UNIVERSIDAD DE VALLADOLID

ESCUELA TÉCNICA SUPERIOR DE INGENIEROS DE TELECOMUNICACIÓN

TRABAJO FIN DE MÁSTER

MÁSTER EN INGENIERÍA DE TELECOMUNICACIÓN

Aplicación del 5G para las operaciones multidominio en las Fuerzas Armadas

Autor:

D. Daniel Sirgo Rodríguez

Tutor:

Dr. D. Juan Carlos Aguado Manzano

Valladolid, 2 de julio 2025

TÍTULO:	**Aplicación del 5G para las operaciones multidominio en las Fuerzas Armadas**
AUTOR:	**D. Daniel Sirgo Rodríguez**
TUTOR:	**Dr. D. Juan Carlos Aguado Manzano**
DEPARTAMENTO:	**Teoría de la Señal y Comunicaciones e Ingeniería Telemática**

TRIBUNAL

PRESIDENTE:	IGNACIO DE MIGUEL JIMÉNEZ
VOCAL:	JAVIER AGUIAR PÉREZ
SECRETARIO:	RAMÓN DE LA ROSA STEINZ
FECHA:	2 DE JULIO DE 2025
CALIFICACIÓN:	

Resumen

Este Trabajo Fin de Máster explora el potencial estratégico y técnico del *5G* y demás tecnologías habilitadoras en el contexto de las operaciones multidominio (MDO) de las Fuerzas Armadas, con especial atención a los desarrollos y estándares definidos por la OTAN y organizaciones como *3GPP*. En los escenarios operacionales complejos que integran los dominios terrestre, aéreo, marítimo, cibernético y espacial, el *5G* emerge como una tecnología clave para mejorar la interoperabilidad multinacional, asegurar conectividad avanzada en tiempo real y aumentar la resiliencia frente a amenazas. El estudio detalla características técnicas específicas del *5G*, destacando tecnologías como *Edge Computing*, redes abiertas y virtualizadas (*O-RAN*), antenas inteligentes (*Massive MIMO)*, redes no terrestres (*NTN*) y segmentación de redes (*Network Slicing*). Dichas tecnologías permiten optimizar las comunicaciones tácticas y estratégicas, facilitar la toma de decisiones rápidas y precisas, y potenciar la integración eficiente de sistemas autónomos y sensores. Además, se analiza la integración del *5G* con tecnologías complementarias como la Inteligencia Artificial (IA), Internet de las Cosas (*IoT*), *Big Data* y Realidad Aumentada, subrayando sus capacidades para mejorar la efectividad operativa y predictiva en el campo de batalla. Asimismo, se identifican importantes desafíos en términos de ciberseguridad, resistencia frente a interferencias electrónicas y limitaciones en la interoperabilidad con sistemas heredados. El trabajo incluye un estudio de casos prácticos terrestres, marítimos y multinacionales, evaluando críticamente el desempeño de redes tácticas *5G* en escenarios simulados. Se concluye enfatizando la necesidad de desarrollar estándares técnicos específicos, adaptar las doctrinas militares existentes e impulsar la cooperación internacional para maximizar los beneficios operacionales y estratégicos del *5G*. Finalmente, se presentan recomendaciones prácticas y líneas futuras de investigación.

Palabras clave

5G, operaciones multidominio (MDO), interoperabilidad, OTAN, *Edge Computing*, *Network Slicing*, ciberseguridad, Inteligencia Artificial, IoT militar, tecnologías habilitadoras

Abstract

This Master's Thesis explores the strategic and technical potential of 5G and enabling technologies within the context of multi-domain operations (MDO) of the Armed Forces, with particular attention to developments and standards defined by NATO and organizations such as 3GPP. In complex operational scenarios integrating land, air, maritime, cyber, and space domains, 5G emerges as a key technology to enhance multinational interoperability, ensure advanced real-time connectivity, and increase resilience against threats. The study details specific technical characteristics of 5G, highlighting technologies such as Edge Computing, open and virtualized networks (O-RAN), intelligent antennas (Massive MIMO), non-terrestrial networks (NTN), and network slicing. These technologies enable optimized tactical and strategic communications, facilitate rapid and precise decision-making, and enhance the efficient integration of autonomous systems and sensors. Furthermore, the thesis analyzes the integration of 5G with complementary technologies such as Artificial Intelligence (AI), Internet of Things (IoT), Big Data, and Augmented Reality, emphasizing their capabilities to improve operational and predictive effectiveness on the battlefield. Significant challenges in terms of cybersecurity, resistance to electronic interference, and interoperability limitations with legacy systems are also identified. The work includes a practical case study analysis in terrestrial, maritime, and multinational contexts, critically evaluating the performance of tactical 5G networks in simulated scenarios. It concludes by emphasizing the need to develop specific technical standards, adapt existing military doctrines, and foster international cooperation to maximize the operational and strategic benefits of 5G. Finally, practical recommendations and future research lines are presented.

Keywords

5G, Multi-Domain Operations (MDO), interoperability, NATO, Edge Computing, Network Slicing, cybersecurity, Artificial Intelligence, military IoT, enabling technologies.

Agradecimientos

Quiero expresar mi más sincero agradecimiento a todas las personas que han hecho posible la realización de este Trabajo Final de Máster, tanto por su apoyo académico como personal a lo largo de este proceso.

En primer lugar, gracias a mi tutor, por su infinita paciencia, comprensión y compromiso durante más de un año de trabajo. A pesar de los cambios de enfoque y temática que ha sufrido este proyecto, su orientación constante y su capacidad para adaptarse a cada nueva etapa han sido fundamentales para llevarlo a buen término.

También quiero agradecer profundamente a mis antiguos compañeros del Ministerio de Defensa, cuya generosidad y profesionalidad me han permitido adentrarme en un ámbito tan complejo como fascinante. Gracias a su experiencia, he podido comprender con mayor profundidad el entorno operativo de la Defensa y aplicar ese conocimiento al presente trabajo. Sin su colaboración y enseñanzas, este TFM no habría sido posible.

A todos ellos, gracias por haber formado parte de este camino.

Este documento ha utilizado IA para la traducción y la mejora de la legibilidad del texto.

Índice

Índice de Figuras

Índice de Tablas

Glosario de Siglas

Sigla	Significado
5G	Quinta generación de redes móviles
6G	Sexta generación de redes móviles
ACT	*Allied Command Transformation (OTAN)*
AI / IA	*Artificial Intelligence / Inteligencia Artificial*
AR/VR	*Augmented Reality / Virtual Reality*
BACSI	Base Conectada, Sostenible e Inteligente
CBRN	*Chemical, Biological, Radiological and Nuclear*
CC	*Coastal Communications*
C2	*Command and Control (Mando y Control)*
CWIX	*Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise*
DGAM	Dirección General de Armamento y Material
EMP	*Electro Magnetic Pulse*
ETSI	*European Telecommunications Standards Institute*
FMN	*Federated Mission Networking*
HAPS	*High Altitude Platform Systems*
HSC	*High Seas Communications*
ISR	*Intelligence, Surveillance and Reconnaissance*
IoT / IoMT	*Internet of Things / Internet of Military Things*
JEMAD	Jefe del Estado Mayor de la Defensa
LHQ	*Large Headquarters*
LEO	*Low Earth Orbit (Órbita terrestre baja)*

Sigla	**Significado**
MCCE	Mando Conjunto del Ciberespacio
MCP	*Mobile Command Post*
MDO	*Multi-Domain Operations (Operaciones Multidominio)*
MEC	*Multi-access Edge Computing*
MINISDEF	Ministerio de Defensa
NCIA	*NATO Communications and Information Agency*
NTF	*Naval Task Force*
NTN	*Non-Terrestrial Networks*
O-RAN	*Open Radio Access Network*
OTAN / NATO	Organización del Tratado del Atlántico Norte
QoS	*Quality of Service*
SDHQ	*Static Deployable Headquarters*
SIEM	*Security Information and Event Management*
SIGINT / IMINT / HUMINT	*Signals / Imagery / Human Intelligence*
SLICE	Segmento lógico de red 5G personalizado
STANAG	*Standardization Agreement (OTAN)*
TTPs	*Tactics, Techniques and Procedures*
UAV / UGV / USV / UUV	*Unmanned Aerial / Ground / Surface / Underwater Vehicle*
URLLC	*Ultra-Reliable Low Latency Communications*
ZTP	*Zero Touch Provisioning*

Capítulo 1. Introducción

1.1. Relevancia del *5G* en el ámbito militar

El *5G* es considerado por las principales organizaciones de Defensa como una tecnología disruptiva que cambiará profundamente la forma en que se planifican y ejecutan las operaciones militares [1]. Su capacidad para proporcionar conectividad segura, fiable y de baja latencia a múltiples nodos en movimiento, así como para sostener la integración de sistemas autónomos, sensores, armas inteligentes y plataformas ISR, lo posiciona como pilar tecnológico en los entornos de batalla futuros y actuales como el de Ucrania con Rusia y el de Israel en Oriente Medio [1][2].

El *5G* facilita una conectividad más robusta y confiable en entornos operativos complejos, donde las redes tradicionales suelen tener limitaciones importantes [1]. La capacidad de interconectar numerosos dispositivos simultáneamente mejora la efectividad de las plataformas autónomas, drones y sistemas de vigilancia, aumentando la conciencia situacional y la capacidad operativa general.

Además, su integración con tecnologías habilitadoras emergentes como la Inteligencia Artificial, el *Big Data*, el *IoT* y las plataformas no tripuladas potencia la capacidad de las Fuerzas Armadas para anticiparse a las amenazas [2], realizar análisis predictivos y optimizar la toma de decisiones operativas en tiempo real.

En el ámbito internacional, la adopción del *5G* impulsa la interoperabilidad y cooperación efectiva en operaciones multinacionales bajo estándares compartidos, promoviendo así una mejor integración entre las fuerzas aliadas y facilitando una respuesta conjunta y coordinada frente a amenazas comunes [3]. Ejercicios como *CWIX* [4], iniciativas como *FMN Spiral 6* [5], el desarrollo de proyectos como ZEUS [6], TRITÓN [7] o BACSI [8], y los planes para desplegar redes tácticas privadas 5G muestran la orientación clara hacia el uso de estas redes como infraestructura crítica militar.

Por estas razones, la incorporación efectiva del 5G se considera crítica para mantener la superioridad tecnológica y operativa de las Fuerzas Armadas en los próximos años.

1.2. Marco estratégico de la OTAN y el concepto de operaciones multidominio

El concepto de operaciones multidominio (MDO) ha sido formalizado por la OTAN como una evolución de las operaciones conjuntas tradicionales. Ha identificado estas operaciones como una prioridad estratégica para afrontar la creciente complejidad del entorno operativo actual, caracterizado por amenazas híbridas, ciberataques y adversarios con capacidades tecnológicas avanzadas. El marco estratégico de la Alianza Atlántica establece claramente la necesidad de integrar plenamente capacidades y esfuerzos en todos los dominios operativos (terrestre, marítimo, aéreo, espacial y cibernético), junto con el espectro electromagnético y el dominio de la información, para garantizar una defensa colectiva eficaz y adaptativa. En la Figura 1, podemos observar este marco MDO [9][10].

Documentos como el *Alliance Concept for MDO* [9] y las directrices de ACT [10][11] y NCIA [12] subrayan la necesidad de transformar tanto la doctrina como las infraestructuras digitales para operar de forma federada, multinivel y multinacional. En este marco, el 5G se incorpora como tecnología de doble uso capaz de garantizar capacidades críticas: comunicaciones resilientes, compartimentación táctica, interoperabilidad federada y soporte a sistemas distribuidos [10].

El concepto oficial de operaciones multidominio de la OTAN [9] subraya la importancia de ejecutar acciones sincronizadas y coordinadas en múltiples dominios, que se pueden observar en la Figura 2 [9], simultáneamente, explotando así las ventajas específicas de cada uno para generar múltiples dilemas operacionales al adversario [9], dificultando sus decisiones y saturando su capacidad de respuesta.

Este enfoque multidominio requiere una estrecha colaboración multinacional, interoperabilidad tecnológica y doctrinal, y una infraestructura de comunicaciones robusta y segura [12], en la cual la tecnología *5G* juega un papel fundamental. El *5G* se posiciona como un elemento esencial dentro del marco estratégico de la OTAN, al proporcionar la capacidad técnica necesaria para conectar plataformas, sensores, centros de mando y personal desplegado en diferentes escenarios operativos.

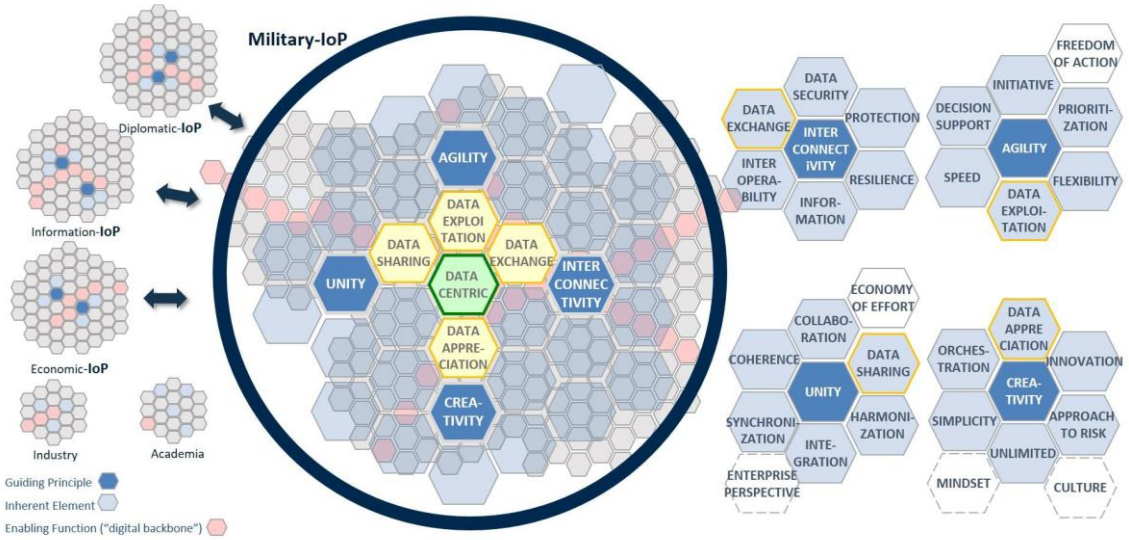

Figura 1: Principios del MDO.

El Plan del JEMAD para la Implantación de las MDO en las Fuerzas Armadas españolas [12] ejemplifica claramente cómo España está alineando su estrategia militar nacional con este concepto multidominio promovido por la OTAN, mediante un esfuerzo estructurado hacia la interoperabilidad, la digitalización y la coordinación efectiva entre dominios.

De esta manera, el marco estratégico de la OTAN impulsa una transformación profunda hacia un modelo operacional integrado y tecnológicamente avanzado, en el cual el *5G* se presenta como una herramienta clave para mantener la ventaja operativa y estratégica de la Alianza [9][10].

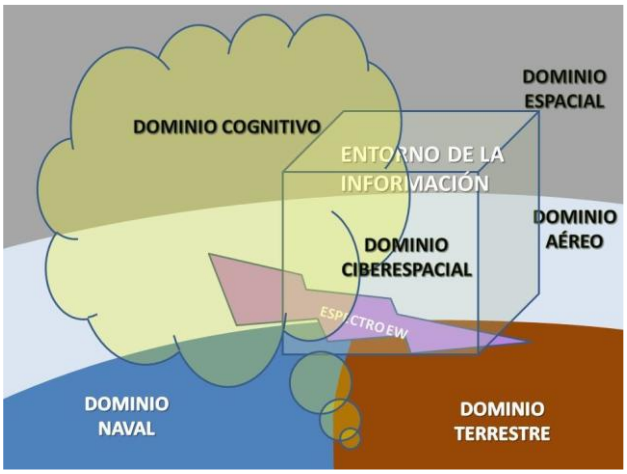

Figura 2: Dominios existentes en el MDO.

1.3. Motivación del proyecto

Este trabajo surge de una experiencia profesional directa en el Estado Mayor de la Defensa (EMAD), donde he desempeñado funciones vinculadas a la planificación y seguimiento de proyectos tecnológicos emergentes [11], con un enfoque especial en la incorporación del *5G* en el entorno de Defensa. Durante un año, participé activamente en reuniones nacionales e internacionales, incluyendo grupos de trabajo especializados de la OTAN como el *IST-220*, del que formo parte [13], así como en iniciativas de cooperación industrial y técnica con organismos como el MCCE [14], JCISAT [15] y DGAM [16].

Esta exposición práctica ha permitido adquirir un conocimiento privilegiado sobre la dinámica de transformación digital de las Fuerzas Armadas, el funcionamiento de los procesos de estandarización técnico-doctrinal [17], la articulación entre actores nacionales e internacionales [9][10] y la gestión de proyectos tecnológicos en un contexto estratégico y multinacional [18]. El presente trabajo pretende capitalizar dicha experiencia para generar una síntesis rigurosa, contextualizada y útil sobre la aplicación del *5G* en operaciones multidominio, aportando una visión integradora entre lo técnico, lo doctrinal y lo operativo, teniendo en cuenta que su implementación está en proceso.

1.4. Metodología de estudio

Este Trabajo Fin de Máster adopta una metodología de revisión estructurada y cualitativa, basada en tres pilares principales: experiencia profesional directa, revisión bibliográfica especializada y análisis documental estratégico.

1. Revisión documental y selección de fuentes:

Se ha llevado a cabo una recopilación exhaustiva de más de 200 documentos, entre los cuales se han seleccionado de forma intencionada 93 fuentes clave para su inclusión directa. Los criterios de selección han sido:

- Temática: solo se incluyeron documentos con relación directa con redes *5G*, tecnologías habilitadoras (*MEC, IA, slicing*), y su aplicación al entorno militar o de Defensa.
- Relevancia institucional: prioridad a documentos de organismos oficiales (OTAN, UE, Ministerio de Defensa de España, *EDA*, *3GPP*), excluyendo literatura sin respaldo técnico o institucional validado.
- Actualización: se priorizó la documentación publicada entre 2020 y 2025, evitando estudios desactualizados ante la rápida evolución tecnológica.
- Disponibilidad pública y legal: se descartaron documentos clasificados o sujetos a reserva interna del Ministerio, incluyendo únicamente aquellos con difusión autorizada o de acceso abierto.

2. Clasificación y tratamiento de fuentes:

Los documentos fueron organizados por categorías temáticas (tecnología, doctrina, programas, casos de uso), por niveles de aplicación (táctico, operacional, estratégico), y por ámbito institucional (nacional, OTAN, UE, industria). Esta clasificación permitió construir una matriz analítica que facilitó el análisis transversal entre dominios y funciones conjuntas.

3. Análisis e integración de contenidos:

- Se empleó un enfoque inductivo para extraer patrones doctrinales, tecnológicos y estratégicos comunes en las fuentes seleccionadas.
- Se han sintetizado múltiples documentos superpuestos en términos de contenido, estructurándolos en una narrativa coherente y accesible.
- Las aportaciones personales se reflejan en la sistematización conceptual de casos de uso, en el mapeo de desafíos operativos y en la correlación entre requisitos técnicos y capacidades militares.

4. Aportación original:

Aunque este trabajo puede clasificarse como una revisión del estado del arte, va más allá de la mera recopilación descriptiva. La experiencia directa en foros técnicos de alto nivel y su conocimiento operativo del funcionamiento institucional del Ministerio de Defensa han permitido construir un análisis crítico y orientado a la toma de decisiones. Se han identificado lagunas de interoperabilidad, necesidades doctrinales emergentes y escenarios realistas de implementación, integrando datos técnicos, normativos y estratégicos en una única visión estructurada.

1.5. Objetivos

El objetivo principal de este Trabajo Fin de Máster es analizar el impacto estratégico y técnico del despliegue de la tecnología *5G* en el ámbito militar, específicamente en el contexto de las operaciones multidominio (*MDO*). Para ello, se evaluará cómo esta tecnología y sus diversas innovaciones asociadas pueden contribuir significativamente a mejorar la capacidad operativa, la interoperabilidad multinacional y la efectividad en la toma de decisiones en escenarios complejos y dinámicos.

Entre los objetivos específicos se incluyen:

- Analizar las características clave del *5G* y cómo estas se alinean con los requisitos operativos y estratégicos de las Fuerzas Armadas.
- Analizar cómo el *5G* se integra con tecnologías emergentes como la inteligencia artificial, el internet de las cosas (*IoT*), los sistemas autónomos, la realidad aumentada o el *Big Data*.
- Evaluar la contribución del 5G en la mejora de la coordinación, integración y comunicación efectiva entre diferentes dominios operativos (terrestre, marítimo, aéreo, espacial y cibernético).
- Identificar y explorar aplicaciones prácticas del *5G* en el contexto militar, incluyendo proyectos específicos en curso en el Ministerio de Defensa, la OTAN y la Unión Europea.
- Examinar en profundidad los desafíos tecnológicos, operativos, legales y regulatorios asociados al uso del *5G* en entornos militares.
- Proporcionar recomendaciones estratégicas y técnicas concretas que faciliten una efectiva implementación del *5G* en operaciones militares multidominio.

Establecer líneas futuras de investigación que permitan continuar explorando y optimizando el uso de tecnologías emergentes como el *5G* en el ámbito de la Defensa.

Capítulo 2. Marco conceptual y técnico

2.1 Definición y evolución de las operaciones multidominio (*MDO*)

Las operaciones multidominio (*Multi-Domain Operations, MDO*) constituyen un concepto doctrinal emergente que busca integrar de manera simultánea y coordinada las acciones militares en los dominios terrestre, marítimo, aéreo, cibernético, espacial y del espectro electromagnético. Su propósito es generar una superioridad operativa sostenida en entornos caracterizados por la complejidad, la incertidumbre y la acción de actores híbridos o tecnológicamente avanzados.

La evolución hacia el enfoque multidominio se ha visto impulsada por el reconocimiento de que los conflictos modernos ya no se desarrollan de manera aislada en un solo dominio, sino que exigen una sinergia continua entre capacidades distribuidas en múltiples entornos físicos y virtuales. Esto implica pasar de una lógica secuencial (operaciones conjuntas clásicas) a una lógica simultánea, interconectada y centrada en la información.

El concepto ha sido formalizado por la OTAN a través del documento *Alliance Concept for MDO* y diversos marcos doctrinales impulsados por el Allied Command Transformation (*ACT*) y la *NATO Communications and Information Agency* (*NCIA*) [9][10][11]. Este concepto se articula en torno a tres principios fundamentales:

- *Cross-domain synchronization:* la capacidad de coordinar efectos en múltiples dominios en tiempo real, anticipándose al adversario y saturando su capacidad de respuesta.
- *Mission threads:* líneas de esfuerzo operativas y técnicas interconectadas que permiten mantener continuidad funcional entre dominios y niveles de mando. Las podemos observar en la Figura 3 [9]. Dependen del tipo de operación y se basan en colaborar, orquestar y converger en un resultado con efectos óptimos en cualquier dimensión.
- *Multi-domain C2 ecosystem:* un ecosistema de mando y control flexible, modular y digitalizado, capaz de operar de forma federada y resiliente.

El documento también establece que el objetivo final es alcanzar una ventaja informativa y de decisión (*information and decision advantage*), lo que implica acelerar el ciclo OODA (Observar-Orientar-Decidir-Actuar) a través de tecnologías como el *5G*, *edge computing*, IA (Inteligencia Artificial), y *data lakes* distribuidos [9].

En el ámbito nacional, el Plan del JEMAD para la implementación de las MDO en las FAS [12] establece las líneas doctrinales, organizativas y tecnológicas que permitirán a las Fuerzas Armadas españolas adaptarse a este nuevo paradigma. Este plan articula la necesidad de contar con nodos de mando distribuidos, comunicaciones persistentes, sensores conectados, sistemas autónomos interoperables y capacidades de decisión acelerada mediante inteligencia artificial y análisis predictivo.

Las MDO suponen, por tanto, una evolución doctrinal que busca garantizar la superioridad en el entorno operativo mediante:

- La integración simultánea de efectos en todos los dominios.
- La capacidad de explotar vulnerabilidades enemigas desde cualquier dominio.
- La interoperabilidad multinacional basada en estándares compartidos (*FMN*, *STANAG*, *3GPP*) [2].
- El uso de redes tácticas avanzadas como el *5G* para garantizar conectividad, resiliencia y velocidad en la toma de decisiones.

Este marco exige una transformación profunda de los sistemas de mando y control (*C2*), la arquitectura de redes y los procedimientos operativos, en los cuales el *5G* se presenta como tecnología catalizadora por su capacidad de operar de forma ubicua, segura y distribuida en todo el espectro operativo, facilitando simultáneamente la ejecución de los *mission threads*, la sincronización de efectos entre dominios y la persistencia de mando en entornos contestados o degradados.

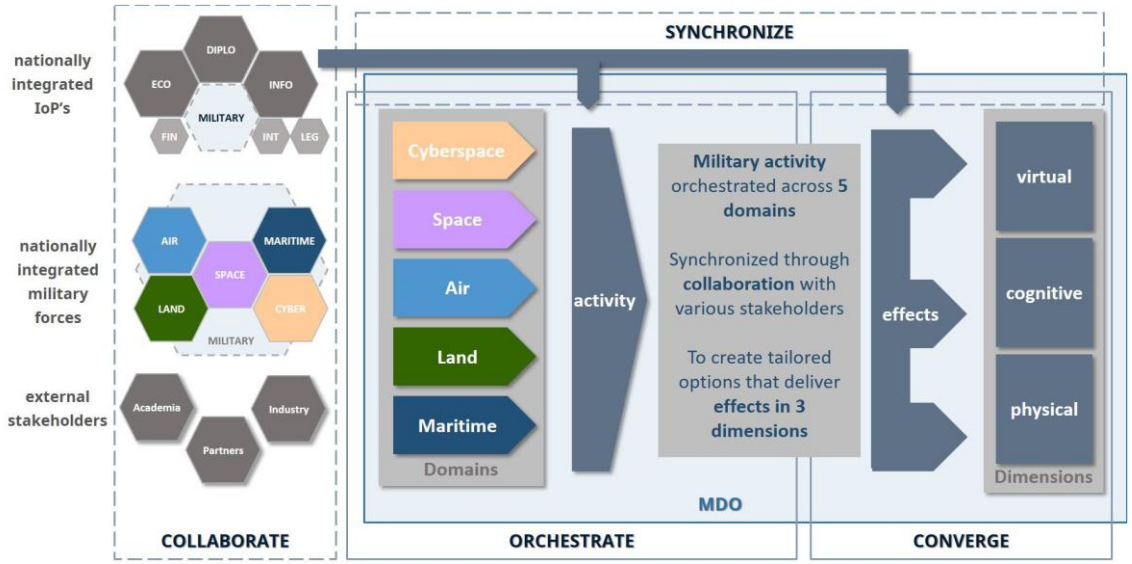

Figura 3: Mission Threads.

2.2 Características principales y evolución de la tecnología *5G*

La tecnología *5G*, desarrollada en el marco de los estándares definidos por el *3rd Generation Partnership Project* (3GPP) [2], supone una evolución significativa respecto a las generaciones móviles anteriores. Diseñada originalmente para usos civiles, su arquitectura escalable, modular y definida por software permite su adaptación a entornos operacionales militares exigentes y altamente dinámicos con ciertas mejoras que se comentarán en apartados siguientes.

5G New Radio (*NR*) es la nueva interfaz aérea diseñada para el *5G*, y reemplaza al *LTE* como tecnología de acceso radioeléctrico a nivel civil, en las FAS nunca se había utilizado tecnologías de datos móviles por no considerarse seguras ni adaptables a las necesidades militares. El *5G* supone un cambio de mentalidad, se ha visto que en los conflictos

actuales es una tecnología que permite tener una ventaja respecto al adversario. Su arquitectura flexible permite operar en un rango de frecuencias que va desde por debajo de 1 GHz hasta las bandas *mmWave* por encima de 24 GHz, lo que la hace ideal tanto para cobertura amplia como para despliegues de alta capacidad. Incluye modos de numerología variable, subtramas flexibles, y soporta tecnologías como *beamforming*, *Massive MIMO*, y comunicación *sidelink* [19]. En el ámbito militar, *5G NR* ofrece ventajas críticas en entornos electromagnéticos (EM) hostiles, permitiendo enlaces seguros, adaptativos y optimizados para el tipo de misión, incluso en situaciones de interferencia o degradación espectral [20]. En este trabajo no nos vamos a centrar en el funcionamiento técnico de las tecnologías, sino que vamos a analizar cuáles y cómo son útiles para el ámbito de la Defensa.

Las principales características técnicas del *5G* que lo hacen especialmente atractivo para su aplicación en Defensa [13] son:

- *Ultra-Reliable Low-Latency Communications* (URLLC): capacidad de comunicación fiable con latencias inferiores a 1 milisegundo, indispensable para operaciones críticas como el control de sistemas autónomos, *C2* en tiempo real o fuego coordinado.
- *Enhanced Mobile Broadband (eMBB):* permite velocidades de transmisión de datos del orden de gigabits por segundo, fundamentales para el intercambio de vídeo *HD*, flujos *ISR* y datos multicanal entre plataformas distribuidas.
- *Massive Machine Type Communications (mMTC):* posibilidad de conectar simultáneamente miles de dispositivos *IoT*, sensores y nodos distribuidos, facilitando la construcción de redes tácticas multisensor basadas en datos.
- *Network Slicing*: segmentación lógica de la red para crear *slices* personalizados por aplicación, nivel de seguridad o tipo de unidad, lo cual permite compartimentar funciones, priorizar servicios críticos y optimizar recursos disponibles.
- Arquitectura nativa en la nube y funciones virtualizadas (*NFV/SDN*): permite la orquestación dinámica, automatización del despliegue y adaptación flexible en redes híbridas (civiles/militares, públicas/privadas).
- *Edge Computing* (*MEC*): despliegue de capacidad de procesamiento cerca del usuario, reduciendo la latencia y aumentando la autonomía operativa, incluso en escenarios sin conectividad a nodos centrales.
- *Time-Sensitive Networking* (*TSN*): sincronización precisa de red, especialmente útil para operaciones coordinadas multisistema y misiones de targeting o mantenimiento predictivo.
- Servicios avanzados de localización: mejora de la capacidad de geoposicionamiento con precisión submétrica, aplicable a *UAVs*, municiones guiadas o posicionamiento de tropas en entornos *GNSS-denegados*.
- Acceso mediante ondas milimétricas (*mmWave*): uso de bandas superiores a 24 GHz para proporcionar enlaces de muy alta capacidad en entornos densos o en escenarios de fuego concentrado, especialmente útiles en nodos de *C2* o puentes de comunicaciones de alta velocidad.
- *Fixed Wireless Access* (*FWA*): despliegue de conectividad similar a la fibra en zonas remotas o sin cobertura terrestre, útil para bases avanzadas o campamentos expedicionarios.

Desde su estandarización inicial en 2018 (*Release* 15), el *5G* ha evolucionado a través de nuevas versiones que incorporan funcionalidades críticas para defensa, como podemos observar en la Figura 4 [2]:

- *Release* 16 y 17: introducción de capacidades avanzadas como redes no terrestres (*NTN*), determinismo temporal, comunicación *sidelink* (*D2D*), servicios de localización y sincronización, y mejoras en seguridad y eficiencia energética.
- *Release* 18 y siguientes: actualmente en desarrollo hacia el concepto de "*5G Advanced*" y base para el futuro *6G*, incorporan IA nativa en la gestión de red, comunicaciones holográficas, redes autónomas auto-gestionadas y mayor resiliencia frente a interferencias.

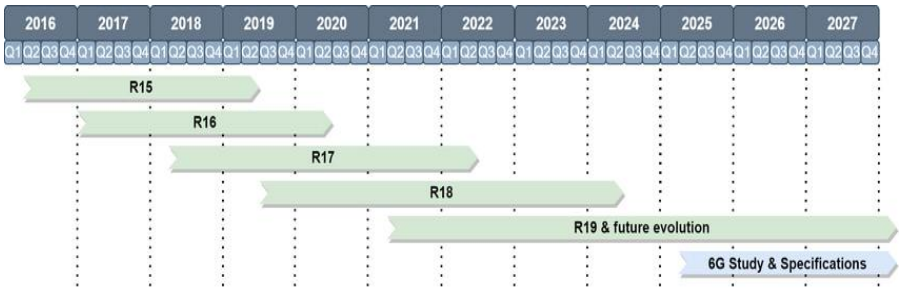

Figura 4: Releases del 3GPP.

A nivel doctrinal, organismos como la OTAN, la Unión Europea, el Ministerio de Defensa español y el *3GPP* han reconocido el carácter dual del *5G*, como tecnología civil de aplicación directa en el ámbito militar [21] [22]. Su despliegue se está validando internacionalmente (CWIX, FMN Spiral 6) y nacionalmente en proyectos como BACSI, TRITÓN y RED OSIRIS [23], integrando nodos *edge* embarcados [24], redes privadas tácticas y arquitecturas en malla *ad-hoc* para mejorar la resiliencia operativa.

En la Figura 5 [2] podemos observar la arquitectura de referencia del *3GPP*, que es susceptible de cambios para mejorar ciertas deficiencias para el entorno militar. El *5G* representa una infraestructura crítica de próxima generación, diseñada para habilitar redes de comunicaciones tácticas que sean seguras, adaptativas, de alta capacidad, resistentes a interferencias y plenamente integradas con plataformas *C4ISR* (Comando, Control, Comunicaciones, Computadoras, Inteligencia, Vigilancia y Reconocimiento), sensores distribuidos y sistemas de armas avanzados.

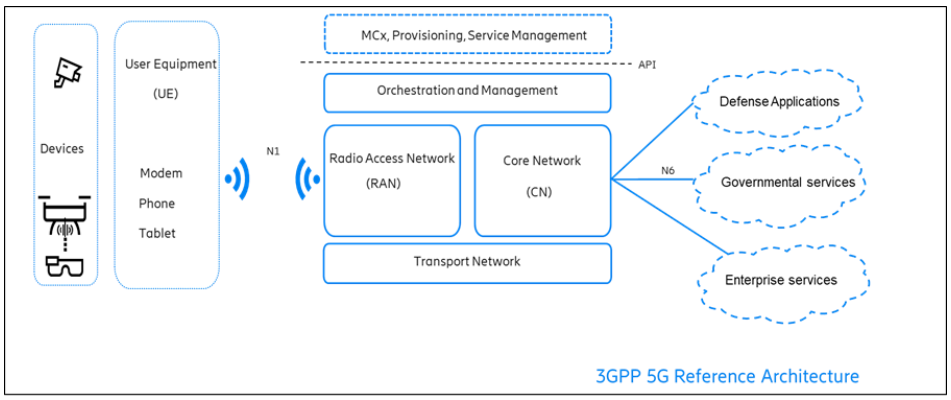

Figura 5: Arquitectura de referencia 5G del 3GPP.

2.3 Relación entre el *5G* y las capacidades multidominio

El despliegue de redes *5G* en el ámbito de la Defensa constituye una pieza fundamental para habilitar la transformación hacia una arquitectura operativa multidominio. Esta relación se manifiesta de forma directa en la manera en que las capacidades técnicas del *5G* permiten ejecutar funciones críticas en entornos caracterizados por la dispersión geográfica, la necesidad de sincronización entre dominios, la velocidad de decisión y la interoperabilidad multinacional.

En primer lugar, el *5G* responde directamente a los requisitos de las *Joint Functions* establecidas por la doctrina OTAN, como Mando y Control (*C2*), Inteligencia, Fuegos, Movilidad, Protección y Sostenimiento [25]. Cada una de estas funciones se ve reforzada por el uso de capacidades como el *Network Slicing* (para la segmentación segura y diferenciada del tráfico por dominio funcional), el *Edge Computing* (para procesamiento local en tiempo real) o el *URLLC* (para control de armas y plataformas autónomas con requisitos temporales críticos) [26].

