Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

El marco FMN como potenciador de la eficacia operativa de la OTAN y de las Naciones

Máster Universitario en Dirección TIC para la Defensa

Alumno:	Óscar Javier Gajete Molina
Director:	José María Núñez Ortuño
Curso académico:	2023-2024

Universidade Vigo

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

El marco FMN como potenciador de la eficacia operativa de la OTAN y de las Naciones

Máster Universitario en Dirección TIC para la Defensa

Especialidad de Sistemas y Tecnologías de Telecomunicación

Universidade Vigo

RESUMEN

El nuevo concepto estratégico de la OTAN hace hincapié en la rápida evolución de las tecnologías y la necesidad de una mayor agilidad y flexibilidad para hacer frente a los nuevos retos. Tal y como señalaba recientemente el General Lavigne, jefe del Mando de Transformación de la Alianza (ACT), "el concepto 2030 de la OTAN requiere adoptar un enfoque centrado en los datos y avanzar en la federación de nuestras redes si queremos obtener el éxito en las operaciones multidominio (MDO)".

Precisamente el núcleo de la transformación de la OTAN es la convergencia de las MDO y la transformación digital (DT), con el fin de obtener una toma de decisiones basada en datos con la mayor velocidad y precisión posible. Para ello es fundamental mejorar la interoperabilidad, entendida por la Alianza como la capacidad de actuar juntos de forma coherente, efectiva y eficiente para lograr los objetivos tácticos, operativos y estratégicos de los aliados.

El concepto FMN (*Federated Mission Networking*) se deriva de la experiencia de la AMN (*Afghanistan Mission Network*) y fue desarrollado por la OTAN para asegurar la interoperabilidad entre las naciones de la Alianza y otras organizaciones y naciones afiliadas. FMN engloba personas, procesos y tecnología y su misión es mejorar el Mando y Control (C2) y la toma de decisiones en las operaciones y ejercicios de sus afiliados, para conseguir una mayor operatividad tanto en el presente como en el futuro.

La participación de nuestras Fuerzas Armadas en misiones internacionales requiere garantizar la máxima interoperabilidad con nuestros aliados, de ahí la importancia para España de disponer de la capacidad de establecer redes de misión federadas. En este Trabajo Fin de Máster (TFM) se analiza cómo funciona FMN y su contribución a la mejora de la eficacia operativa de la OTAN y de las naciones, identificando los nuevos retos y riesgos a los que se enfrentan sus miembros en los nuevos escenarios operativos.

PALABRAS CLAVE

Federación, misión, interoperabilidad, escenario, afiliado.

AGRADECIMIENTOS

En primer lugar, agradecer a mi tutor Don José María Núñez Ortuño sus orientaciones durante todo el desarrollo del TFM, para conseguir el enfoque más adecuado. También su paciencia en la revisión de borradores y propuesta de mejora continua.

También quiero hacer mención a los buenos consejos recibidos de varios compañeros de profesión con los que me entrevisté personalmente en las primeras fases de este trabajo. Gracias al Coronel Don José Antonio Martínez del Campo, al Teniente Coronel Don Carlos Martínez de Bujo y al Comandante Don José Luis Rodríguez Méndez por sus comentarios sobre el planeamiento de capacidades CIS.

Agradecer a mis compañeros destinados en las estructuras FMN tanto nacionales (EMAD) como internacionales (OTAN) toda la información que me han proporcionado y su inestimable ayuda para la resolución de multitud de dudas que fueron surgiendo en un tema tan complejo como la interoperabilidad. Al personal del Comité FMN-ESP del MCCE (EMAD) que me facilitó información actualizada y la posibilidad de asistir a su reunión anual sobre la evolución de FMN. A la Teniente Coronel Doña Mónica Mateos Calle, Oficial de Enlace FMN en SHAPE durante el segundo semestre del año 2023 y a Don José Antonio Díaz Damián, ingeniero destinado en la estructura permanente del Secretariado FMN con una larga experiencia en la agencia NCIA de OTAN. Mi más sincero agradecimiento por haber dedicado vuestro tiempo a leer el trabajo y proponerme cambios para mejorar el resultado final.

