estas tecnologías digitales está principalmente en manos del sector civil, lo cual plantea cuestiones sobre la soberanía efectiva que tienen los estados y la forma de ejercerla. Grandes empresas tecnológicas acaban siendo las propietarias de los datos, los algoritmos y los sistemas de comunicaciones, lo cual las convierte en las verdaderas fuentes de poder en el entorno digital.

Esto exigirá que los suministradores tradicionales de armamento y material militar deban acostumbrarse a la entrada en el mercado de otros competidores con un fuerte componente digital. A su vez, los estados deberán ser capaces de desarrollar los acuerdos de seguridad adecuados con estos suministradores, de forma que los intereses de unos y otros se mantengan siempre alineados, incluso en casos de conflicto bélico, y se mantenga la autonomía estratégica que aporta la industria como capacidad nacional.

Impacto económico de las nuevas tecnologías. Otro aspecto fundamental relacionado con la tecnología es que, si bien ésta es cada vez más accesible para la sociedad en general, el coste de integrarla en sistemas de armas complejos de forma segura y resiliente es cada vez mayor. La UE debe ser consciente del impacto que en los presupuestos de defensa tiene el hecho de que las nuevas generaciones de sistemas de armas incrementarán su coste de forma significativa a lo largo de todo su ciclo de vida.

Desde un punto de vista conjunto-combinado, los principales retos identificados se orientan al desarrollo de la capacidad de combate en el multidominio; a la adecuada convivencia de sistemas de armas de diferentes generaciones y fabricantes a lo largo de Europa; a mantenerse en el primer orden mundial en el desarrollo de nuevos tipos de armamento, incluyendo el componente ciber, los sistemas de armas autónomos, el desarrollo de capacidades espaciales, el armamento de hipervelocidad o de energía dirigida.

En algunos casos resulta crucial abordar la obsolescencia de los sistemas de defensa, reducir la brecha entre sistemas de vieja y nueva generación, y rebajar o eliminar la dependencia de sistemas de la antigua Unión Soviética en determinados países.

Uno de los aspectos más relevantes, en relación con el combate multidominio, se refiere a la evolución de las capacidades ISR en un entorno de constante digitalización y con una creciente cantidad de datos e información a explotar. Esto requiere un aumento de los sistemas y plataformas de reconocimiento y vigilancia en todos los ámbitos para identificar elementos hostiles, dirigir los movimientos de las tropas y evitar daños colaterales.

Gestionar grandes volúmenes de datos, difundir información desde las plataformas de vigilancia hasta los centros de toma de decisión o integrar inteligencia proveniente de múltiples fuentes son también desafíos críticos en las operaciones modernas de vigilancia.

En este ámbito, el desarrollo de la nube de combate y la integración de múltiples tipos de plataformas (aéreas, espaciales, terrestres o marítimas) tanto tripuladas como no tripuladas, presentan desafíos significativos. Estos van desde la propia definición del concepto de nube de combate, hasta la integración técnica de las tecnologías adecuadas, pasando por la adaptación de las doctrinas, tácticas, técnicas y procedimientos, que adquieren especial relevancia en entornos particulares como el combate urbano o el submarino, donde la orografía, los obstáculos físicos o el propio medio dificultan la integración de tecnologías digitales, particularmente de sistemas de comunicaciones con gran ancho de banda.

Cabe destacar que la industria europea de sensores está compuesta por unas pocas grandes empresas capaces de diseñar, fabricar e integrar los sistemas, que, además, adolecen de una dependencia a nivel de componente de países no europeos.

Ante la constante digitalización del campo de batalla y el intercambio de información entre diferentes dominios, será fundamental el desarrollo de las capacidades cibernéticas, tanto ofensivas como defensivas y de inteligencia, vigilancia y reconocimiento, que permitan mantener el resto de las capacidades plenamente operativas.

Relacionado con lo anterior, y dado el creciente uso del espectro electromagnético, resulta también fundamental la mejora de las capacidades de guerra electrónica, incluyendo la neutralización de este tipo de operaciones que pueda realizar el adversario.

Dentro del combate multidominio, resultará fundamental la conceptualización de un entorno de integración entre sistemas tripulados y no tripulados, así como una redefinición de la forma en que el ser humano interactúa en el mismo. Pasar de ser operador de un sistema de armas a comandar una unidad de sistemas autónomos exige una redefinición de las funciones, procedimientos y capacidades del personal.

Finalmente, se incluyen una serie de retos específicos asociados a las capacidades militares, tanto comunes a los cinco ámbitos analizados, como específicos a cada uno de ellos.