Entre los aspectos más relevantes de esta relación destacan:

- Sincronización multidominio: el *5G* permite la ejecución simultánea de *mission threads* entre dominios mediante enlaces fiables, dinámicos y de baja latencia. Esto es esencial para mantener operaciones coordinadas entre fuerzas navales, terrestres, aéreas y cibernéticas.
- Arquitecturas distribuidas de *C2*: gracias al *Edge Computing*, se habilita el mando distribuido desde puestos de mando móviles o nodos embarcados, sin necesidad de conexión constante a centros estratégicos.
- Interoperabilidad táctica y multinacional: el *slicing* permite la coexistencia segura de múltiples grupos de fuerzas aliadas sobre una misma infraestructura, facilitando la colaboración OTAN-UE sin comprometer la soberanía digital de cada nación.
- Integración de plataformas autónomas y sensores: el *mMTC* permite desplegar redes masivas de sensores, *UAVs* o plataformas no tripuladas (*UXVs*) que operen de manera coordinada y en tiempo real.

En conjunto, el *5G* no solo mejora la eficiencia técnica de las comunicaciones militares, sino que constituye un habilitador doctrinal y estratégico para la implementación real de las *MDO*. Tal y como recoge el *Alliance Concept for MDO*, la capacidad de operar con persistencia, resiliencia y agilidad a través de todos los dominios requiere una red de comunicaciones ubicua, dinámica, federada y segura; condiciones todas ellas nativamente ofrecidas por el ecosistema *5G* [2][9][20].

Este marco conceptual, alineado con iniciativas nacionales como el Plan del JEMAD y con la doctrina OTAN, posiciona al *5G* no como un simple avance técnico, sino como un multiplicador estratégico de capacidades operativas multidominio.

2.4 Tecnologías habilitadoras relacionadas

Con el uso del *5G* y de las siguientes tecnologías se busca ser capaz de tener redes privadas, seguras en cualquier clase de entorno y reconfigurables desde cualquier tipo de cuartel permitiendo un acceso variable a los miembros que formen parte de la operación en función de su rango y su necesidad de conocimiento.

2.4.1 *Edge Computing y Multi-access Edge Computing* (*MEC*)

El *Edge Computing* y su variante estandarizada para redes móviles, *Multi-access Edge Computing* (*MEC*) [13][27], constituyen tecnologías fundamentales para habilitar la descentralización del procesamiento de datos en entornos tácticos. En lugar de enviar toda la información a centros de datos centrales, el *MEC* permite realizar análisis, filtrado y procesamiento local directamente en el borde de la red, lo que reduce drásticamente la latencia y mejora la autonomía operativa. En la Figura 6 [13] podemos observar un ejemplo de cómo funciona esta tecnología en una federación de redes. Se representa todas las capas de *IT*, red y seguridad asociadas a los requisitos para federar las comunicaciones a través de canales *LAN* o redes de área extensa *WAN*/*MAN*. En este escenario, la orquestación de servicios gestionará la movilidad sin fisuras de los usuarios. Los servicios se soportarán dondequiera que se encuentre el usuario en la red. Esto requiere la orquestación y federación de todos los componentes de la red: Radio, Core y *MEC*. Incluye orquestaciones de seguridad y orquestaciones de *IT* para sincronizar y llevar a cabo dinámicamente el control dinámico de la movilidad de los usuarios.

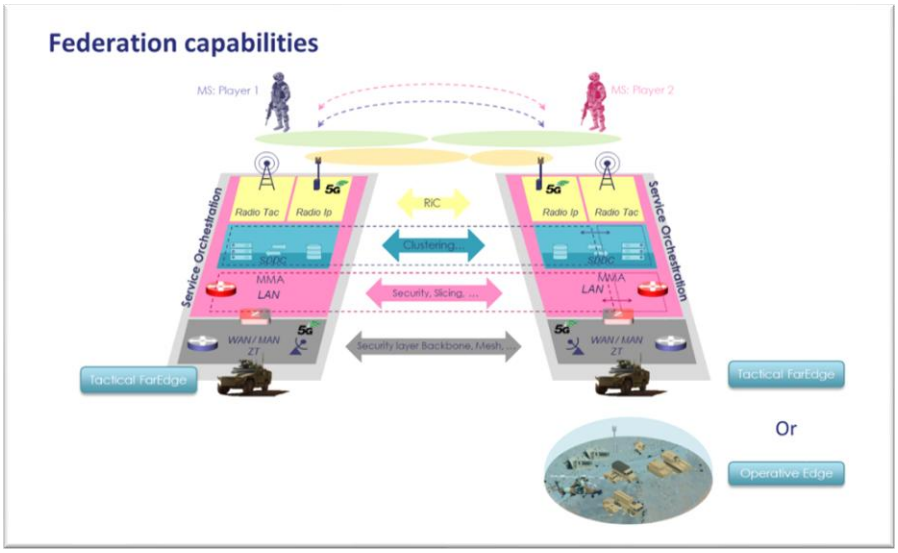

Figura 6: Ejemplo de federación de redes utilizando MEC.

En el contexto militar, esta capacidad es clave para:

- Ejecutar aplicaciones críticas (*C2*, *ISR*, *targeting*) incluso en condiciones de desconexión temporal [28].
- Apoyar el funcionamiento de plataformas autónomas (*UAVs*, *UGVs*, *USVs*) mediante procesamiento en tiempo real.

- Mantener la persistencia operativa en entornos contestados o degradados, donde los enlaces con la nube táctica o estratégica pueden estar comprometidos.

Ejercicios como *CWIX* y pruebas OTAN han demostrado la utilidad del *MEC* para mejorar la resiliencia táctica. Además, proyectos como TRITÓN o las arquitecturas de BACSI en España están adoptando nodos *edge* embarcados o modulares para facilitar su despliegue.

Además, se han desarrollado iniciativas como la arquitectura *DCIS Cube* [29], mostrada en la Figura 7, que es una colaboración entre *NCIA* y las industrias *ICT* para desarrollar los sistemas desplegables OTAN.

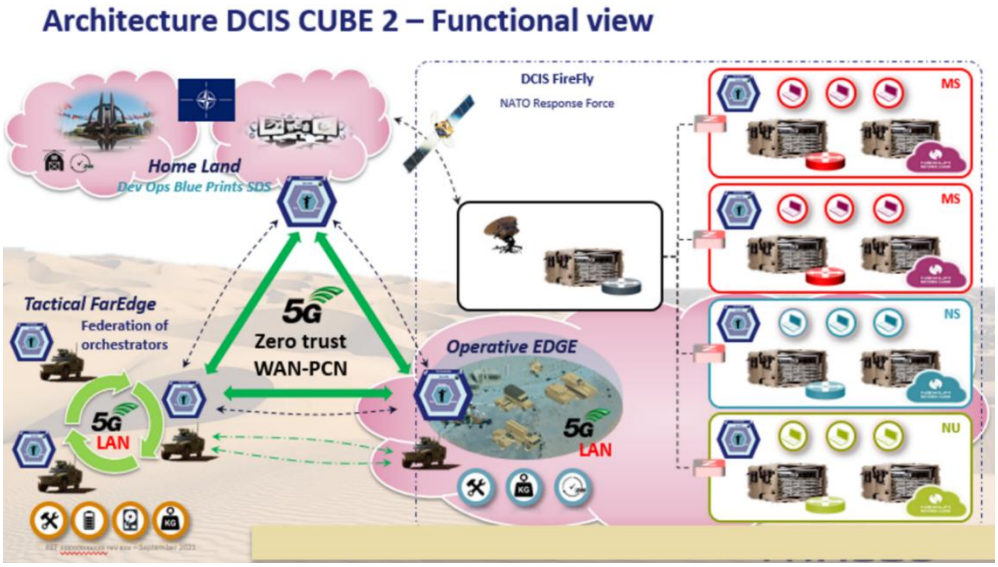

Figura 7: Arquitectura DCIS CUBE 2.

2.4.2 Redes abiertas y virtualizadas (*O-RAN*)

El concepto de *Open Radio Access Network* (O-RAN) [13][30] promueve una arquitectura abierta, desagregada e interoperable para las redes móviles. Esto permite sustituir los sistemas propietarios tradicionales por soluciones basadas en *software* (*NFV/SDN*), modulares y más fácilmente auditables.

Sus ventajas en defensa incluyen:

- Interoperabilidad multinacional mediante interfaces estandarizadas.
- Ciberseguridad reforzada gracias a la posibilidad de auditar y controlar cada componente.
- Despliegue ágil de funciones de red sobre infraestructuras comerciales o militares.
- Optimización de costes y reducción de la dependencia de proveedores únicos.

La OTAN ha señalado que *O-RAN* facilita la implementación de *slices* privados, la gestión federada y la flexibilidad para adaptar la red a múltiples escenarios operativos, desde operaciones embarcadas hasta despliegues en terreno austero [31].

2.4.3 Antenas inteligentes y Massive MIMO

El uso de sistemas de antenas inteligentes, incluyendo tecnologías como *Massive MIMO* (*Multiple Input, Multiple Output*), constituye un pilar técnico esencial del *5G*. Estas antenas permiten mejorar la eficiencia espectral, aumentar el alcance, reducir interferencias y direccionar haces de señal (*beamforming*) de manera dinámica y adaptable al entorno [13][32].

En el ámbito militar, estas capacidades resultan especialmente relevantes en entornos electromagnéticos hostiles o altamente saturados. Las tecnologías emergentes asociadas al diseño de antenas para defensa incluyen:

- *Beamforming* dinámico: permite concentrar la energía de transmisión hacia el receptor deseado, reduciendo la probabilidad de detección (*LPI/LPD*) y aumentando la resistencia frente a *jamming* o interferencias deliberadas [2].
- Diversidad espacial y polarización: el uso simultáneo de múltiples caminos de propagación y configuraciones de polarización cruzada mejora la fiabilidad del enlace y reduce la vulnerabilidad al *fading*.
- Adopción de bandas *mmWave* (24–100 GHz): aunque con limitaciones en alcance, estas bandas permiten enlaces de muy alta capacidad y menor exposición a interferencias civiles, siendo especialmente útiles para nodos de *C2* o relés embarcados.
- Antenas adaptativas y auto-configurables: capaces de ajustar su patrón de radiación y potencia en función de las condiciones espectrales y tácticas en tiempo real, optimizando el uso del espectro y mejorando la cobertura.
- Integración con Inteligencia Artificial: algoritmos de aprendizaje automático permiten optimizar dinámicamente la configuración de haces, el uso del canal y la asignación de usuarios, en función del tipo de misión, prioridad o comportamiento enemigo.
- Técnicas de mitigación de interferencias: como *null-steering*, supresión de lóbulos secundarios o adaptación dinámica de frecuencias, especialmente relevantes frente a entornos con presencia de guerra electrónica (*EW*) o *spoofing*.
- Tamaño compacto y modularidad: algunos diseños permiten la integración directa de estos sistemas en vehículos tácticos, *UAVs* o *shelters* desplegables, facilitando su uso en arquitectura *mesh*.

En operaciones tácticas, estos sistemas han demostrado ser claves para mantener la conectividad en presencia de medios de guerra electrónica, asegurar la continuidad del mando y reducir la firma electromagnética de unidades desplegadas [33]. Además, son esenciales para el despliegue eficiente de enlaces de acceso y *backhaul* en configuraciones como *Integrated Access and Backhaul* (*IAB*), especialmente en redes móviles privadas y topologías *ad-hoc* como las utilizadas en los proyectos RED OSIRIS o BACSI.

La sinergia entre antenas inteligentes, *beamforming* avanzado, *mmWave* y técnicas de mitigación de interferencias permite que el *5G* táctico no solo sea más veloz y capaz, sino también más resistente, discreto y adaptable a escenarios de combate modernos.

2.4.4 Redes no terrestres (*NTN*) y plataformas aéreas de gran altitud (*HAPS*)

Las Redes No Terrestres (*Non-Terrestrial Networks*, *NTN*), contempladas en la *Release* 17 del *3GPP* [2], amplían la cobertura de las redes *5G* mediante el uso de satélites en órbitas *LEO/MEO/GEO*, globos estratosféricos y plataformas aéreas de gran altitud (*High Altitude Platform Systems, HAPS*). Estas tecnologías permiten extender la conectividad más allá de las limitaciones geográficas y topográficas de las redes terrestres tradicionales.

En el ámbito militar, el uso de *NTN* y *HAPS* [34] ofrece ventajas clave:

- Cobertura estratégica en áreas remotas o inaccesibles: permite mantener el mando y control en escenarios sin infraestructura terrestre (desiertos, océanos, selvas o áreas montañosas).
- Redundancia táctica: en caso de sabotajes, destrucción de nodos o interferencias severas, estas plataformas permiten mantener la conectividad operativa y asegurar la continuidad de la misión.
- Integración multidominio: posibilita enlaces simultáneos aire-mar-tierra entre fuerzas conjuntas, mejorando la interoperabilidad en escenarios distribuidos.
- Movilidad y flexibilidad de despliegue: los sistemas *HAPS* pueden ser reposicionados en función del teatro de operaciones, proporcionando conectividad en zonas de maniobra o zonas de desembarco.
- Persistencia *ISR* y *relay* de comunicaciones: las plataformas *HAPS* pueden alojar sensores, retransmisores de señal y sistemas de guerra electrónica, actuando como nodos persistentes de vigilancia o como repetidores de red *5G*.

Los sistemas *NTN* también son útiles como *backhaul* táctico, enlazando nodos *edge* o redes privadas desplegadas en tierra con centros de mando a través de satélites comerciales o gubernamentales. Su compatibilidad con enlaces cifrados, *beamforming* satelital y técnicas de *switching* dinámico permite operaciones seguras y resilientes incluso en escenarios con amenazas EM elevadas.

En España, el Ministerio de Defensa ha explorado el uso de estos sistemas en el marco de proyectos como BACSI, integrando capacidades *HAPS* para el refuerzo de redes privadas tácticas y comunicaciones de alta disponibilidad. A nivel internacional, la OTAN los considera elementos clave dentro de una arquitectura federada, escalable y resiliente que sustente las *MDO* [35].

Además, se contempla su aplicación en despliegues de ayuda humanitaria, defensa civil, o gestión de emergencias, donde la conectividad *5G* vía *NTN* puede ser habilitada sin requerir infraestructuras locales preexistentes.

En conjunto, las *NTN* y los *HAPS* permiten a las Fuerzas Armadas operar con mayor flexibilidad, alcance y resiliencia en entornos extremos, complementando las redes terrestres con una capa superior de conectividad estratégica y táctica.

2.4.5 *Network Slicing*

El *Network Slicing* [2][20] es una funcionalidad clave del *5G* que permite crear múltiples redes lógicas independientes sobre una misma infraestructura física, cada una con su propio perfil de calidad de servicio (QoS), seguridad, ancho de banda y latencia. Esta capacidad resulta fundamental en el contexto militar, donde diferentes funciones y niveles operativos requieren comunicaciones con requisitos diferenciados y estrictos niveles de aislamiento.

Aplicaciones clave en Defensa:

- Segmentación por dominio funcional: *slices* dedicados para *C2*, *ISR*, logística, sostenimiento, *targeting* o guerra electrónica, evitando interferencias entre flujos y asegurando el rendimiento de cada misión. Además, permite reconfigurar los perfiles en función del desarrollo de las operaciones de una forma sencilla.
- Aislamiento de tráfico crítico (*Isolation Slicing*): configuración de *slices* con acceso restringido y políticas de reconfiguración rápida para redes *C2*, en operaciones de alta sensibilidad o con presencia de amenazas cibernéticas.
- *Slicing* multinacional y federado: creación de *slices* independientes por nación o por coalición dentro de una infraestructura compartida OTAN/UE, garantizando soberanía digital y compartimentación operativa.
- Uso de *slices* sobre redes públicas: implementación de *slices* seguros sobre redes comerciales en zonas urbanas o escenarios civiles-militares, utilizando mecanismos de priorización y cifrado extremo a extremo.
- *Slicing* dinámico en el borde: activación temporal de *slices* en nodos *edge* desplegados sobre terreno (como *shelters*, vehículos o buques), con perfiles adaptados según el tipo de unidad o situación táctica.

Además, el uso de *IAB* (*Integrated Access and Backhaul*) permite establecer conexiones inalámbricas entre nodos *5G* que sirven simultáneamente como estaciones base de acceso y como repetidores para enlazar con el núcleo de red, eliminando la necesidad de infraestructura física cableada. Esta funcionalidad resulta crítica en despliegues rápidos, entornos remotos o situaciones de emergencia, como en los proyectos previstos.

El *slicing* puede gestionarse mediante orquestadores multinodo, que permiten controlar y monitorizar los recursos asignados a cada *slice*, priorizar servicios en tiempo real y adaptar la configuración de red a las condiciones operativas. Estas capacidades han sido validadas en ejercicios como *CWIX* y en programas como FMN Spiral 6, demostrando su eficacia para:

- Garantizar continuidad operativa en entornos degradados.
- Separar comunicaciones aliadas con reglas de acceso diferenciadas.
- Optimizar el uso de espectro y recursos de red según el tipo de unidad o misión.

La capacidad de definir y controlar *slices* de manera flexible convierte al *Network Slicing* en un verdadero multiplicador táctico y estratégico, como muestra la Figura 8 [13], alineado con las necesidades de interoperabilidad, seguridad y agilidad que requieren las operaciones multidominio.

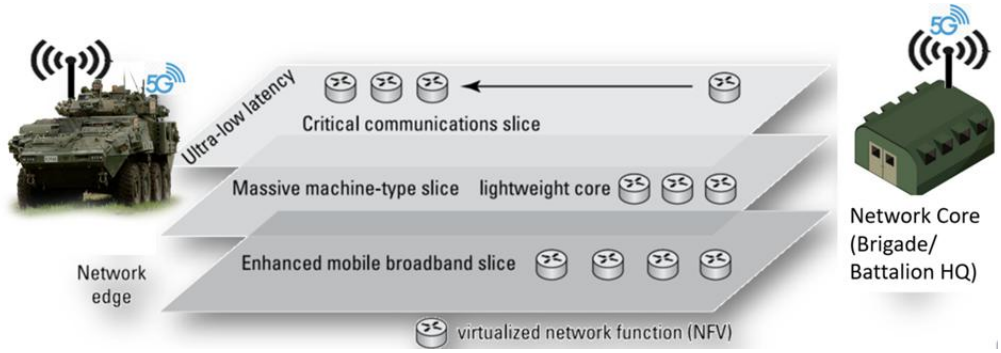

Figura 8: Ejemplo de Network Slicing.

2.4.6 Arquitecturas híbridas y despliegues tácticos

Los despliegues *5G* en el entorno militar no responden a un modelo único, sino que combinan distintas arquitecturas en función del entorno, la misión y la disponibilidad de infraestructura. Esta flexibilidad da lugar a arquitecturas híbridas capaces de operar tanto de manera autónoma como dependiente, y de integrarse con tecnologías heredadas o civiles [13][36].

Los principales enfoques incluyen:

- Infraestructura autónoma (*SA*) vs. no autónoma (*NSA*): en el modelo *SA* (*Stand-Alone*), todo el núcleo de red y acceso se basa en tecnología *5G*, permitiendo funcionalidades completas como *slicing* y *MEC*. En el modelo *NSA* (*Non-Stand-Alone*), el acceso *5G* se apoya en redes *4G LTE* existentes, útil para despliegues iniciales o en zonas con infraestructura parcial.
- Redes híbridas móviles: integración de nodos *5G* en vehículos tácticos, *shelters* desplegables, *UAVs*, buques o plataformas *HAPS*, que pueden actuar como estaciones base móviles, repetidores o puntos de conexión *edge*.
- Despliegues modulares y portátiles: sistemas compactos de rápida activación, como los empleados en TRITÓN, permiten establecer redes *5G* privadas completas en cuestión de minutos, con núcleo de red embebido, *slicing* autónomo y enlaces seguros con nodos centrales o satélites.
- Interoperabilidad con redes heredadas o civiles: integración de redes *5G* con sistemas de comunicación *legacy* (propios de las FAS), *SATCOM*, *HF/VHF/UHF* o enlaces de microondas, así como su coexistencia con redes comerciales con prioridad militar mediante acuerdos regulados.
- Operaciones en malla (*mesh networks*): topologías dinámicas que permiten a cada nodo funcionar como retransmisor, ideal para entornos EM contestados o con alta movilidad, mejorando la resiliencia y el alcance de la red.

Estas arquitecturas, validadas en ejercicios multinacionales y programas piloto OTAN/UE, permiten adaptarse a distintos niveles de amenaza, cobertura, movilidad y persistencia, asegurando que las redes *5G* tácticas sean robustas, seguras, interoperables y altamente disponibles.

Un elemento crucial para facilitar este tipo de despliegues es el uso de *Zero-Touch Provisioning* (ZTP) [13], una funcionalidad que permite la configuración automática de

los nodos de red sin intervención manual, lo que reduce el tiempo de activación, minimiza errores humanos y mejora la escalabilidad. Esta capacidad se implementa a través de orquestadores multinivel, que permiten la detección, inicialización, configuración y supervisión remota de elementos como *UPFs, AMFs, SMFs* y nodos *MEC*.

Ejercicios como *CWIX* han demostrado que los despliegues automatizados con *ZTP* son viables incluso en escenarios multinacionales, permitiendo activar *slices* personalizados, servicios *C2* y aplicaciones críticas desde nodos *edge* móviles o embarcados. Además, proyectos como TRITÓN han incorporado soluciones *ZTP* en sus redes tácticas, facilitando el despliegue rápido de *shelters* de mando, vehículos conectados o *UAVs* como relés temporales.

En conjunto, la automatización del despliegue mediante *ZTP* y orquestación inteligente constituye un componente esencial para lograr la agilidad operativa, la resiliencia de red y la adaptación dinámica que requieren las operaciones multidominio en escenarios exigentes.

Capítulo 3. Aplicaciones del *5G* en operaciones multidominio

3.1 Comunicación y conectividad avanzada

La comunicación y la conectividad avanzada son aspectos críticos para la ejecución efectiva de operaciones multidominio (*MDO*), permitiendo una coordinación precisa y sincronizada entre unidades y plataformas desplegadas en diferentes dominios operativos. En este contexto, la tecnología *5G* se posiciona como una solución tecnológica disruptiva, ofreciendo capacidades que superan ampliamente a las generaciones anteriores (*3G* y *4G*) y resolviendo limitaciones tradicionales asociadas a las comunicaciones militares.

El *5G* aporta una conectividad robusta y ultrarrápida, con velocidades de transferencia de datos que alcanzan hasta varios gigabits por segundo (Gbps). Según lo validado en ejercicios como *CWIX*, esta capacidad permite gestionar de forma efectiva grandes volúmenes de datos generados por sensores *ISR* (Inteligencia, Vigilancia y Reconocimiento), plataformas no tripuladas (*UAV, UGV, USV*) y sistemas distribuidos de vigilancia y seguimiento, generando una conciencia situacional integral y precisa en tiempo real [4][36].

Una característica diferencial clave del *5G* es su ultra baja latencia (*URLLC - Ultra Reliable Low Latency Communications*), capaz de reducir los tiempos de respuesta a valores próximos a 1 milisegundo. Esto resulta crítico para la eficacia operativa de misiones que requieren decisiones rápidas y precisas, tales como el control remoto de vehículos autónomos, operaciones de *targeting* y fuego coordinado, o sistemas avanzados de armamento guiado. Proyectos nacionales como TRITÓN y BACSI han demostrado empíricamente en escenarios reales cómo estas capacidades mejoran significativamente la velocidad y precisión de las decisiones tácticas y estratégicas [7][8].

El *5G* también proporciona conectividad masiva (*mMTC - Massive Machine Type Communications*), que permite interconectar simultáneamente millones de dispositivos por kilómetro cuadrado, algo imposible con tecnologías anteriores. Esta capacidad es esencial en operaciones que demandan una coordinación estrecha entre múltiples plataformas no tripuladas, unidades de combate dispersas geográficamente, nodos de mando móviles (*MCP*, *SDHQ*, *LHQ*), que se desarrollarán en el apartado 5, y redes masivas de sensores desplegadas en los dominios terrestre, marítimo, aéreo y cibernético. Proyectos específicos han validado el uso de *mMTC* para la gestión efectiva de unidades desplegables en entornos tácticos, asegurando comunicaciones seguras y resilientes.

Además, el despliegue efectivo del *5G* en entornos militares se complementa estratégicamente con tecnologías como el *Edge Computing* (MEC) y el *Network Slicing* [28][29]. El *Edge Computing* permite procesar localmente datos críticos en tiempo real, reduciendo aún más la latencia operativa y mejorando la autonomía táctica de los nodos desplegados en entornos contestados o degradados. Por su parte, el *Network Slicing* ofrece la posibilidad de segmentar la red en múltiples redes lógicas independientes, proporcionando perfiles diferenciados en términos de seguridad, calidad del servicio (*QoS*) y capacidad operativa. Documentos técnicos y ejercicios multinacionales como los realizados por la OTAN han validado ampliamente la utilidad del *slicing* para aislar y

proteger flujos críticos de información en operaciones conjuntas y multinacionales [37].

La integración del *5G* con tecnologías emergentes como la Inteligencia Artificial (IA), el *Big Data* y el Internet de las Cosas (*IoT*) militar amplifica aún más sus beneficios operacionales. La IA, por ejemplo, permite realizar análisis predictivos y de optimización en tiempo real, mientras que el *Big Data* potencia la capacidad de procesar y explotar enormes volúmenes de datos operativos para mejorar la conciencia situacional y la eficacia táctica.

La combinación de velocidades de transmisión ultrarrápidas, latencia mínima, capacidad de conexión masiva y tecnologías complementarias como *MEC*, *slicing*, IA, *Big Data* e *IoT* militar, hacen del *5G* una infraestructura crítica para las comunicaciones avanzadas necesarias en operaciones multidominio, permitiendo que las Fuerzas Armadas operen con niveles superiores de efectividad, coordinación e interoperabilidad [13].

3.2 Interoperatibilidad en operaciones multinacionales

La interoperabilidad multinacional constituye un pilar esencial para la eficacia de las operaciones multidominio realizadas por coaliciones y alianzas internacionales como la OTAN y la Unión Europea. En este marco, la tecnología *5G*, con su arquitectura flexible y basada en estándares abiertos, emerge como una herramienta clave para facilitar y mejorar significativamente la interoperabilidad técnica, doctrinal y operativa entre fuerzas aliadas.

Una de las principales ventajas que ofrece el *5G* en este ámbito es la posibilidad de desplegar redes compartidas o federadas con múltiples niveles de prioridad y segmentación (mediante técnicas como el *Network Slicing*), lo que permite a los distintos países participantes operar sobre una misma infraestructura física, pero con entornos de red lógicamente aislados y personalizados. Esta capacidad resulta esencial para mantener la seguridad de la información y los requisitos operativos propios de cada nación, sin comprometer la colaboración táctica.

El *5G* permite una rápida integración de nodos aliados y dispositivos heterogéneos gracias al uso de arquitecturas abiertas como *O-RAN*, mecanismos de autoconfiguración como el *Zero Provisioning* e interfaces estandarizadas por el *3GPP* a nivel civil y los *STANAGs* a nivel OTAN [29][38]. Esto facilita el despliegue ágil de infraestructuras conjuntas en escenarios dinámicos. Esta capacidad es crucial para operaciones conjuntas donde múltiples países o unidades requieren comunicaciones aisladas y seguras con niveles específicos de rendimiento y privacidad, como ejercicios multinacionales, despliegues combinados o misiones de la Fuerza de Respuesta Rápida de la OTAN.

La capacidad de *Multi-access Edge Computing* (*MEC*) integrada en las redes *5G* también mejora la interoperabilidad al permitir procesar y compartir información crítica directamente en el borde de la red [28][37]. Esta característica es especialmente útil en escenarios multinacionales donde distintos niveles de mando y diferentes naciones requieren acceso en tiempo real a información táctica precisa y coherente.

Asimismo, la implementación del *5G* en ejercicios multinacionales ha demostrado la capacidad de estas redes para integrarse eficazmente con plataformas heredadas y

sistemas preexistentes *(legacy systems*), reduciendo significativamente la necesidad de reemplazo total de infraestructuras anteriores y facilitando una transición tecnológica gradual y sostenible.

En conjunto, la tecnología *5G* representa un habilitador clave para la interoperabilidad efectiva entre fuerzas aliadas, garantizando no solo la compatibilidad técnica, sino también una mayor eficiencia operativa, autonomía táctica y cohesión estratégica en el marco de operaciones multinacionales.

3.3 Reducción de latencia para operaciones en tiempo real

La latencia, definida como el tiempo que tarda un paquete de datos en ir desde el origen hasta el destino, es un factor crítico en entornos operativos donde la rapidez de reacción y la sincronización son determinantes. En el contexto de este trabajo, se hace referencia principalmente a la latencia extremo a extremo (*E2E*) medida desde la capa de usuario de la aplicación hasta el plano de usuario del receptor, tal como la define el *3GPP* [2]. No se contempla la latencia total desde aplicación a aplicación, sino el retardo introducido en la red de acceso y transporte. La tecnología *5G* introduce una mejora sustancial en este ámbito, con capacidades de comunicación que permiten reducir la latencia hasta niveles inferiores a 1 milisegundo, frente a los 30-50 ms característicos de las redes *4G*.

Esta ultra baja latencia resulta esencial para una amplia gama de aplicaciones tácticas y estratégicas en operaciones multidominio. Entre ellas destacan el control remoto de plataformas no tripuladas (*UAVs, UGVs, USVs*), la operación de sistemas de armamento inteligente, el guiado de misiles en tiempo real, y el soporte a la toma de decisiones basada en inteligencia artificial distribuida [8][36].

En el dominio cibernético, la latencia reducida también contribuye a mejorar la detección y respuesta frente a amenazas, permitiendo la implementación de sistemas de defensa activos y adaptativos que pueden responder en milisegundos ante un ciberataque.

Del mismo modo, en el ámbito espacial y aéreo, las comunicaciones de baja latencia permiten el enlace seguro y preciso con plataformas en movimiento (como satélites *LEO* o aeronaves de combate) para la transmisión de datos de misión, imágenes *ISR* (Intelligence, Surveillance and Reconnaissance) o comandos de vuelo.

El uso combinado de *5G* con tecnologías como *Edge Computing* y redes no terrestres (*NTN*) refuerza aún más esta ventaja, ya que el procesamiento de la información se realiza en proximidad al usuario final, eliminando cuellos de botella y mejorando la eficiencia en tiempo real [28][30].

Por tanto, la reducción de latencia proporcionada por el *5G* representa una ventaja táctica decisiva para garantizar una superioridad operativa basada en la velocidad de ejecución, la precisión en la respuesta y la sincronización efectiva entre múltiples dominios.

3.4 Apoyo a la coordinación de dominios cibernético, espacial, aéreo, terrestre y marítimo

Uno de los principales desafíos de las operaciones multidominio es lograr una coordinación efectiva entre todos los dominios operativos, que anteriormente han funcionado de forma parcialmente independiente. Tradicionalmente, cada dominio (terrestre, aéreo, naval, cibernético y espacial) disponía de sistemas *CIS* propios, con arquitecturas, frecuencias y doctrinas de empleo distintas, lo que dificultaba la interoperabilidad táctica y obligaba a realizar procesos de fusión de datos de forma manual o centralizada. La tecnología *5G*, gracias a su capacidad para proporcionar conectividad ubicua, baja latencia y transmisión segura de datos en tiempo real, permite superar estas barreras y establecer una integración operativa sin precedentes entre dominios.

En el dominio cibernético, el *5G* permite una comunicación segura entre nodos distribuidos, centros de mando y sensores en red, lo cual fortalece la resiliencia y capacidad de reacción ante amenazas híbridas y ciberataques. En el dominio espacial, facilita la interconexión con satélites de órbita baja (*LEO*) y estaciones terrestres, mejorando la transmisión de inteligencia geoespacial y servicios de posicionamiento [34].

A nivel aéreo, el *5G* proporciona enlaces de alta capacidad entre aeronaves, *UAVs* y centros de control, permitiendo compartir en tiempo real datos *ISR* o vídeo de reconocimiento, y mejorando la coordinación con el dominio terrestre en tiempo de combate [36].

En el dominio marítimo, se integran sensores embarcados, plataformas no tripuladas y sistemas de navegación que operan sincronizados con redes tácticas desplegadas en tierra o aire [35].

En tierra, la conectividad *5G* permite coordinar vehículos de combate, tropas desplegadas, sistemas autónomos terrestres y sensores de vigilancia perimetral, proporcionando un entorno operacional digitalizado donde la información fluye en tiempo real entre todos los actores implicados [13].

La arquitectura del *5G* facilita esta coordinación mediante el uso de *Network Slicing* y *Edge Computing*, que permiten adaptar dinámicamente la red a las necesidades particulares de cada dominio y misión [28] [29]. Esto se traduce en una mayor capacidad de sincronización táctica, respuesta conjunta y eficiencia operativa.

En conjunto, el *5G* se presenta como un catalizador clave para la fusión operativa de dominios, permitiendo a las fuerzas armadas alcanzar una verdadera superioridad multidominio mediante la integración continua, coordinada y adaptativa de todos los entornos operativos.

3.5 Redes privadas y tácticas militares

El uso de redes privadas *5G* en entornos militares tácticos representa una evolución clave en la forma en que las Fuerzas Armadas gestionan la conectividad, la seguridad y la autonomía operativa en escenarios desplegados. Estas redes están diseñadas para operar de forma independiente de las infraestructuras civiles, garantizando mayor control, flexibilidad y resiliencia ante amenazas electrónicas, ciberataques o fallos de red.

Una red privada *5G* permite a una unidad militar establecer su propia infraestructura de comunicaciones sobre el terreno, con capacidad de autoconfiguración, segmentación lógica y gestión autónoma del tráfico. Esto es posible gracias a tecnologías como el *Network Slicing*, *O-RAN* y, especialmente, el *Zero Touch Provisioning* (ZTP), también conocido como *Zero Provisioning* [13]. Esta tecnología permite desplegar y configurar automáticamente nodos, *routers* y componentes de red sin intervención humana, reduciendo significativamente los tiempos de puesta en marcha, minimizando errores operativos y eliminando la necesidad de técnicos especializados en el campo de operaciones.

El *Multi-access Edge Computing* (*MEC*) juega un papel fundamental al proporcionar capacidad de procesamiento local en el borde de la red, garantizando autonomía operativa en condiciones de comunicación limitada o degradada. En conjunto, estas tecnologías habilitan la creación de redes privadas tácticas altamente adaptativas y robustas, fundamentales para las operaciones multidominio modernas.

El *ZTP* cobra especial relevancia en situaciones donde la rapidez de despliegue y reconfiguración y la autonomía táctica son determinantes: operaciones especiales, misiones de entrada inicial, unidades desplegadas en entornos hostiles o aislados, o escenarios multinacionales donde se requiere una infraestructura común adaptada a cada actor participante. En la Figura 9 [13] podemos observar un ejemplo de preparación de una misión empleando esta tecnología. Gracias a esta tecnología, una unidad puede activar una red privada segura desde el momento en que los dispositivos reciben alimentación eléctrica, autoconfigurándose con parámetros previamente definidos, pero reconfigurables en cualquier momento, y conectándose automáticamente a nodos *edge* o redes superiores [28][29]. En las FAS se busca tener soberanía propia y no depender de los operadores de telecomunicaciones existentes, por lo que se llevan a cabo proyectos y negociaciones para convertirse en un proveedor y tener tarjetas *SIM* propias y actuar como un operador.