Finalmente doy las gracias a mi familia por el apoyo incondicional durante estos meses de intenso trabajo, ayudándome a compaginar de la mejor manera posible la realización del TFM con las obligaciones personales y profesionales. A mi esposa María, a mis hijos Osquitar y Mariquilla, deciros una vez más que sois extraordinarios, con vuestra paciencia y comprensión ha sido posible cumplir el objetivo y ha merecido la pena el esfuerzo. Enhorabuena EQUIPO.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Introducción

Han sido varios los motivos que me han llevado a la elección de la iniciativa *Federated Mission Networking* como tema de desarrollo para el Trabajo Fin de Máster o TFM. Por un lado, me ha permitido conocer mejor la Organización del Tratado del Atlántico Norte (OTAN), alianza política y militar de la que España forma parte desde el año 1982 y que en la actualidad cuenta con 31 países miembros. La Alianza, tal y como expone en su concepto estratégico del año 2022, tiene como propósito fundamental garantizar la defensa colectiva de sus miembros, mediante tres tareas básicas: disuasión y defensa, prevención y gestión de crisis y seguridad cooperativa [1].

A su vez, el concepto *NATO Network Enabled Capability* (NNEC) [2] señala que uno de los principales retos de la Alianza es la capacidad de compartir información en red para su empleo en las operaciones, con el fin de obtener ventaja en el combate, mediante la superioridad en la información, en el conocimiento y en la decisión. El estudio de FMN me permite profundizar en el ámbito de la interoperabilidad, requisito clave para optimizar la colaboración entre los aliados y que abarca tres dimensiones: personas, procesos y tecnología.

FMN es una capacidad formada por tres componentes (Gobierno, Marco FMN y Red de Misión) y que abarca multitud de aspectos tales como la doctrina, el planeamiento de recursos, la definición y obtención de medios, la instrucción y el adiestramiento, la seguridad o la organización, y que tienen como objetivo conseguir unas fuerzas interoperables desde el primer día de la operación. Esto permite que el TFM tenga un enfoque global en línea con la variedad de contenidos que se han visto en las diferentes asignaturas del Máster de Dirección TIC para la Defensa (normativa, organización, gestión de proyectos, tecnologías, sistemas de telecomunicación, sistemas de información, liderazgo o ciberseguridad entre otras).

Otra motivación para tratar sobre FMN es su alcance operativo y su impacto a nivel estratégico, operacional y táctico. Su objetivo es posibilitar la acción conjunta de los participantes en una red de misión federada desde el primer momento del despliegue, explotar una ventaja estratégica que se consigue estableciendo dicha red con antelación gracias al trabajo previo de las estructuras permanentes de la iniciativa FMN. Veremos cómo FMN proporciona la agilidad, flexibilidad, seguridad y escalabilidad necesarias para la gestión de los requisitos que precise cualquier red de misión en operaciones.

España es una nación afiliada desde 2014 y ha participado de forma muy activa en la implantación de la capacidad FMN, realizando pruebas y ejercicios que le permiten evaluar de forma periódica cómo mejora la interoperabilidad de las diferentes herramientas que proporcionan los servicios a las redes de misión federadas. En el año 2016 el JEMAD impulsó el establecimiento de las líneas generales para la implantación de la capacidad FMN en las FAS, dejando atrás el anterior concepto de redes y ordenando la elaboración de un plan de acción que desarrollase y coordinase las acciones específicas para la implantación de la capacidad FMN en España [3].

Por último y no menos importante es interesante analizar como la OTAN y FMN afrontan los nuevos retos derivados de la transformación digital y de las operaciones multidominio. En el entorno estratégico futuro, la visión de FMN contempla la adaptación de todos los afiliados, transformando sus capacidades para seguir manteniendo su ventaja estratégica. Los recursos disponibles son limitados y son numerosas las misiones a las que hay que hacer frente, de ahí que además de la reutilización de estándares sea necesario fomentar unas economías de escala que favorezcan la interoperabilidad y el intercambio de información. De esta manera FMN contribuye a la mejor preparación para las operaciones futuras, con un rápido despliegue de fuerzas que proporciona unas capacidades federadas y una eficaz toma de decisiones en cualquier entorno operativo [4].

1.2 Organización de la memoria

La memoria se organiza de la siguiente forma:

Un capítulo dedicado a la introducción y objetivos, en el que se exponen los motivos de la elección de FMN como tema del TFM. Se destaca que la iniciativa FMN es parte de una organización política y militar de la máxima relevancia a nivel mundial y que cuenta en la actualidad con 31 países miembros. Por parte de FMN son 38 los participantes en la iniciativa entre naciones afiliadas, entidades no pertenecientes a la OTAN, organismos, agencias y la propia Alianza. El concepto FMN abarca las tres dimensiones de la interoperabilidad, personas, procesos y tecnología por lo que supone un ámbito de estudio con un enfoque global y que al mismo tiempo es de vital importancia para que España esté alineada con el objetivo de disponer de unas redes de misión federadas desde el primer momento del despliegue de la fuerza.