CAPACIDADES TERRESTRES

Dentro del ámbito terrestre, cabe destacar la problemática asociada a los materiales acorazados y a su uso en el entorno operativo. Venimos de años en los que se ha puesto en cuestión la necesidad de este tipo de plataformas, sin embargo, los conflictos recientes demuestran que su uso sigue siendo relevante. El análisis de la situación de los vehículos acorazados en la UE muestra una gran diversidad de necesidades y desafíos, incluyendo diferentes plazos de modernización de flotas entre estados, y la necesidad de colaboración en aspectos técnicos que facilite la modularidad y la comunalidad de estas plataformas.

Respecto a la artillería autopropulsada y los sistemas MLRS, la mayoría de las iniciativas e innovaciones provienen de fuera de Europa, lo que plantea fuertes desafíos de autonomía ante la necesidad de modernizar las flotas. El desafío principal para Europa radica en mantener una industria competitiva global y preservar la autonomía estratégica en el desarrollo de plataformas.

Otro aspecto importante que, si bien afecta a otros ámbitos es especialmente relevante en el terrestre, es el que se refiere al uso de armas de precisión guiadas. En los escenarios operativos actuales, con la presencia de amenazas híbridas o el desarrollo de operaciones en entornos urbanos, se incrementa la demanda de armas y proyectiles de precisión.

En consecuencia, los principales desafíos incluyen la integración de las nuevas municiones en las plataformas existentes, la reducción de costes asociados, el desarrollo de innovaciones en guiado para aumentar la precisión y la reducción de la dependencia de sensores no pertenecientes a la UE, como el GPS.

En lo que se refiere a los vehículos terrestres no tripulados existen múltiples retos que deben abordarse desde una perspectiva europea, Estos incluyen aspectos como la definición de conceptos de operaciones comunes, determinación de los niveles de autonomía que se proporciona a los sistemas, o mantener una capacidad tecnológica europea a la altura de otros competidores globales.

Existen claras oportunidades de colaboración a nivel europeo en el desarrollo de regulaciones asociadas al uso de vehículos no tripulados, así como en la identificación de conceptos operativos comunes y formación del personal en el uso y mantenimiento de las plataformas.

En cuanto al combatiente a pie, uno de los retos más destacados es la dificultad de incorporar las tecnologías emergentes sin afectar a la ergonomía y movilidad del soldado. Las dificultades se presentan en muchas ocasiones porque las tecnologías aún no están lo suficientemente maduras para ser implementadas de forma ergonómica o por problemas asociados a la sobrecarga de información. Los factores humanos siguen siendo condicionantes a la hora de implementar la tecnología en los entornos operativos, poniendo de manifiesto la necesidad de encontrar un adecuado equilibrio entre la integración de tecnologías en el combatiente y la operatividad.

CAPACIDADES NAVALES

Si analizamos el ámbito marítimo, éste juega un papel fundamental en el nuevo contexto geopolítico anteriormente descrito. No cabe duda de que el dominio del entorno marítimo sigue siendo crucial para asegurar el suministro de bienes y servicios. En consecuencia, diferentes actores, principalmente estados emergentes, están disputando la hegemonía que ostentan los Estados Unidos en muchas partes del planeta.

Ello se traduce en la aparición de tensiones derivadas de la ambición geográfica por el control de determinadas zonas y puntos estratégicos, un desarrollo tecnológico exacerbado que supere las limitaciones de los medios tradicionales de guerra naval, o el desarrollo de tácticas hibridas que dificulten igualmente el uso de tales medios.

Hasta tal punto es así, que actualmente, se observa un posible cambio de paradigma en las operaciones navales con respecto a las dos últimas décadas. En el presente se baraja la posibilidad de que la guerra naval más 'tradicional', basada en el empleo de la fuerza naval para el dominio y control de rutas, vuelva a cobrar importancia, eso sí, adaptada a los nuevos desarrollos de tecnologías tanto en materia de armamento como de protección de las plataformas. Así, además de la capacidad de proyección de la fuerza naval en tierra, es previsible que deba afrontarse de nuevo el combate propiamente en el mar. Consecuentemente, la readaptación constituye un reto para las fuerzas navales de muchos países occidentales, que ya habían renunciado hace tiempo a este tipo de capacidades específicas.

Lo que sí parece claro en este contexto es que las amenazas asociadas son cada vez más variadas y en constante cambio y evolución. Esto exigirá una capacidad de respuesta cada vez mayor, así como una mayor capacidad de adaptabilidad por parte de las fuerzas navales. Parece cobrar mayor importancia disponer de flotas más resilientes, versátiles, distribuidas e interoperables, quizá con más buques de menor porte y sistemas autónomos, pero manteniendo o incluso incrementando la capacidad de fuego.