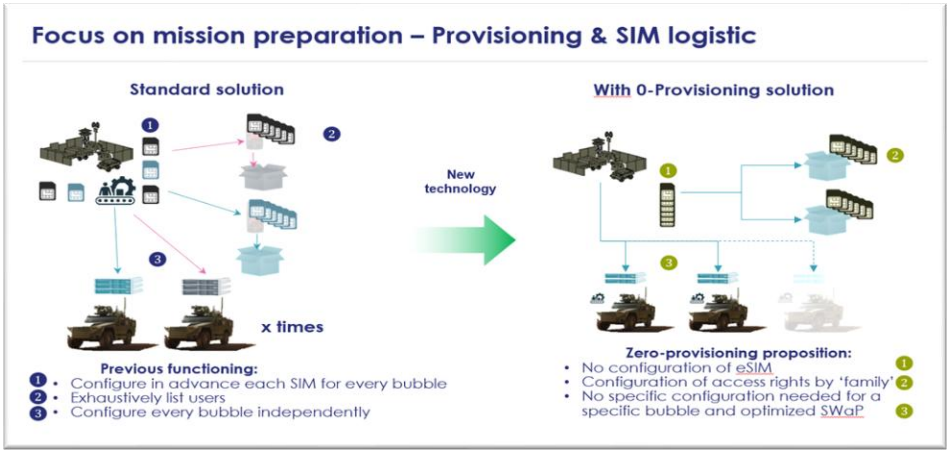

Figura 9: Ejemplo de ZTP.

Estas redes privadas permiten integrar sensores *ISR*, plataformas no tripuladas (*UAVs*, *UGVs*, *USVs*), dispositivos *IoT* militares y sistemas *C2*, gestionando todos estos elementos de forma local, con baja latencia y alta fiabilidad. Esto es crucial para operaciones distribuidas que dependen de la coordinación simultánea de activos en múltiples dominios.

Otra ventaja es la capacidad de operar incluso sin conexión a redes centrales o enlaces satelitales, lo que proporciona un nivel adicional de resiliencia y continuidad operativa. Esta independencia permite mantener el mando y control, el flujo de inteligencia y las comunicaciones tácticas incluso en escenarios degradados.

Los ensayos documentados demuestran que estas redes pueden establecer enlaces seguros y escalables entre buques, vehículos, puestos de mando y sensores en operaciones conjuntas. Asimismo, proyectos del Ministerio de Defensa como ZEUS, y experimentos con plataformas HAPS, han validado el uso de redes privadas 5G como soluciones viables para despliegues reales [7][8][13].

3.6 Proyectos 5G en el Ministerio de Defensa

El Ministerio de Defensa español ha desarrollado e impulsado una serie de proyectos piloto y demostradores tecnológicos para evaluar la aplicabilidad del *5G* en entornos militares reales. Estos proyectos, impulsados por organismos como EMAD, JCISAT, DGAM, MCCE o la UME, se centran tanto en el entorno táctico como estratégico, y reflejan una visión integral de transformación digital multidominio.

• Proyecto ZEUS (Ejército de Tierra): Liderado por JCISAT, ZEUS estudia el uso del *5G* como infraestructura base para redes tácticas móviles. Incluye pruebas con vehículos conectados, integración de sensores, realidad aumentada, *edge computing*, y despliegue de nodos *C2* en tiempo real. Se han realizado demostraciones en escenarios con guerra electrónica degradada y entornos de alta movilidad [6].

• Proyecto TRITÓN (Armada): Este proyecto busca validar el uso de *5G* como tecnología de conectividad embarcada para operaciones navales, incluyendo el enlace con *UAVs* y nodos costeros. El proyecto ha sido vinculado a pruebas de proyección anfibia,

segmentación de red y soporte de plataformas tipo *HAPS* y satelitales [7].

• Proyecto BACSI (Base Conectada, Sostenible e Inteligente): Impulsado por el Ministerio de Defensa y el de Transportes, BACSI transforma bases militares en nodos inteligentes que combinan *5G*, IA, *IoT*, sensores, *edge computing* y sostenibilidad energética [8].

• Proyecto *FANET* (*Federated Artificial-intelligence over Networked Edge Topologies*): Busca integrar IA distribuida y capacidades de federación de datos en redes *edge 5G*. Coordinado por DGAM y MCCE, investiga cómo desplegar inteligencia artificial táctica en redes no centralizadas y escenarios sin cobertura satelital o terrestre directa [39].

• LAB *5G* del MCCE: El Mando Conjunto del Ciberespacio ha puesto en marcha un laboratorio de experimentación *5G* para validación doctrinal y técnica de tecnologías como *MEC*, *NS*, conectividad con *UxV*, ciberdefensa federada y resiliencia operativa. Este laboratorio está vinculado al proyecto NUCOCAS y se orienta a definir arquitecturas *5G* modulares y escalables [40].

• Proyecto con la UME: La UME ha participado en ejercicios de despliegue rápido de nodos *5G* para gestión de emergencias, comunicaciones de resiliencia en zonas devastadas y enlaces entre drones y puestos de mando avanzados. Las pruebas se han realizado en colaboración con operadoras y fabricantes nacionales, aplicando el *5G* como infraestructura crítica dual [41].

• Proyecto CDAP 5G DEF (Centro de Desarrollo, Adiestramiento y Pruebas para Operaciones Militares en Ciberdefensa con tecnología 5G): Este centro se dedica a la preparación, desarrollo y ejecución de la política de defensa en el ámbito de la ciberdefensa, utilizando tecnología 5G.

•Nube de Combate: NUCOCAS, liderado por el MCCE, diseña la futura arquitectura de red del MINISDEF, basada en principios *cloud* y *edge*, segmentación lógica y virtualización completa de funciones de red (*NFV*). Este modelo está orientado a redes privadas *5G* escalables, seguras y federables para uso conjunto de los tres Ejércitos [43].

•Proyecto *5G* Conjunto: Consolida la coordinación entre Ejército de Tierra, Armada, Ejército del Aire y del Espacio, y organismos conjuntos (EMAD, MOPS, MCCE, DGAM), para experimentar con despliegues *5G* federados, interoperabilidad multinacional, y uso de *slices* OTAN. Incluye iniciativas doctrinales asociadas al Plan JEMAD para las MDO [44].

Además, se han explorado sinergias con tecnologías habilitadoras como la Inteligencia Artificial (IA), el *Big Data* o la ciberseguridad aplicada al entorno militar, donde se reconoce al *5G* como uno de los facilitadores clave para los nuevos sistemas inteligentes de defensa. La integración de estas capacidades también se ha abordado en foros y reuniones técnicas como el Grupo de Trabajo de Digitalización del MOPS [45] donde se destacan líneas prioritarias como la automatización de despliegues, la segmentación lógica de redes y la necesidad de una arquitectura modular para facilitar la interoperabilidad multinacional.

En conjunto, los proyectos *5G* desarrollados por el Ministerio de Defensa reflejan un enfoque integral que combina experimentación tecnológica, adaptación doctrinal y colaboración con la industria, siendo Telefónica e Indra empresas que participan activamente con las Fuerzas Armadas en estas clases de proyectos, sentando las bases para una futura implantación a gran escala del *5G* en las operaciones multidominio de las Fuerzas Armadas.

3.7 Proyectos *5G* internacionales (UE y OTAN)

Tanto la Unión Europea como la OTAN han identificado la tecnología *5G* como un elemento estratégico para transformar las capacidades de Defensa, aumentar la resiliencia operativa y garantizar la interoperabilidad entre aliados. En ambos casos, se han puesto en marcha iniciativas, programas de experimentación y ejercicios multinacionales que consolidan el *5G* como tecnología clave para el entorno operativo multidominio.

Unión Europea: La Agencia Europea de Defensa (*EDA*) y la Comisión Europea canalizan la inversión en tecnologías *5G* de defensa a través de los programas:

- *European Defence Fund* (*EDF*): Financia proyectos como COMP4DRONES, PADIC o EUDAAS, que exploran la integración de plataformas autónomas, conectividad táctica y *edge computing* con redes 5G [46].

- *Permanent Structured Cooperation* (*PESCO*): Incluye proyectos de interoperabilidad *C2* y conectividad entre sistemas no tripulados, donde el *5G* aparece como tecnología habilitadora para redes distribuidas [46].

- *Smart Networks and Services Joint Undertaking* (*SNS JU*): En su segunda fase ha priorizado la aplicación de *5G* en sectores críticos como seguridad y defensa, estableciendo hojas de ruta para su despliegue en contextos tácticos, incluyendo *NS*, *MEC* y conectividad resiliente [21].

- Proyecto *MN5G* (*Multinational 5G*): Iniciativa multinacional para el desarrollo conjunto de capacidades *5G* en entornos de Defensa. Liderado por varios Estados miembros, promueve un enfoque colaborativo para el despliegue de redes privadas tácticas, interoperabilidad federada y conectividad de alta seguridad [47].

OTAN: Reconoce el *5G* como tecnología disruptiva en sus documentos estratégicos como el *Digital Transformation Implementation Strategy* (*DTIS*) [48] y el *Allied Concept for Multi-Domain Operations (AC-MDO)* [9][10].

- *FMN Spiral 6*: Esta sexta iteración del programa *Federated Mission Networking* incluye la adopción de servicios *5G*, redes virtualizadas, *Edge Computing* y *Network Slicing*. Busca crear una arquitectura, mostrada en la Figura 10, federada y común entre aliados, adaptable a misiones conjuntas, interoperable y cibersegura [5].

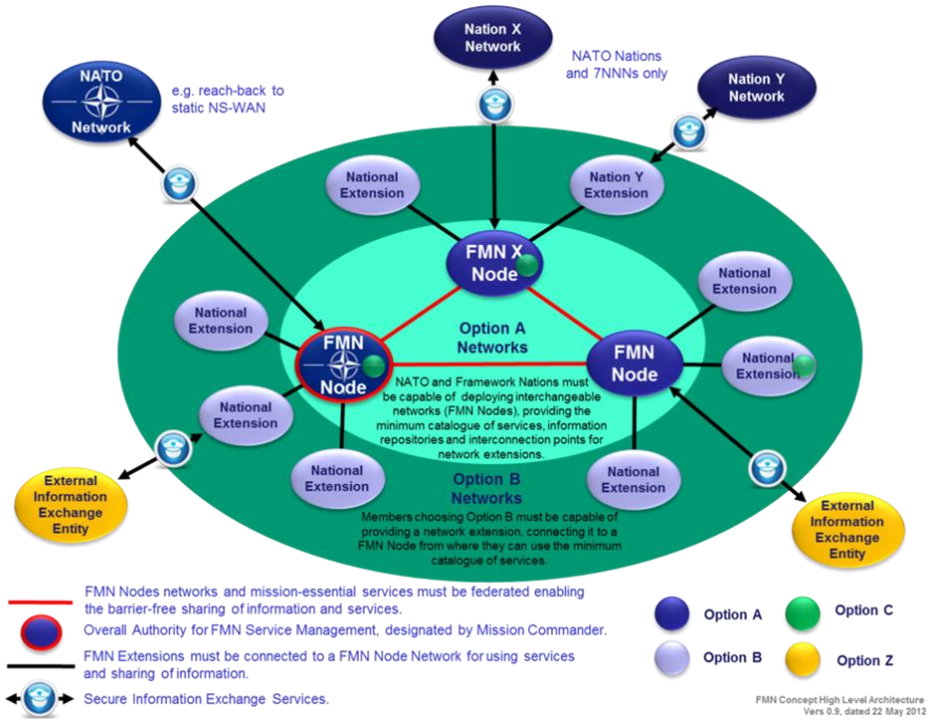

Figura 10: Arquitectura FMN.

- *COMPAD 5G* (*Coalition Operations for Mission Planning and Decision-making*): Proyecto piloto para validar cómo el *5G* y tecnologías asociadas pueden mejorar las capacidades de mando y control en coaliciones, incluyendo *edge tactical clouds*, *slicing* por tipo de misión y sensores distribuidos [49].

- *DIBAX* (*Deployable Integrated Backbone for Allied eXpeditionary networks*): Aunque no es exclusivo del *5G*, este programa analiza redes de *backbone* militares desplegables con integración de tecnologías emergentes. En las fases más recientes se explora la inclusión de nodos 5G en redes móviles de campaña [50].

- *CWIX* (*Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise*)**:** En *CWIX* 2024, se han evaluado soluciones *5G* tácticas, conectividad entre plataformas no tripuladas (*UxV*), nodos *C2 edge*, y compartición de inteligencia multisensorial sobre redes federadas. Estas pruebas contribuyen a la generación de estándares OTAN interoperables [52].

- *STO* (*Science and Technology Organization*)**:** A través de paneles, como *IST* (*Information Systems Technology*) y *SCI* (*System Concepts and Integration*), se han publicado estudios sobre *5G* para entornos operacionales, centrándose en aspectos como resiliencia, espectro compartido, y ciberseguridad federada. Ejemplos notables son el *GT IST-220* y los *Technical Reports TR-SET-293 y IST-ET-123* sobre comunicaciones tácticas *5G* y nodos *edge* distribuidos [13][52].

Capítulo 4. Desafíos y limitaciones del *5G* en entornos operativos militares

4.1 Resiliencia frente a amenazas electrónicas e interferencias

Uno de los principales retos para la implementación del *5G* en escenarios operativos es su exposición a amenazas electrónicas, especialmente las interferencias deliberadas (*jamming*, es decir, la emisión intencionada de señales para bloquear o degradar la comunicación en frecuencias específicas), *spoofing* (la suplantación de identidad de un emisor legítimo con señales falsas para confundir o tomar el control de los sistemas de comunicaciones), y el uso hostil del espectro [33]. A pesar de sus capacidades avanzadas, las redes *5G* utilizan el espectro radioeléctrico, lo que las convierte en vulnerables a ataques de guerra electrónica, degradación de señal y saturación del canal. Las frecuencias utilizadas por el *5G*, en particular las bandas medias (3,5 GHz) y milimétricas (*mmWave*), ofrecen gran capacidad de transmisión, pero tienen menor alcance y mayor susceptibilidad a obstáculos físicos y perturbaciones electromagnéticas.

Para mitigar estas amenazas, el diseño de redes tácticas *5G* debe incorporar funcionalidades de detección y adaptación dinámica, como *beamforming* direccional, protocolos de salto de frecuencia (*frequency hopping*), diversificación de enlaces, *MIMO* masivo, y algoritmos de selección de canal en tiempo real. Asimismo, arquitecturas resilientes como las propuestas en el *IST-220* [13] contemplan segmentación prioritaria del tráfico crítico, recuperación autónoma de nodos comprometidos, y reconfiguración de rutas mediante *SDN*.

Además, se recomienda infraestructuras marítimas *5G* reforzadas con *RAN* inteligentes y elementos de seguridad física y lógica, incluyendo *RF sensing* y medidas anti-interferencia [35]. En ejercicios *CWIX*, se validaron despliegues con *switching* automático entre múltiples enlaces (*5G, LTE, UHF*), con tolerancia a ataques electrónicos dirigidos y latencia mantenida bajo condiciones adversas. El proyecto ZEUS incorpora módulos de detección de *jamming* y *switching* automático hacia enlaces redundantes (por ejemplo, *SATCOM*), garantizando continuidad operativa [6].

4.2 Ciberseguridad: protección de redes y gestión de datos

La introducción del *5G* en redes de Defensa incrementa la complejidad del ecosistema de ciberseguridad. Su arquitectura basada en funciones virtualizadas (*NFV*), control por software (*SDN*), conectividad masiva y *edge computing* descentralizado introduce nuevos vectores de ataque que requieren una protección integral. El principio de seguridad por diseño (*security-by-design*) se convierte en un pilar fundamental para prevenir, detectar y responder ante amenazas persistentes avanzadas (*APT*).

La Estrategia de Ciberseguridad del MINISDEF [53] define como prioridad la detección temprana mediante sensores inteligentes, segmentación lógica adaptativa basada en contexto operacional, y respuesta automatizada basada en inteligencia artificial. El documento de arquitectura NUCOCAS propone un modelo federado y modular, con

funciones desplegadas en contenedores aislados, autenticación distribuida y control granular de acceso [43]. Este enfoque permite implementar *Zero Trust* y aplicar mecanismos de aislamiento dinámico en caso de compromiso.

Además, el uso de *MEC* introduce retos adicionales de seguridad local: requiere aplicar cifrado robusto (*IPSec, TLS 1.3*), firmas digitales para funciones orquestadas y orquestadores de confianza verificados [54]. La protección del plano de control y la segregación de *slices* mediante mecanismos de *VNF chaining* seguro resultan críticos para impedir movimientos laterales y accesos no autorizados entre segmentos de red.

4.3 Cobertura extrema y sostenibilidad en zonas remotas

Las operaciones militares se desarrollan frecuentemente en áreas sin infraestructura civil, como desiertos, montañas, regiones árticas o zonas marítimas. En estos contextos, el despliegue y mantenimiento de redes *5G* presenta un desafío logístico importante. Aunque las redes *5G* pueden operar en formato compacto (*small cells*, gNodeBs embarcadas), su cobertura limitada en bandas altas requiere soluciones complementarias.

Se ha detallado el uso de plataformas de gran altitud como *Zephyr* o *Sceye*, capaces de mantener nodos *5G* activos durante semanas, operando a más de 20 km de altitud, con enlaces persistentes a estaciones móviles en tierra [55]. Estas soluciones se integran con sistemas de energía solar, refrigeración pasiva y enlaces redundantes (incluyendo *SATCOM*). Las plataformas *NTN* descritas en el *Release* 17 de *3GPP*, incluyendo satélites *LEO*, complementan esta arquitectura proporcionando cobertura persistente para nodos móviles en entornos sin *LoS* (*Line of Sight*) terrestre [2][29].

Asimismo, el uso de nodos embarcados en vehículos, *UAVs* o mochilas portátiles permite extender la cobertura y crear topologías de red *mesh* en tiempo real. Los diseños validados por proyectos como TRITÓN y NUCOCAS combinan estos elementos con nodos *edge* y orquestación dinámica para asegurar continuidad operativa, incluso sin conectividad con centros de datos centrales [7][43].

4.4 Integración de 5G con tecnologías heredadas y futuras

La transición hacia el *5G* requiere mantener la compatibilidad con plataformas ya desplegadas en las Fuerzas Armadas, incluyendo radioenlaces *HF/VHF/UHF*, enlaces satelitales y sistemas *C2* preexistentes. La interoperabilidad entre tecnologías es esencial para garantizar la efectividad en operaciones conjuntas y multinacionales.

El diseño modular basado en servicios (*SBA*) permite integrar funciones *5G* dentro de arquitecturas híbridas. NUCOCAS propone *gateways* físicos y virtuales, con doble pila *IPv4/IPv6*, traducción de protocolos heredados (ej. *Link-11, 1553B*) y adaptadores *SDR* programables. El uso de contenedores y funciones virtuales (*VNFs*) desplegables mediante *Zero Provisioning* facilita una integración ágil, permitiendo conectar nuevos nodos sin intervención técnica manual [43].

La orquestación multinodo validada en *CWIX* demuestra que las redes híbridas pueden operar con *slicing* federado, gestionando flujos entre nodos *5G*, enlaces satelitales y redes tácticas legadas sin comprometer la seguridad ni la eficiencia [4][5]. Además, tecnologías

como *IAB (Integrated Access and Backhaul)* permiten extender redes *5G* sin necesidad de infraestructura de transporte fija, clave para operaciones en movilidad o en despliegues rápidos [56].

4.5 Retos legales y regulatorios en el uso militar del espectro radioeléctrico 5G

El despliegue del *5G* por parte de las Fuerzas Armadas requiere acceso garantizado al espectro radioeléctrico, frecuencias que actualmente están asignadas mayoritariamente a operadores civiles. Esto plantea tensiones regulatorias, especialmente en tiempos de paz, donde el uso militar del espectro debe coordinarse con autoridades civiles y con normativas nacionales e internacionales.

El documento de la Comisión Interministerial del Espectro del MINISDEF [57] plantea soluciones como:

- Uso compartido dinámico mediante gestión cognitiva del espectro (*CRRM*).
- Corredores espectrales temporales para despliegues y ejercicios.
- Reservas prioritarias en regiones específicas bajo esquemas de licencias temporales o preasignadas.

En paralelo, la OTAN promueve la armonización regional del espectro militar, estableciendo bandas preferentes comunes para sus miembros (por ejemplo, en el rango n77/n78) y políticas para la reserva anticipada en ejercicios conjuntos. Estos lineamientos están siendo integrados en el marco de *FMN Spiral 6* [5][58][59][60].

Desde el punto de vista técnico, la implementación de radios definidas por software (*SDR*) y gestión dinámica del espectro mediante inteligencia artificial permitirá adaptar las emisiones a las condiciones normativas y operativas en tiempo real, asegurando cumplimiento legal y eficacia táctica [61][62].

Capítulo 5. Casos de uso

5.1 Doctrina militar

Para comprender el impacto y la aplicación de tecnologías como el 5G en operaciones militares, es fundamental establecer primero el marco doctrinal que estructura el empleo de la fuerza en diferentes contextos. En la doctrina militar, los niveles de operación y los tipos de entornos definen cómo se organizan, planifican y ejecutan las misiones [64]. Además, la terminología asociada a estos conceptos permite interpretar correctamente el contenido técnico-operativo descrito en este trabajo.

1. Niveles de operación: Las operaciones militares se dividen en tres niveles que, aunque interrelacionados, cumplen funciones distintas [65][66][67]:

- Nivel Estratégico: Se enfoca en los objetivos políticos y militares a largo plazo de una nación o una coalición (como la OTAN o la UE). En este nivel se toman decisiones sobre el uso de la fuerza, la planificación de capacidades y la proyección de poder. Involucra la dirección del conjunto de las Fuerzas Armadas y la integración con la política exterior.
- Nivel Operacional: Actúa como puente entre lo estratégico y lo táctico. Se ocupa del diseño y ejecución de campañas y operaciones conjuntas en un teatro de operaciones, mediante el uso de medios militares para alcanzar efectos concretos. El arte operacional considera el espacio, el tiempo y los recursos necesarios para lograr los objetivos estratégicos.
- Nivel Táctico: Es el nivel más próximo al combate directo. Implica la planificación y conducción de acciones específicas de unidades militares (batallones, compañías, escuadrones, etc.) en el campo de batalla. Se centra en maniobras, fuego, movimientos y uso inmediato de recursos en un entorno específico. En el contexto táctico, las Fuerzas Armadas se estructuran en diferentes niveles jerárquicos que determinan su capacidad operativa. La unidad básica es el pelotón, compuesto por unos 10 a 30 efectivos, que se agrupa en secciones y, a su vez, en compañías. Varias compañías forman un batallón, normalmente con entre 300 y 1.000 soldados, que constituye una unidad táctica autónoma con capacidades de maniobra y apoyo. Los regimientos o grupos tácticos agrupan varios batallones, y son subordinados a estructuras mayores como las brigadas, que integran miles de efectivos con medios de apoyo logístico, artillería y mando propio. Por encima de ellas se encuentran las divisiones (de 10.000 a 20.000 efectivos) y los cuerpos de ejército, que coordinan múltiples divisiones. Estas organizaciones permiten proyectar poder a distintos niveles del conflicto, desde operaciones limitadas hasta campañas estratégicas conjuntas. La correcta comprensión de estas escalas es fundamental para entender cómo se integran tecnologías como el *5G*, la IA o el *Edge Computing* en las operaciones militares, ya que muchas de estas innovaciones deben desplegarse y adaptarse según el nivel organizativo y la autonomía de cada unidad.

Ejemplos ilustrativos:

- Estratégico: Decidir si una nación debe intervenir militarmente en un conflicto internacional.
- Operacional: Planificar una campaña conjunta para recuperar una zona ocupada.
- Táctico: Organizar un ataque coordinado de una unidad de infantería contra una posición enemiga.

2. Entornos de operación: En la terminología doctrinal, el término "entorno" se utiliza para describir tanto el contexto físico como el funcional en el que se desarrolla la acción militar [68][69][70]:

- Entorno operacional: Es el contexto geopolítico, físico, informacional y tecnológico en el que se lleva a cabo una campaña militar. Incluye tanto los factores de amenaza como las condiciones del teatro de operaciones. Es un concepto amplio, empleado principalmente a nivel estratégico y operacional.
- Entorno operativo: Hace referencia al espacio físico inmediato donde se ejecutan las acciones tácticas. Puede abarcar terrenos urbanos, desérticos, marítimos o aéreos, e incluye todos los elementos que influyen en las decisiones tácticas (clima, visibilidad, orografía, etc.).
- Entorno multidominio: Describe un modelo de operaciones que integra simultáneamente acciones en los dominios terrestre, aéreo, marítimo, cibernético y espacial. El *5G* se convierte en una tecnología habilitadora clave para este tipo de entorno, al proporcionar conectividad y sincronización entre todos los dominios.

3. Términos comunes: A lo largo del trabajo se emplean términos específicos que forman parte del lenguaje técnico-doctrinal de las Fuerzas Armadas [69]:

- Campo de batalla: Espacio donde se desarrollan operaciones militares directas. Puede ser físico o digital (como en el ciberespacio).
- Cuartel General (*HQ*): Centro de mando que dirige y coordina una operación. Puede estar desplegado (*SDHQ*) o en retaguardia (*LHQ*).
- Nodo *C2*: Punto de mando y control que centraliza la información y la toma de decisiones.
- Red federada: Estructura en la que redes militares de diferentes países o unidades cooperan manteniendo su soberanía operativa y seguridad.
- Sistema autónomo o *UxV* (*UAV, UGV, USV, UUV*): Plataforma no tripulada utilizada en tareas *ISR*, logística, desminado u operaciones ofensivas.
- Interferencia electromagnética (*jamming*): Emisión hostil destinada a interrumpir o degradar las comunicaciones de radiofrecuencia.
- *Spoofing*: Técnica de engaño que suplanta señales legítimas (por ejemplo, *GPS* o *C2*), con el objetivo de confundir o controlar sistemas enemigos.

- *Datalink:* Sistema de comunicaciones que permite intercambiar información táctica, como posición, órdenes, imágenes o estado de fuerzas, entre plataformas (aviones, barcos, vehículos, centros de mando) de forma segura, rápida y coordinada. Su objetivo es mejorar la conciencia situacional y la eficacia operativa en el campo de batalla.

5.2 Descripción del contexto operacional

La implementación de redes *5G* en operaciones militares multidominio se ha consolidado como un pilar estratégico para las Fuerzas Armadas y organizaciones internacionales como la OTAN y la Unión Europea [71][72]. Los casos de uso del *5G* táctico se estructuran conforme a las funciones conjuntas (*Joint Functions*) definidas en la *Allied Joint Publication* (AJP)-3 de la OTAN, con énfasis en las capacidades de *Network Slicing* y *Multi-access Edge Computing* (MEC) [20][29[69][73]. Se hace especial foco en los dominios de Sostenimiento (*Sustainment*) y Mando y Control (*Command and Control - C2*), en los cuales estas tecnologías tienen aplicación directa.

- *Network Slicing* permite crear redes virtuales aisladas y seguras sobre infraestructuras compartidas, con perfiles diferenciados de calidad de servicio (QoS) y seguridad. Sus aplicaciones más relevantes incluyen el aislamiento de tráfico por tipo de misión, la separación entre aplicaciones o unidades, y el uso compartido de infraestructura civil con garantías militares. La orquestación dinámica de estas redes mediante técnicas avanzadas como el *Zero Provisioning* (*ZTP*), permite configuraciones rápidas y seguras incluso en entornos operativos cambiantes y hostiles [13].
- *Multi-access Edge Computing* aporta capacidad de procesamiento local en el borde de la red, reduciendo la latencia y permitiendo operar aplicaciones críticas de forma autónoma, incluso en ausencia de enlaces con la nube central o en ambientes degradados [13].

En la Tabla 1[13] se muestran diferentes despliegues de red que se realizan el ámbito de Defensa. Los casos de uso evaluados incluyen tanto configuraciones terrestres como marítimas, integrando múltiples tecnologías y soluciones tácticas. Las funcionalidades clave incluyen conectividad persistente, operación distribuida, resiliencia frente a interferencias, y soporte a plataformas no tripuladas [6][35].

Cuando se detallan las capacidades de los equipos de usuario (*UEs*), se hace referencia tanto a terminales comerciales (*COTS – Commercial Off-The-Shelf*) adaptados, como a dispositivos de diseño militar específico. En escenarios tácticos, los equipos comerciales suelen ser insuficientes por sus limitaciones de resistencia física, autonomía, protección EMI y seguridad. Por ello, en muchos casos es necesario desarrollar soluciones personalizadas a través de colaboración público-privada, con integradores industriales especializados en defensa. El proceso implica requisitos de homologación militar, integración de software de misión, y compatibilidad con estándares OTAN o nacionales. En algunos escenarios, como *MCP* o *AC*, los *UEs* requieren capacidad de operación en entornos hostiles, conectividad mesh, e interfaces específicos con sistemas *C2* o sensores [74][75].

Despliegue de Red	Área Objetivo	Solución de Red 5G	Tamaño de la Red	Número Máximo de Terminales
Red de defensa de área amplia	Áreas con EW benigno, dentro o cerca de territorios aliados utilizando redes móviles de operadores confiables	Red de seguridad pública o segmento (*slice*) de una red pública	Área amplia	Muchos
Red de defensa de área base	Áreas con EW benigno dentro o cerca de territorios aliados con red y aplicaciones locales	Red privada 5G estática. Típicamente, instalaciones fijas de equipos de red	1-10 estaciones base	<10,000
Red de defensa temporal	Áreas con EW de moderada a alta, dentro o cerca de territorios adversarios	Red privada 5G con equipos transportables o montados en vehículos para permitir un despliegue flexible y rápido	1-10 estaciones base	<1,000

Tabla 1: Posibles tipos de despliegue de redes 5G y características para defensa.

Mientras que los dispositivos comerciales pueden ser suficientes para tareas no clasificadas, las misiones críticas requieren terminales personalizados desarrollados junto a la industria [74], con características como:

- Alta rugerización para entornos hostiles.
- Compatibilidad con funciones de red privada *5G* (como *slices* dedicados o *eSIM* segura).
- Cifrado militar y capacidades de control remoto.

Estos desarrollos se realizan mediante contratos específicos con empresas nacionales o aliadas (ej. INDRA, Telefónica Defensa, Airbus DS), y se prueban en entornos privados pertenecientes al MINISDEF. La personalización también incluye sistemas *C2* embarcados, nodos *edge* móviles, y *gateways* de interoperabilidad multinacional [6][8][14].

Las aplicaciones militares típicas empleadas en estos entornos presentan los requisitos técnicos mostrados en la Tabla 2 [13].

Aplicación	Velocidad de datos (*Downlink/Uplink*)	Latencia extremo a extremo (*E2E*)	*Jitter* tolerado
Voz Táctica	64 kbps / 64 kbps	< 50 ms	< 10 ms
Vídeo *ISR* (*HD*)	4 Mbps / 1 Mbps	< 100 ms	< 20 ms
RA/RV Entrenamiento	50 Mbps / 25 Mbps	< 20 ms	< 5 ms
Aplicación *C2*	512 kbps / 256 kbps	< 100 ms	< 20 ms
Control *UAV/UGV*	128 kbps / 128 kbps	< 10 ms	< 5 ms
CBRN Sensor Data	256 kbps / 128 kbps	< 50 ms	< 10 ms

Tabla 2: Requisitos técnicos para aplicaciones militares

5.3 Caso terrestre

Las estructuras validadas por la OTAN en escenarios terrestres han sido experimentados con arquitecturas de referencia que incluyen topologías en malla, controladores distribuidos y funciones de *slicing* dinámico. En los estudios del IST-220 presentan diagramas funcionales y métricas clave de rendimiento (latencia <30ms, *throughput* >1 Mbps, *jitter* <10ms) [13].

5.3.1 *LHQ* (*Large Headquarters*)

El escenario *LHQ* es el conjunto terrestre de casos de uso que comprenden las operaciones terrestres de una gran unidad militar, constituye un cuartel general de mando y control (*C2*) para una amplia gama de unidades y operaciones militares en una extensa área geográfica.

Es necesario formular algunos supuestos e información de contexto para determinar el alcance de las operaciones del escenario *LHQ*, los cuales deben considerarse para un análisis posterior de las soluciones tecnológicas correspondientes. Estos se enumeran a continuación:

- El *LHQ* está compuesto por una infraestructura permanente de una gran unidad operativa terrestre, con numerosos equipos de usuario (*UE*) fijos y móviles, así como soporte para una amplia gama de aplicaciones de usuario. Los escalones militares a nivel de división y superiores deben ser abordadas en las operaciones del *LHQ*.
- El *LHQ* se instala en lo profundo del territorio del país anfitrión o aliado. El entorno electromagnético es benigno, y la mayor parte de las interferencias no son intencionales y son generadas por unidades de señalización conocidas que pueden ser mitigadas fácilmente en cuanto se detectan. Se asume que el *LHQ* nunca será un elemento activo en un entorno operacional de conflicto.
- El *LHQ* actúa como el centro logístico principal o principal/intermedio para el suministro de equipos y raciones, así como centro médico/hospital para las unidades tácticas y fuerzas de menor escalón bajo la supervisión *C2*. Redes ferroviarias, pistas de aterrizaje, autopistas, etc., son elementos habilitadores de la gestión logística e integrales a este escenario.
- El *LHQ* admite una amplia gama de operaciones federadas, incluidas operaciones conjuntas/coalición, así como operaciones multidominio.
- El *LHQ* tiene capacidad de enlace hacia otras unidades *C2* en múltiples continentes.
- En caso de una alta diversidad de operaciones del cuartel general, el *LHQ* necesita ser descentralizado, es decir, desagregado según la estructura organizativa.
- Existe suficiente disponibilidad de puntos de acceso inalámbrico fijo (*FWA*), así como redes *LAN* y/o cables de fibra óptica (FO) en los establecimientos principales/estáticos.
- El entorno físico incluye edificios (electromagnéticamente no transparentes, es decir, las bandas de alta frecuencia son propensas a la atenuación), así como tiendas militares (electromagnéticamente transparentes, es decir, baja o nula atenuación).

- Existe la posibilidad de que haya redes civiles/públicas en las cercanías. Es prácticamente imposible tener un aislamiento electromagnético completo respecto a las redes públicas, por lo que se deben establecer los mandatos doctrinales y las regulaciones necesarias para la coexistencia de redes públicas y militares.
- El personal autorizado dentro de las instalaciones del *LHQ* tiene acceso a sus propios dispositivos de usuario. Esto genera preocupaciones de seguridad respecto al uso mixto de dispositivos personales (*BYOD – bring your own device*) frente a los proporcionados por el cuartel general, lo cual es particularmente relevante cuando una fuerza militar incorpora reservistas en el *LHQ*.
- La distribución de los dispositivos de red es relativamente homogénea desde una perspectiva local, y el cambio en la distribución es predecible.
- Existirán múltiples redes para distintas clasificaciones, y los miembros del cuartel general coordinarán con múltiples agencias externas, incluidas entidades civiles, servicios de emergencia, agencias interinstitucionales y organizaciones multinacionales. Por lo tanto, se requieren múltiples niveles de clasificación de seguridad (desde *NATO-TopSecret* hasta *NATO-Unclassified).* Esto hace necesaria la utilización de comunicaciones satelitales, radios tácticas y formas de onda compatibles con soluciones existentes no basadas en *5G*.
- Debido a la variedad de aplicaciones y tecnologías, se requieren unidades especializadas para la planificación, el despliegue y el mantenimiento de la red. Podría ser necesario el apoyo de especialistas remotos en redes. Las redes privadas pueden requerir actualizaciones/mantenimiento regular por parte del proveedor del equipo. Una evolución temporal hacia la provisión de servicios por terceros podría ser una solución a largo plazo.
- Se requieren características de alto rendimiento (t*hroughput*) y baja latencia para admitir todas las aplicaciones necesarias, además de una gran cantidad de dispositivos basados en sensores. Por lo tanto, desde la perspectiva de *5G*, deben admitirse todos los modelos de canal (*uRLLC, eMBB, mMTC*).