Un segundo capítulo que trata sobre el entorno operativo actual y hacia dónde se dirige el esfuerzo de la OTAN y de la iniciativa FMN. Las Fuerzas Armadas de España y de los países de la Alianza tienen la mirada puesta en el horizonte 2030 donde los conflictos mantienen ciertas características como la violencia o la incertidumbre, y al mismo tiempo demandan una mayor flexibilidad y adaptabilidad para conseguir los objetivos establecidos. En todos los escenarios se requiere la máxima interoperabilidad que garantice el intercambio de información entre los participantes en la misión y permita la toma de decisiones oportuna y en el menor tiempo. FMN tiene que adaptarse a las operaciones multidominio, a la transformación digital y a los nuevos cambios que vive la OTAN, como la implantación del concepto *NATO Warfighting Corps Capstone* [5] para aumentar su eficacia operativa.

En el tercer capítulo se profundiza en la evolución de la iniciativa FMN, desde sus inicios derivados de la red de misión AMN que estuvo operativa en la misión ISAF, de la que España formó parte y contribuyó con un nodo FMN, hasta la descripción de los componentes principales de FMN, tanto a nivel de gobernanza como de gestión. Para ello se analizan los elementos fundamentales del plan de implementación de la iniciativa FMN, sus objetivos, estructuras y procedimientos de cara a desarrollar las redes de misión federadas que puedan ser implementadas por los afiliados en ejercicios y operaciones.

El capítulo cuarto está orientado a la instanciación de las redes de misión y a cómo los afiliados participan en la iniciativa FMN. Además de describir los productos principales que emanan de las estructuras de gestión de FMN, se detalla la contribución nacional necesaria para conseguir la coherencia en la definición, desarrollo, validación, verificación y operación de las redes. Además, se describen algunas de las capacidades implementadas por los afiliados en las denominadas espirales donde se recogen los requisitos operativos para la interoperabilidad presente y futura.

2 EL ENTORNO OPERATIVO

2.1 Retos en los nuevos escenarios

En la Estrategia de Seguridad Nacional del año 2017 se destacaban como principales amenazas los conflictos armados internacionales, los estados frágiles o fallidos, el crimen organizado, el terrorismo y la proliferación de armas de destrucción masiva (ADM), la amenaza cibernética y las campañas de manipulación y desinformación. Como puede observarse en la guerra de Ucrania o en la guerra entre Israel y Hamás, algunas de estas amenazas siguen presentes y a la vez se han unido otras nuevas.

Ante estos retos a nuestra seguridad, nuestras FAS deben de aprovechar cualquier oportunidad para mejorar la respuesta, por ejemplo, adoptando las medidas necesarias en materia de cooperación en el seno de las organizaciones internacionales de seguridad y defensa (OISD) de las que forman parte [6]. En este sentido es necesaria una mayor interoperabilidad, aprovechando la innovación tecnológica en los distintos ámbitos: computación cuántica, robótica, inteligencia artificial, sistemas de información y telecomunicaciones (CIS) o sistemas autónomos. Cualquier respuesta requiere un conocimiento preciso de la situación (*Situational Awareness* o SA) que se verá mejorado por los avances tecnológicos en el ámbito del consulta, computadores, C2 y de los sistemas de vigilancia, reconocimiento e inteligencia (C4ISR por sus siglas en inglés). Pero al mismo tiempo los adversarios serán capaces de integrar sistemas y sensores conformando una red asociada a sus elementos de ataque para operar desde el nivel estratégico hasta el nivel táctico.

En los conflictos armados existen factores que no varían, como la violencia o la incertidumbre, y otros que evolucionan y que se manifiestan dando forma a un determinado entorno operativo. El entorno operativo puede definirse como “el marco donde interactúan todas las variables que tienen influencia inmediata en las acciones que, para alcanzar o satisfacer sus objetivos políticos, desarrollan los diferentes actores a través del ejercicio de las operaciones militares” [7]. El entorno operativo consta de sujetos estatales y no estatales que se relacionan entre ellos, de estrategias que se desarrollan en los diferentes dominios (terrestre, marítimo, aeroespacial, ciberespacial y cognitivo), medios, capacidades, operaciones y todo tipo de retos y oportunidades que condicionan la forma de actuar de las Fuerzas Armadas.