En lo que respecta a su relación con las operaciones multidominio, no debemos olvidar que la guerra naval afecta a otros espacios físicos como el aire y el espacio, además de la superficie del mar, bajo el agua e incluso las zonas litorales que son escenario de operaciones anfibias. Cada plataforma marítima puede formar parte de un sistema multidominio que integra gran variedad de capacidades, siendo esta su cualidad diferencial, más que el enfoque en las propias tecnologías navales de forma aislada.

Desde el punto de vista de la protección de la fuerza, una gama creciente de amenazas, en muchos casos derivadas de nuevos desarrollos tecnológicos, hacen que los buques sean cada vez más vulnerables. En términos generales, podemos afirmar que las contramedidas actuales disponibles en estas plataformas han quedado rezagadas con respecto a nuevos tipos de armamento, con mayor precisión, alcance y velocidad. Las fuerzas navales deben invertir en capacidades de protección con el fin de reducir la brecha tecnológica observada entre las capacidades ofensivas y las contramedidas.

En particular, será necesario hacer frente al armamento basado en energía dirigida y misiles hipersónicos, el cual tendrá gran efecto en los próximos conflictos, exigiendo mucha mayor rapidez de respuesta y toma de decisiones. Al igual que la implementación efectiva de dicho armamento supone un reto tecnológico importante, también lo supone el desarrollo de una defensa efectiva contra el mismo.

Y del mismo modo que ocurre en otros dominios, el desarrollo e implementación de la robótica, municiones autónomas, vehículos no tripulados, tecnologías ciber y nuevos sistemas de información y comunicaciones en las fuerzas navales representan un desafío significativo. Todo ello conllevará una redefinición de los conceptos actuales de guerra antiaérea, anti-superficie, anti-submarina o contra-minas.

CAPACIDADES AÉREAS ANTE EL FCAS

En el ámbito aéreo, si bien Europa parece estar alineada para el desarrollo del futuro concepto de combate aéreo y de las capacidades asociadas, es cierto que el plazo para los que se plantean los correspondientes proyectos de desarrollo puede

hacer que Europa se tenga que saltar una generación para su consecución, entre los aviones de la cuarta y la sexta. Está por ver si el diferencial con potenciales adversarios, en cuanto a capacidades asociadas a la superioridad aérea, pueda verse reducido antes de que los actuales conceptos de combate aéreo en desarrollo en Europa estén plenamente implantados.

Cabe destacar que en las capacidades de defensa antiaérea y de supresión de sistemas de defensa aérea enemigos, aunque las necesidades y requisitos varían mucho de unos países a otros de la UE, se considera que la situación en Europa del Este está facilitando aunar una visión común. Por ello, se cree que existe una oportunidad para definir un enfoque común que permita confrontar la proliferación de sistemas SAM en la frontera oriental. Esto abre oportunidades de colaboración en términos de adiestramiento y realización de ejercicios comunes para asegurar la interoperabilidad y los procedimientos operativos comunes.

La creciente variedad de amenazas aéreas, desde UAVs hasta misiles de hipervelocidad, requiere la armonización de requisitos, soluciones y conceptos operativos para contrarrestarlas. La ausencia de estándares internacionales y la falta de claridad en ciertos aspectos legales representan una oportunidad de colaboración entre los países europeos para definir pautas comunes, aunque también plantean desafíos, dada la diversidad del rendimiento de los sistemas C-UAS y de las leyes que los regulan.

Desde el punto de vista estratégico, el transporte aéreo, destaca por los retos asociados a la explotación eficiente de los recursos de la UE para satisfacer las necesidades de carga de gran tamaño. Es crucial potenciar y mantener los marcos de colaboración existentes, mientras que las acciones a largo plazo deben enfocarse en minimizar la dependencia externa y gestionar los riesgos de manera efectiva.

En el transporte táctico/operacional es necesario explorar la viabilidad de soluciones de carga autónomas combinadas con plataformas tripuladas, y desarrollar modelos de logística y distribución que potencien la integración de los tres entornos, estratégico, operacional y táctico.

Por último, parece observarse la necesidad de una mayor estandarización de procedimientos, particularmente en operaciones de evacuación estratégica, sanitaria o de no combatientes (STRATEVAC, MEDEVAC o NEO). Esto conlleva poner en común tanto aspectos operativos como de formación o legales, indispensables para la implementación efectiva de la capacidad de evacuación.