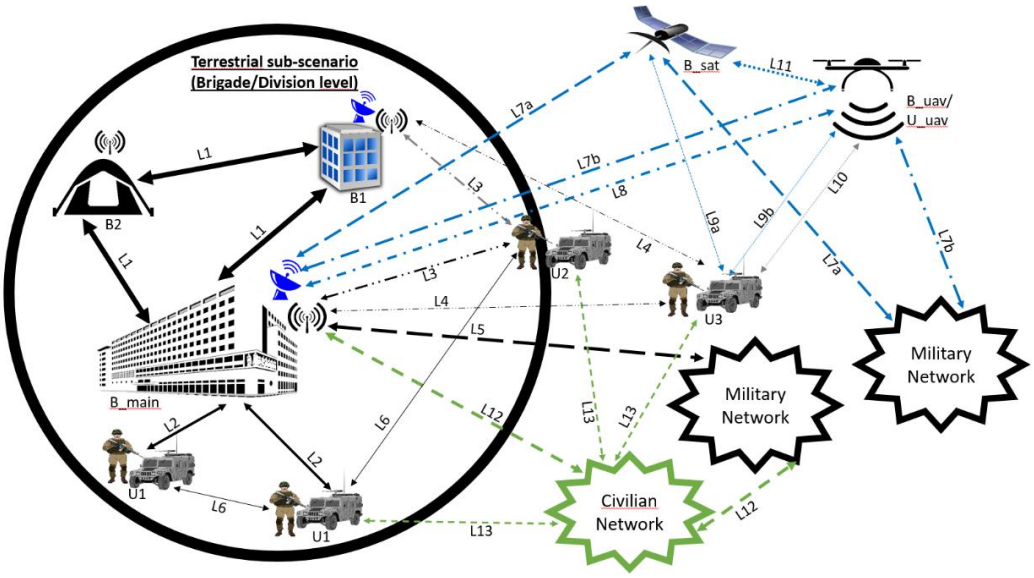

Figura 11: Escenario LHQ.

Los subescenarios y casos de uso dentro del escenario *LHQ*, tal como se indica en las leyendas de la Figura 11 [13], se definen utilizando:

a) una clasificación basada en dispositivos (en la Tabla 3 [13]).

b) una clasificación basada en enlaces (en la Tabla 4 [13]).

Cabe destacar que los dispositivos se categorizan además en dos componentes principales:

1. Un dispositivo tipo B, que indica una estación base.
2. Un dispositivo tipo U, que indica un equipo de usuario (*UE*), ya sea de banda estrecha (*NB*) o de banda ancha (*WB*).

Notas sobre la Figura 11:

- Un enlace *TN* (Red Terrestre) se representa en negro.
- Un enlace *NTN* (Red No Terrestre) y *TN-NTN* se representa en azul.
- Una red pública y sus enlaces asociados se representan en verde.
- Los enlaces dentro de edificios o estructuras (como bloques de tiendas de campaña) no se representan en la Figura 11, sin embargo, forman parte integral de los casos de uso relacionados con las comunicaciones en interiores.
- Dado que algunos usuarios se encuentran dentro de instalaciones o estructuras como edificios o tiendas de campaña, no han sido representados en la Figura 11, sin embargo, forman parte integral de los casos de uso asociados a las comunicaciones en interiores.

ID del Dispositivo	Descripción
B_main (Estación Base – BS)	Edificio principal de oportunidad / Cuartel General de *CIS* militar. Centro logístico y de recopilación de datos que respalda el sostenimiento general de las operaciones. El *gNB* está conectado a la red central *5G* y a la red de datos local.
B1 (BS)	Edificio subordinado de oportunidad. Unidad(es) de respaldo para redundancia como sistema de seguridad, en caso de que la unidad B_main original se vea comprometida; puede convertirse en el nuevo B_main. Réplica exacta de la Red Central (*CN*) como en B_main.
B2 (BS)	Tienda subordinada. *5G gNB - DU*.
B_sat (BS)	Terminal de estación base satelital.
B_uav (BS)	Estación base montada en *UAV*.
U1 (UE)	Usuario final basado en soldado de infantería/vehículo tripulado/vehículos terrestres no tripulados (*UGV*) dentro del área operativa de B_main/B1.
U2 (UE)	Soldado/vehículo tripulado/*UGV* en transición hacia o desde el área operativa del subescenario terrestre. Eventual conversión a U1.
U3 (UE)	Soldado/vehículo tripulado/*UGV* fuera del área operativa de cualquier subescenario terrestre. Eventual conversión a U2 y luego a U1.
U1_in (UE)	Usuario final dentro de un edificio.
U2_in (UE)	Usuario final dentro de una tienda.
U_uav (UE)	Usuario final de vehículos aéreos no tripulados (*UAV*).

Tabla 3: Lista de definiciones de dispositivos del diagrama de casos de uso de LHQ

ID del Enlace	Descripción
L1	Enlace entre B_main y B1, o B_main y B2, o B1 y B2, o entre dos B2. (Fibra óptica; alternativa: *FWA* punto a punto - *PTP*).
L2	Enlace entre B_main/B1/B2 y U1.
L3	Enlace entre B_main/B1/B2 y U2.
L4	Enlace entre B_main/B1/B2 y U3.
L5	Enlace (solo terrestre) entre B_main y otra red militar del mismo o diferente escalón. (Fibra óptica; alternativa: *FWA* punto a punto - *PTP*).
L6	Enlace entre dos dispositivos U1 o entre U1 y U2.
L7a	Enlace entre B_main y B_sat.
L7b	Enlace entre B_main y B_uav.
L8	Enlace entre B_main y U_uav.
L9a	Enlace entre B_sat y U3.
L9b	Enlace entre B_uav y U3.
L10	Enlace entre U_uav y U3.
L11	Enlace entre B_sat y B_uav/U_uav.
L12	Conexión (no un enlace directo) entre B_main y una red civil. (Fibra óptica; alternativa: *FWA* punto a punto - *PTP*).
L13	Enlace entre un UE militar (U1/U2/U3) y una red civil.
L1_in	Enlace entre U1_in y B_main/B1. Comunicaciones en interiores.
L2_in	Enlace entre U1_in_in y B2. Comunicaciones en interiores.

Tabla 4: Lista de definiciones de enlaces del diagrama de casos de uso de LHQ

5.3.1.1 Características

Para que el escenario *LHQ* sea relevante en el contexto de operaciones militares reales, se deben asumir ciertos parámetros y requisitos del sistema, frente a los cuales se puedan proponer soluciones tecnológicas. La Tabla 5 [13] resume dichas características.

La interoperabilidad multinacional en el contexto *LHQ* se asegura mediante el cumplimiento de estándares técnicos OTAN como los definidos por *FMN Spiral 6* y diversos *STANAGs* específicos [5][38]. Estos estándares garantizan que las redes tácticas *5G* implementadas en el *LHQ* puedan integrarse plenamente con sistemas aliados y agencias civiles, gestionando de manera efectiva múltiples niveles de clasificación (desde *NATO-Top Secret hasta NATO-Unclassified*), mediante mecanismos técnicos y doctrinales ampliamente validados en ejercicios internacionales.

Parámetro	Características
Número de usuarios finales	6000 usuarios totales: • 1400 *UEs* militares • 700 *UEs* civiles • Algunos *UEs C2* • 3500 dispositivos *IoT* militares • Algunos dispositivos *IoT* de equipo (División ≈ 10,000 soldados + 600 *staff*; Brigada ≈ hasta 3000 soldados)
Número de *gNBs* (Redundancia para evitar punto único de fallo)	6/8/14/21/25 estaciones base fijas + auxiliares para redundancia Supercélula: máx. 300 km (teórico); 100 km (probado)
Frecuencia de cambio de ubicación de estaciones base	Baja (Cuerpo y División) Media (Brigada)
Variabilidad de posición y movilidad de estaciones base	Fijas Ubicaciones estáticas – sin movilidad durante la operación
Ubicación de *CN* y nodos *Edge*	*CN* dentro del área operativa + nodos *Edge* cerca de los límites de red Redundancia suficiente para evitar puntos únicos de fallo Enlaces por fibra óptica/microondas; en su ausencia, respaldo por *NTN* para unidades tácticas fuera del área
Alcance máximo de enlaces *TN* (Red Terrestre)	Dentro del área operativa: 1.5 km Mismo escalón: 25 km Escalón inferior: hasta 60 km Control: cientos de km
Velocidad media/máx. de unidades móviles terrestres	20–40 km/h / 50 km/h
Altura máx. del mástil de estación base	15 m + altura del edificio (~100 m)
Potencia máx. de transmisión de *gNB*	Muy alta (referencia: dimensión de supercélula)
Área de cobertura	7 km² + Espacios de almacenamiento (por ejemplo, 15 palets de munición ocupan 200–300 m²/día)
Densidad de red (Usuarios finales/área de cobertura)	MEDIA: • 304 por km² • 813 por km² (incl. dispositivos *IoT*)
UEs en estado *RRC* conectado (Usuarios activos simultáneamente)	50%
Requisitos espectrales	• Sub 1 GHz = *HF (BLoS)/VHF/UHF/GSM*/Banda táctica OTAN (larga distancia) • Sub 6 GHz (Banda IV OTAN) + *mmWave* (solo interiores, alta capacidad) → Requiere agilidad espectral
Rendimiento máx./real (Mbps/Gbps)	(Usuarios x rendimiento por usuario) 2133.56 / 1066.78 Mbps
Conectividad de *backhaul* de red de área local	< 180 Mbps (bajada)
Conectividad entre nodos de red	*LHQ* a *SDHQ/MCP*: < 50 Mbps
Enrutamiento local del tráfico en el nodo de red	Obligatorio
Disponibilidad de red *5G*	Continua
Vida útil	Permanente
Tiempo de despliegue	Largo – del orden de meses o años
Provisionamiento y propiedad de la red	Red privada local – *NSA/SA* + Red pública Propiedad/operación gubernamental (*GOGO*) o propiedad comercial y operación gubernamental (*COGO*) → Equipos adquiridos de proveedores confiables

Tabla 5: Características de capacidad tabuladas para el escenario LHQ.

5.3.1.2 Evaluación tecnológica

La evolución de los estándares *5G* definidos por *3GPP* a través de las *Releases* 15, 16 y 17 [2] proporciona una base tecnológica progresivamente más robusta para aplicaciones militares. A continuación, la Tabla 6 presenta las principales capacidades incorporadas

en cada *release* y su relevancia para el escenario *LHQ*:

Release	Capacidades clave	Aplicabilidad al *LHQ*
REL 15	• Introducción del *network slicing* • Tipos de *slice* definidos: *eMBB, URLLC, mMTC* • Soporte de frecuencias sub-6 GHz • *mmWave* (limitado; no apto para *BLOS*) • *massive MIMO* (mMIMO) • *Beamforming* • *URLLC* / eMBB	Base tecnológica inicial para: • Alta capacidad de transmisión • Baja latencia • Comunicaciones diferenciadas por tipo de servicio • Aplicaciones en interiores y enlaces terrestres de corto alcance
REL 16	• Mejoras en mMIMO • Mejoras en *slicing* y URLLC • Mejoras en soporte mmWave (nueva modulación) • Inclusión de V2X	Habilita: • Mejor rendimiento en red densa • Mayor seguridad y segmentación • Aplicaciones de movilidad terrestre y control de MUS terrestres
REL 17	• Mejoras continuas en *mMIMO* y *slicing* • Incorporación de *NTN* (*Non-Terrestrial Networks*) • Soporte para *UAS* (*Uncrewed Aerial Systems*)	Fundamental para: • Comunicaciones más allá de la línea de vista (BLOS) • Integración de *UAVs/UAS* • Conectividad resiliente en escenarios dispersos o con infraestructura limitada

Tabla 6: Tecnologías 5G (Rel específicas) que pueden explotarse potencialmente en el escenario LHQ.

Ejercicios multinacionales como *CWIX* han validado específicamente en escenarios similares al *LHQ* las capacidades clave del *5G*, tales como resistencia ante interferencias intencionales (*jamming*), segmentación avanzada mediante *Network Slicing*, interoperabilidad multinacional bajo estándares *FMN Spiral 6*, y operación integrada de aplicaciones críticas de mando y control (*C2*) [4][5].

El despliegue de capacidades *5G* en escenarios militares como el del *LHQ* implica una evaluación integral de las tecnologías disponibles frente a los requisitos operativos definidos. La siguiente evaluación se centra en la madurez, adaptabilidad, rendimiento y riesgos asociados al uso de 5G y tecnologías relacionadas en entornos tácticos.

- Madurez tecnológica y disponibilidad:

La tecnología *5G*, tanto en su versión *NSA* (*Non-Standalone*) como *SA* (*Standalone*), ha alcanzado un nivel de madurez suficiente para su aplicación en entornos civiles y está en proceso de adaptación para entornos militares. Numerosos estudios y programas piloto, tanto nacionales como de la OTAN, han demostrado la viabilidad de su uso en redes privadas desplegables, en combinación con tecnologías emergentes como *Edge Computing* y *Non-Terrestrial Networks* [6][8][13].

- Cobertura y rendimiento:

Las pruebas realizadas en escenarios reales demuestran que el *5G* puede ofrecer:

  - Alta velocidad de transmisión (>1 Gbps teóricos; >200 Mbps reales en campo),
  - Latencia reducida (<10 ms en condiciones óptimas),
  - Conexiones simultáneas masivas (más de 1000 dispositivos por celda),

- Fiabilidad mejorada a través de técnicas como *beamforming* y *network slicing*.

Sin embargo, el alcance limitado en bandas altas (como *mmWave*) limita su uso a comunicaciones en interiores o distancias cortas. Para enlaces de largo alcance, se requiere soporte complementario mediante enlaces ópticos, radioenlaces terrestres o satélites *LEO* (*NTN*). También, el uso de *Integrated Access and Backhaul* (*IAB*) podría extender eficientemente la cobertura *5G* sin necesidad de infraestructura de transporte fija adicional, facilitando conexiones rápidas entre nodos desplegados en escenarios donde la infraestructura física está limitada [29].

- Interoperabilidad e integración:

El *5G* ofrece ventajas significativas en interoperabilidad, especialmente mediante protocolos basados en *IP* que permiten integrar nodos militares, civiles y multinacionales. Tecnologías como *Link 22* sobre *5G* y la posibilidad de interoperabilidad con redes públicas (*GOGO / COGO*) facilitan la integración en operaciones conjuntas.

Además, la incorporación de *UEs* militares, *IoT*, sensores y sistemas no tripulados bajo una arquitectura común estandariza el control, reduce la carga logística y mejora el intercambio de datos en tiempo real. [13]

- Seguridad y resiliencia:

La arquitectura *5G* permite aplicar cifrado de extremo a extremo, segmentación lógica (*slicing*), y mecanismos avanzados como comunicaciones dirigidas (*beamforming*), dificultando la detección y el *jamming* por parte de adversarios. Aun así, deben considerarse vulnerabilidades en entornos de alta intensidad, especialmente en redes comerciales compartidas o ante amenazas cibernéticas avanzadas. Se recomienda la selección estricta de proveedores confiables y la implementación de políticas de seguridad tipo *Zero Trust Security* para fortalecer la seguridad operativa del *LHQ*, especialmente en la gestión de accesos y protección frente amenazas internas y externas [13][53].

- Escalabilidad y sostenibilidad:

Los despliegues modulares permiten escalar la red en función del tamaño de la fuerza (de brigada a división), integrando fácilmente estaciones base fijas, repetidores o nodos embarcados (por ejemplo, en *UAVs*). El impacto físico del equipamiento *5G* es menor comparado con sistemas *legacy V/UHF*, mejorando la estabilidad estructural de las plataformas y reduciendo los requisitos de energía.

- Limitaciones actuales:
  - Dependencia de infraestructura física (fibra, energía, torres).
  - Sensibilidad a obstáculos físicos y condiciones meteorológicas (particularmente en frecuencias altas).
  - Tiempo de despliegue prolongado (meses o años para escenarios permanentes).
  - Requiere planificación espectral cuidadosa y coordinación con actores civiles.

5.3.1.3 Brechas y desafíos basados en 5G

La implementación de redes *5G* en escenarios tácticos como el del *LHQ* representa un importante salto tecnológico, pero también revela ciertas brechas estructurales y desafíos que deben ser abordados para asegurar una integración eficaz y segura.

Una tecnología crucial para superar algunos desafíos operativos es el *Zero Provisioning* (*ZTP*), permitiendo la configuración automática y segura de las estaciones base y terminales en despliegues rápidos y flexibles del *LHQ*, minimizando la intervención manual y asegurando una rápida adaptación a cambios en la configuración operativa del cuartel general.

- Limitaciones del estándar 3GPP:
    - Falta de integración segura para accesos no IP seleccionados, como radios militares o *SATCOM* heredados.
    - Ausencia de continuidad de servicio eficaz entre redes *NTN* (No Terrestres) y *TN* (Terrestres).

- Desafíos tecnológicos y operativos:
    - Baja disponibilidad de equipos altamente integrados verticalmente, así como personal técnico especializado en despliegue, operación y mantenimiento de redes privadas 5G.
    - Necesidad de capacitación avanzada para unidades especializadas según las aplicaciones previstas.
    - Limitada disponibilidad de sistemas *FWA 5G* que operen en bandas de 26 GHz, necesarias para distribución *LAN* de alta capacidad. Aunque ofrecen *beamforming* y *MIMO/SISO*, presentan importantes restricciones de propagación [2]:
        - Atenuación significativa en estructuras no transparentes electromagnéticamente.
        - Imposibilidad de comunicaciones más allá de la línea de vista (*BLoS*) en estas bandas.
        - La lluvia puede afectar negativamente el rendimiento de la señal.
    - La utilización de bandas de baja frecuencia (como la Banda IV de la OTAN) para cubrir largas distancias conlleva [36]:
        - Consumo de espectro estratégico para enlaces de comunicación con otros *HQs*.
        - Reducción significativa del rendimiento dentro de grandes sedes desplegadas (*DHQ*).

- Desafíos específicos para sistemas ACR basados en 5G:
    - Disponibilidad de implementaciones en bandas sub-1 GHz, preferentemente dentro de la banda táctica OTAN 225–400 MHz [13].

- Capacidad de combinar funciones de WMAN (*Wireless Metropolitan Area Network*) y ACR sobre los mismos elementos físicos de red (CN) [13].

5.3.2 *SDHQ (Small Deployable Headquarters)*

El caso de uso *SDHQ* se refiere a los casos de uso terrestres que se centran en operaciones basadas en tierra de una unidad militar desplegable y nómada. El elemento clave aquí es la flexibilidad para configurar y desmantelar rápidamente la infraestructura táctica, así como la adaptabilidad a la topografía y al alcance de las operaciones.

Es necesario formular algunos supuestos e información de contexto para determinar el alcance de las operaciones en el escenario *SDHQ*, que deben considerarse para un análisis posterior de las soluciones tecnológicas correspondientes. Estos se enumeran a continuación [13]:

- El *SDHQ* está compuesto por una unidad operativa terrestre pequeña, con múltiples equipos de usuario (UE) fijos y móviles, así como soporte para una variedad de aplicaciones de usuario. El *SDHQ* es una unidad desplegable que se puede configurar o desmontar de forma rápida y sencilla. El despliegue de la red es nómada, estacionario, pero altamente portátil. Los escalones militares considerados dentro del alcance de operaciones del *SDHQ* son Brigadas, Batallones o Compañías de gran tamaño.
- El *SDHQ* se despliega dentro de los límites territoriales de la nación anfitriona o aliada, cerca de zonas de conflicto. El entorno electromagnético es relativamente benigno, aunque puede transformarse en un entorno hostil dependiendo de las operaciones militares en curso. Además de interferencias no intencionales, se espera cierto nivel de interferencia intencional por parte del adversario. El *SDHQ* actúa como punto *CIS* local para unidades tácticas más pequeñas involucradas en conflictos activos. Esto hace necesaria la utilización de radios tácticas y formas de onda compatibles con soluciones existentes no basadas en 5G [38].
- El *SDHQ* actúa como unidad de mando y control (C2) para operaciones federadas, incluidas operaciones conjuntas/de coalición, así como operaciones multidominio.
- Se asume la disponibilidad de puntos de acceso inalámbrico fijo (*FWA*), redes de área local (*LAN*) y/o cables de fibra óptica (FO) en los establecimientos principales/estáticos. Sin embargo, la infraestructura de red debe ser autosuficiente en caso de no contar con estas tecnologías [26]. El entorno físico está compuesto únicamente por tiendas militares (electromagnéticamente transparentes, es decir, con baja o nula atenuación).
- Existe la posibilidad de que haya redes civiles/públicas en las cercanías, con superposición en el entorno electromagnético. Se requiere establecer mandatos doctrinales y regulaciones para permitir la coexistencia de redes militares y públicas.
- Se asume que el *SDHQ* no da soporte a civiles ni a reservistas, es decir, no se admite el uso de dispositivos personales (*BYOD*). Se requieren unidades robustas con estaciones base, equipos de usuario y tarjetas SIM preconfiguradas, portátiles y resistentes a golpes.

- Puede ser necesaria la disponibilidad de soporte técnico remoto, potencialmente proporcionado por la nación marco, para operaciones desplegadas.
- La distribución de dispositivos de red es relativamente heterogénea.
- Existe una red común con capacidad de conexión a escalones superiores, entidades civiles, servicios de emergencia, etc. El nivel de clasificación de seguridad no debe ser superior a *NATO-Confidential.*
- Se requieren características de alta capacidad de transmisión (*throughput*) y baja latencia para soportar todas las aplicaciones necesarias, además de dispositivos basados en sensores. Por lo tanto, desde la perspectiva de 5G, deben admitirse todos los modelos de canal (*uRLLC, eMBB y mMTC).*
- En escenarios de conflicto activo, si la infraestructura de comunicaciones públicas es destruida o controlada por el enemigo, una configuración tipo *SDHQ* podría actuar como proveedor alternativo de red, especialmente para personal de gestión de crisis o equipos de primera respuesta. Por otro lado, también puede ser desplegado para misiones humanitarias en escenarios no conflictivos.

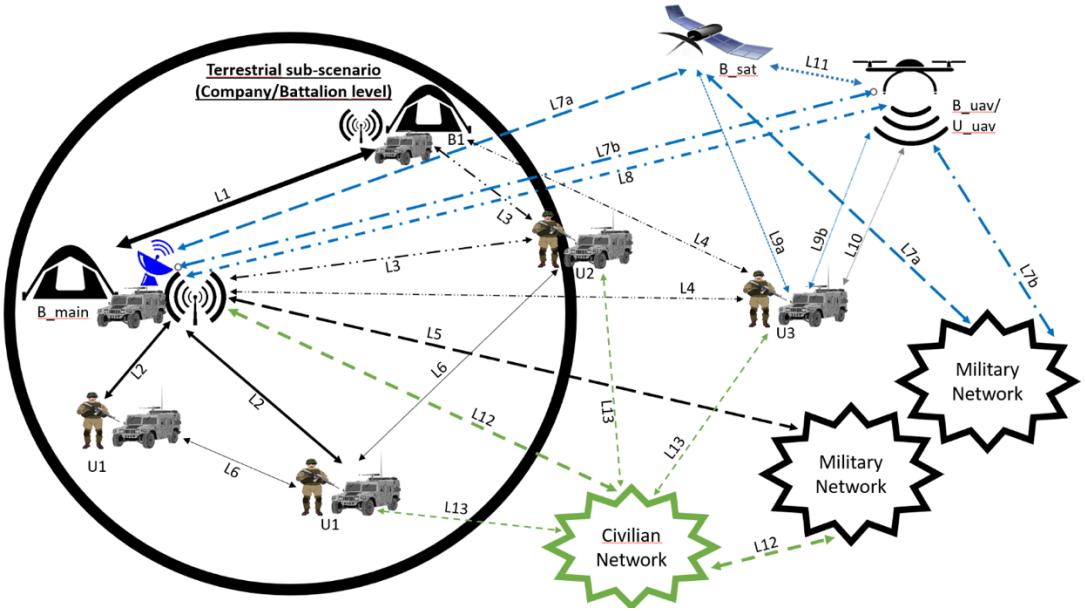

Figura 12: Escenario SDHQ.

Los subescenarios y casos de uso dentro del escenario SDHQ, tal como se indica en la leyenda de la Figura 12 [13], se definen mediante:

a) una clasificación basada en dispositivos (en la Tabla 7 [13]).

b) una clasificación basada en enlaces (en la Tabla 8 [13]).

Cabe destacar que los dispositivos se categorizan, además, en dos componentes principales:

1. Un dispositivo tipo B, que indica una estación base.

2. Un dispositivo tipo U, que indica un equipo de usuario (de banda ancha o banda estrecha).

ID del Dispositivo	Descripción
B_main (BS)	Tienda principal / Cuartel General CIS militar. Centro logístico y de recopilación de datos. La estación base está conectada a la red central 5G y a la red de datos. La altura del mástil debe ser baja para minimizar la detectabilidad visual.
B1 (BS)	Tienda subordinada Unidad de respaldo para redundancia como sistema de seguridad si la unidad B_main es comprometida — puede convertirse en la nueva B_main. Replicación exacta del núcleo de red (CN) como en B_main La altura del mástil debe ser baja para minimizar la detectabilidad visual.
B_sat (BS)	Terminal de estación base satelital
B_uav (BS)	Estación base montada en UAV
U1 (UE)	Soldado a pie / vehículo tripulado / UGV — Equipo de usuario dentro del área operativa de B_main/B1
U2 (UE)	Soldado a pie / vehículo tripulado / UGV — Equipo de usuario en transición dentro o fuera del área operativa del subescenario terrestre Conversión eventual a U1.
U3 (UE)	Soldado a pie / vehículo tripulado / UGV — Equipo de usuario fuera del área operativa de cualquier subescenario terrestre Conversión eventual a U2 y luego a U1.
U_uav (UE)	Usuario final a bordo de UAV

Tabla 7: Lista de definiciones de dispositivos del diagrama de casos de uso de SDHQ

Dado que algunos usuarios se encuentran dentro de edificios o estructuras como bloques de tiendas de campaña, no han sido representados en la Figura 12; sin embargo, forman parte integral de los casos de uso asociados a las comunicaciones en interiores.

ID del Enlace	Descripción
L1	Enlace entre B_main y B1 (Fibra óptica; respaldo: FWA punto a punto – PTP)
L2	Enlace entre B_main/B1 y U1
L3	Enlace entre B_main/B1 y U2
L4	Enlace entre B_main/B1 y U3
L5	Enlace (solo terrestre) entre B_main y otra red militar del mismo o diferente escalón (Fibra óptica; respaldo: FWA punto a punto – PTP)
L6	Enlace entre dos dispositivos U1 o entre U1 y U2
L7a	Enlace entre B_main y B_sat
L7b	Enlace entre B_main y B_uav
L8	Enlace entre B_main y U_uav
L9a	Enlace entre B_sat y U3
L9b	Enlace entre B_uav y U3
L10	Enlace entre U_uav y U3
L11	Enlace entre B_sat y B_uav/U_uav
L12	Conexión (no un enlace directo) entre B_main y una red civil (Fibra óptica; respaldo: FWA punto a punto – PTP)
L13	Enlace entre un UE militar (U1/U2/U3) y la red civil

Tabla 8: Lista de definiciones de enlaces del diagrama de casos de uso SDHQ

Para los enlaces representados en la Figura 12:

- Un enlace terrestre se representa en negro.
- Un enlace *TN-NTN* se representa en azul.
- Una red pública y sus enlaces correspondientes se representan en verde.

Además, los enlaces dentro de edificios o bloques de tiendas de campaña no se han representado en la Figura 12; sin embargo, forman parte integral de los casos de uso asociados a las comunicaciones en interiores.

5.3.2.1 Características

Para que el escenario *SDHQ* sea relevante en el contexto de operaciones militares reales, es necesario asumir ciertos parámetros y requisitos del sistema, frente a los cuales puedan proponerse soluciones tecnológicas. A continuación, en la Tabla 9 [13], se formula una lista de características para el escenario *SDHQ*.

En términos de seguridad, se recomienda el uso de arquitecturas basadas en principios de *Zero Trust*, así como autenticación robusta mediante *eSIM* con múltiples perfiles, lo que permite una gestión segura y dinámica del acceso, adaptándose a los requisitos operativos del *SDHQ* y mitigando riesgos de seguridad inherentes al entorno táctico [75].

Parámetro	Características de capacidad
Número de usuarios finales	950 usuarios totales: • 330 *UEs* militares • Algunos *UEs C2* • 550 dispositivos *IoT* militares • Algunos dispositivos *IoT* de equipo
Número de estaciones base (*gNBs*) (Redundancia para evitar punto único de fallo)	1–4 estaciones base fijas (+ auxiliares para redundancia)
Frecuencia de cambio de posición de la estación base	Media
Variación de posición y movilidad de las estaciones base	Nómada • En operaciones humanitarias: posiciones ágiles, sin movilidad durante la operación • En operaciones de combate: cambios frecuentes de posición / móviles para evitar ser objetivos de alto valor
CN / Nodos *Edge* y ubicaciones	*CN* dentro del área operativa + nodos *edge* cerca de los límites de red Redundancia suficiente para evitar puntos únicos de fallo Respaldo por *CN* vía *NTN* para unidades tácticas fuera del área operativa
Alcance máximo del enlace *TN* (Red Terrestre)	• Dentro del área operativa: 200 metros • Mismo escalón: 15 km • Escalón superior/inferior: 15–30 km
Velocidad media/máxima de unidades móviles terrestres	20–40 km/h / 50 km/h
Altura máxima del mástil de estación base	Máx. 2–3 metros (preferentemente ≤ 1 metro)
Potencia máxima de transmisión del *gNodeB*	Baja a media
Área de cobertura	0,25 km²

Densidad de red (Usuarios finales / área de cobertura)	ALTA: • 1360 por km² • 3640 por km² (incl. dispositivos *IoT*)
UEs conectados en estado *RRC* (Porcentaje de usuarios activos simultáneamente)	75%
Requisitos espectrales	• Sub 1 GHz = *HF (BLoS) / VHF / UHF / GSM* / Banda táctica OTAN (larga distancia) • Sub 6 GHz (Banda IV OTAN) + *mmWave* (para alto rendimiento) → Se requiere agilidad espectral
Rendimiento máx./real (Mbps/Gbps) (N.º de usuarios × rendimiento por usuario)	340.57 / 255.428 Mbps
Conectividad de backhaul de red de área local	< 60 Mbps (bajada)
Conectividad entre nodos de red	< 15 Mbps entre *SDHQs*
Enrutamiento local del tráfico en el nodo de red	Obligatorio
Disponibilidad de red *5G*	Continua
Vida útil	Del orden de semanas/días
Tiempo de despliegue	Deseado: 3/4 horas Máximo: 6/8 horas
Provisionamiento y propiedad de la red	Red privada local – *NSA/SA* *GOGO* (propiedad y operación gubernamental)

Tabla 9: Características de capacidad tabuladas para el escenario SDHQ.

5.3.2.2 Evaluación tecnológica

La aplicación de redes *5G* al escenario *SDHQ* implica considerar un entorno altamente dinámico, con requisitos de despliegue rápido, movilidad intermedia y una alta densidad de usuarios en un área reducida. En la Tabla 10 y en la Tabla 11 [13] se hace una evaluación de los dispositivos necesarios y forma de los enlaces necesarios.

Dispositivo	Tecnologías/Soluciones 5G
B_main	• *gNodeB* (estación base 5G) con acceso compartido por radio • Funcionalidades *CN/RAN* requeridas • *Slicing* para la segregación de aplicaciones (por requisitos de seguridad, separación de grupos de usuarios, priorización de aplicaciones, etc.) • Solo red *5G SA. NSA* con anclaje 4G/LTE aún en uso a corto plazo • Interfaces N1, N2, N3, N6
B1	• *gNodeB* (estación base 5G) con acceso compartido por radio • Funcionalidades *CN/RAN* requeridas • *Slicing* para la segregación de aplicaciones • Estación base 5G con función de *relay*
B_sat	• 5G NTN: varias opciones para uso satelital como *backhaul* o acceso directo
B_uav	• 5G NTN: varias opciones para uso satelital como *backhaul* o acceso directo
U1	*Beamforming* y MIMO
U2	• *eSIM* con múltiples perfiles • Servidor de control de movilidad
U3	• *eSIM* con múltiples perfiles • Servidor de control de movilidad • Uso de *HAPS (High Altitude Platform Systems)* o satélites *LEO* • *UE* con capacidad de acceso directo a satélite
U_in	• Repetidor en apoyo de *ProSe (Proximity Services)* / Conectividad *ad hoc*
U_uav	• *mIoT / mMTC* (comunicaciones masivas máquina a máquina)

Tabla 10: Evaluación de los dispositivos en el escenario de uso SDHQ.

Enlace	Tecnologías / Soluciones 5G
L1	Cable de fibra óptica (secundario: *5G FWA* punto a punto; *NR WMAN*) Fuera del alcance de la arquitectura *5G*, pero posible arquitectura distribuida: a) *gNB* en una ubicación distinta del Core *5G* b) Funciones del *Core 5G* distribuidas en diferentes ubicaciones c) Conexión a redes distintas (*local break-out, central break-out*)
L2	*UE 5G* a *gNB* mediante *NR-Uu*; conexión *UE* <--> estación base Uso de *Massive MIMO* y *Beamforming*
L3	UE 5G a gNB mediante NR-Uu punto a punto; conexión UE <--> estación base Requiere eSIM multiperfil y gestión de movilidad *Massive MIMO* y *Beamforming*
L4	Red terrestre 5G (posiblemente *super cell* para mayor alcance) *Massive MIMO* y *Beamforming*
L5	Cable de fibra óptica (secundario: *5G FWA* punto a punto; *NR WMAN*) Fuera del alcance de la arquitectura *5G*, pero posible arquitectura distribuida: a) *gNB* en ubicación distinta al Core *5G* b) Funciones del *Core 5G* distribuidas c) Conexión a redes distintas
L6	Conexión *D2D* (dispositivo a dispositivo) UE-UE (para V2V, V2S, S2S) vía *5G* PC5 • Conexión de retransmisión *D2D UE-UE* • Conexión de retransmisión *D2D UE-red*
L7a	Varias opciones: 5G NTN con backhaul para gNB y acceso directo UE-gNB Conectividad directa al gNB mediante antena directiva (fija o nómada)
L7b	gNB a Core 5G mediante interfaz NG; conexión de datos basada en IP Conectividad 5G NTN hacia gNB montado en dron
L8	UE 5G a gNB mediante NR-Uu; conexión UE <--> estación base Conectividad *5G NTN* directa con dispositivos montados en dron
L9a	*5G NTN* para acceso directo del UE (*UE 5G* a *gNB* vía NR-Uu) Conectividad 5G NTN directa con dispositivos montados en vehículos o portátiles
L9b	Igual que L9a: conectividad directa *NTN* con dispositivos vehiculares o portátiles
L10	*(Sin descripción especificada)*
L11	gNB a Core 5G mediante interfaz *NG;* conexión de datos basada en IP Conectividad directa *5G NTN* con dispositivos montados en dron
L12	Movilidad del *UE*: *roaming* (puede requerir *eSIM* multiperfil y control de movilidad) Conectividad a nivel de red: *backhaul* a internet
L13	UE 5G a gNB mediante NR-Uu Requiere eSIM multiperfil, multi-SIM, gestión de movilidad y/o *roaming* entre red privada y pública Redes móviles 5G (posiblemente *super cell* para alcance extendido)
L_in	*UE 5G* a *gNB* mediante *NR-Uu*; conexión *UE* <--> estación base

Tabla 11: Evaluación de los enlaces en el escenario del caso de uso SDHQ.

La evolución de los estándares *5G* definidos por *3GPP* a través de las *Releases* 15, 16 y 17 proporciona una base tecnológica progresivamente más robusta para aplicaciones militares. A continuación, la Tabla 12 [2] presenta las principales capacidades incorporadas en cada *release* y su relevancia para el escenario *SDHQ*:

REL 15	REL 16	REL17
• Bandas sub-6GHz • Frecuencias *mmWave* (no aptas para *NLoS*) • *Beamforming* • *Massive MIMO* • *Slicing* • *URLLC* • *eMBB*	• Mejora de *mMIMO* • Mejora de *slicing* • Mejora de *URLLC* • Mejora del soporte *mmWave* (ej. nueva modulación)	• Mejora de *mMIMO* • Mejora de *slicing* • *NTN* • *UAS*

Tabla 12: Tecnologías 5G (específicas de REL) que pueden explotarse potencialmente en el escenario SDHQ.