Muchos de los recientes conflictos armados en los que han participado nuestras FAS derivan del debilitamiento de los Estados, teniendo como resultado una respuesta donde el componente militar no actúa de forma convencional. Se imponen despliegues de contingentes tanto en grandes coaliciones como en otras de menor tamaño, donde los adversarios emplean todo tipo de técnicas y las estrategias híbridas son empleadas con mayor frecuencia. En aquellos casos en los que estas estrategias sean consideradas como demasiado arriesgadas, los posibles agresores también explotan la denominada zona gris para tener opciones de éxito frente a adversarios militar y económicamente superiores.

La frontera entre los ámbitos de operación o dominios se han ido difuminando lo que supone que las operaciones militares tengan que realizarse atendiendo a una respuesta integral donde el factor tecnológico es un elemento clave para conseguir el éxito en la misión. La tecnología permite cada vez más una mejor localización e identificación de objetivos, evitando daños colaterales. Pero también posibilita que todos los actores desarrollen sistemas anti acceso y de denegación de área (A2/AD), lo que supone para nuestras Fuerzas Armadas y para el resto de nuestros socios mayores riesgos y una pérdida de libertad de movimientos.

Atendiendo a un análisis externo del entorno operativo desarrollado por el Instituto Español de Estudios Estratégicos (IEEE) en el año 2019, los retos del futuro escenario geopolítico y de seguridad podrían describirse según el conocido como entorno VUCA (Volatilidad, Incertidumbre, Complejidad y Ambigüedad). Los cambios vertiginosos dificultan la capacidad de respuesta de las Fuerzas Armadas y

aumentan la incertidumbre a la hora de dar una respuesta adecuada a un escenario concreto. Un acontecimiento no vendrá provocado por una única causa por lo que la toma de decisiones se presenta más compleja y será necesaria una visión holística y una mayor flexibilidad ante situaciones ambiguas y desconocidas [8].

Aunque hay zonas que han venido sufriendo un mayor número de conflictos a lo largo de su historia, no resulta fácil determinar dónde se verán desplegadas nuestras Fuerzas Armadas en el futuro. Tampoco es sencillo atisbar cuáles podrían ser los espacios de confrontación, pero normalmente los contendientes tenderán a buscar zonas donde obtengan el mayor beneficio al menor coste, lo que incluye nodos de transporte, infraestructuras críticas, centrales de energía o espacios comunes globales (*Global Commons* como el ciberespacio, espacio marítimo, espacio aéreo y ultraterrestre).

La principal característica de las Fuerzas Armadas para el entorno 2035 será la agilidad, tanto a nivel de organización como del personal que la integra. Para conseguirlo se requiere flexibilidad ante la diversidad de contextos operativos, versatilidad, capacidad de respuesta y resiliencia. Pero todas estas características se consideran de carácter general para cualquier tipo de operación, tanto en territorio nacional como fuera de nuestras fronteras [9].

Si nos centramos en las operaciones multidominio que nuestras FAS realizan integradas en contingentes multinacionales (OISD, coaliciones, etc.), el requisito clave es la interoperabilidad. Según el portal de administración electrónica (PAe), la interoperabilidad se define como "la capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos". La interoperabilidad es un elemento transversal a todos los componentes que analizan los órganos de planeamiento de las FAS para conseguir mejorar sus capacidades (material, infraestructuras, recursos humanos, adiestramiento, doctrina y organización). Precisamente es en la interoperabilidad en lo que trabaja la iniciativa FMN de OTAN, abarcando a personas, procesos y tecnología [10].

Si nos fijamos en los conflictos actuales, el enfrentamiento en campo abierto luchando por dominar grandes extensiones de terreno sigue vigente, como puede observarse en la guerra de Ucrania. No obstante, las capacidades para operar en un entorno urbano y densamente poblado son cada vez más demandantes, lo cual requiere una mejor gestión de la información para ejercer el C2 sobre todas las funciones operativas (adquisición de objetivos, acciones de ciberdefensa, obtención de inteligencia o comunicación estratégica). El conflicto entre Israel y Hamás ha puesto de manifiesto que además de la potencia de combate se necesita dominar las operaciones de información [11].

De todo lo anterior se puede afirmar que independientemente del escenario donde desplieguen nuestras unidades, tanto en las áreas urbanas como en los grandes espacios con baja densidad de población, será necesario actuar de forma conjunta para disminuir el tiempo necesario en la toma de decisiones.

2.2 Operaciones multidominio

La aparición de nuevos conceptos en el ámbito de la seguridad y defensa tiene su origen en diversas fuentes, desde las industrias de defensa hasta las agencias y organismos estatales. El concepto de operaciones multidominio (MDO) fue desarrollado por los marines y el ejército de tierra estadounidense con el objetivo de poder combatir a un enemigo que emplea las nuevas tecnologías para desafiar la superioridad tecnológica y militar que hasta el momento habían tenido las fuerzas armadas estadounidenses [12].