CAPACIDADES ESPACIALES

En lo que al ámbito de las capacidades espaciales se refiere, se espera un importante crecimiento en los próximos años. Este se verá sustentado por el desarrollo de satélites de menor porte, más económicos, y fáciles de desplegar, haciendo del espacio un dominio más accesible, pero también más disputado.

Si bien hasta ahora la carrera espacial ha estado encabezada por estados y agencias gubernamentales, recientemente ha pasado a ser el sector privado el que lleva iniciativa, a lo que se une el ya mencionado mayor número de países con capacidad o aspiraciones de acceder al espacio.

Se espera que diversas empresas y organizaciones ofrezcan a corto plazo fácil acceso a una gama de desarrollos comerciales que incorporan tecnologías con alto potencial de doble uso, llegando incluso a reemplazar a las agencias gubernamentales en algunos aspectos, como ya está pasando en el caso de la puesta en órbita de satélites.

Para los programas de adquisición y provisión de servicios, supondrá un reto la coordinación entre los organismos gubernamentales y el sector privado, de forma que se mantenga una autonomía estratégica, una ventaja tecnológica y la información crítica de forma segura.

Estas mismas ventajas en manos del adversario constituirían una nueva amenaza que exige el desarrollo de contramedidas y capacidades de protección específicas. Además, las acciones espaciales sobre activos militares, normalmente, también afectan a activos civiles, siendo cada vez más difusa la línea que separa lo civil de lo militar.

En cuanto al tipo de amenazas que nos podemos encontrar en este dominio, cabe destacar la gran diversidad, tanto de procedencia natural como provocadas. Entre las primeras se incluyen algunas como la colisión con objetos naturales que orbitan la Tierra, radiación o actividad solar, o derivadas de la actividad humana habitual. Entre las segundas, se pueden incluir amenazas como interferencias, colisión con basura espacial generada intencionalmente, suplantación de satélites, ataques cinéticos, detonaciones nucleares, y otras provocadas por la difusión de tecnologías cada vez más accesibles.

Así, las capacidades de protección no se deben limitar únicamente a diseñar un mejor vuelo orbital o una mejor maniobrabilidad, sino que además deben incluir medidas pasivas para mitigar la exposición a la interrupción del servicio o a la degradación del rendimiento de los sistemas. La industria tiene el reto de desarrollar activos espaciales robustos, confiables, resilientes, y redundantes, con el objetivo de mantener intacta la disponibilidad operativa.

Ejemplos de acciones en este campo son las iniciativas orientadas a proporcionar capacidades de auto-reparación a las plataformas, mayor maniobrabilidad o nuevos métodos de puesta en órbita que permitan reponer de manera ágil una capacidad dañada.

Se espera que los activos espaciales den forma al despliegue operativo de una gran variedad de capacidades, entre las cuales destacan unas comunicaciones mejoradas más allá de la línea del horizonte, vigilancia permanente en tiempo real, perfeccionamiento de la inteligencia, apoyo a armas de precisión, detección de lanzadores de misiles y sus lanzamientos, y garantizar un mando y control efectivo.

Cobra especial relevancia el ámbito de la inteligencia, pues el creciente número de satélites dificulta a los países ocultar sus actividades. Las futuras operaciones militares se verán ligadas al uso extensivo de estas capacidades, como pieza clave a la hora de lograr la superioridad de la información, así como para realizar labores de inteligencia y proporcionar comunicaciones con gran ancho de banda, además de tener implicaciones directas en el resto de los dominios tratados.

CAPACIDADES DEL CIBERESPACIO

El ciberespacio es un dominio no físico y transversal al resto de dominios, en el que conviven tanto el ámbito civil como el militar. Ha cobrado gran relevancia en los últimos tiempos, debido al fuerte desarrollo tecnológico digital y a la capacidad de generar, almacenar, gestionar y transformar grandes cantidades de datos. El desarrollo de capacidades militares para mantener la superioridad en el ciberespacio se convierte en una prioridad fundamental, y permite disponer de una capacidad tanto de disuasión como de actuación sin precedentes.

Al tratarse de un dominio esencialmente desarrollado por el ser humano, las reglas que lo gobiernan son muy diferentes a las del resto. Además de la necesaria eficacia y rapidez en las acciones, existe una constante evolución del entorno, así como una falta de regulación y supervisión, lo que genera una infinidad de vulnerabilidades y vectores de ataque potenciales.