Ejercicios como *CWIX* han validado capacidades críticas del *5G* en escenarios *SDHQ*, especialmente en términos de resistencia ante interferencias activas (*jamming*), segmentación avanzada mediante *Network Slicing*, e interoperabilidad multinacional según especificaciones *FMN Spiral 6*, confirmando así su eficacia para operaciones dinámicas y altamente móviles [4][5].

A continuación, se presenta una evaluación tecnológica frente a los requisitos operativos definidos:

- Madurez y disponibilidad tecnológica:

Las redes privadas 5G en configuraciones *NSA/SA* han demostrado ser viables para despliegues temporales y de corto plazo, como los que exige un *SDHQ*. La disponibilidad de equipamiento compacto y modular, con soporte para funcionalidades como *beamforming*, *network slicing*, y nodos *edge*, permite su adaptación a contextos de alta densidad, pero corta duración.

- Cobertura y rendimiento:

El escenario SDHQ requiere [13]:

  - Cobertura eficaz en un área de ~0.25 km², lo cual es adecuado para frecuencias sub-6 GHz, incluso con transmisores de baja o media potencia.
  - Altura de mástil limitada (<3 m), por razones de ocultamiento visual, lo que impone restricciones en propagación que deben compensarse mediante densificación o antenas de alto rendimiento.
  - Conectividad confiable entre escalones mediante enlaces terrestres o *NTN* de respaldo, especialmente dado el uso de redes nómadas o móviles en contextos de combate.

- Velocidad de despliegue y configuración:

El tiempo de configuración estimado (3 a 8 horas) es realista utilizando soluciones actuales tipo *plug-and-play* con *gNBs* integrados y *core* embarcado. La configuración automatizada, combinada con plantillas de red predefinidas, permite desplegar capacidades completas en plazos cortos, cumpliendo con el ritmo operativo del *SDHQ* [13].

- Densidad y concurrencia:

Con más de 3600 dispositivos por km² (incluyendo *IoT*), y un 75% de usuarios activos simultáneamente, el *SDHQ* exige una solución capaz de manejar tráfico intensivo con múltiples tipos de dispositivos. Las capacidades de *5G* en *mMIMO* y *slicing* ofrecen soporte adecuado para segmentar tráfico entre C2, *IoT*, y aplicaciones tácticas, siempre que exista planificación de espectro y capacidad suficiente de *backhaul* [13].

- Desafíos y limitaciones:
    - Baja altura de antena y potencia limitada reducen significativamente el alcance de las celdas, lo que puede requerir mayor número de estaciones base en áreas irregulares.
    - La movilidad del *SDHQ* en combate impone desafíos para el mantenimiento de la conectividad persistente, especialmente si se emplean bandas altas (*mmWave*).
    - Propagación limitada de señales en interiores (tiendas o vehículos) puede requerir soluciones específicas (*indoor small cells*, repetidores o nodos *mesh*).
    - Capacidad de *backhaul* limitada (<60 Mbps) y enlaces entre nodos (<15 Mbps) podrían volverse cuellos de botella si no se gestiona adecuadamente la priorización del tráfico [13].
- Seguridad y resiliencia:

El entorno *SDHQ* exige comunicaciones seguras, con resistencia a interferencias y detección. La integración de funcionalidades como *beamforming*, *eSIM*, y segmentación lógica ofrece herramientas clave para garantizar comunicaciones resilientes y seguras incluso con potencia reducida y en condiciones hostiles. Adicionalmente, el uso de tecnologías como *Zero Provisioning* (ZTP) es crucial para un despliegue rápido y automático del *SDHQ*, asegurando configuraciones iniciales rápidas y seguras. Asimismo, la implementación de soluciones *Integrated Access and Backhaul* (*IAB*) podría mejorar la conectividad en áreas con infraestructura limitada, proporcionando enlaces dinámicos entre estaciones base y facilitando despliegues ágiles y flexibles [13][27][52].

5.3.2.3 Brechas y desafíos basados en 5G

- Limitaciones de *3GPP*:
    - Integración segura de accesos no IP seleccionados (por ejemplo, radios militares y *SATCOM*).
    - Continuidad del servicio entre redes *NTN* (No Terrestres) y *TN* (Terrestres) [2][13].
- Desafíos:
    - Disponibilidad de equipos operativos altamente integrados y de fácil configuración/desmantelamiento.

- Disponibilidad de bandas espectrales militares dedicadas en el rango medio de frecuencias sub-6 GHz (idealmente en la Banda IV de la OTAN).
- Disponibilidad de UEs 5G y terminales de red que permitan una conectividad inalámbrica fluida.
- Incompatibilidad entre *UEs 5G* que operan en distintas bandas espectrales utilizadas por diferentes países de la OTAN.
- Diseño de forma de onda táctica resistente a interferencias activas o amenazas de guerra electrónica (*EW*). Si esto no se aborda dentro del proceso de estandarización 5G, al menos debería existir un mecanismo para detectar la presencia de *EW* en la red. Tras la detección, se podría evaluar el cambio a otras bandas de frecuencia o a una forma de onda más resiliente.
- Minimización de la huella electromagnética (EM) en escenarios de conflicto, para evitar la interceptación por redes adversarias.
- Garantizar la disponibilidad continua del servicio o un nivel mínimo de calidad de servicio (*QoS*), incluso fuera del área de cobertura o en presencia de interferencias *EW*.
- Enlaces de comunicación degradados y alta densidad de dispositivos: el uso de bandas de frecuencia más altas podría ser beneficioso en estos casos [13].

5.3.3 *MCP* (*Mobile Command Post*)

El caso de uso *MCP* se refiere a los casos de uso terrestres centrados en las operaciones basadas en tierra de una unidad militar completamente móvil. El elemento clave aquí es la movilidad, es decir, la unidad es autosuficiente y puede proporcionar servicios de red en movimiento [13].

Es necesario formular algunos supuestos e información de contexto para determinar el alcance de las operaciones en el escenario *MCP*, que deben considerarse para un análisis posterior de las soluciones tecnológicas correspondientes. Estos se enumeran a continuación [13]:

- El *MCP* está compuesto por una pequeña unidad táctica terrestre con únicamente equipos de usuario móviles (*UEs*) y soporte para aplicaciones de usuario específicas. El *MCP* es una unidad desplegable que está lista para operar inmediatamente y no requiere configuración adicional. El despliegue de la red es completamente móvil, es decir, hay presencia de estaciones base montadas en vehículos que son totalmente funcionales mientras están en movimiento. Los escalones militares incluidos en el alcance de las operaciones del *MCP* son escuadrones, pelotones o compañías pequeñas.
- El *MCP* opera completamente dentro de territorio adversario en medio del conflicto, o dentro de los límites territoriales del país anfitrión o aliado, pero muy cerca de zonas de combate. El entorno electromagnético (EM) es altamente hostil, con presencia de interferencias activas. Además, debido a la movilidad de las estaciones base, se espera una considerable cantidad de interferencias no intencionales. Se requiere equipamiento resistente con radios tácticas y formas de onda capaces de operar en entornos EM altamente disputados. A pesar de condiciones extremas de guerra electrónica (*EW*), se debe mantener conectividad continua con todos los *UEs*.

- El uso de equipamiento de pequeño tamaño es útil para reducir la detectabilidad. Un tamaño menor también permite mantenerse discreto en zonas de conflicto. Dado que la operación es completamente móvil, no hay una fuente de energía constante disponible. Por lo tanto, las limitaciones de tamaño, peso y consumo de energía (*SWaP*) son particularmente exigentes.
- El *MCP* puede formar parte de operaciones federadas más amplias, incluidas operaciones conjuntas/de coalición y multidominio, con enlace hacia una unidad *C2* local. Sin embargo, también debe ser capaz de operar de forma autónoma, sin conexión a otras unidades *C2*.
- Existe una red común con posibilidad de conexión a escalones superiores, entidades civiles, servicios de emergencia, etc. El nivel de clasificación de seguridad no debe superar *NATO-Restricted*.
- La dimensionalidad del *MCP* puede variar significativamente dependiendo del tipo de operación a realizar. Por ejemplo:
    - El uso de armas obliga a mantener mayor separación entre personas (una ametralladora tiene un alcance efectivo de 2,4 km, por lo que deben evitar interferencias entre sí).
    - Un pelotón o compañía deben separarse por cientos de metros para sobrevivir.
    - Una batería de artillería puede ocupar hasta 1 km².
- No se dispone de puntos *FWA* ni *LAN/FO*, ya que no hay unidades con posiciones fijas.
- Las redes civiles/públicas cercanas solo pueden ser útiles para el *backhaul* o para la descarga de tráfico (*offloading*), pero no se debe depender de su disponibilidad. El *MCP* no da soporte a civiles ni reservistas, es decir, no se admiten dispositivos *BYOD*. Se requieren unidades robustas con estaciones base y *UEs* preconfigurados, portátiles y resistentes a impactos.
- La distribución de dispositivos de red es altamente heterogénea y dinámica. El MCP también puede ser una unidad táctica diseñada para operaciones especiales como reconocimiento y vigilancia, fuerzas expedicionarias, transporte de armamento sensible/peligroso, artillería, etc.
- Se requiere baja latencia, incluso en presencia de guerra electrónica, para soportar las aplicaciones necesarias. Por lo tanto, desde la perspectiva de *5G*:
    - *uRLLC* es el requerimiento principal.
    - *eMBB* es un requerimiento deseable.
    - *mMTC* podría ser útil dependiendo de la cantidad de dispositivos de banda estrecha necesarios según los requerimientos operativos.

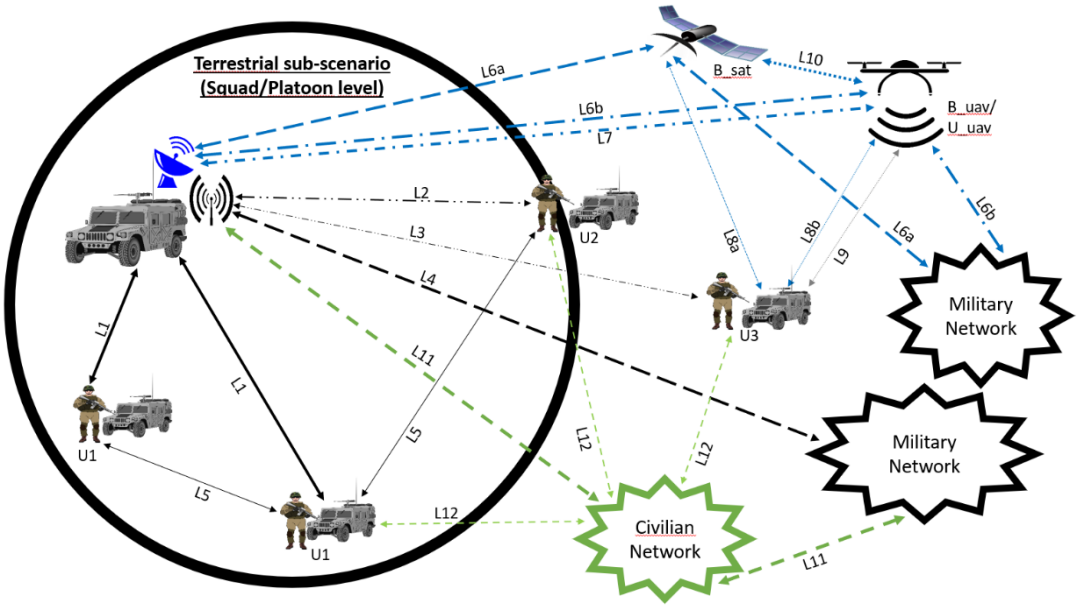

Figura 13: Escenario MCP.

En el escenario *MCP*, los subescenarios y casos de uso se definen utilizando:

a) Clasificación basada en dispositivos (en la Tabla 13 [13]).
b) Clasificación basada en enlaces (en la Tabla 14 [13]).

Además, los dispositivos se categorizan en dos componentes principales:

- Dispositivo tipo B: indica una estación base.
- Dispositivo tipo U: indica un equipo de usuario (de banda ancha o banda estrecha).

Notas sobre la Figura 13 [13]:

- Un enlace terrestre se representa en negro.
- Un enlace no terrestre o de terrestre a no terrestre se representa en azul.
- Una red pública y los enlaces correspondientes se representan en verde.

ID del Dispositivo	Descripción
B_main (BS)	Estación base principal montada en vehículo o portátil. Posible núcleo de red 5G remoto mediante enlace satelital.
B_sat (BS)	Terminal de estación base satelital.
B_uav (BS)	Estación base montada en *UAV*.
U1 (UE)	Soldado a pie, vehículo tripulado o *UGV* basado en *UE* dentro del área operativa de B_main.
U2 (UE)	Soldado a pie, vehículo tripulado o *UGV* en transición dentro o fuera del área operativa del subescenario terrestre. Conversión eventual a U1.
U3 (UE)	Soldado a pie, vehículo tripulado o *UGV* fuera del área operativa de cualquier subescenario terrestre. Conversión eventual a U2 y luego a U1.
U_uav (UE)	Usuario final *UAV*.

Tabla 13: Lista de definiciones de dispositivos del diagrama de casos de uso de MCP.

ID del Enlace	Descripción
L1	Enlace entre B_main y U1.
L2	Enlace entre B_main y U2.
L3	Enlace entre B_main y U3.
L4	Enlace (solo terrestre) entre B_main y otra red militar del mismo o diferente escalón.
L5	Enlace entre dos dispositivos U1 o entre U1 y U2.
L6a	Enlace entre B_main y B_sat.
L6b	Enlace entre B_main y B_uav.
L7	Enlace entre B_main y U_uav.
L8a	Enlace entre B_sat y U3.
L8b	Enlace entre B_uav y U3.
L9	Enlace entre U_uav y U3 (caso de uso de sensor a tirador).
L10	Enlace entre B_sat y B_uav/U_uav.
L11	Conexión (no un enlace directo) entre B_main y una red civil (fibra óptica; alternativa es *FWA PTP*).
L12	Enlace entre un UE militar (U1/U2/U3) y la red civil.

Tabla 14: Lista de definiciones de enlaces del diagrama de casos de uso MCP.

5.3.3.1 Características

Para que el escenario *MCP* sea relevante para operaciones militares reales, es necesario asumir ciertos parámetros y requisitos del sistema, contra los cuales se podrían proponer soluciones tecnológicas. Dicha lista de características para el escenario *MCP* se formula en la Tabla 15 [13].

Parámetro	Características de Capacidad
Número de usuarios finales	30 dispositivos *UE* militares + algunos dispositivos *UE* de C2 50 dispositivos *IoT* militares + algunos dispositivos *IoT* de equipos
Número de estaciones base (*gNBs*) (Redundancia para evitar un único punto de fallo en la red)	1-4 estaciones base móviles principales (+ auxiliares para redundancia)
Frecuencia de cambio de posición de la estación base	Alta
Variación de posición y movilidad de las estaciones base	Completamente móviles
Nodos *CN/Edge* y ubicaciones	Solo nodo de borde en el área operativa. Redundancia suficiente para evitar un único punto de fallo. Soporte de backhaul *CN* basado en *NTN* desde el centro de comando *CIS*
Alcance máximo del enlace de datos *TN*	Dentro del área operativa: 100 ms Mismo escalón: 3-5 km Escalón superior: hasta 5 km (Un pelotón puede tener hasta 400-500m entre secciones con 13-14 personas a pie. Las unidades mecanizadas pueden ser mucho más grandes. Múltiples km en tamaño de burbuja. Las operaciones especiales pueden ser de hasta cientos de km)
Velocidad promedio/máxima de unidades móviles terrestres	20-40 km/h / 50 km/h
Altura máxima del mástil de la estación base	Máximo 1 metro. Flexible. Solo omnidireccional.
Potencia máxima de transmisión del *gNodeB*	Muy baja, fuertes restricciones de *SWaP* y *LPI/LPD*
Área de cobertura	0.12 km²

(para determinar la potencia de transmisión de las estaciones base)	
Densidad de la red (Número de usuarios finales/Área de cobertura)	BAJA 258 por km² 692 por km² (incluyendo dispositivos *IoT*)
Ues conectados por RRC (Porcentaje de usuarios activos simultáneamente)	100%
Requisitos espectrales	Sub 1 GHz = *HF (BloS)/VHF/UHF/GSM/*Banda táctica de la OTAN para largo alcance + Sub 6 GHz (Banda IV de la OTAN) + *mmWave* (para mejorar la *QoS* en corto alcance y menor firma de radio) Se requiere agilidad espectral
Rendimiento máximo/real (Mbps/Gbps) (Número de usuarios finales * rendimiento por usuario)	31.052/31.052 Mbps
Conectividad de backhaul de la red de área local	< 20 Mbps (Enlace descendente)
Conectividad entre nodos de red	< 10 Mbps entre *MCPs*
Enrutamiento local del tráfico en el nodo de red	Opcional (la alternativa es el enlace lateral)
Disponibilidad de la red 5G (periódica/esporádica/continua)	Periódica (puede haber momentos de necesidad continua, pero también períodos de silencio de radio)
Duración	Orden de horas
Tiempo de configuración	Tiempo real
Provisionamiento y propiedad de la red	Red privada local – *NSA/SA GOGO*

Tabla 15: Características de capacidad tabuladas para el escenario MCP.

La seguridad operativa del *MCP* se ve reforzada mediante principios de *Zero Trust Security*, que minimizan la vulnerabilidad frente a amenazas internas y externas en condiciones hostiles. Además, la aplicación específica de técnicas avanzadas como *beamforming* y *mMIMO* es clave para reducir la huella electromagnética (*LPI/LPD*), mitigando el riesgo de detección y *jamming* enemigo [13][75].

5.3.3.2 Evaluación tecnológica

La evolución de los estándares *5G* definidos por *3GPP* a través de las *Releases* 15, 16 y 17 proporciona una base tecnológica progresivamente más robusta para aplicaciones militares [2]. A continuación, la Tabla 16 [13] presenta las principales capacidades incorporadas en cada *release* y su relevancia para el escenario *MCP*:

REL 15	REL 16	REL17
• *Sub-6GHz frequency bands* • *mmWave frequencies (not in case of NLoS)* • *Beamforming* • *mMIMO* • *Slicing* • *URLLC* • *eMBB*	• *mMIMO enhancement* • *Slicing enhancement* • *URLLC enhancement* • *mmWave support enhancement (e.g. new modulation)*	• *mMIMO enhancement* • *Slicing enhancement* • *NTN* • *UAS*

Tabla 16: Tecnologías 5G (REL-específicas) que pueden explotarse potencialmente en el escenario MCP.

Ejercicios internacionales, especialmente *CWIX*, han demostrado la viabilidad de implementar soluciones *5G* en contextos similares al *MCP*, con especial énfasis en capacidades críticas tales como resistencia a *jamming* activo, segmentación dinámica mediante *slicing*, y la interoperabilidad táctica según especificaciones *FMN Spiral 6*, confirmando así la robustez y eficacia del *5G* en operaciones completamente móviles.

Para cumplir con los requerimientos operativos altamente móviles y autónomos del *MCP*, es especialmente útil la incorporación de tecnologías como *Zero Provisioning* (ZTP), que facilita configuraciones rápidas y automáticas en tiempo real sin intervención manual. Asimismo, el uso específico de *Network Slicing* para escenarios de movilidad extrema permite gestionar eficientemente los recursos de red, asegurando una *QoS* constante en condiciones dinámicas y hostiles.

5.3.3.3 Brechas y desafíos basados en 5G

- Deficiencias de 3GPP:
    - Integración segura de accesos seleccionados no-IP (por ejemplo, radios militares y SATCOM).
    - Continuidad del servicio entre redes no terrestres (NTN) y terrestres (TN) [2][13].

- Desafíos:
    - Disponibilidad de equipos de usuario (*UE*) y estaciones base (*BS*) robustecidos.
    - Disponibilidad de bandas espectrales militares dedicadas en el rango medio de frecuencias sub-6 GHz (idealmente la Banda IV de la OTAN) para una mejor calidad de servicio (*QoS*).
    - Disponibilidad de dispositivos *5G UE* y terminales de red para una conectividad inalámbrica fluida.
    - Las aplicaciones en los dispositivos *UE* deben ser muy fáciles de usar, requiriendo una formación mínima.
    - Diseño de forma de onda táctica resiliente, inmune al *jamming* activo u otras amenazas de guerra electrónica. Debería existir al menos un método para comprender o detectar la presencia de *EW* en la red. Tras la detección, se requeriría un cambio a otras bandas de frecuencia o a una forma de onda más resiliente.
    - Huella electromagnética mínima en un escenario de conflicto para evitar escuchas por parte de redes adversarias.
    - Proporcionar disponibilidad continua del servicio o una *QoS* mínima al estar fuera del área de servicio o en presencia de *EW*.
    - No disponibilidad de funciones/equipos que permitan el acceso *no-IP/3GPP* al sistema 5G.
    - Falta de equipos que permitan el cambio y direccionamiento del tráfico dentro de estos contextos de tecnologías de acceso *no-IP/3GPP* [13].

5.4 Caso marítimo

La OTAN ha validado configuraciones navales específicas para la implementación de redes *5G* embarcadas. Estos entornos se benefician del uso de tecnologías como *Integrated Access and Backhaul* (*IAB*), antenas *AESA (Active Electronically Scanned Array)*y operación en bandas de 1-6 GHz para equilibrio entre alcance y capacidad [13][35].

5.4.1 *HSC (High Seas Communications)*

El caso de uso *HSC* se refiere a los casos de uso navales enfocados en las comunicaciones entre buques y dentro del buque en alta mar (aguas internacionales), donde no existen regulaciones territoriales respecto a los parámetros de señalización. Además de los buques navales, también se integran unidades aéreas que son instrumentales para las operaciones navales.

Es necesario formular algunos supuestos e información de contexto para determinar el alcance de las operaciones en el escenario *HSC*, que deben considerarse para el análisis de soluciones tecnológicas correspondientes. Estos se enumeran a continuación:

- El *HSC* comprende comunicaciones navales en alta mar, donde no existen regulaciones territoriales. Se incluyen:
    - Comunicaciones intra-buque, donde cada buque es capaz de proporcionar capacidades CIS a todos los UEs a bordo.
    - Comunicaciones entre buques (*ship-to-ship*).
    - Comunicaciones sobre la superficie entre boyas/submarinos con buques y plataformas aéreas (incluidos jets).
    - Comunicaciones entre jets, así como con buques y unidades sensoras (boyas, etc.).
- Debido a la ausencia de regulaciones espectrales, se puede utilizar una cartera amplia de bandas *IMT* (*International Mobile Telecommunications*) reservadas para el uso comercial, lo que permite optimizar la calidad de servicio (*QoS*) y mitigar interferencias.
- El *HSC* incluye enlaces de comunicación entre los buques y los equipos de abordaje, incluyendo comunicaciones de voz y transmisiones de video en vivo.
- Existe una varianza considerable en el tamaño y dimensiones de los buques. Sin embargo, las lanchas pequeñas o patrulleras no se consideran buques independientes en este escenario.
- Se asume que los buques están en movimiento durante todo el ciclo operativo.
- El entorno electromagnético puede variar desde altamente disputado hasta no disputado, dependiendo de la proximidad con unidades navales adversarias. Ambos escenarios deben considerarse. Las condiciones EM son propensas a cambiar rápidamente y de forma espontánea.

- Las fuerzas marítimas deben ser capaces de federarse con fuerzas locales, incluso si están desconectadas del cuerpo principal de fuerzas.
- Se deben incluir plataformas aéreas como satélites, sistemas de plataformas de gran altitud, *UAVs*, drones, etc., para extender el rango de cobertura masiva. La latitud geográfica es un factor importante en la elección de la plataforma aérea.
- Las emisiones de radio (especialmente aquellas detectables por sistemas hostiles de medidas de apoyo electrónico, *ESM*) deben restringirse en niveles de amenaza elevados. No obstante, las comunicaciones deben mantenerse (modo solo recepción) durante estos períodos de silencio.

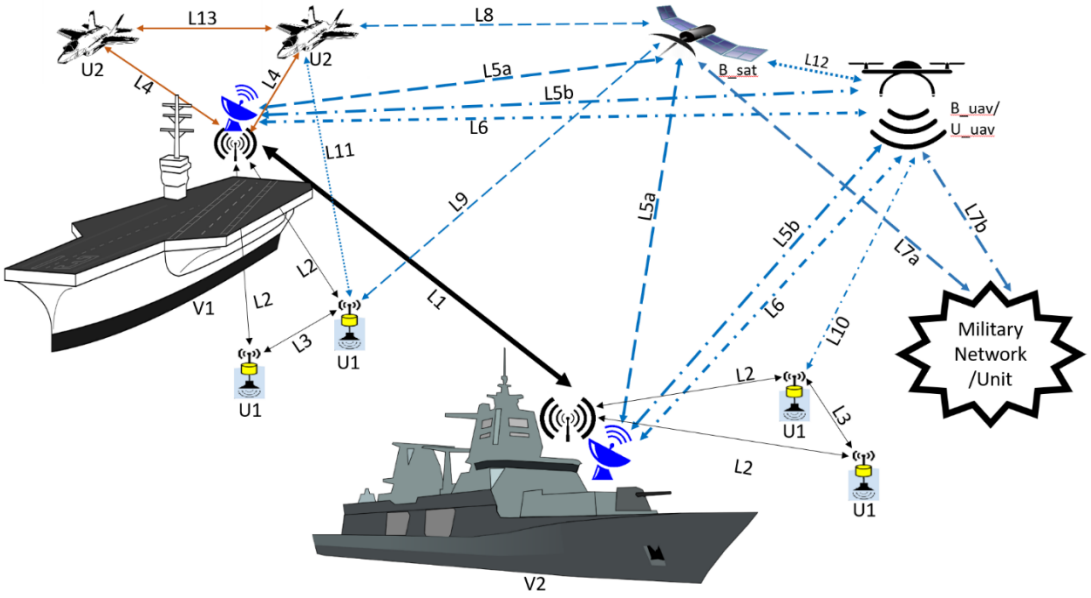

Figura 14: Escenario HSC.

Los subescenarios y casos de uso dentro del escenario HSC, según se indica en las leyendas de la Figura 14 [13][35], se definen utilizando:

a) una clasificación basada en dispositivos (en la Tabla 17 [13][35]).

b) una clasificación basada en enlaces (en la Tabla 18 [13][35]).

Para los enlaces en la Figura 14:

- Un enlace naval se representa en negro.
- Un enlace no terrestre o terrestre-a-naval se representa en azul.
- Los enlaces en naranja representan aviones de apoyo, es decir, de movilidad extremadamente alta.
- Como se mencionó anteriormente, los enlaces submarinos están fuera del alcance del análisis dentro del RTG.
- Un dispositivo tipo V que indica una estación base en una embarcación.
- Un dispositivo tipo B que indica una estación base.

- Un dispositivo tipo U que indica un equipo de usuario (de banda ancha o banda estrecha).

ID del Dispositivo	Descripción
V1 (BS)	Buque en alta mar. Buque insignia/nave nodriza en una Fuerza de Tarea Naval (NTF). Equipado con una red central y de datos.
V2 (BS)	Buque en alta mar. Equipado con una red central y de datos.
B_sat (BS)	Terminal de estación base satelital.
B_uav (BS)	Estación base montada en un Vehículo Aéreo No Tripulado (UAV).
U1 (UE)	Boyas submarinas/de superficie (vehículos submarinos no tripulados – UUVs / vehículos de superficie no tripulados – USVs) desplegadas por un buque.
U2 (UE)	Avión a reacción.
U_in (UE)	Equipo de usuario dentro de un barco.
U_uav (UE)	Usuario final en un UAV.

Tabla 17: Lista de definiciones de dispositivos del diagrama de casos de uso de HSC.

ID del Enlace	Descripción
L1	Enlace entre V1 y V2.
L2	Enlace entre V1/V2 y U1s. No se consideran enlaces submarinos.
L3	Enlace entre dos U1s.
L4	Enlace entre V1/V2 y U2.
L5a	Enlace entre V1/V2 y B_sat.
L5b	Enlace entre V1/V2 y B_uav.
L6	Enlace entre V1/V2 y U_uav.
L7a	Enlace entre B_sat y una red militar terrestre.
L7b	Enlace entre B_uav y una red militar terrestre.
L8	Enlace entre U2 y B_sat.
L9	Enlace entre U1 y B_sat.
L10	Enlace entre U1 y B_uav.
L11	Enlace entre U1 y U2.
L12	Enlace entre B_sat y B_uav/U_uav.
L13	Enlace entre dos U2s.
L_in	Enlace entre U_in y V1/V2 (comunicaciones intra-buque).

Tabla 18: Lista de definiciones de enlaces del diagrama de casos de uso de HSC.

5.4.1.1 Características

Para que el escenario *HSC* sea relevante para operaciones militares reales, es necesario asumir ciertos parámetros/requisitos del sistema, contra los cuales se podrían proponer soluciones tecnológicas. Dicha lista de características para el escenario *HSC* se formula en la Tabla 19 [13].

Parámetro	Características de Capacidad
Número de usuarios finales	Portaaviones: 3500 Crucero: 300 Destructor: 200 Fragata: 120
Número de Estaciones Base (*gNBs*) (Redundancia para evitar un único punto de fallo en la red)	Al menos 1 estación base por buque, según el tamaño del barco. Número suficiente de repetidores/puntos de acceso para la cobertura de red en toda la embarcación.
Frecuencia de cambio de posición de la estación base	Inexistente dentro de la perspectiva intra-buque. Alta dentro de la perspectiva inter-buque.

Variación de posición y movilidad de las estaciones base	Inter-buque: completamente móviles Intra-buque: estáticas con movilidad limitada (a velocidad de caminata).
Nodos *CN/Edge* y ubicación	Núcleo *5G* en cada buque.
Alcance máximo del enlace de datos *TN*	Intra-buque: Portaaviones: 150 m Crucero: 100 m Destructor: 75 m Fragata: ~60-70 m Las fuerzas navales pueden constar de 10-12 barcos juntos o separados por cientos de kilómetros. Comunicaciones inter-buque: de 20 millas náuticas (mn) hasta 100 mn. Máx. 1000 mn de borde a borde. Alcance máximo de comunicación en línea de visión: 21 mn / 38 km
Velocidad media/máxima de unidades móviles	Inter-buque: Portaaviones: 30 nudos Crucero: 30 nudos Destructor: 30 nudos Fragata: 35 nudos Avión de combate: < 1.5 Mach Intra-buque: nula (velocidad a pie)
Altura máxima del mástil de la estación base	Portaaviones: 75 m Crucero: 55 m Destructor: 45 m Fragata: 35 m
Área de cobertura (para determinar la potencia de transmisión de las estaciones base)	Intra-buque: Portaaviones: 300 m x 70 m Crucero: 175 m x 40 m Destructor: 150 m x 35 m Fragata: ligeramente más pequeña que el destructor Inter-buque: muy extensa; con soporte *NTN*
Densidad de red (Número de usuarios finales / área de cobertura)	Intra-buque: Portaaviones: 160,000 por km² Crucero: 43,000 por km² Destructor: 38,000 por km² Fragata: 35,000 por km² Inter-buque: muy dispersa (casi nula)
UEs conectados por *RRC* (Porcentaje de usuarios activos simultáneamente)	100%
Requisitos espectrales	Sub 1 GHz = *HF (BLoS) / VHF / UHF* / Banda táctica OTAN para largo alcance + *NTN/HAPS* y *SATCOM* para cobertura extendida, comunicaciones con unidades terrestres y *backhaul* de red + Agilidad espectral y capacidad de cambio rápido de bandas operativas, especialmente para comunicaciones inter-buque o buque-aéreo
Rendimiento máximo/real (Mbps/Gbps) (Número de usuarios * rendimiento por usuario)	El requisito de rendimiento de los equipos de abordaje pequeños sirve como referencia.
Conectividad de *backhaul* de la red local	< 100 Mbps (enlace descendente) por buque
Conectividad entre nodos de red	< 100 Mbps entre buques

Enrutamiento local del tráfico en el nodo de red	Obligatorio
Disponibilidad de red *5G* (periódica / esporádica / continua)	Continua (aunque puede haber momentos de control de emisiones o receptores objetivo fuera del horizonte de radio)
Duración operativa	Orden de semanas/meses
Tiempo de configuración	No aplica
Provisionamiento y propiedad de la red	Red privada local – *NSA/SA GOGO*

Tabla 19: Características de capacidad tabuladas para el escenario HSC.

En el contexto *HSC*, la reducción de la huella electromagnética (*LPI/LPD*) mediante el uso de tecnologías avanzadas como *beamforming y mMIMO* es especialmente crítica. Estas tecnologías permiten comunicaciones más seguras y discretas, reduciendo significativamente la probabilidad de detección e interferencia por fuerzas adversarias, lo cual es esencial en operaciones navales sensibles.

En este escenario, la fuerza naval podría utilizar el ancho de banda *5G* sin restricciones, ya que las aguas internacionales se consideran un bien común global sin limitaciones legales de frecuencia.

Como vemos en la Figura 15 [35], una situación posible dentro de este caso de uso podría ser la de un portaaviones comandando una Fuerza de Tarea Naval (*NTF*). Además, se pueden desplegar diferentes medios como *UAVs* y *USVs* para realizar diversas funciones.

Todos estos elementos necesitan estar conectados, y es necesario que toda la información recopilada por los diferentes sensores desplegados pueda ser transmitida y procesada en el menor tiempo posible, reduciendo así el ciclo *OODA* [13][35].

Las diferentes operaciones que esta fuerza de tarea naval podría llevar a cabo pueden incluirse en las denominadas Guerra de Superficie, Guerra Antiaérea y Guerra Antisubmarina. Cada uno de estos dominios requiere un uso diferente de aplicaciones e información intercambiada.

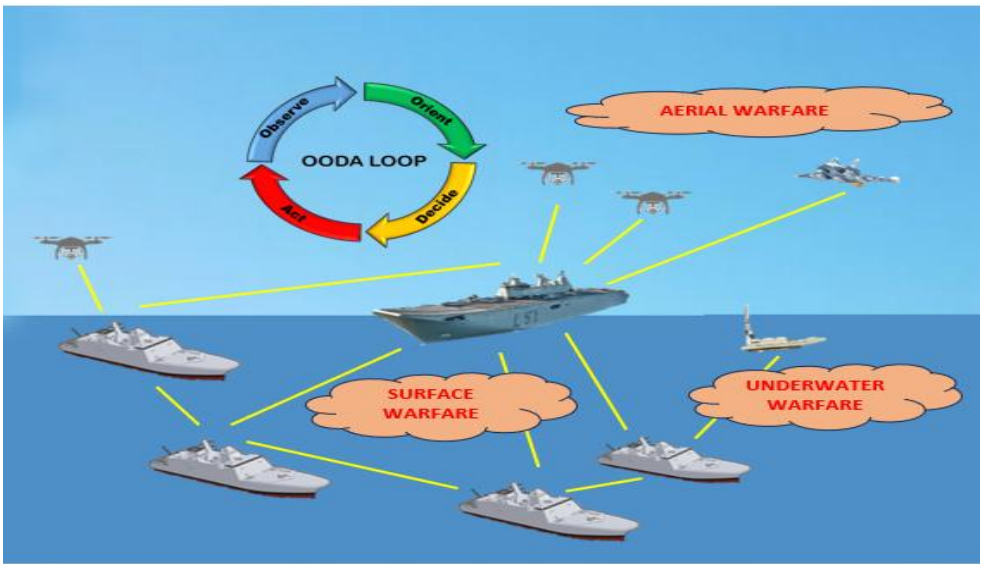

Figura 15: Ejemplo de situación real marítima.