El nuevo concepto MDO impulsado por los EE.UU. ha supuesto un cambio en el enfoque de la OTAN y de los aliados. En el año 2020 el EMAD publicó su concepto sobre MDO y las definía como "operaciones conjuntas, ágiles y complejas que requieren interoperabilidad de sistemas, procesos y personas, conectividad en la nube, sistemas de C2 y un cambio de mentalidad de los cuadros de mando a todos los niveles" [13].

Las operaciones multidominio hacen referencia al impulso para que la OTAN lleve a cabo actividades militares en cualquier dominios y entorno operativo [14]. Mientras que en nuestra doctrina se refiere a ámbitos de operación, la OTAN (y muchos de nuestros aliados) emplea el término dominio, identificando como tales a cinco áreas: marítima, terrestre, aérea, espacial y ciberespacio. Debido a la velocidad con la que se transmite la información, el volumen de datos y las capacidades tecnológicas de los adversarios, la Alianza necesita sincronizar todas sus actividades militares en todos los dominios y actuar como una sola fuerza.

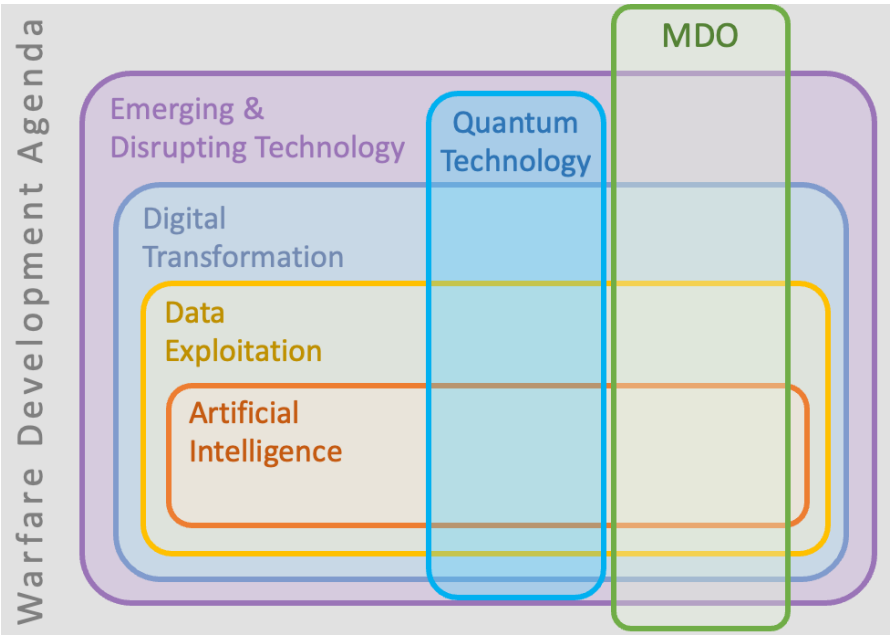

Figura 1. Contexto operacional y nuevos conceptos [14].

La diferencia respecto a las operaciones conjuntas, que ya eran conocidas en nuestra doctrina, viene sobre todo por la complejidad del entorno operativo que ya se ha descrito anteriormente. Para responder a las nuevas amenazas, la OTAN, los aliados y otros actores han de sincronizar todas sus capacidades (militares y no militares) para actuar como una sola fuerza en todos los dominios. Los principios de las operaciones multidominio son el posicionamiento y gradación de la fuerza, el empleo de formaciones resilientes y las capacidades convergentes que posibiliten la maniobra [15].

Las MDO requieren una combinación de fuerzas expedicionarias con otras de presencia avanzada para favorecer la disuasión. La resiliencia de las unidades deberá ir acompañada de agilidad y movilidad para hacer converger las capacidades interarmas necesarias en el lugar adecuado y en el momento oportuno. En cuanto a la convergencia o integración de capacidades en todos los dominios, permitirán crear sinergias que posibiliten mayores opciones de explotar la iniciativa y el éxito [12].

Las MDO buscan penetrar y desintegrar los sistemas A2/AD del adversario y explotar la libertad de movimiento resultante. Para ello es clave la neutralización de los sistemas de largo y medio alcance del enemigo mediante la actualización continua de la inteligencia en los múltiples dominios. A su vez, la

ejecución de la maniobra en las MDO requiere un C2 conjunto en todos los dominios, de manera que las fuerzas de cada escalón de mando mantengan el contacto en cada fase de la operación.