En este dominio destaca especialmente la gran asimetría existente entre las capacidades requeridas para un atacante y las que necesita quien se defiende. El coste para desarrollar una capacidad que produzca efectos significativos es mucho menor que el coste de desarrollarla para defender el ciberespacio propio. Todos podemos recordar las escenas, ya mostradas en las pantallas, en las que se recrean las consecuencias de un ataque ciber a una ciudad en su conjunto, o a partes críticas de la misma como las estaciones de metro y ferrocarril o los aeropuertos.

Esta circunstancia hace especialmente atractiva la actuación en este dominio, dando cabida a actores gubernamentales y no gubernamentales, tales como organizaciones terroristas, criminales, o hacktivistas.

Se trata, a su vez, de un dominio con un crecimiento constante, debido al creciente grado de interconexión entre redes y sistemas de muy diferente índole. Cada vez más estructuras críticas, tradicionalmente aisladas, se benefician del hecho de encontrarse interconectadas entre ellas, mejorando de manera significativa la efectividad del sistema completo, lo cual no está exento de riesgos. Los sistemas de armas no son una excepción y si a esto le sumamos el hecho de que las tecnologías digitales, por su novedad, presentan en muchas ocasiones nuevas vulnerabilidades, el número y tipología de amenazas asociadas se multiplica con respecto a otros dominios.

Al ser un dominio tan cambiante y más ligado a la innovación tecnológica, para que los esfuerzos sean efectivos y persistentes, las capacidades en el ciberespacio deben evolucionar al ritmo de los nuevos cambios tecnológicos, aprovechando las oportunidades que brindan y afrontando nuevos retos y amenazas.

Debido al carácter transversal del ciberespacio, está aún más ligado al desarrollo del concepto de operaciones multidominio, caracterizado por su complejidad y la necesidad de conectividad. Este debe cubrir todo el espectro de los conflictos, desde la paz hasta el conflicto de alta intensidad. Esta misma transversalidad se observa también entre el entorno civil y el militar, dando lugar a amenazas híbridas que comparten el uso de tecnologías y objetivos tanto civiles como militares.

Desde el punto de vista internacional, supone un reto potenciar y armonizar las capacidades nacionales sin por ello menoscabar la soberanía de los estados. En este contexto cobra relevancia el concepto de fronteras virtuales, que limiten el campo de acción o las áreas de interés para una organización concreta, y permitan gestionar los flujos de comunicación segura entre ellos.

Para el dominio del ciberespacio resulta fundamental el desarrollo de una fuerza dedicada y conformada por personal más cualificado tecnológicamente, que incluya equipos de respuesta contra amenazas híbridas, al igual que la potenciación y coordinación de las políticas nacionales de ciberdefensa y el fomento de la colaboración internacional.

Tomadas en su conjunto estas conclusiones nos permiten reflexionar sobre la importancia que está cobrando la actuación en el multidominio y la influencia de la tecnología en su desarrollo, siendo ambos partes interactuantes de un todo único, ya que el primero no se desarrollará sin la segunda y, ésta, la tecnología por sí sola no obtendrá la supremacía suficiente si no es en el contexto del multidominio.

Establecida esta interacción habrá que poner los medios para avanzar de forma complementaria en ambas vías.

La puesta en práctica del concepto de multidominio significará avanzar en la dirección y control de los sistemas de sistemas con las interacciones humano-máquina que ya tenemos sobre la mesa. La realidad de la nube de combate multidominio hará evolucionar el concepto y la ejecución del mando y control, teniendo en cuenta la necesidad de dejar a la iniciativa de los diferentes escalones de mando las actividades transversales, fundamentales, como se está comprobando en los conflictos actuales, para la consecución del objetivo principal.

El desarrollo de la tecnología pertinente será una mezcla de “hardware” y “software” con una sofisticación sin precedentes y que precisará de requisitos muy elaborados que solo se podrán realizar mediante la colaboración de la industria capaz de estar a la altura y llevarlo a cabo. Una vez más la consideración de la industria de defensa como un pilar más de la misma será fundamental, pero para ello su implicación y compromiso tienen que estar fuera de dudas.

En definitiva, cuando creíamos tener resuelto el viejo problema de “ver más allá de la colina” nos tropezamos con el reto de dirigir y controlar todo lo que vemos y sentimos, mediante un gran número de sensores, cuya información se establece en el espectro electromagnético en su gran mayoría. Problema del que seguramente sólo estamos viendo la punta del iceberg.

J. Daniel González Galdo
Alfredo Peña Ruiz
Juan Manuel García Montaño

Isdefe
C/ Beatriz de Bobadilla, 3
28040 Madrid
Tel.: +34 91 411 50 11
Email: general@isdefe.es
www.isdefe.es