5.4.1.2 Evaluación tecnológica

Los enlaces de datos tácticos como *Link-11, Link-16* y *Link-22* son los medios convencionales para operaciones multidominio que no quedarían obsoletos debido al uso de bandas de frecuencia más bajas (*HF/VHF/UHF*) utilizadas para lograr una mayor distancia de cobertura. Sin embargo, el *5G* tiene el potencial de establecer una base para enlaces de datos no formateados que, por ejemplo, pueden admitir transmisiones de video (para equipos de abordaje, etc.) con características de alta capacidad y baja latencia. Se puede hacer referencia a tecnologías como *MARLIN* y la operación "directa al módem" de aplicaciones de teletipo por radio [13][35].

Ejercicios multinacionales como *CWIX* han demostrado que el uso de redes 5G en escenarios navales *HSC* permite comunicaciones tácticas avanzadas y efectivas, específicamente validando capacidades como resistencia al *jamming*, enlaces seguros mediante *slicing* dinámico y cumplimiento estricto de especificaciones técnicas *FMN Spiral 6* para interoperabilidad naval multinacional [4][5][13][35].

La implementación de soluciones *Integrated Access and Backhaul (IAB)* es especialmente valiosa en el entorno naval para establecer enlaces flexibles y dinámicos entre buques en alta mar, especialmente cuando se opera sin soporte *SATCOM* directo. Además, la adopción de enfoques de seguridad *Zero Trust* marítimo puede proporcionar protección adicional frente a amenazas internas y externas en escenarios operativos altamente variables [13][35].

5.4.1.3 Brechas y desafíos basados en 5G

Componentes como radares de alta potencia o sensores ESM pueden interferir con los sistemas 5G, por lo que es necesario cambiar a otras bandas de frecuencia [13][35].

- Desafíos:
    - Disponibilidad de equipos altamente integrados (verticalmente) que sean fáciles de instalar y operar por operadores y no por técnicos.
    - El *SATCOM* se degrada gravemente más allá de los 78 grados de latitud norte. Una topografía complicada o guerra electrónica activa pueden reducir aún más el alcance hasta los 60 grados de latitud norte.
    - Uso estandarizado y completamente descentralizado de una topología de red mallada de acceso inalámbrico de retorno (*WAB*), particularmente en operaciones militares conjuntas multinacionales.
    - Según las especificaciones actuales del *3GPP*, el uso de enlaces laterales (*sidelink*) o *WAB* puede no ser muy útil para los requisitos de la red.
    - El enfoque centralizado punto-a-multipunto (*PTMP*) genera vulnerabilidad en relación con un único punto de fallo (*gNB* central).
    - Limitaciones de propagación en línea de visión (*LoS*) o más allá de la línea de visión (*BLoS*), así como el riesgo de interferencia y suplantación en ausencia de soporte NTN.
    - Variabilidad del entorno electromagnético y posibilidad de interferencia significativa tanto de fuerzas enemigas (rojas) como propias (azules).

- Utilización espectral dinámica. En aguas profundas, debido a la interferencia reducida o inexistente de redes terrestres (principalmente públicas) que operan en bandas *IMT*, es posible utilizar dicho espectro, lo cual es beneficioso. En aguas poco profundas, las comunicaciones deben cumplir con las regulaciones de espectro impuestas por las autoridades nacionales (costeras).

5.4.2 *AC (Amphibious Communications)*

El caso de uso *AC* se refiere a los casos de uso navales enfocados en las comunicaciones entre buques y tierra en zonas de conflicto. Se asume que el dominio naval está ocupado por fuerzas aliadas (azules), mientras que el dominio terrestre presenta una presencia significativa de fuerzas adversarias (rojas). En este escenario no se considera la integridad territorial [13][35].

Es necesario formular algunos supuestos e información de contexto para determinar el alcance de las operaciones en el escenario *AC*, que deben considerarse para el análisis de soluciones tecnológicas correspondientes. Estos se enumeran a continuación:

- El *AC* comprende comunicaciones navales cercanas a la costa (ignorando cualquier regulación territorial existente). Se incluyen:
  - Comunicaciones entre buques, especialmente entre un cuartel general *CIS* y las plataformas de desembarco.
  - Comunicaciones buque-a-tierra entre unidades navales y fuerzas de desembarco.
  - Comunicaciones sobre la superficie entre boyas/submarinos y buques.
  - Comunicaciones dispositivo a dispositivo terrestres.
  - Comunicaciones superficie-aire entre unidades terrestres y aviones de combate (caso de uso tipo sensor-a-tirador).
- No hay soporte por parte de infraestructuras/redes terrestres.
- Las operaciones anfibias incluyen tanto ataques o reconocimientos (avance naval hacia tierra) como retiros (retorno desde tierra hacia mar).
- La distribución de dispositivos de red es altamente heterogénea y dinámica. La predictibilidad es muy baja.
- Aunque pueden existir regulaciones espectrales, no es necesario cumplirlas, ya que también las usan los adversarios. Por ello, se deben tener en cuenta dos aspectos clave:
  - Libertad para usar un amplio rango de bandas de frecuencia.
  - Existencia de altos niveles de interferencia y bloqueo (*jamming*) → la agilidad y diversidad espectral son fundamentales para mantener la calidad de servicio (*QoS*).
- El entorno electromagnético es altamente disputado. Se requiere una huella EM baja (*LPI/LPD – Low Probability of Intercept / Detection*). Es necesaria la utilización de equipamiento robusto, con radios tácticas y formas de onda que funcionen en

entornos EM muy hostiles. A pesar de condiciones extremas de guerra electrónica, debe mantenerse conectividad fluida con todos los *UEs*.

- Las unidades navales, terrestres y aéreas pueden formar parte de una fuerza multinacional. Por tanto, la interoperabilidad es un criterio clave para los sistemas CIS entre fuerzas federadas.
- Se deben incluir plataformas aéreas como satélites, *HAPS*, *UAVs*, drones, etc., para extender el alcance de cobertura masiva. La latitud es un factor importante para seleccionar la plataforma aérea adecuada.
- El uso de enjambres de terminales no tripulados (*UGVs*, *UAVs*, drones) es fundamental, especialmente en operaciones de reconocimiento y vigilancia.
- Los vehículos submarinos no tripulados (*UUVs*) y vehículos de superficie no tripulados (*USVs*) son esenciales para la vigilancia naval, especialmente antes del inicio de operaciones navales.

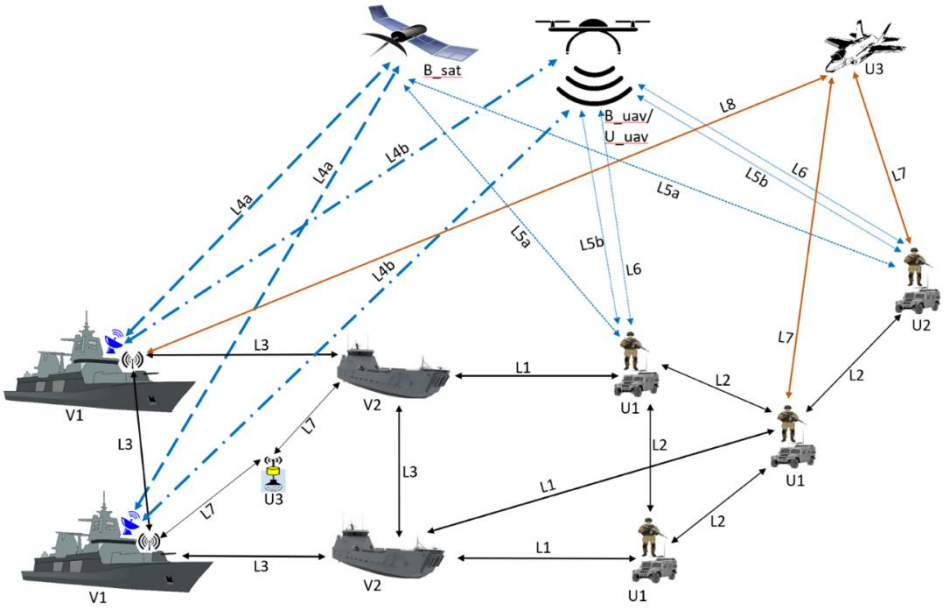

Figura 16: Escenario AC.

Los subescenarios y casos de uso dentro del escenario *AC*, según se indica en las leyendas de la Figura 16 [13][35], se definen utilizando:

a) una clasificación basada en dispositivos (en la Tabla 20 [13]).

b) una clasificación basada en enlaces (en la Tabla 21 [13].).

Cabe señalar que los dispositivos se categorizan además en tres componentes principales:

1. Un dispositivo tipo V que indica una estación base en una embarcación.
2. Un dispositivo tipo B que indica una estación base.
3. Un dispositivo tipo U que indica un equipo de usuario (de banda ancha o banda estrecha).

Notas sobre la Figura 16:

- Un enlace naval se representa en color negro.
- Un enlace no terrestre o de terrestre a naval se representa en color azul.
- Los enlaces en naranja representan aquellos que apoyan a los aviones de combate, es decir, con movilidad extremadamente alta.

Como se mencionó anteriormente, los enlaces submarinos están fuera del alcance del análisis.

ID del Dispositivo	Descripción
V1 (BS)	Buque cerca de la costa. Buque insignia/nave nodriza en una Fuerza de Tarea Naval (*NTF*). Buque equipado con una red central y de datos.
V2 (BS)	Lanchas de desembarco (con red de retorno desde V2) o plataformas de desembarco (con toda la red a bordo).
B_sat (BS)	Terminal de estación base satelital.
B_uav (BS)	Estación base montada en un vehículo aéreo no tripulado (*UAV*).
U1 (UE)	Soldado a pie/vehículo tripulado/vehículo terrestre no tripulado (*UGV*) basado cerca de V2.
U2 (UE)	Soldado a pie/vehículo tripulado/*UGV* basado lejos de V2.
U3 (UE)	Avión de reacción.
U4 (UE)	Boyas submarinas/superficiales (vehículos submarinos no tripulados - *UUVs*/vehículos de superficie no tripulados - *USVs*) desplegados por un buque.
U_uav (UE)	Usuario final *UAV*.

Tabla 20: Lista de definiciones de dispositivos del diagrama de casos de uso de AC.

ID del Enlace	Descripción
L1	Enlace entre V2 y U1.
L2	Enlace entre dos U1.
L3	Enlace entre dos V1 y V2.
L4a	Enlace entre V1 y B_sat.
L4b	Enlace entre V1 y B_uav.
L5a	Enlace entre U1/U2 y B_sat.
L5b	Enlace entre U1/U2 y B_sat.
L6	Enlace entre U1/U2 y U_uav. Caso de uso de sensor a tirador.
L7	Enlace entre U1/U2 y U3 (*D2D*). Caso de uso de sensor a tirador. Los tipos de sensores incluyen: video, infrarrojo (IR), luz, visual, electro-óptico (EO), radar de apertura sintética (*SAR*), etc.
L8	Enlace entre U3 y V1/V2.

Tabla 21: Lista de definiciones de enlaces del diagrama de casos de uso de AC.

5.4.2.1 Características

Para que el escenario *AC* sea relevante para operaciones militares reales, es necesario asumir ciertos parámetros y requisitos del sistema, sobre los cuales se puedan proponer soluciones tecnológicas. A continuación, en la Tabla 22, se presenta una lista de características para el escenario AC [13][35].

Lista de parámetros	Características de capacidad
Número de usuarios finales	Terminales en V1 según las especificaciones del *HSC* + terminales en V2/terrestres que comienzan con dimensiones del *MCP* (en las etapas iniciales) hasta dimensiones del *SDHQ* (en las etapas posteriores)
Número de estaciones base (*gNBs*) (Redundancia para evitar un único punto de fallo en la red)	1 estación base en un buque tipo V1 + auxiliar en V2 o B_sat/B_uav
Frecuencia de cambio de posición de la estación base	Alta
Variación de posición y movilidad de las estaciones base	Completamente móviles
Nodos *CN/Edge* y ubicaciones	Núcleo *5G* en la unidad *DCIS* del V1
Alcance máximo del enlace de datos *TN*	Comunicaciones en línea de vista con un alcance máximo de 21 millas náuticas / 38 km. Repetidores/buques con enlace de retransmisión de no más de 20 km.
Velocidad media/máxima de las unidades móviles terrestres	Ver *HSC* para buques tipo V1. Buques de desembarco: 5-15 nudos Aviones de combate: ~ 1.5 Mach Unidades terrestres: velocidades vehiculares < 60 km/h
Altura máxima del mástil de la estación base	Ver *HSC* para alturas de mástil en V1. No hay estaciones base terrestres.
Área de cobertura (para determinar la potencia de transmisión de las estaciones base)	No aplica. Altamente dinámica
Densidad de la red (Número de usuarios finales/Área de cobertura)	No aplica. Grandes variaciones en la topología de red y niveles de escalón
UEs conectados por *RRC* (Porcentaje de usuarios activos simultáneamente)	100%
Requisitos espectrales	Sub 1 GHz = *HF* (más allá de línea de vista*)/VHF/UHF*/Banda táctica de la OTAN para largo alcance + *NTN/HAPS* y *SATCOM* para cobertura extendida, comunicaciones con unidades terrestres y red de retorno + Agilidad y diversidad espectral como requisitos clave
Rendimiento máximo/real (Mbps/Gbps) (Número de usuarios finales * rendimiento por usuario)	Igual que en el escenario *HSC*
Conectividad de red de área local (*backhaul*)	< 100 Mbps (bajada) por buque
Conectividad entre nodos de red	< 100 Mbps entre buques
Enrutamiento local del tráfico en el nodo de red	Obligatorio
Disponibilidad de red *5G* (periódica/esporádica/continua)	Se requiere conectividad continua. Se asume de forma pragmática como esporádica debido a limitaciones por guerra electrónica
Vida útil	Equipos de ataque inicial: 24/48 horas Operaciones de reconocimiento posteriores: del orden de días/semanas Sostenimiento y logística: del orden de semanas/meses
Tiempo de configuración	No aplica
Provisión y propiedad de la red	Red privada local – *NSA/SA GOGO*

Tabla 22: Características de capacidad tabuladas para el escenario AC.

En una operación anfibia, compuesta por las fuerzas desembarcadas, fuerzas navales (buques) y elementos de apoyo como helicópteros y dispositivos autónomos como

vehículos terrestres no tripulados (*UGVs*) y vehículos submarinos no tripulados (*UUVs*), todos estos elementos necesitarán tener conectividad para intercambiar información.

El *UUV* recogería imágenes de la costa antes de la operación de desembarco y el *UGV* llevaría a cabo tareas de reconocimiento terrestre. La fuerza terrestre dispondría de sus propias aplicaciones para el mando y control (*C2*), en las que se integraría la información de los diferentes sensores desplegados. Asimismo, estas fuerzas necesitarían comunicarse con el buque para monitorear la operación.

En el contexto del escenario anfibio (*AC*), que podemos observar en la Figura 17 [13], el uso intensivo de técnicas avanzadas como *Beamforming* y *Massive MIMO* es crítico para mantener comunicaciones discretas y resilientes frente a detección e interferencia enemiga (*LPI/LPD*). Estas técnicas permiten minimizar la huella electromagnética, asegurando la continuidad operativa y la protección de las fuerzas desplegadas en tierra durante las operaciones anfibias [13][35].

Figura 17: Ejemplo real de AC.

5.4.2.2 Evaluación tecnológica

Dada la alta dinámica y hostilidad del escenario anfibio, la tecnología *Zero Provisioning* facilita la configuración rápida y automática de nodos tácticos desplegados en tierra desde unidades navales. Asimismo, el uso de *Network Slicing* dinámico permite gestionar eficientemente cambios rápidos en la topología de red, asegurando comunicación continua entre fuerzas de desembarco y buques de mando. La adopción adicional de modelos de seguridad *Zero Trust Architecture* (*ZTA*) es crucial para proteger los enlaces en un entorno altamente disputado y minimizar riesgos de ciberseguridad [13][35].

Ejercicios multinacionales como *CWIX* han confirmado la eficacia operativa de soluciones *5G* en entornos anfibios, especialmente validando capacidades clave tales como la interoperabilidad multinacional según estándares *FMN Spiral 6* [5], resistencia ante interferencias electromagnéticas intensas (jamming activo), y eficacia del *slicing* dinámico en condiciones de movilidad extrema, asegurando comunicaciones fiables en operaciones conjuntas de desembarco [13][35].

5.4.2.3 Brechas y desafíos basados en *5G*

Componentes como radares de alta potencia y sensores *ESM* pueden interferir con los sistemas *5G*, por lo que es necesario el cambio a otras bandas de frecuencia [13][35].

- Desafíos:
    - La SATCOM geoestacionaria se degrada severamente más allá de los 78 grados de latitud norte. La topografía desafiante o la guerra electrónica activa pueden reducir aún más el alcance hasta los 60 grados de latitud norte.
    - El uso estandarizado y completamente descentralizado de redes de acceso inalámbrico de retorno (WAB), particularmente en operaciones militares conjuntas multinacionales, es difícil de lograr con los sistemas COTS actuales. El escenario AC necesita una topología de red completamente mallada/distribuida.
    - Según las especificaciones actuales de 3GPP, el enlace lateral (*sidelink*)/WAB puede no ser muy útil para los requisitos de red, es decir, se requieren mejoras adicionales en los estándares. El enlace de datos D2D es un habilitador clave.
    - Un alto nivel de guerra electrónica conlleva una alta vulnerabilidad de los dispositivos de usuario (UEs) y de los enlaces de comunicación. Es necesario modificar los terminales comerciales y las formas de onda para cumplir con las necesidades operativas.
    - Se requiere agilidad espectral con baja latencia en el cambio de banda para mantener los enlaces de comunicación y cumplir con los requisitos de calidad de servicio (QoS).
    - Disponibilidad de diferentes tipos de funciones de 5G NR y CN de distintos proveedores para las mismas unidades de defensa.

Finalmente, para superar algunos de estos desafíos, es esencial adherirse estrictamente a estándares técnicos específicos para operaciones anfibias definidos en *STANAGs* navales y terrestres relevantes, así como al marco *FMN Spiral 6*. Estos estándares proporcionan protocolos comunes, interfaces técnicas validadas internacionalmente, y guías doctrinales claras, garantizando una interoperabilidad efectiva y comunicación continua entre unidades multinacionales en operaciones anfibias complejas y dinámicas [13].

5.4.3 *CC (Coastal Communications)*

El caso de uso *CC* se refiere a los casos de uso navales que engloban las comunicaciones entre unidades navales y terrestres, es decir, cerca de puertos o zonas costeras. Las unidades navales deben mantener el cumplimiento de las regulaciones territoriales correspondientes [13][35].

Es necesario formular algunos supuestos e información de contexto para determinar el alcance de las operaciones en el escenario *CC*, que deben considerarse para el análisis de soluciones tecnológicas correspondientes. Estos se enumeran a continuación:

- El caso CC se enfoca principalmente en las comunicaciones navales en aguas someras, dentro o cerca de la integridad territorial del país correspondiente o de naciones aliadas. Se incluyen:

  - Comunicaciones entre unidades navales y unidades terrestres.
  - Comunicaciones entre buques (inter-buque) en aguas territoriales o cercanas.
  - Comunicaciones sobre la superficie entre boyas/submarinos y buques.

- Existe un punto de acceso costero que facilita las comunicaciones entre las unidades navales y terrestres.
- Las unidades navales deben cumplir con las regulaciones espectrales del país bajo cuya integridad territorial se encuentra el puerto o zona considerada.
- También se incluyen embarcaciones pequeñas como lanchas patrulleras o unidades navales de guardacostas.
- Los buques pueden estar en movimiento (fase de transición desde alta mar) o estacionarios (cuando están atracados para carga/descarga de equipos y personal, etc.).
- El entorno electromagnético es benigno, y cualquier interferencia sería no intencional. El territorio pertenece a una nación propia o aliada, por lo tanto, no se esperan amenazas *EW*.
- Las plataformas aéreas, incluyendo satélites, *HAPS*, *UAVs*, drones, etc., deben incluirse para ampliar el rango de cobertura, incluyendo la conectividad con buques en alta mar.
- Las comunicaciones con buques en alta mar o entre unidades terrestres quedan excluidas de este escenario, para evitar redundancias, ya que ya fueron consideradas en casos de uso anteriores.
- Existe cooperación interagencial entre entidades marítimas y portuarias para operaciones de apoyo al pilotaje, como rompehielos, marina, guardacostas, etc.
- Establecer una infraestructura completamente privada, donde ya existe infraestructura pública para apoyar a unidades de defensa (particularmente nodos terrestres), no es rentable. Por lo tanto, se deben emplear los servicios públicos disponibles, agregando un nivel adicional de seguridad transparente para la red pública.
- La coexistencia con redes públicas o con redes militares terrestres es un elemento clave en este caso de uso.

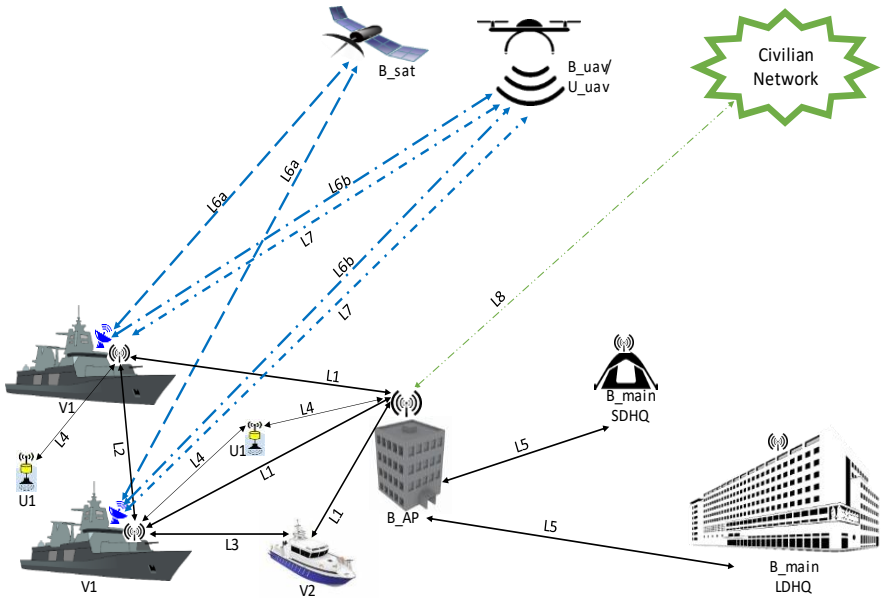

Figura 18: Escenario CC.

El escenario *CC* considera elementos del escenario *HSC*, así como de los escenarios terrestres *LHQ* y *SDHQ*. Por lo tanto, para evitar análisis redundantes, todos los artefactos operativos ya cubiertos en *HSC/LHQ/SDHQ* se omiten en el escenario *CC*.

Los subescenarios y casos de uso dentro del escenario CC, según se indica en las leyendas de la Figura 18 [13], se definen utilizando:

a) una clasificación basada en dispositivos (en la Tabla 23 [13][35]).

b) una clasificación basada en enlaces (en la Tabla 24 [13][35]).

Ten en cuenta que los dispositivos se clasifican además en tres componentes principales:

- Un dispositivo tipo V que indica una estación base en un buque,
- Un dispositivo tipo B que indica una estación base.
- Un dispositivo tipo U que indica un equipo de usuario (NB o WB).

Notas sobre la Figura 18:

- Los enlaces navales y terrestres se representan en negro.
- Los enlaces no terrestres o de terrestre a naval se representan en azul.
- Una red civil y su enlace correspondiente se representan en verde.

Como se mencionó anteriormente, los enlaces submarinos están fuera del alcance del análisis.

ID del dispositivo	Descripción
V1 (BS)	Buque cerca del puerto/aguas poco profundas/aguas territoriales. Buque equipado con una red central y de datos (buque grande/buque insignia).
V2 (BS)	Buque pequeño cerca del puerto/aguas poco profundas/aguas territoriales. Buque respaldado con servicios de red por un buque más grande.
B_AP (BS)	Estación base de punto de acceso terrestre. Conexión extendida y posible parte de la red terrestre local (*LHQ/SDHQ*). Equipado con red central.
B_main (BS)	Edificio principal (LHQ)/Tienda de campaña (*SDHQ*)/Cuartel general de *CIS* militar. Centro de logística y recopilación de datos. La estación base está conectada a la red central *5G* y a la red de datos.
B_sat (BS)	Terminal de estación base satelital.
B_uav (BS)	Estación base montada en *UAV*.
U1 (UE)	Boyas submarinas/superficiales (*UUVs/USVs*) desplegadas por un buque.
U_uav (UE)	Usuario final de *UAV*.

Tabla 23: Lista de definiciones de dispositivos del diagrama de casos de uso de CC.

ID del Enlace	Descripción
L1	Enlace entre B_AP y V1/V2
L2	Enlace entre dos V1
L3	Enlace entre V1 y V2
L4	Enlace entre V1/V2/B_AP y U1s
L5	Enlace entre B_AP y B_main (LHQ/SDHQ)
L6a	Enlace entre V1 y B_sat
L6b	Enlace entre V1 y B_uav
L7	Enlace entre V1 y U_uav
L8	Enlace entre B_AP y red civil

Tabla 24: Lista de definiciones de enlaces del diagrama de casos de uso CC.

5.4.3.1 Características

Para que el escenario *CC* sea relevante para operaciones militares reales, es necesario asumir ciertos parámetros y requisitos del sistema, sobre los cuales se puedan proponer soluciones tecnológicas. A continuación, en la Tabla 25 [13] se presenta una lista de características para el escenario *CC*.

Lista de parámetros	Características de capacidad
Número de usuarios finales	Corbeta: 60 Barco dragaminas: 50 Lancha patrullera: 25
Número de estaciones base (*gNodeBs*)	Al menos 3 (1 a bordo del buque + 1 punto de acceso terrestre + 1 *LHQ/SDHQ* terrestre) (+ auxiliares para redundancia)
Frecuencia de cambio de posición de la estación base	Inexistente en perspectiva intra-buque Alta en perspectiva inter-buque + Características de *LHQ/SDHQ*
Variación de posición y movilidad de estaciones base	Estaciones estáticas en perspectiva intra-buque Estaciones móviles en perspectiva inter-buque + Características de *LHQ/SDHQ*
Nodos *CN/Edge* y ubicaciones	Núcleo 5G en buque insignia + Núcleo 5G en punto de acceso marítimo + Características de *LHQ/SDHQ*
Alcance máximo del enlace de datos *TN*	Intra-buque: Corbeta: 150 m Barco dragaminas: 100 m Lancha patrullera: 75 m

	Buque a costa: Alcance de 12 nmi/22 km según regulaciones internacionales. Cobertura alcanzable hasta 76 km (banda de 700 MHz)
Velocidad media/máxima de unidades móviles terrestres	Corbeta: 25 nudos Barco dragaminas: 15 nudos Lancha patrullera: 25 nudos Terrestre: velocidades vehiculares en *LHQ/SDHQ*
Altura máxima del mástil de la estación base	Corbeta: 25 m Barco dragaminas: 15 m Lancha patrullera: <10 m Punto de acceso: 100 m + altitud del punto de instalación
Área de cobertura	Intra-buque: Corbeta: 100 m x 20 m Barco dragaminas: 50 m x 10 m Lancha patrullera: 30 m x 5 m Terrestre: 0.25 km² (*SDHQ*) o 7 km² (*LHQ*)
Densidad de la red	Intra-buque: Corbeta: 30,000 por km² Barco dragaminas: 100,000 por km² Lancha patrullera: 160,000 por km² Terrestre: 813 por km² (*LHQ* bajo) / 3,640 por km² (*SDHQ* medio)
UEs conectados por RRC	Características *HSC* para buques + Características *LHQ/SDHQ* El punto de acceso terrestre está siempre activo
Requisitos espectrales	Sub 1 GHz = *HF* (más allá de la línea de visión)/*VHF/UHF/GSM/*Banda táctica OTAN para largo alcance + Sub 6 GHz (Banda IV OTAN) + *mmWave* (comunicaciones interiores/firma de radio baja) para alto rendimiento Se requiere agilidad espectral; compatibilidad con regulaciones locales
Rendimiento máximo/real (Mbps/Gbps)	Características *HSC* + Características *LHQ/SDHQ*
Conectividad de backhaul de la red de área local	< 100 Mbps (bajada) por buque
Conectividad entre nodos de red	< 100 Mbps (bajada) por buque hacia la costa << 100 Mbps entre buques
Enrutamiento local del tráfico en nodo de red	Obligatorio
Disponibilidad de red 5G	Continua (pueden existir periodos de control de emisiones de radio)
Duración	Híbrido (Buque + *LHQ/SDHQ*)
Tiempo de configuración	No aplica
Provisión y propiedad de la red	Red privada local – *NSA/SA* + Red pública *GOGO/COGO* El uso oportunista de redes públicas de forma integral es una característica atractiva y rentable.

Tabla 25: Características de capacidad tabuladas para el escenario CC.

En un escenario de proximidad de un buque a la zona litoral, una de las principales necesidades de comunicación para el buque se centra en cuestiones logísticas y administrativas. Es necesario enviar información relacionada con el sostenimiento, el mantenimiento del buque, la gestión del personal a bordo, la formación, etc. Estas necesidades afectarían tanto a los buques de superficie como a los submarinos.

Uno de los principales desafíos para el uso de comunicaciones *5G* en este escenario es la

existencia de regulaciones en el uso de frecuencias. Esto implica que, en este escenario, se puede contemplar la posibilidad de utilizar Redes Públicas de Telefonía Móvil (*PLMN*), con las medidas de seguridad adecuadas según el tipo de información intercambiada [13][35].

Dado que el uso oportunista e integral de redes públicas es una característica clave en el escenario *CC*, la implementación de modelos de seguridad *Zero Trust Architecture* (*ZTA*) es indispensable. Esto permite gestionar eficazmente los riesgos asociados al uso compartido de infraestructura pública, asegurando comunicaciones militares seguras y confiables a través de mecanismos robustos de autenticación, segmentación lógica y monitoreo continuo.

5.4.3.2 Evaluación tecnológica

La implementación de tecnologías como Zero Provisioning (ZTP) es particularmente útil en escenarios costeros para simplificar y acelerar la configuración automática de puntos de acceso terrestres y nodos navales, especialmente cuando se integran redes privadas militares con redes públicas locales. Asimismo, el *Network Slicing* híbrido facilita una segmentación clara y segura del tráfico entre infraestructura pública y privada, asegurando la coexistencia eficiente y segura de comunicaciones militares y civiles en áreas costeras reguladas [13][35].

Ejercicios multinacionales como *CWIX* han validado con éxito las capacidades específicas del *5G* en escenarios *CC*, incluyendo la coexistencia segura con redes públicas mediante *slicing* híbrido, la interoperabilidad técnica multinacional según estándares *FMN Spiral 6*, y la eficacia operativa del *beamforming* y Massive MIMO para mantener comunicaciones fiables cerca de zonas costeras con alta densidad espectral [4][5][13][35].

5.4.3.3 Brechas y desafíos basados en 5G

- Desafíos:
    - Dependiendo del nivel de cooperación entre el organismo de Defensa propietario de las unidades militares y el proveedor de infraestructura de red, la disponibilidad de una conexión directa entre la porción de red de Defensa y la red de datos de Defensa garantizaría una mejor calidad de servicio (*QoS*). Las unidades navales y terrestres pueden pertenecer a diferentes naciones, lo que convierte la interoperabilidad en un requisito primordial.
    - Disponibilidad de equipos altamente integrados, fáciles de configurar y operar.
    - Disponibilidad de topologías combinadas punto-a-multipunto (*PTMP*, centralizadas) y en malla (descentralizadas) con redes públicas.
    - *PTMP* + *Sidelink* puede resultar en un alcance de cobertura limitado, especialmente en la dirección de subida (*uplink*), debido a las características desventajosas de los equipos de usuario (*UEs*).
    - Disponibilidad de diferentes tipos de funciones *5G NR* y *CN* de distintos proveedores para las mismas unidades de defensa.
    - Incompatibilidad en el uso estandarizado de porciones de redes públicas con redes privadas, particularmente cuando las unidades navales pertenecen a una

nación distinta de la soberanía de la costa y, por tanto, del proveedor de red pública.

Además, para enfrentar estos desafíos, es fundamental la adherencia estricta a estándares específicos *STANAG* y acuerdos bilaterales o multilaterales entre naciones aliadas y proveedores civiles locales. Estas regulaciones técnicas y acuerdos intergubernamentales permiten asegurar la interoperabilidad y cumplimiento regulatorio territorial, manteniendo la calidad del servicio (*QoS*) y la seguridad operacional en comunicaciones costeras conjuntas.

5.4.4 5G en el dominio marítimo

5G tiene el potencial de marcar una gran diferencia en el entorno marítimo. En este ámbito, el *WiFi* no proporciona comunicaciones estables en los rangos necesarios, mientras que se ha demostrado que el *5G* es estable; ciertas frecuencias ofrecen buenos alcances y un ancho de banda suficiente según lo requerido. La tecnología *5G* se considera una *Tecnología Emergente y Disruptiva* (*EDT*) en el dominio marítimo, ya que posee las características necesarias para revolucionar los procedimientos y capacidades de los sistemas de comunicaciones a bordo de unidades navales, y podría ser decisiva en futuros enfrentamientos en el mar [13][35].

Dada la complejidad de las comunicaciones navales y la diversidad de actores con los que se requiere coordinación y comunicación en las operaciones marítimas (fuerzas anfibias, fuerzas aeronavales, agencias de seguridad marítima, centros de operaciones en tierra, etc.), la implementación de *5G/xG* debe realizarse de forma progresiva y por fases. No todos podrán llevar a cabo la transición al *5G* al mismo tiempo, por lo que la convivencia con los sistemas de transmisión heredados será inevitable. Sin embargo, ya se han identificado varios casos de uso cuya aplicación podría lograrse en un período de tiempo relativamente corto, y que la OTAN ya ha reconocido. Estos se documentan a continuación [13][35].

5.4.4.1 *LEO SATCOM* y *5G*

Una de las aspiraciones en cuanto a comunicaciones marítimas debe ser mantener las capacidades de ancho de banda, con el fin de poder disponer de todos los servicios necesarios de mando, control y coordinación.

Una de las primeras alternativas a las comunicaciones satelitales tradicionales, basadas en satélites geoestacionarios en las bandas *Ku, X* y *Ka*, son los satélites que operan en órbitas bajas. En la mayoría de los casos, estos servicios de comunicación son proporcionados por empresas privadas y, en muchas ocasiones, emplean tecnología *5G*.

El uso de este tipo de satélites presenta grandes ventajas, ya que se han identificado anchos de banda amplios y latencias muy bajas, lo que los hace ideales para aumentar la capacidad de los servicios *C2*. Además, el tamaño de las constelaciones comerciales, algunas del orden de decenas de miles de satélites, da la idea de que el servicio estaría garantizado incluso en caso de ataque, aunque estos satélites distan mucho de ser invulnerables. El despliegue de esta capacidad a bordo proporciona un primer nivel de redundancia en las comunicaciones satelitales y justifica por sí solo el uso de la tecnología *5G* en el entorno marítimo.

Sin embargo, pueden existir inconvenientes, ya que se trata de un servicio comercial que puede estar sujeto a intereses ajenos o representar un riesgo para la seguridad en operaciones de alta intensidad (*OPSEC*). Existe la posibilidad de que un adversario logre identificar la celda geográfica desde la cual se realiza la conexión, revelando la posición aproximada de la unidad marítima y facilitando acciones de inteligencia y localización enemigas. Los sistemas S*ATCOM* de órbita terrestre baja (*LEO*) también son sensibles a interferencias y acciones de *geofencing* que podrían limitar su uso en caso de conflicto abierto.

Existen iniciativas, particularmente desde los Estados Unidos, dirigidas a resolver estas limitaciones, pero el acceso a estas constelaciones especialmente dedicadas a operaciones militares aún es limitado y, aunque prometedoras, su eficacia aún no ha sido comprobada [13][35].

5.4.4.2 *Maritime LoS Access Points* (*MLoS AP*).