Los estudios realizados por el *US Army* conciben a las Fuerzas que participan en las MDO como unidades interarmas y escalables, con capacidad para trabajar en un entorno VUCA, en zona gris e hiperconectadas por el uso masivo de la digitalización. La superioridad tecnológica en el campo de batalla, por ejemplo, con la presencia de sistemas autónomos robotizados, permite disminuir el personal del contingente sobre el terreno y evitar asignarles las misiones que entrañen mayor peligrosidad. En cuanto al sistema de C2, las unidades despliegan puestos de mando que permiten la explotación de los datos en un entorno de información único y con conocimiento de la situación de forma deslocalizada [16].

La conectividad con actores ajenos al ámbito militar proporciona a la OTAN el acceso a una mayor cantidad de información en un tiempo más reducido, lo cual sirve para mejorar el proceso de toma de decisiones. Por ejemplo, la Alianza puede aprovechar los sistemas de observación y vigilancia de un proveedor comercial para la identificación de objetivos. En cualquier caso, el entorno y el concepto MDO añaden más complejidad y mayor necesidad de sincronización respecto a las operaciones conjuntas, de ahí la importancia de iniciativas como FMN que sirvan para coordinar los esfuerzos en el ámbito de la interoperabilidad entre todos los actores que participan en una misión [14].

2.3 La transformación digital

En el mundo de la empresa, se puede definir la transformación digital como la incorporación de tecnologías digitales en todas sus operaciones para responder a mercados cambiantes y prestar mejor servicio a los clientes. Supone un cambio cultural para aportar valor al negocio, generar ingresos y ser más eficientes utilizando la automatización, el *cloud* híbrido u otras soluciones digitales para optimizar el empleo de los datos y agilizar la toma de decisiones.

En la Estrategia TIC de la Administración General del Estado (AGE) se entiende por transformación digital "la revisión integral de las tareas, actividades y procesos de gestión de los bienes y servicios consustanciales a la naturaleza y misiones de cada organización, que se basa en la integración de los recursos y capacidades de las Tecnologías de la Información en dichas actividades y procesos" [17].
Lo mismo sucede en el ámbito de la FAS, donde estamos inmersos en un proceso de adaptación al entorno digital para combatir en los nuevos escenarios[1]. El Plan de Acción para la Transformación Digital se aprobó en el año 2018 por el Ministerio de Defensa y se estructura en acciones que afectan a personas, procesos, sistemas y a la información.

La 4ª revolución industrial o revolución 4.0 tiene sus aplicaciones en el sector de la defensa, y entre las tecnologías más relevantes en el campo de batalla podemos citar la computación y las nuevas arquitecturas de nube, el Internet de las cosas (IoT), la implantación de la tecnología 5G (y 6G) o las técnicas de inteligencia artificial (IA). Para obtener la superioridad de la información es fundamental conseguir la superioridad tecnológica, lo cual tendrá su impacto en el resultado que nuestras fuerzas obtengan en el entorno táctico.

Uno de los avances más significativos se está produciendo en la conversión de procesos en datos para su análisis y almacenamiento. La previsión es que el despliegue de numerosas redes de sensores dará lugar a un exceso de información y el reto será su gestión con las herramientas y técnicas adecuadas. Otro de los elementos necesario será la hiperconectividad para coordinar en tiempo real todas las actividades que

[1] En la actualidad hay en marcha diversos programas de transformación digital (BACSI o Base Aérea Conectada Sostenible Inteligente en el Ejército del Aire, Astillero 4.0 y gemelo digital en la Armada y Base Logística del Ejército de Tierra) en línea con el proyecto de Fuerza 2035.

se realizan en las distintas operaciones que tienen lugar en un entorno multidominio. En el intercambio masivo de información será clave la capacidad de procesamiento durante la transmisión y seleccionar el tipo de información que cada usuario requiere. La tecnología 5G en sus versiones más desarrolladas ya contempla el desarrollo de este tipo de redes inteligentes donde la información se modifica mientras fluye por la red, lo cual será de interés para las futuras redes de telefonía móvil y comunicaciones satelitales que se desplieguen en el campo de batalla.

En cuanto a los sistemas autónomos capaces de cambiar su respuesta frente a un cambio de situación, permitirán reducir los riegos y el número de bajas. La mayor capacidad de computación proporcionará una mayor potencia de cálculo en tiempo real, empleando técnicas de IA. Precisamente la evolución de la IA dará a los sistemas de armas, C2, inteligencia, guerra electrónica y medios de transporte mayores capacidades para tomar mejores decisiones. La introducción de cualquier innovación del ámbito civil al ámbito militar podría ser a priori más lenta por las condiciones que deben soportar los sistemas militares, pero en cualquier caso habrá que acortar los plazos de renovación para evitar obsolescencias [18].

La transformación digital se basa fundamentalmente en el dato como "el oxígeno que hará funcionar los procesos de trabajo del Ministerio de Defensa y también de las Fuerzas Armadas". Para conseguir disponer de una organización orientada al dato, nuestras FAS necesitan conectividad basada en la Infraestructura Integral de Información para la Defensa (I3D) y disponer de una única red con capacidad de gestionar gran cantidad de información. También será necesario un Sistema de Mando y Control (SC2N) que ofrezca servicios adecuados y compatibles a unos usuarios que requieren de un cambio de mentalidad y de una formación adecuada [19].

En el entorno táctico las tecnologías más interesantes son las relacionadas con las redes definidas por software (SDN), las comunicaciones móviles inalámbricas basadas en 5G, la computación en la nube, las comunicaciones por satélite y el tratamiento de la información mediante el empleo de la IA. A la hora de modernizar las telecomunicaciones tácticas se debe tener en cuenta el componente de red, su arquitectura y la necesidad de integrar dispositivos externos a esa red. Todo lo anterior conforma las características específicas de la red de misión, en la que se seguirán destinando grandes recursos para implementar los diferentes servicios conforme a los estándares y protocolos que garanticen la interoperabilidad.

La transformación digital en el entorno táctico contempla una deslocalización de la información en redes dinámicas y descentralizadas, con sistemas de telecomunicaciones modulares, escalables y que emplean arquitecturas abiertas. Esto supone entre otras cosas acortar los tiempos para desarrollar las nuevas capacidades que han de desplegarse en las misiones y resaltar la importancia de las tecnologías de uso dual. Respecto a la red táctica de combate para un entorno multidominio, el objetivo es conseguir la mayor interconectividad entre los puestos de mando y cualquier medio o sensor que participa en la misión. Entre los grandes nodos de computación de la nube táctica y el *Tactical Edge*, se despliega toda una panoplia de comunicaciones por satélite y de banda ancha como *Starlink*, comunicaciones móviles 5G (y también 6G) y radios definidas por software (SDR) que proporcionan una conectividad flexible y segura para obtener el conocimiento compartido del campo de batalla [20].

Ahora bien, ningún usuario puede acceder a las redes tácticas sin que se lleve a cabo un exhaustivo control, es lo que se conoce como principio de confianza cero o *Zero Trust*. No se trata de proteger la red táctica, sino los recursos, mediante la implantación de un proceso de autenticación de usuarios muy exigente. Para ello se conceden los mínimos privilegios de acceso y se monitoriza la red de forma permanente, sin que la protección de la red frente a incidentes provoque que su rendimiento no sea el esperado. En este sentido se produce una evolución de las técnicas de ciberdefensa, menos preocupada por el perímetro de la red y más por el flujo de datos y por una arquitectura de seguridad que hoy es más granular.

La OTAN ha puesto en marcha su plan de transformación digital cuya estrategia fue aprobada el pasado mes de mayo por el *Military Committee* (MC).

Digital Transformation Vision Statement: By 2030, NATO Digital Transformation will *enable the Alliance to conduct multi-domain operations*, ensure interoperability across all domains, *enhance situational awareness*, and *facilitate political consultation and data-driven decision-making*									
Strategic Outcome 1	Multi-Domain Operations Enabled Alliance								
Strategic Outcome 2	Ensured Interoperability across all domains								
Strategic Outcome 3	Enhanced situational awareness								
Strategic Outcome 4	Enhanced political consultation and data-driven decision-making								
DT Vision Goals / **Strategic Deliverables**	**DT Vision Goal 9.1**	**DT Vision Goal 9.2**	**DT Vision Goal 9.3**	**DT Vision Goal 9.4**	**DT Vision Goal 9.5**	**DT Vision Goal 9.6**	**DT Vision Goal 9.7**	**DT Vision Goal 9.8**	**People , Processes and Technology pillars are cross cutting across all Goals and Strategic Deliverables**
7.1 Alliance Digital Initiatives			X	X	X				
7.2 Alignment of ~~Digital~~ Programmes			X		X				
7.3 Digital-ready Workforce	X						X	X	
7.4 Digital-ready Combat Forces			X				X	X	
7.5 ICT Services for a Data-Driven Alliance	X	X			X	X	X		
7.6 Data-Centric Governance	X	X	X				X		
7.7 Digital Interoperability Framework		X	X	X					
7.8 Digital Ready Processes	X	X					X	X	
7.9 Digital Backbone	X	X	X	X		X		X	
7.10 Alliance Data Sharing Ecosystem	X	X	X			X	X	X	
7.11 Cooperation with Industry and academia	X					X			

Tabla 1. Objetivos estratégicos en DT [21].