Una alternativa a las comunicaciones satelitales son las comunicaciones mediante ondas de radio terrestres, tradicionalmente en *HF*. La evolución de las comunicaciones *HF* hacia *IP* (*BRIPES*) permite ofrecer, de manera limitada, servicios *C2* esenciales para la conducción de operaciones navales. El acceso a estos servicios se realiza a través de los denominados Puntos de Acceso Más Allá de la Línea de Vista (*BLoS AP)*, que no son más que estaciones de radio navales tradicionales mejoradas y actualizadas para ofrecer servicios sobre IP.

Como complemento a estos *BLoS AP*, la OTAN tiene la intención de desplegar Puntos de Acceso Marítimos en Línea de Vista (*MLoS AP*), basados en tecnología *5G*, cuya principal limitación es el alcance debido al horizonte provocado por la curvatura de la Tierra. La Figura 19 [13] indica varias situaciones operativas en las que estos *MLoS AP* resultan útiles. Estas situaciones incluyen la conectividad con *MLoS AP* mediante:

a) Enlaces directos con *MLoS* que dan servicio a puertos de descanso o Bases Navales.
b) Enlaces con *MLoS AP* durante operaciones en zonas costeras.
c) Repetidores que podrían establecerse utilizando otros buques o sistemas no tripulados, para mantener servicios de comunicación 5G en alta mar.

Estos *MLoS AP* podrían permitir a las fuerzas navales prescindir del uso de satélites durante las operaciones. Diversos estudios nacionales han identificado que, en las frecuencias más bajas del espectro *5G*, se pueden alcanzar hasta 60 millas náuticas en línea recta, por lo que una forma eficaz de extender el alcance de los *MLoS AP* es mediante el uso de repetidores o la instalación de antenas en ubicaciones elevadas.

Siempre existe una compensación entre frecuencia, alcance y ancho de banda. Los anchos de banda proporcionados por las frecuencias más bajas en las que opera el *5G* multiplican por cinco el requisito mínimo de ancho de banda para las comunicaciones satelitales expresado en la edición actual del *MC195*, por lo que estas serían las frecuencias principales en las que trabajar en el entorno marítimo, y particularmente para los *MLoS AP*.

Por último, los *MLoS* pueden servir como punto de conexión para el control y explotación de los sensores de los Sistemas Marítimos No Tripulados (*MUS*), que podrían desplegarse tanto desde zonas portuarias como mediante bases automatizadas semi-fijas. Estas bases también podrían actuar como repetidores de comunicaciones, ampliando aún más el radio de acción de estos sistemas, incluso sin la presencia de buques nodriza. La flexibilidad de la tecnología *5G* permitiría controlar y explotar los *MUS* bajo los principios de "hombre en el bucle" o "sobre el bucle" [13][35].

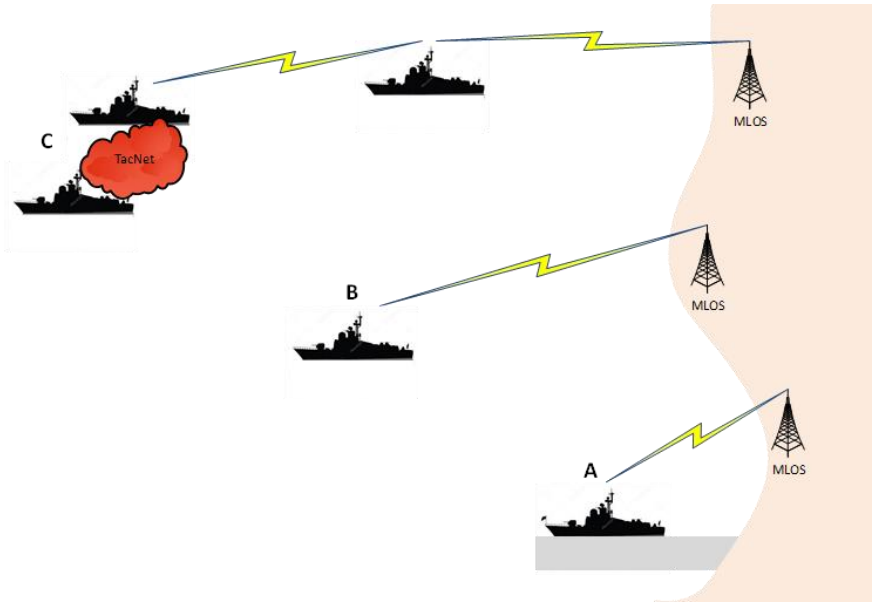

Figura 19: Escenario para MLOS.

5.4.4.3 Comunicaciones tácticas marítimas

Existen diversos subcasos de uso que evidencian el potencial de la tecnología *5G* en los enlaces tácticos marítimos [13][35].

- Aumento de la seguridad en las comunicaciones:

Un nodo *5G* a bordo de buques y aeronaves navales puede sustituir parcialmente a los circuitos de voz y datos *V/UHF* que actualmente se utilizan para la coordinación y ejecución de operaciones navales a nivel táctico dentro del horizonte, mediante la técnica de *Network Slicing*.

El uso de un nodo *5G* para reemplazar las comunicaciones de corto alcance puede tener efectos beneficiosos al facilitar la aplicación de cifrado en todos los circuitos. Asimismo, versiones futuras deberían permitir la aplicación de *beamforming* a las comunicaciones navales, buscando la máxima direccionalidad posible. Estas comunicaciones direccionales pueden evitar que un adversario registre las transmisiones para su posterior descifrado mediante tecnologías cuánticas, lo que añade una capa adicional de seguridad.

El *beamforming* también dificultará que nuestras fuerzas sean detectadas mediante técnicas *COMESM* o que se vean afectadas por acciones de interferencia del adversario, lo que puede representar una ventaja decisiva en combate naval.

Otras posibilidades que deben estudiarse son el uso de *frequency hopping* en las bandas asignadas a operaciones navales, incluso a costa de reducir el ancho de banda disponible, con el objetivo de lograr las comunicaciones más seguras posibles [13][35].

- Repetidor por subred / Red Táctica Marítima (*MTW*):

Uno de los desafíos que presentarán los *BLOS AP* en *HF* sobre *IP* es la posible saturación del espectro si una fuerza naval, incluso mediana o pequeña, accede simultáneamente al mismo punto de acceso [13][35].

La doctrina experimental de uso del *BRIPES* establece que, en los casos en que la fuerza naval sea igual o superior a cuatro buques, solo uno de ellos realizará el acceso al *BLOS AP*, utilizando alguno de los canales mencionados para la difusión de los servicios *C2* recibidos (mensajería formal, *Recognized Maritime Picture* (*RMP*), chat, correo electrónico o envío de archivos). Una red *5G* podría configurarse como el enlace ideal para esta tarea.

Además, este tipo de enlaces *5G* permitiría establecer fácilmente *MTWs* (*Maritime Tactical WAN*) como los descritos en el *ACP 200*. Una *MTW* permitirá compartir información de Inteligencia, Vigilancia y Reconocimiento (*ISR*) y *targeting* a nivel táctico entre los buques de una Fuerza o Grupo de Tarea, en línea con lo establecido en el *ATP 102* y otros documentos tácticos relacionados [13][35].

- Enlaces de Datos:

Un caso más específico es el uso de *5G* en enlaces de datos tácticos, concretamente para el *Link 22*. Este enlace tiene la capacidad de implementar de forma nativa hasta 18 formas de onda distintas, de las cuales solo se han desarrollado nueve. El uso de *Link 22* a través de *5G* puede dar lugar a formas de onda adicionales que mejoren la eficiencia de la red, evitando el riesgo de saturación.

Asimismo, debe implementarse el protocolo *IP* de *Link 22*, perfectamente adaptado a las comunicaciones *5G* y desarrollado por la Agencia de Comunicaciones e Información de la OTAN (*NCIA*), con el fin de facilitar la integración de otros actores clave en las redes *TDL* (*Tactical Data Link*), como los centros de operaciones marítimas (*MOC*) [13][35].

- Sistemas Marítimos No Tripulados (*MUS*) de tamaño medio:

La implementación de tecnología *5G* a bordo, la necesidad de estandarizar y reducir la huella logística de los sistemas, así como las características propias de esta tecnología, ancho de banda, baja latencia y direccionalidad, hacen que el 5G facilite la estandarización de las comunicaciones entre los buques y sus sistemas no tripulados.

Los *MUS* están destinados a complementar y apoyar a los buques de superficie en múltiples tareas. Es fácil visualizar a los *MUS* realizando funciones de *ISR*, *targeting*, lucha contra minas (*MCM*), o incluso apoyando con armamento propio en combate naval [13][35].

- Tareas de protección de fuerzas:

El *5G* puede facilitar la implementación a bordo de sistemas *C2* para los *MUS*, estandarizando canales de control y la representación táctica en tiempo real de la información recogida por sus sensores. Estas características permitirán avanzar hacia la intercambiabilidad de sistemas no tripulados, en un concepto similar al que se aplica actualmente en la aviación naval.

La intercambiabilidad permitirá que un sistema no tripulado de una nación opere en apoyo de buques de distintas nacionalidades, transmitiendo datos de sensores a través del mismo enlace de datos. Asimismo, si se logra un grado suficiente de interoperabilidad y comunalidad, en determinadas ocasiones el control del *MUS* podría transferirse entre buques de diferentes países, aumentando la flexibilidad táctica de las fuerzas navales aliadas [13][35].

5.4.4.4 Nube de combate naval

Las operaciones navales se distinguen particularmente por requerir un mando y control descentralizados y, sin embargo, en el futuro funcionarán mejor bajo una coordinación que permita un alto nivel de intercambio de información.

El concepto de *Naval Combat Cloud* aún está por definirse, pero la aspiración es, al menos, alcanzar algunos de los beneficios previstos en el concepto de Capacidades Habilitadas por Red de la OTAN tales como una mayor eficiencia, un drástico aumento en la interoperabilidad entre naciones, una forma mejorada y segura de compartir información, una mayor calidad de la información o una toma de decisiones más rápida y con mayor velocidad de mando, capacidades que nunca llegaron a desarrollarse completamente.

Sin embargo, la implementación a bordo de buques de nuevas capacidades aún en desarrollo, como el *data lake*, la seguridad centrada en los datos (*data-centric security*), o el *edge* y *fog computing*, permitirá el procesamiento descentralizado de la información, alejado de los CPD y, en su caso, de los centros de operaciones en tierra. La fuerza naval aliada debe ser independiente y capaz no solo de gestionar la transmisión de datos a una velocidad y distancia suficientes que le permitan alcanzar la superioridad en combate, sino también de integrar fuerzas de otros dominios, especialmente el aéreo, terrestre y espacial [13][35].

La sostenibilidad de la fuerza naval en el mar dependerá de su autonomía en aspectos de personal, logística, inteligencia o planificación. Toda esta información deberá poder compartirse en un entorno táctico y de forma flexible, permitiendo que la información adecuada llegue al destinatario adecuado. El medio que debe utilizarse para esta transmisión de datos, debido a las características ya mencionadas en este trabajo, será el *5G*. Aunque no está directamente relacionado con la tecnología *5G*, su aplicación puede generar beneficios colaterales. Uno o dos nodos *5G* requieren menos peso y espacio que las actuales radios *V/UHF*, que suelen ser pesadas y afectan a la estructura del buque, lo que mejora la estabilidad y la reserva de flotabilidad de cara a futuras modernizaciones del mismo.

5.5 Ejercicios multinacionales

En los ejercicios multinacionales ya mencionados se integraron redes *5G* con sistemas *C2*, *ISR* y plataformas legadas en escenarios combinados.

En ellos se validó:

- Interoperabilidad total.
- Configuraciones multinodo con *slicing* federado.
- Seguridad multicapa y mitigación de interferencias (*jamming*, *spoofing*).

Han demostrado:

- Viabilidad de *slices* federados entre aliados y compartición de red física con control lógico independiente.
- Aplicación de *slicing* para aislamiento multinacional, separación por funciones y control de recursos.
- MEC útil para operaciones sin conectividad central o en entornos EM denegados.
- Despliegue automatizado mediante ZTP y gestión de servicios a través de orquestadores multimodo.

5.6 Análisis comparativo y evaluación de resultados

Los casos de uso evaluados incluyen tanto configuraciones terrestres como marítimas, integrando múltiples tecnologías y soluciones tácticas. Las funcionalidades clave incluyen conectividad persistente, operación distribuida, resiliencia frente a interferencias, y soporte a plataformas no tripuladas. En la Tabla 26 podemos observar cómo afectan las tecnologías más relevantes en los diferentes escenarios antes desarrollados.

Caso de Uso	Aplicaciones de *NS*	Aplicaciones de *MEC*
LHQ (Large HQ)	*Slices* diferenciados por dominio funcional (*C2*, inteligencia, logística, organización OTAN); aislamiento multinacional; *QoS* garantizado.	Procesamiento local de datos de operaciones; reducción de latencia para sistemas *C2*; menor dependencia de nube.
SDHQ (Small Deployable HQ)	Separación de tráfico táctico, logístico y apoyo; uso de *slice* público seguro en redes civiles; aislamiento por aplicación.	Procesamiento autónomo en despliegues iniciales; soporte a sensores e *IoT*; continuidad operativa en entornos degradados.
MCP (Mobile Command Post)	Uso de *slices URLLC* para comunicaciones críticas; conexión con redes públicas sin necesidad de espectro militar; slicing dedicado E2E.	Soporte a *UGV/UAV*; autonomía táctica para unidades móviles; continuidad de red sin escalón superior.
HSC (High Seas Communications)	Tres *slices* por función: sensores *UAV/USV*, control autónomo, *C2* naval; diferenciación de tráfico simultáneo.	*MEC* embarcado; toma de decisiones autónoma; IA para mantenimiento; descongestión de *SATCOM* y *HF*.
AC (Amphibious Communications)	*Slices* para *C2* de unidades, control de dispositivos autónomos y sensores; optimización de recursos de red durante desembarcos.	Procesamiento de datos *UUV* y sensores costeros; soporte a mando en fases de desembarco; autonomía táctica.
CC (Coastal Communications)	*Slicing* sobre red pública para reducir infraestructura propia; aislamiento funcional y disponibilidad garantizada.	*MEC* terrestre complementario al embarcado; reducción de carga en enlaces tierra-mar; apoyo a *C2 costero*.

Tabla 26: Aplicación de NS y MEC en los diferentes escenarios.

- *Network Slicing* resulta clave para entornos con múltiples aplicaciones y usuarios concurrentes, garantizando seguridad, *QoS* y segmentación funcional.
- *MEC* aporta resiliencia, baja latencia y autonomía, especialmente útil en comunicaciones tácticas, sensores o *ISR* en tiempo real.
- Ambas tecnologías han demostrado su efectividad en entornos reales y simulados, pero requieren planificación avanzada, orquestación federada, y adaptación al espectro disponible.

La Tabla 27 presenta un resumen de las tecnologías *5G* consideradas en distintos casos de uso operativos, incluyendo sus principales ventajas y limitaciones en escenarios específicos.

Escenario	*mMIMO, Beamforming, Spatial multiplexing*	*mmWaves*
LHQ (Large HQ)	- Alta tasa de datos (*beamforming* y multiplexado espacial). - Mejor señal *downlink*. - Mayor ganancia en dirección deseada (*3D beamforming, MU-MIMO/SISO*).	Difícil implementación debido a rango limitado, pérdidas de propagación, penetración limitada, dependencia climática, complejidad del equipo y regulación.
SDHQ (Small Deployable HQ)	- Alta tasa de datos y reducción de emisiones no deseadas (menor detección). - Limitada resistencia a *jamming*. - Apto para enlaces *PTP/PTMP*. - Baja probabilidad de detección.	Difícil implementación por pérdidas de propagación, penetración limitada, dependencia climática, complejidad y consumo energético.
MCP (Mobile Command Post)	- Alta tasa de datos y reducción de emisiones no deseadas. - Limitada resistencia a jamming. - Movilidad limitada por tamaño y consumo (necesidad de antenas pequeñas). - Reducción de firma EM.	Adecuado para comunicaciones tiempo real, baja latencia, uso en plataformas móviles. Limitaciones por alto consumo energético y rango limitado.
HSC (High Seas Communications)	- Alta ganancia y reducción de emisiones no deseadas. - Compensación activa de desalineación de antena. - Mejor rendimiento en *LoS* y condiciones EM extremas.	Difícil implementación debido a rango limitado, pérdidas de propagación, penetración limitada y dependencia climática.
AC (Amphibious Communications)	- Alta tasa de datos, reducción de emisiones no deseadas. - *MIMO/beamforming* para mejor rendimiento y coexistencia con redes comerciales. - Movilidad y flexibilidad de equipos necesaria.	Posible uso en plataformas móviles (vehículos, *UAVs*). Limitaciones en rango, pérdidas de propagación, dependencia climática, complejidad y consumo energético.
CC (Coastal Communications)	- Mejor eficiencia espectral y tasa de datos alta. - Simplificación de coexistencia con redes comerciales. - Reducción de emisiones no deseadas en entornos EW moderados.	Difícil implementación por rango limitado, pérdidas de propagación, penetración limitada, dependencia climática y regulaciones.

Tabla 27: Aplicación de tecnologías específicas en los diferentes escenarios.

Por último, en la Tabla 28, vemos un resumen donde se recomienda la implementación de cada escenario cuando existan requerimientos de seguridad reforzada, procesamiento local, independencia operativa o despliegue ágil en entornos multinacionales o EM degradados.

Caso de Uso	Entorno Operacional	Movilidad	Entorno EM	Infraestructura de Red	Soporte a BYOD/Civiles	Clasificación de Seguridad
LHQ (Large HQ)	Interior de territorio aliado	Estática con infraestructura permanente	Benigno, interferencia no intencional	*LAN, FO, FWA* disponible	Sí, con riesgos de seguridad	Hasta *NATO-TopSecret*
SDHQ (Small Deployable HQ)	Cerca de zonas de conflicto	Estática pero portátil / desplegable	Relativamente benigno, con riesgo de interferencia adversaria	Autosuficiente si no hay *LAN/FO*	No permitido	Hasta *NATO-Confidential*
MCP (Mobile Command Post)	Territorio adversario o zonas de alto riesgo	Totalmente móvil (en movimiento)	Altamente hostil, con *jamming* activo	Sin infraestructura fija; totalmente móvil	No permitido	Hasta *NATO-Restricted*
HSC (High Seas Communications)	Alta mar (aguas internacionales)	Buques móviles en alta mar	Variable: de no disputado a altamente disputado	Redes embarcadas; uso de bandas *IMT*	No especificado (en general no)	Flexible, uso de múltiples bandas
AC (Amphibious Communications)	Zonas costeras en conflicto	Buques y fuerzas anfibias en transición	Altamente disputado; requiere *LPI/LPD*	Sin infraestructura terrestre; alta agilidad espectral	No permitido	Flexible, con alto grado de interferencia
CC (Coastal Communications)	Puertos y zonas costeras aliadas	Buques en tránsito o atracados	Benigno, sin amenazas *EW*	Acceso costero; uso de redes públicas cuando sea viable	Uso de redes públicas (cuando posible)	Cumple regulaciones territoriales

Tabla 28: Despliegue de los diferentes escenarios en función de diferentes factores.

5.7 Redes *5G* embarcadas en aeronaves militares

El uso de tecnología *5G* a bordo de aeronaves militares representa un ámbito de gran potencial, pero con importantes limitaciones tecnológicas actuales. A diferencia de otras plataformas móviles (vehículos, buques, *UGVs*), las aeronaves tripuladas presentan una serie de restricciones que dificultan su integración como nodos *5G* autónomos o completos.

Principales limitaciones:

- Interferencias electromagnéticas (*EMI*): el *5G* opera en bandas que pueden interferir con equipos críticos de navegación, comunicación y guerra electrónica a bordo de aeronaves.
- Restricciones físicas y de certificación: las aeronaves militares deben cumplir con estrictas normativas aeroespaciales. Cualquier sistema *5G* embarcado debe pasar

procesos largos y costosos de homologación, especialmente en aeronaves de combate.
- Alta velocidad y movilidad: el cambio rápido de celda, el efecto *Doppler* y la pérdida de línea de visión con nodos terrestres complican el *handover* y la estabilidad de los enlaces *5G* estándar.
- Ausencia de infraestructura aérea: actualmente no existen redes *5G* terrestres preparadas para mantener conectividad estable con aeronaves a media o alta altitud (por encima de 1.5 km), salvo en configuraciones experimentales con *LEO-SATCOM* o *HAPS.*

Iniciativas actuales:

- *DIBAX* ha estudiado el uso de aeronaves como nodos intermedios entre dominios terrestre y aéreo, aunque sin desplegar 5G completo en la aeronave.
- *COMPAD 5G* contempla escenarios donde aeronaves pueden actuar como clientes *5G* (*UEs*) para recibir datos *ISR* o *C2*, pero no como nodos de red completos.
- *MN5G* y *CWIX* han evaluado enlaces *5G* para *UAVs* y nodos embarcados de baja altitud, sin alcanzar aún configuraciones robustas para aeronaves tripuladas en vuelo.

Perspectiva de futuro:

La posibilidad de dotar a las aeronaves de capacidades *5G* completas (*gNodeB* o *edge node* embarcado) está condicionada al desarrollo de:

- Equipos certificados de baja interferencia electromagnética.
- Protocolos *3GPP* adaptados a movilidad aérea (>500 km/h).
- Integración con sistemas *LEO-SATCOM* y *backhaul* aéreo resiliente.

En el medio plazo, se espera que el uso de *5G* en aeronaves se limite a aplicaciones como:

- Conectividad en tierra o estacionadas (mantenimiento, transferencia de datos, entrenamiento).
- Redes internas para compartimentación y *C2* a bordo.
- Recepción de datos *ISR* desde sensores o *UAVs* durante misiones coordinadas.

Al margen de esto, un avance significativo en la integración de tecnología *5G* en plataformas aéreas tuvo lugar el 3 de octubre, cuando el Ejército del Aire y del Espacio completó con éxito el primer vuelo de un sistema *5G Stand Alone* (*SA*) aeronáutico instalado en un avión reactor E25 (C101), como vemos en la Figura 20 [24]. Esta demostración se enmarca dentro del proyecto BACSI (Base Aérea Conectada, Sostenible e Inteligente), concretamente en el ámbito del Área Funcional 6.

El sistema fue desarrollado por *Airbus Defence and Space* y Telefónica Empresas Defensa y Seguridad, y su instalación requirió una modificación estructural específica diseñada conjuntamente por el Mando de Apoyo Logístico (MALOG), la Maestranza Aérea de Albacete y *Airbus Defence and Space*. El proceso completo de diseño,

integración, calificación y certificación experimental, junto con las pruebas en laboratorio, en tierra y en vuelo, se completó en menos de seis meses, evidenciando una destacada capacidad de integración tecnológica [26][32].

El vuelo fue ejecutado desde la base aérea de Getafe por personal del Centro Logístico de Armamento y Experimentación (CLAEX), logrando superar registros previos en velocidad, alcance de comunicación y maniobrabilidad para sistemas similares en entornos comparables. Este logro posiciona a España en la vanguardia tecnológica respecto a la experimentación con redes *5G* embarcadas en aeronaves.

Además de reforzar la capacidad operativa del Ejército del Aire y del Espacio, esta iniciativa proporciona una valiosa plataforma de pruebas para futuras aplicaciones de *5G* en el entorno aeronáutico y multidominio. Su utilidad como banco de ensayos facilitará el desarrollo de nuevos enlaces de datos, sistemas de comunicación y capacidades asociadas a redes *edge* distribuidas, alineándose con los objetivos de sostenibilidad, digitalización y superioridad operativa definidos por el proyecto BACSI [24].

Figura 20: Avión reactor E25

Capítulo 6. Impacto de otras tecnologías habilitadoras en las operaciones multidominio

6.1 Inteligencia Artificial para análisis y toma de decisiones

La Inteligencia Artificial (IA) se ha consolidado como un habilitador crítico en el marco de las Operaciones Multidominio (*MDO*). Tanto el Ministerio de Defensa español como la OTAN y la UE reconocen su potencial transformador en la doctrina, la capacidad operativa y los procesos de toma de decisiones. Lejos de ser solo una tecnología de apoyo, la IA se percibe como una capacidad operativa esencial, en particular cuando se combina con tecnologías como el *5G*, el *Edge Computing* y las arquitecturas *C2* distribuidas.

6.1.1 Marco institucional y estratégico

El MINISDEF, a través de su Estrategia Nacional [76], establece tres líneas principales:

- Integración de la IA en sistemas de armas, inteligencia, ciberdefensa y logística.
- Desarrollo de una red de centros tecnológicos militares especializados.
- Implantación de un marco ético, interoperable y alineado con las iniciativas de la OTAN y la UE.

En paralelo, dentro de la DIVPLA del EMAD [77] se detalla el estado actual de adopción, las capacidades existentes, los pilotos en curso y el enfoque federado con el que se busca acelerar el despliegue de soluciones IA en los ejércitos.

A nivel OTAN, el *NATO Artificial Intelligence Strategy* y la hoja de ruta de *Emerging and Disruptive Technologies* (*EDTs*) [78] priorizan la IA en dominios como *ISR*, logística, mantenimiento predictivo, *targeting*, ciberdefensa, sistemas no tripulados y mando y control distribuido. La interoperabilidad y la gobernanza responsable son pilares centrales de estos marcos.

6.1.2 Aplicaciones clave de IA en el entorno militar

Entre los casos de uso operativos más relevantes ya identificados y validados en entornos OTAN y MINISDEF destacan [4][7][14]:

- Análisis automatizado de inteligencia multisensorial (*SIGINT, IMINT, HUMINT*) mediante modelos entrenados en detección de patrones, identificación de amenazas y clasificación de comportamiento hostil. Estos modelos se integran en plataformas *C2* para facilitar la toma de decisiones en tiempo real.
- Apoyo a sistemas *C2* mediante IA cognitiva, que propone cursos de acción (*COA*) optimizados en base a simulaciones y aprendizaje reforzado. Esto se ha probado con éxito en escenarios federados como *CWIX* y experimentaciones del EMAD y la DGAM.
- Asistentes virtuales entrenados con doctrina militar, como el caso del sistema Gonzalo, desarrollado por el MCCE. Este asistente utiliza *LLMs* especializados y

funciones de *RAG* (*Retrieval Augmented Generation*) para asistir en la redacción de planes operativos, informes técnicos y búsqueda contextualizada de documentos doctrinales. Mejora significativamente la trazabilidad documental y reduce la carga cognitiva del personal de estado mayor.

- IA en ciberdefensa activa, aplicada a la detección de comportamientos anómalos, reconocimiento de patrones maliciosos y orquestación de contramedidas automáticas en redes distribuidas. Esta línea de trabajo, impulsada por el MCCE, ya se encuentra integrada con soluciones de *Security Information and Event Management* (*SIEM*) con capacidades predictivas.
- IA embarcada sobre redes *edge* y nodos *5G*, que permite aplicar modelos de inferencia local en condiciones de conectividad limitada, ideal para misiones *ISR*, *targeting* y control de plataformas no tripuladas (*UxV*). Esto ha sido especialmente relevante en proyectos como TRITÓN y NUCOCAS, donde la latencia reducida y el procesamiento distribuido son esenciales para la autonomía táctica.
- IA para mantenimiento predictivo de plataformas, particularmente útil en entornos navales (BACSI, TRITÓN), donde los sistemas de IA analizan datos en tiempo real de sensores embarcados para anticipar fallos y optimizar ciclos de vida.

6.1.3 Convergencia IA-5G: acelerador operacional

La convergencia entre IA y redes *5G/MEC* permite llevar inteligencia al borde (t*actical edge*), mejorando:

- La velocidad de inferencia.
- La eficiencia energética de los UEs.
- La autonomía operativa sin dependencia de la nube táctica o estratégica.

Esta sinergia es crucial en entornos altamente degradados o contestados, y se encuentra en fase de experimentación avanzada en entornos como las bases BACSI y los *SDHQs* desplegables validados por OTAN [8][13].

6.2 Internet de las cosas (IoT) militar

El Internet de las Cosas Militar (*IoMT – Internet of Military Things*) constituye un componente esencial en la transformación digital de las operaciones multidominio (*MDO*). Su objetivo es integrar sensores, plataformas y dispositivos en una red inteligente y distribuida que proporcione datos operacionales críticos en tiempo real, con capacidad de actuar de forma autónoma o federada en entornos dinámicos y hostiles.

En el entorno del Ministerio de Defensa, el *IoMT* ha evolucionado desde arquitecturas aisladas de sensores hacia un ecosistema interoperable basado en redes privadas *5G*, procesamiento *edge* (*MEC*) y nodos desplegables. Proyectos como BACSI, NUCOCAS, TRITÓN, y pilotos en entornos *SDHQ/LHQ* han consolidado su uso en distintos dominios [6][7][8][13][43].

6.2.1 Aplicaciones operativas del IoMT en escenarios multidominio

A continuación, se detallan los casos de uso operativos más relevantes que combinan el *IoMT* con *5G* y *Edge Computing*:

- "*Warrior-as-a-sensor*": sensores biométricos, de movimiento y ambientales integrados en el equipamiento del combatiente generan datos en tiempo real sobre su estado físico, estrés térmico, posición y entorno. Este tipo de sensorización está validado en contextos de BACSI y batallones experimentales de Infantería de Marina.
- Plataformas no tripuladas (*UxV*): *UAVs, UGVs y USVs* transmiten telemetría, vídeo *HD*, estado técnico, datos de misión y parámetros de salud estructural a nodos *edge* mediante enlaces *5G*. Estas transmisiones pueden ser procesadas localmente o en *MEC* embarcados, activando alertas de mantenimiento predictivo o generando mapas *ISR* autónomos.
- Sistemas de vigilancia perimetral en bases inteligentes: las bases de *BACSI* incorporan sensores acústicos, *RF, IR*, cámaras inteligentes y radares pasivos en red para protección de perímetro. Estos sensores son gestionados mediante *slicing* lógico que garantiza la prioridad de tráfico crítico (ej. detección de intrusos o disparos).
- Redes de sensores en entorno *NBQ/CBRN*: estaciones portátiles desplegables, sensores distribuidos y microdrones integran información atmosférica, partículas en suspensión, temperatura, humedad o contaminación para detectar y rastrear amenazas químicas o biológicas.
- Monitorización estructural en plataformas navales y terrestres mediante sensores *IoT* embarcados que reportan vibraciones, microfisuras, niveles de combustible o datos de presión y temperatura de sistemas críticos.

6.2.2 Infraestructura técnica y doctrinal

La OTAN considera al *IoMT* como parte estructural de la evolución hacia una arquitectura *C4ISR* distribuida, resiliente y federada. En el marco de *FMN Spiral 6*, el *IoMT* debe cumplir requisitos como [5]:

- Interoperabilidad multinacional mediante perfiles *FMN* y STANAGs (ej. STANAG 4586 para interoperabilidad de UxV) [79].
- Gestión federada del tráfico sensorial mediante *Network Slicing*.
- Procesamiento distribuido con MEC, lo que permite autonomía táctica incluso en condiciones de desconexión parcial o degradación del entorno electromagnético.

Ejercicios como *CWIX* han validado escenarios de despliegue con más de 10.000 dispositivos *IoT* simultáneos, gestionados mediante orquestadores *5G*, nodos *edge* con capacidad de inferencia IA, y políticas de *QoS* diferenciadas por función (inteligencia, logística, sostenimiento, etc.) [4].

6.2.3 Desafíos actuales y líneas de desarrollo

A pesar de los avances, el *IoMT* enfrenta desafíos estructurales y técnicos que condicionan su despliegue masivo:

- Ciberseguridad del *IoT* militar: los dispositivos *IoMT* deben contar con identidad criptográfica, *firmware* validado y comunicaciones cifradas extremo a extremo, incluso en redes parcialmente compartidas (*GOGO/COGO*).
- Saturación del canal radioeléctrico: en escenarios de alta densidad de sensores, es necesario aplicar políticas de *slicing* jerárquico, protocolos *NB-IoT* y esquemas de frecuencia adaptativa (*DSS* o *frequency hopping*).
- Orquestación y escalabilidad: la gestión de topologías en red mallada (*mesh*), el *handover* de sensores móviles (por ejemplo, *UAVs* en vuelo) y la integración de nodos en redes federadas sigue requiriendo herramientas automatizadas y estándares abiertos compatibles con entornos OTAN.
- Limitaciones *SWaP* (*Size, Weight and Power*) para nodos *edge* y *UEs*, especialmente en despliegues de *MCP* o *UGV/UAV* ligeros.

6.2.4 Tendencias emergentes

El futuro del *IoMT* se orienta hacia arquitecturas basadas en:

- *eSIMs* programables por perfil de misión.
- Identidad federada entre redes nacionales y aliadas.
- Inferencia IA embebida en sensores inteligentes, reduciendo la necesidad de *backhaul*.
- Integración con *data lakes* tácticos, donde los sensores generan metadatos procesables a través de reglas de negocio o inferencia semántica.

6.3 Big Data y análisis predictivo

La gestión y explotación de grandes volúmenes de datos se ha convertido en un factor crítico para la superioridad operativa en escenarios multidominio. En el entorno militar actual, el *Big Data* permite transformar la complejidad informacional en conocimiento procesable, facilitando la anticipación, la optimización táctica y la toma de decisiones en tiempo real.

La sinergia entre *Big Data*, redes *5G* y procesamiento *edge* potencia significativamente la arquitectura *C4ISR* moderna, habilitando operaciones basadas en datos y elevando el concepto de superioridad informativa al núcleo del diseño operativo.

6.3.1 Aplicaciones operativas del Big Data en defensa

Entre las aplicaciones más relevantes se encuentran:

- Análisis predictivo de amenazas: mediante la correlación de señales de inteligencia multisensorial (*SIGINT, HUMINT, IMINT*) y patrones históricos, se

pueden anticipar acciones hostiles, planear contramedidas y optimizar el ciclo de decisión *OODA*.

- Mantenimiento predictivo en plataformas complejas: *UAVs*, *UGVs*, fragatas o blindados transmiten telemetría a través de 5G, alimentando modelos de fallo que permiten programar mantenimientos antes de la avería. Este modelo está en despliegue en los entornos BACSI y NUCOCAS [8][43].
- Logística inteligente y reabastecimiento autónomo: algoritmos de optimización sobre datos en vivo de consumo, ubicación, estado del entorno y capacidades de transporte permiten recalcular rutas y prioridades logísticas de forma dinámica.
- Fusión e inferencia de inteligencia: correlación de datos procedentes de sensores *ISR*, redes sociales, señales *RF*, datos meteorológicos, tráfico marítimo, etc., para producir escenarios operativos enriquecidos.
- Modelado y simulación de escenarios: se generan escenarios futuros mediante la extrapolación de datos históricos y proyecciones IA. Estas capacidades se utilizan en la planificación operativa y en sistemas de entrenamiento avanzado como entornos de Realidad Aumentada o Gemelo Digital [80].

6.3.2 Arquitectura técnica: del *data lake* al *combat cloud*

Un *data lake* es un repositorio centralizado que almacena grandes cantidades de datos en bruto, en su formato original, ya sean estructurados, semiestructurados o no estructurados. Dentro del EMAD se analiza la implementación de una arquitectura federada de datos tipo data *mesh*, desplegada mediante plataformas de virtualización (propuesta por la empresa Denodo) y gobernanza distribuida [81]. Esta estructura:

- Permite el acceso en tiempo real a fuentes heterogéneas (bases nacionales, OTAN, UE, sensores *ISR*, sistemas logísticos).
- Mantiene el control de acceso por roles, trazabilidad y cumplimiento normativo (*compliance*).
- Facilita la explotación distribuida a través de nodos *edge* desplegables, incluso sin conexión constante a centros de datos estratégicos.

En el plano aliado, la *NATO Data Exploitation Framework* [82] establece los principios para la explotación de Big Data militar en entornos federados, priorizando:

- Federación semántica e interoperabilidad mediante estándares compartidos.
- Procesamiento en el borde (*edge*) mediante IA para análisis situacional en tiempo real.
- Compatibilidad con plataformas nacionales y comerciales (*dual use*).

El objetivo final es lograr una "*combat cloud*" táctica, donde los datos operacionales se compartan de forma segura, oportuna y contextualizada entre todos los niveles de mando y plataformas desplegadas.

6.3.3 Desafíos actuales en el empleo militar del Big Data

A pesar del alto potencial, persisten retos importantes:

- Calidad de datos en condiciones de campo: sensores en entornos hostiles, interferencias electromagnéticas, pérdida de conectividad o falta de sincronización pueden comprometer la precisión de los modelos.
- Integración semántica multinacional: la coexistencia de fuentes aliadas y nacionales requiere mapeos ontológicos, diccionarios comunes y perfiles *FMN* compartidos.
- Seguridad y protección de datos sensibles: los datos agregados, si se interceptan, pueden revelar patrones operativos críticos. Se requieren medidas de *data-centric security*, segmentación lógica (*slicing*) y cifrado extremo a extremo.

El *Big Data*, cuando se combina con tecnologías como el *slicing*, el *Edge Computing* y la IA, permite transformar datos crudos en ventaja operativa en tiempo real, consolidando el modelo de operaciones centrado en datos que define las futuras *MDO (Multi-Domain Operations)*.

6.4 Realidad Aumentada y Realidad Virtual para formación y despliegue

Las tecnologías de Realidad Aumentada (RA) y Realidad Virtual (RV) se han consolidado como habilitadores clave en el adiestramiento militar y la mejora de la conciencia situacional en operaciones multidominio. Su integración con redes *5G*, E*dge Computing* e Inteligencia Artificial (IA) permite generar entornos inmersivos, interactivos y dinámicos, capaces de replicar escenarios tácticos reales con alta fidelidad y adaptabilidad.

Estas tecnologías forman parte del conjunto de Capacidades Emergentes y Disruptivas (*EDTs*) reconocidas por la OTAN y la UE, y se encuentran recogidas como líneas de acción prioritarias tanto en el Plan de Acción para la Digitalización del MINISDEF como en las iniciativas del MCCE sobre centros de simulación desplegable [3].

6.4.1 Aplicaciones principales en el entorno militar:

- Adiestramiento avanzado y simulación táctica:
  - Reproducción de entornos multidominio (terrestre, aéreo, marítimo, cibernético y espacial) sin necesidad de despliegue real de unidades.
  - Simulación de operaciones complejas como asaltos urbanos, desembarcos anfibios o reconocimiento aéreo.
  - Entrenamiento de combate en salas de simulación multijugador, sincronizadas por red *5G* con sistemas RA/RV.
  - Evaluación objetiva del desempeño mediante recolección de datos biométricos y análisis de patrones de movimiento.
- Soporte a la operación táctica:

  - Despliegue de dispositivos RA sobre gafas tácticas o visores integrados (*HUDs*), con superposición en tiempo real de:
    - Mapas topográficos, rutas de patrulla y puntos de interés.
    - Posiciones aliadas y amenazas detectadas.
    - Indicaciones para navegación autónoma de *UxVs*.
  - Aplicación directa al combatiente conectado en plataformas como el proyecto "soldado del futuro" del Ejército de Tierra.
- Planeamiento y mando y control:
  - Exploración inmersiva de escenarios 3D para planificar cursos de acción (*wargaming*).
  - Visualización táctica de evolución de operaciones en centros de mando federados (como se propone en el concepto de *Naval Combat Cloud*).
  - Simulación federada con aliados en ejercicios multinacionales como en *CWIX*, usando entornos RV interoperables.

6.4.2 Ventajas técnicas al integrarse con redes 5G:

- Alta capacidad de transmisión (hasta 1 Gbps), necesaria para transmitir contenidos RV en resolución *HD* y entornos dinámicos.
- Ultra baja latencia (*URLLC*), crítica para mantener la sincronización y respuesta en tiempo real en operaciones simuladas o reales.
- Posibilidad de segmentación por aplicación mediante *Network Slicing* (e.g., slice exclusivo para simulación táctica vs. slice para operaciones reales).
- Procesamiento distribuido gracias a *Multi-access Edge Computing*, que permite que los contenidos RA/RV se rendericen localmente, evitando congestiones de red.

6.4.3 Limitaciones y desafíos actuales:

- Asegurar la compatibilidad electromagnética de los dispositivos RA/RV con los entornos EM hostiles y redes tácticas militares.
- Desarrollar estándares interoperables de contenido (formatos gráficos, bases de datos, protocolos de sincronización) para uso multinacional.
- Garantizar la ciberseguridad y autenticación de los dispositivos conectados, especialmente en entornos degradados o con adversarios con capacidades de interferencia.
- Superar los requisitos de *SWaP* para gafas y cascos tácticos, especialmente en operaciones prolongadas.

6.4.4 Proyectos destacados:

- *NextGen Simulations* (UE): iniciativa para plataformas RA interoperables en entrenamiento conjunto [83].
- Gemelo Digital de Batallón OTAN (propuesta *NCIA*): construcción de entornos virtuales gemelos para análisis predictivo y formación de unidades [81].
- Asistente Gonzalo: proyecto del MCCE que explora el uso de IA y RA para asistir a planificadores en redacción de planes y generación de opciones tácticas [14].

Las RA y RV no solo suponen una evolución en los métodos de instrucción militar, sino también una extensión natural del ecosistema digital que impulsa las *MDO*. Su despliegue operacional, combinado con *5G*, IA y *Edge Computing*, transforma la forma en que las Fuerzas Armadas se adiestran, planifican y actúan, mejorando radicalmente la preparación, la interoperabilidad y la eficacia táctica en escenarios cada vez más exigentes y tecnológicos. En la Figura 21 [13] podemos observar un ejemplo de despliegue.

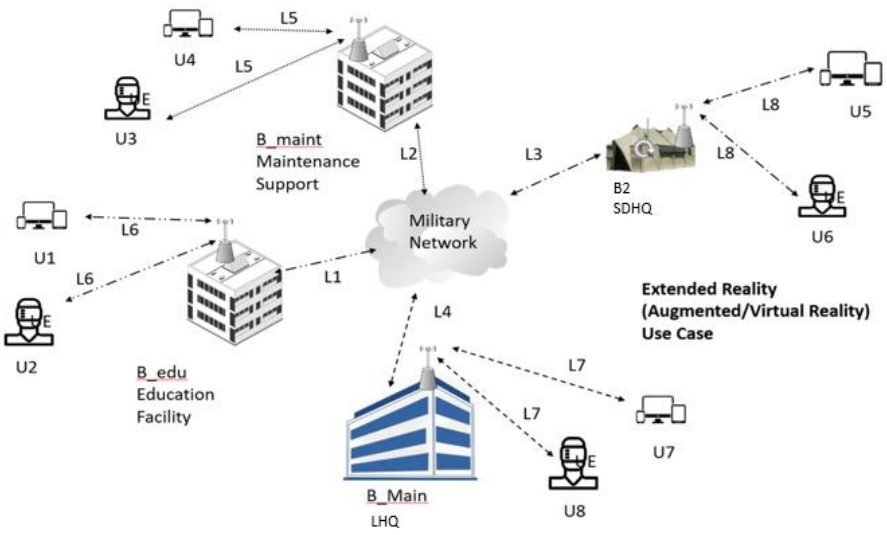

Figura 21: Ilustración de dispositivos RA/RV en escenarios de instrucción y combate simulado.

6.5 Automatización y sistemas autónomos (UXVs)

La automatización y el uso de sistemas autónomos (*UXVs*, por sus siglas en inglés: *Unmanned X Vehicles*) constituyen una de las líneas más disruptivas en la evolución de las capacidades militares en operaciones multidominio. Incluyen vehículos terrestres (*UGV*), aéreos (*UAV*), navales de superficie (*USV*) y submarinos (*UUV*), con distintos niveles de autonomía, sensorización y conectividad.

La combinación de estas plataformas con redes *5G*, *Edge Computing* e inteligencia artificial permite operar de forma descentralizada, reducir la exposición de personal y ejecutar misiones de reconocimiento, vigilancia, guerra electrónica o ataque de manera más precisa y rápida. Estas capacidades son fundamentales en entornos de combate modernos, donde la velocidad de reacción, la persistencia y la flexibilidad son determinantes.

6.5.1 Aplicaciones actuales más relevantes

- *UGVs* tácticos para transporte logístico automatizado, desminado, reconocimiento de ruta o fuego de apoyo en ambientes hostiles.
- *UAVs* de corto y medio alcance con capacidades *ISR*, retransmisión de comunicaciones, ataque de precisión o interferencia electrónica.
- *USVs/UUVs* navales para patrulla costera, contramedidas de minas, exploración de puertos o seguimiento de submarinos enemigos.

El proyecto TRITÓN, liderado por la Armada Española, explora el empleo de redes *5G* embarcadas para conectar *UAVs* y *USVs* en escenarios navales [7]. Del mismo modo, el Ejército de Tierra experimenta con *UGVs* y *micro-UAVs* integrados en redes tácticas *5G*, aprovechando la ultra baja latencia y el *slicing* para garantizar prioridades de misión. Estas capacidades se complementan con funciones de *Edge Computing* desplegadas en nodos móviles y plataformas embarcadas.

Desde el punto de vista doctrinal, la OTAN contempla el despliegue de *swarms* (enjambres) de plataformas autónomas cooperativas, que toman decisiones descentralizadas, asignan tareas dinámicamente y se adaptan al entorno en tiempo real [13]. Estas arquitecturas requieren una conectividad robusta, baja latencia y procesamiento distribuido, condiciones que el *5G* y el *MEC* satisfacen de forma nativa.

Asimismo, la interoperabilidad multinacional de plataformas autónomas y su integración en redes federadas (*FMN*) son áreas prioritarias de desarrollo [5][13].

6.5.2 Desafíos clave asociados

- Integración segura con sistemas *C2* y supervisión humana (*human-in-the-loop* o *human-on-the-loop*).
- Interoperabilidad multinacional de plataformas autónomas mediante estándares abiertos y enlaces tácticos comunes (ej. *Link 16, Link 22*) [84].
- Implicaciones éticas, legales y normativas del uso de sistemas de armas autónomos.
- Mitigación de amenazas en el dominio electromagnético mediante técnicas de *beamforming, hopping* espectral y radio cognitiva [85].

El uso de *5G*, combinado con *slicing* y capacidades *edge*, permite además establecer canales dedicados por tipo de misión, aislamiento de flujos críticos y procesamiento distribuido para minimizar la latencia. Esto es clave para la operación de enjambres autónomos en misiones simultáneas. En la Tabla 29 podemos observar las funcionalidades claves que aporta el *5G* a estas plataformas.

Tipo de Plataforma	Funcionalidades clave *5G*	Capacidades habilitadas
UAV (aéreo)	*URLLC, slicing, sidelink*	ISR, retransmisión, ataque de precisión, *EW*
UGV (terrestre)	*mMIMO, edge, D2D*	Reconocimiento, desminado, logística
USV (superficie)	*NTN, slicing, MEC*	Patrulla, control marítimo
UUV (submarino)	*LoS*/interfaz nodo-*UxV*	Exploración subacuática, seguimiento submarinos

Tabla 29: Relación entre tipos de UXVs, funcionalidades 5G y capacidades tácticas.

En conjunto, los sistemas autónomos conectados a través de redes *5G* suponen un multiplicador estratégico para las Fuerzas Armadas. Como podemos ver en guerras actuales como la de Rusia y Ucrania, no solo reducen el riesgo humano, sino que extienden el alcance, persistencia y capacidad de respuesta en todos los dominios. Su despliegue debe realizarse con una arquitectura robusta, interoperable y segura, conforme a estándares OTAN y bajo principios éticos y legales definidos. Esta sinergia entre

automatización, conectividad y toma de decisiones distribuidas consolida a los *UXVs* como herramientas clave en el modelo operativo de las MDO del presente y futuro.

6.6 Data Center Security

La seguridad de los centros de datos constituye un pilar fundamental en la arquitectura digital de defensa, especialmente cuando se integran redes *5G*, *Edge Computing*, virtualización de funciones de red (*NFV*) y entornos distribuidos. Se busca seguir una filosofía de seguridad centrada en el dato (*data centric security, DTS),* con políticas de seguridad centradas en proteger directamente el dato, en lugar de enfocarse en el perímetro, en la red o los dispositivos. Se realizan controles de acceso basado en atributos, etiquetado de datos y cifrado persistente. Esta filosofía sigue con la lógica del *Zero Trust* y permite compartir inteligencia sin comprometer integridad y es clave en redes militares.

En el marco de operaciones multidominio (*MDO*), donde los datos operativos fluyen entre centros estratégicos, nodos *edge* y plataformas desplegadas, garantizar la integridad, disponibilidad y confidencialidad de estos entornos es esencial para la continuidad operativa y la resiliencia cibernética.

En entornos militares, los centros de datos no son estructuras homogéneas, sino que responden a distintos niveles de operación [64]:

- Centros estratégicos: ubicados en retaguardia o nubes privadas de defensa, con altos niveles de seguridad física, redundancia y capacidad de orquestación.
- Centros tácticos: nodos *edge* desplegables cerca del área de operaciones, con arquitectura modular, capacidad de computación local, y requisitos específicos de baja latencia, robustez y autonomía.

6.6.1 Principales ejes de seguridad para Data Centers militares en *MDO*

- Segmentación lógica: uso de técnicas como el *Zero Trust Architecture* (*ZTA*) y *Network Slicing* para aislar flujos críticos (*C2*, *ISR*, logística, ciberdefensa) sobre una misma infraestructura, impidiendo el movimiento lateral de amenazas.
- Cifrado extremo a extremo (*E2E*): tanto en datos en tránsito (*TLS, IPSec*) como en reposo (*FIPS* 140-3, cifrado de disco) con claves gestionadas en *HSMs* militares, especialmente en entornos multinacionales (*NATO Secret, EU Restricted*).
- Gestión federada de identidades (*IAM*): con autenticación multifactor (*MFA*), control de acceso basado en atributos (*ABAC*) y federación entre aliados para el acceso a servicios según niveles de clasificación y responsabilidad operacional.
- Resiliencia ante ciberamenazas: integración de soluciones *SIEM* (*Security Information and Event Management*), *NDR* (*Network Detection and Response*), honeypots, microsegmentación dinámica y capacidades de respuesta automatizada ante ataques *APT*.
- Protección física y medioambiental: con redundancia eléctrica (*UPS*, generadores), sistemas de extinción, climatización de precisión, detección de intrusos, y blindaje electromagnético para nodos edge en entornos hostiles [84].

6.6.2 Iniciativas españolas relevantes

- BACSI (Base Conectada, Sostenible e Inteligente): incluye la construcción de centros de datos duales civil-militar, con arquitectura *cloud-edge* federada, capacidades de orquestación automatizada, virtualización NFV y compatibilidad con estándares OTAN y UE [8].
- NUCOCAS: define una arquitectura de red del MINISDEF basada en contenedores, *SDN*, orquestadores distribuidos y nodos *edge* con despliegue rápido mediante *Zero Touch Provisioning* (ZTP), lo que permite resiliencia operativa y escalabilidad táctica en escenarios OTAN-UE [43][44].

6.6.3 Doctrina OTAN y marcos de seguridad aliados

- *NATO Cybersecurity Framework* [85] y *STANAGs* [86] como el 4778 establecen políticas de clasificación, cifrado, y control de acceso para infraestructuras conjuntas.
- La OTAN promueve el concepto de federación de *data centers*, donde la capacidad de cómputo y almacenamiento puede ser compartida entre países aliados mediante mecanismos de seguridad y control de soberanía digital.

La convergencia entre centros de datos seguros, tecnologías *5G*, virtualización, IA y *Edge Computing* da lugar a una infraestructura de defensa flexible, descentralizada y robusta. Esta arquitectura no solo asegura el flujo continuo de información crítica en entornos multidominio, sino que permite la interoperabilidad multinacional, la compartición controlada de servicios y la capacidad de recuperación rápida frente a incidentes cibernéticos o físicos.

6.7 Tecnologías emergentes complementarias

El despliegue de *5G* en entornos de Defensa no puede abordarse de forma aislada. Su integración óptima requiere considerar un conjunto de tecnologías emergentes y disruptivas (*EDTs*) que, en sinergia, potencian su impacto operativo.

Estas tecnologías complementan y refuerzan las capacidades del ecosistema *5G*, preparándolo para enfrentar los retos técnicos, operativos y estratégicos que plantea el entorno multidominio. Su incorporación progresiva a las doctrinas y arquitecturas de Defensa asegurará no solo la continuidad tecnológica, sino también la resiliencia y superioridad en los teatros de operación del futuro.

A continuación, se destacan algunas de las más relevantes en los actuales desarrollos doctrinales de la OTAN, la UE y el Ministerio de Defensa español, que no se han desarrollado anteriormente:

- *Sidelink / PC5 Communication* (comunicación *D2D*): Estandarizada en *3GPP* para permitir la comunicación directa entre dispositivos sin necesidad de infraestructura intermedia [2][87]. Sus aplicaciones incluyen:

  - Coordinación táctica en enjambres de *UAVs*, *UGVs* o *MUS*.
  - Continuidad operativa en entornos EM degradados o con denegación de servicio.
  - Enlaces entre unidades desplegadas bajo condiciones EM.

- Servicios de localización *5G*: Basados en técnicas como *TDOA*, *AoA* y *fingerprinting*, permiten una geolocalización de alta precisión sin depender de *GPS* [88]. Resultan esenciales en:

  - Navegación autónoma de vehículos no tripulados.
  - Posicionamiento táctico en entornos *GNSS-denied*.
  - Seguridad en identificación de posición y coordinación de maniobras.

- Cifrado post-cuántico y distribución cuántica de claves (*QKD*): Frente a la amenaza futura de la computación cuántica [89], se exploran soluciones como:

  - Algoritmos resistentes a ataques cuánticos.
  - Protocolos de distribución de claves *QKD* en nodos estratégicos o embarcados.

  Aunque aún en fase inicial, ya se investigan dentro del marco de ciberseguridad OTAN y los *STANAGs* en evolución.

Capítulo 7. Perspectivas estratégicas y doctrinales

7.1 Adaptación de doctrinas militares para el uso de 5G

La adopción de redes *5G* en entornos militares exige una transformación doctrinal profunda que trasciende los niveles táctico y técnico para impactar directamente en la estructura estratégica de la Fuerza Conjunta. Esta transformación afecta al diseño de redes *C4ISR*, al modelo de operación de los cuarteles generales desplegables (como *SDHQ* y *MCP*), y al concepto de "*Persistent C2*".

El Plan del JEMAD para la implementación de las MDO [12] identifica expresamente la necesidad de adaptar las doctrinas existentes a un nuevo entorno operativo caracterizado por la conectividad ubicua, el análisis distribuido de datos y la sincronización interdominio. El *5G* facilita la ejecución de estos objetivos al permitir:

- Segmentación funcional de redes mediante *Network Slicing*, con aislamiento lógico de flujos C2, *ISR*, logística o coalición.
- Despliegues rápidos y configurables de infraestructura táctica, mediante el uso de nodos *MEC*, provisión automatizada (*ZTP*) y *NTN*.
- Integración de tecnologías habilitadoras como IA, *IoMT*, *Edge Computing* o plataformas autónomas (*UXVs*).

Doctrinas como la *Allied Joint Publication* (AJP)-3 [67] y el *Allied Command Transformation Concept for MDO* [10] apuntan ya a modelos doctrinales centrados en "*decision advantage*", que requieren una red adaptativa, resiliente y federada. A este respecto, se están desarrollando nuevos CONOPS (Concepto de operaciones) y *TTPs* para redes privadas *5G*, sistemas *C2* distribuidos y federación de servicios en operaciones multinacionales.

7.2 Colaboración entre la OTAN, aliados y la industria

La transformación digital militar, y en particular el despliegue del *5G* táctico, exige un ecosistema de cooperación multidimensional, que abarque organismos doctrinales (*ACT*), agencias normativas (*NCIA/NATO STANAG*), socios industriales y estructuras operativas nacionales.

Ejemplos concretos incluyen:

- *CWIX y FMN Spiral 6*, donde se validan perfiles técnicos interoperables, arquitecturas de *slicing* federado y despliegues *edge* con orquestación multinacional [4][5],
- Proyectos *PESCO* y *EDF*, como *COMPAD 5G* o NUCOCAS, centrados en arquitecturas conjuntas de red *5G SA/NSA* y modelos de segmentación doctrinal entre países [46][49].
- Relación entre usuarios finales, cuerpos *CIS* y diseñadores de tecnología, que se formaliza en grupos técnicos de interoperabilidad (*IST-220*, *NISP*, *AI Task*

Forces) y en el alineamiento con estándares civiles (*3GPP, O-RAN, ETSI*) [13][90].

Esta colaboración también se materializa en el desarrollo de infraestructuras duales (civil-militar), como en el caso de BACSI, donde se comparten nodos edge, capacidades cloud y enlaces satelitales con medidas de seguridad diferenciadas por segmento.

7.3 Proyecciones de desarrollo del 5G militar y estándares internacionales

El *roadmap* evolutivo del *5G* militar contempla varias líneas estratégicas:

- Estandarización de perfiles de misión OTAN basados en *slices* funcionales, con distintos niveles de seguridad, prioridad y disponibilidad.
- Automatización completa del despliegue y la configuración de red, mediante tecnologías como *Zero Touch Provisioning* (*ZTP*), *SDN/NFV*, orquestadores multinodo y controladores *edge* distribuidos.
- Convergencia entre redes terrestres y no terrestres (*NTN/LEO/HAPS*), habilitando continuidad operativa en escenarios dispersos o denegados.
- Preparación para el *6G* militar, con integración de IA nativa, redes holográficas, *beamforming* inteligente, comunicaciones cuánticas seguras y arquitecturas auto-reconfigurables [91].

En términos normativos, la coordinación entre OTAN, UE, *3GPP* y *ETSI* [2][92] es fundamental. La implementación de marcos como *STANAG 4774* [93] sobre protección de la información clasificada, o las guías del *NATO Interoperability Standards and Profiles (NISP)*, garantizan una transición segura hacia arquitecturas de red federadas [90].

7.4 Impacto geopolítico del 5G en las relaciones internacionales

El *5G* no es solo una cuestión tecnológica, sino un activo geoestratégico crítico, cuya posesión, control y soberanía determinan la autonomía operativa de las naciones y coaliciones.

Los riesgos identificados incluyen:

- Dependencia de proveedores de alto riesgo, lo que podría derivar en vulnerabilidades estructurales o pérdida de integridad de la cadena de suministro.
- Injerencias espectrales, especialmente en entornos operacionales próximos a redes civiles no aliadas.
- Compromiso del dato estratégico, derivado del uso de redes públicas sin segmentación adecuada.

Frente a ello, se impulsa la creación de ecosistemas tecnológicos soberanos, con capacidades de auditoría completa, componentes europeos/OTAN-certificados, y

despliegues federados bajo acuerdos multinacionales (como los *slices* por nación o función).

La Brújula Estratégica de la UE y la Estrategia de Transformación Digital de la OTAN convergen en priorizar la soberanía digital, la defensa del espectro electromagnético y la superioridad en el ciberespacio como ejes clave de la seguridad colectiva.

Capítulo 8. Conclusiones

8.1 Ideas principales

Con este trabajo se pretende dar a conocer que el *5G* y las tecnologías habilitadoras asociadas (IA, *IoT*, *MEC, NS*, etc.) representan un cambio de paradigma en las operaciones militares multidominio (*MDO*). Las capacidades de baja latencia, alta densidad de dispositivos, procesamiento distribuido y segmentación lógica de red posicionan al *5G* como una tecnología fundamental para apoyar la transformación digital de las Fuerzas Armadas.

A lo largo del estudio se ha constatado que el uso del *5G* permite mejorar la interoperabilidad multinacional, reducir tiempos de decisión, aumentar la resiliencia frente a amenazas del espectro electromagnético y facilitar la integración de sistemas autónomos y sensores avanzados en redes robustas y seguras.

8.2 Retos operativos y tecnologías clave

Pese a sus ventajas, la adopción del *5G* militar se enfrenta a importantes desafíos, entre los que destacan:

- Asegurar la ciberseguridad integral y la compartimentación de datos en entornos federados y multinacionales.
- Garantizar la interoperabilidad con sistemas heredados y redes legadas en operaciones combinadas.
- Reforzar la resiliencia frente a amenazas en el espectro electromagnético como el *jamming*, el *spoofing* y los pulsos electromagnéticos (*EMP*).
- Alcanzar una cobertura adecuada y sostenibilidad operativa en zonas remotas o degradadas.

Para abordar estos retos, se requiere la integración de soluciones avanzadas como el *NS* para compartimentar servicios críticos, el *MEC* para reducir la latencia y aumentar la autonomía, los sistemas autónomos en red para tareas tácticas y el *ZTP* para facilitar despliegues automatizados y escalables.

8.3 Recomendaciones estratégicas y técnicas para su implementación

- Definir y estandarizar perfiles de *slice* OTAN y nacionales, alineados con las funciones conjuntas y niveles de seguridad.
- Promover arquitecturas híbridas (privadas/públicas) de red *5G* que permitan desplegar capacidades de forma escalable y segura.
- Desarrollar doctrinas, CONOPS y *TTPs* específicos para el empleo táctico y estratégico de redes *5G* en operaciones *MDO*.
- Impulsar centros de datos tácticos resilientes y federados, con seguridad multicapa y capacidades *edge*.

- Consolidar la cooperación industrial, multinacional y doctrinal en el marco de la OTAN, UE y los programas de Defensa europeos.

8.4 Líneas futuras de investigación

- Evaluar la transición progresiva hacia el 6G, incluyendo comunicaciones holográficas, uso de bandas de terahercios y redes cognitivas con IA integrada.
- Desarrollar doctrinas para el despliegue de enjambres autónomos (*swarms*) interconectados mediante *5G*, orientados a misiones *ISR*, *EW* y defensa y ataque activos.
- Explorar el uso de simuladores inmersivos basados en RA/RV con parámetros *5G* reales para mejorar la instrucción doctrinal y el planeamiento conjunto.
- Analizar la viabilidad operativa de redes no terrestres *5G* (*LEO*, *HAPS*) como capa redundante de conectividad táctica en entornos sin infraestructura terrestre.

La implementación del *5G* como eje estratégico en Defensa requiere una visión multidimensional que combine desarrollo tecnológico, adaptación doctrinal, interoperabilidad multinacional y ciberresiliencia. Solo así será posible dotar a las Fuerzas Armadas de las capacidades necesarias para afrontar con éxito los desafíos de las operaciones multidominio del presente y del futuro.

Referencias

[1] Estado Mayor de la Defensa (EMAD), *Plan para la implantación del concepto de Operaciones Multidominio (MDO) en las Fuerzas Armadas*, 2023.

[2] 3rd Generation Partnership Project (3GPP), *"Releases 16, 17 and 18 Specifications,"* 2020–2024. [Online]. Available: https://www.3gpp.org/

[3] Ministerio de Defensa de España, *Estrategia de Transformación Digital del Ministerio de Defensa*, 2024.

[4] CWIX, *Coalition Warrior Interoperability Exercise – Summary Report*, 2023.

[5] NATO Communications and Information Agency (NCIA), *FMN Spiral 6 Technical Profile*, 2023.

[6] Ejército de Tierra – JCISAT, *Proyecto ZEUS: Infraestructura de red táctica basada en 5G*, 2022.

[7] Armada Española, *Proyecto TRITÓN: Comunicaciones 5G en proyección anfibia*, 2022.

[8] Ministerio de Defensa y MITMA, *Proyecto BACSI – Base Aérea Conectada, Sostenible e Inteligente*, 2023.

[9] NATO, *Alliance Concept for Multi-Domain Operations (MDO)*, 2022.

[10] NATO ACT, Allied Command Transformation Concept for MDO, 2023.

[11] NCIA, Digital Transformation Guidelines for MDO Architectures, 2023.

[12] Estado Mayor de la Defensa, *Plan JEMAD para la Implantación de las MDO en las Fuerzas Armadas*, 2024.

[13] NATO STO IST-220 Research Group, *Federated 5G Tactical Networks*, 2024.

[14] Mando Conjunto del Ciberespacio (MCCE), *Documentación técnica interna sobre nodos edge y redes tácticas (Gonzalo)*, 2023.

[15] Jefatura de los Sistemas de Información, Telecomunicaciones y Asistencia Técnica (JCISAT), *Documentación sobre redes 5G tácticas*, 2023.

[16] Dirección General de Armamento y Material (DGAM), *Guía de innovación tecnológica en defensa*, 2022.

[17] NATO, *NATO Network Enabled Capabilities (NNEC) Baseline Concept*, 2018.

[18] NATO STO, *5G and Beyond for Defence Environments – CMRE Study*, 2023.

[19] 3rd Generation Partnership Project (3GPP), *Technical Specification Group Radio Access Network; NR and NG-RAN Overall Description; Release 17*, 2022.

[20] Indra Sistemas, *Estudios sobre slicing y resiliencia 5G en escenarios militares*, 2023.

[21] European Commission, *Smart Networks and Services Joint Undertaking – Phase 2: Defence and Security Use Cases*, 2024.

[22] European Commission, *Secure and Resilient Connectivity Initiative (LEO-HAPS)*, 2022.

[23] DIGEID, *Catálogo de capacidades IA y edge en el entorno táctico*, 2023.

[24] Ejército del Aire y del Espacio, *Lecciones aprendidas del vuelo BACSI-C101*, 2023.

[25] NATO, *MC 195 – Minimum Military Requirements for Communications and Information Systems*, 2021.

[26] Telefónica Defensa, *Integración 5G en plataformas tácticas móviles. Informe técnico*, 2023.

[27] European Defence Agency (EDA), *Strategic Context Case for 5G-enabled Defence Capabilities*, 2022.

[28] DIGEID, *Plan estratégico para la integración de IA en Defensa*, 2023.

[29] NCIA, *DCIS Cube Architecture Reference – NATO Deployable ICT Systems*, 2023.

[30] European Commission, *Cyber Resilience Act Proposal*, 2022.

[31] NATO C3B, *Recommendations on Open RAN Implementation in Tactical Environments*, 2023.

[32] Airbus Defence and Space, *Sistemas de comunicaciones embarcados y edge nodes*, 2023.

[33] CESEDEN, *Cuadernos de Estrategia: La digitalización del campo de batalla*, 2023.

[34] European Union Agency for the Space Programme (EUSPA), *Use of 5G/LEO for Defence Applications*, 2023.

[35] NATO, *NWP-250011 AComP-5665 – 5G Cellular Communications for Defence – Maritime Proposal*, 2022.

[36] Ministerio de Defensa, *Manual de Mando y Control en Operaciones Conjuntas*, CESEDEN, 2022.

[37] NATO STO, TR-IST-ET-123 Tactical 5G Networks and Edge Cloud, 2023.

[38] NATO C3B, STANAG Series for Tactical Communications Interoperability, 2022.

[39] DGAM y MCCE, Informe técnico sobre FANET, 2024.

[40] MCCE, Informe de capacidades del LAB 5G y resiliencia táctica, 2023.

[41] UME, Pruebas 5G para gestión de emergencias, 2023.

[42] Ministerio de Defensa, CDAP 5G DEF: Ciberseguridad con 5G, 2023.

[43] Estado Mayor de la Defensa, NUBE DE COMBATE CONJUNTA, 2025.

[44] Estado Mayor de la Defensa, Proyecto 5G Conjunto – Coordinación MOPS/JEMAD, 2024.

[45] Grupo de Trabajo de Digitalización del MOPS, Acta técnica.

[46] European Commission, EDF Projects for Defence Digitalisation, 2023.

[47] European Defence Agency (EDA), MN5G – Multinational Tactical 5G Programme, 2024.

[48] NATO, *Digital Transformation Implementation Strategy (DTIS)*, 2022.

[49] NATO ACT, COMPAD 5G Tactical Command Project Report, 2023.

[50] NATO, DIBAX Technical Framework for Coalition Backbones, 2023.

[51] NATO CWIX, Summary of 5G Interoperability Trials, 2024.

[52] NATO STO, TR-SET-293: Resilience and EM Environment for Tactical 5G, 2023.

[53] Ministerio de Defensa, Estrategia de Ciberseguridad del MINISDEF, 2023.

[54] NCIA, Cybersecurity Baselines for Tactical Networks, 2022.

[55] MOPS, Documento interno sobre plataformas HAPS – conectividad 5G estratosférica, 2023.

[56] JCISAT, Informe sobre Enlaces de Datos Tácticos (TDL) y 5G, 2023.

[57] Ministerio de Defensa, Documento técnico – Gestión del espectro 5G en Defensa, 2023.

[58] NATO, STANAG sobre armonización de espectro militar para 5G, 2022.

[59] NATO C3B, Framework for Spectrum Allocation and Sharing – Military Requirements, 2022.

[60] European Commission, Harmonised Use of 5G Spectrum Bands in Defence Context, 2023.

[61] NATO FMN, Guidelines for Spectrum Coordination in Federated Mission Networks – FMN Spiral 6, 2023.

[62] CESEDEN, Estudio sobre radios definidas por software en entornos OTAN, 2023.

[63] DIGEID, Estudio técnico sobre SDRs e IA para gestión dinámica del espectro en operaciones tácticas, 2024.

[64] CESEDEN, Manual de doctrina conjunta y niveles operacionales, CESEDEN, 2021.

[65] Ministerio de Defensa, Concepto de empleo de las Fuerzas Armadas en el marco estratégico, 2020.

[66] CESEDEN, Cuaderno de estrategia sobre el nivel operacional, 2022.

[67] NATO, Allied Joint Doctrine for the Conduct of Operations (AJP-3), 2021.

[68] NATO, Framework for Future Operations Environment Analysis, 2023.

[69] Ministerio de Defensa, Glosario de términos doctrinales del EMAD, 2022.

[70] CESEDEN, Organización y estructura de las Fuerzas Armadas: Niveles y capacidades, 2021.

[71] European Commission, EU Strategic Compass for Security and Defence, 2022.

[72] NATO, NATO Warfighting Capstone Concept (NWCC), 2021.

[73] NATO, AJP-3 – Allied Joint Doctrine for the Conduct of Operations, 2022.

[74] Indra, Sistemas Tácticos Edge con IA embarcada – Proyectos MINISDEF, 2023.

[75] DIGEID, Requisitos de ciberseguridad en redes privadas 5G, 2023.

[76] Ministerio de Defensa, Estrategia de Inteligencia Artificial para la Defensa Nacional, 2024.

[77] UO DIVPLA-SEPLAT, Nota Informativa NI-023 sobre capacidades y despliegue de IA en Defensa, 2024.

[78] NATO, Artificial Intelligence Strategy and EDTs Roadmap, 2022.

[79] NATO C3B, STANAG 4586 – Standard Interfaces of UAV Control System, 2021.

[80] NCIA, *Virtualization and Simulation Strategies for Future Operations*, 2023.

[81] UO DIVPLA-SEPLAT, *Documentación interna sobre arquitectura federada de datos para defensa*, 2024.

[82] NATO, *NATO Data Exploitation Framework*, 2022.

[83] European Commission, *NextGen Simulations for Joint Training and Interoperability*, 2024.

[84] NATO, Zero Trust and Electromagnetic Protection for Tactical Data Centers, 2023.

[85] NATO, *Cybersecurity Framework for Federated and Tactical Networks*, 2023.

[86] NATO, STANAG 4778 – Information Assurance Policy, 2022.

[87] 3GPP, Sidelink and PC5 Communications for D2D Operations – Technical Report, 2023.

[88] European GNSS Agency (GSA), 5G Positioning Technologies for GNSS-Denied Environments, 2023.

[89] NATO, Quantum-Resilient Cryptography and Key Distribution for Defence, 2023.

[90] NATO, NATO Interoperability Standards and Profiles (NISP) – Edition 15, 2023.

[91] European Commission, 6G for Defence Applications – Strategic Foresight Report, 2024.

[92] ETSI, Standardisation for Military Use of 5G/6G Networks, 2023.

[93] NATO, STANAG 4774 – Confidentiality and Information Labeling Policy, 2022.