Sus objetivos estratégicos son la capacidad de realizar operaciones multidominio, la interoperabilidad en todos los dominios (tierra, mar, aire, ciber y espacio), la mejora de la conciencia situacional y la optimización del proceso de toma de decisiones a todos los niveles. Para conseguirlo se desarrollan una serie de documentos de referencia, alineados con la iniciativa FMN, centrados en las personas, en los procesos y en la tecnología, con el objetivo de conseguir la disponibilidad digital de las unidades operativas, la gobernanza centrada en el dato, la compartición global de la información y la cooperación entre el ámbito académico, la industria y la OTAN [21].

2.4 Interoperabilidad y FMN en el MINISDEF

La Orden DEF/2639/2015, de 3 de diciembre, establece la Política de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa (Política CIS/TIC) y en su artículo 6.2.c) recoge como uno de sus ejes estratégicos el potenciar la utilización de sistemas normalizados, homogéneos e interoperables [17].

En su artículo 7.3.a) y con el fin de regir el planeamiento y la obtención de los recursos CIS/TIC, se recoge su normalización técnica a través de arquitecturas CIS/TIC organizadas de forma jerarquizada: Arquitectura Global de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa (AG CIS/TIC), Arquitecturas de Referencia y Arquitecturas Objetivo.

Estas arquitecturas sirven de guía para el desarrollo de las capacidades CIS/TIC del MINISDEF, asegurando durante todo el ciclo de vida de los sistemas la coherencia e integridad técnica y el cumplimiento de los requisitos operativos [22].

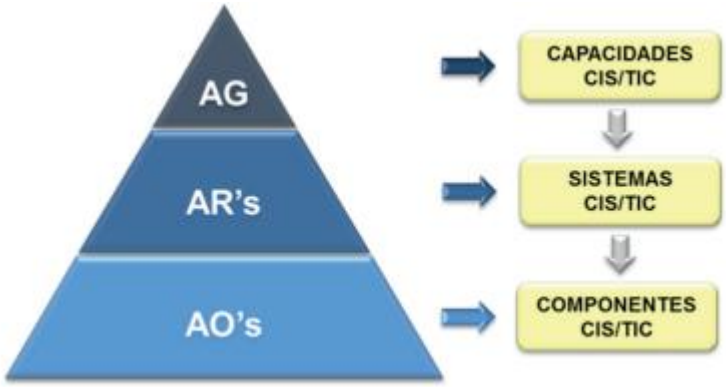

Figura 2. Niveles de Arquitecturas [17].

La AG CIS/TIC describe a alto nivel las capacidades CIS/TIC resultantes del Proceso de Planeamiento de la Defensa [23] y fija los principios para el desarrollo del resto de arquitecturas de los CIS permanentes y desplegables [24] , con el objetivo de asegurar la interoperabilidad. En la Arquitectura Global se distinguen, conforme al modelo de vistas del Marco de Arquitectura de la OTAN o NAF, los siguientes componentes: Vista general o descripción a alto nivel de todas las capas de la AG; Vista de capacidades operativas, que describe el contexto operativo; Vista operativa, que muestra el despliegue de las unidades/organismos del MINISDEF y sus requisitos operativos; Visión del CIO; Vista de Capacidades CIS/TIC, donde se identifican las capacidades permanentes y desplegables, y se desglosan en servicios y equipos; Vista de Servicios, que identifica y clasifica los servicios siguiendo la Taxonomía C3 de la OTAN (artículo 7.3.d) de la Política CIS/TIC del MINISDEF) y Vista Técnica (incluye el Catálogo Unificado de Estándares CIS/TIC del MINISDEF o CUE, según el artículo 7.3.c) de la Política CIS/TIC), de acuerdo a los modelos NISP (*NATO Interoperability Standards and Profiles*) de la OTAN[2] y el Esquema Nacional de Interoperabilidad (ENI) de la AGE.

Tanto en las Arquitecturas de Referencia (AR) como en las Arquitecturas Objetivo (AO) se incluyen igualmente las vistas y las subvistas necesarias conforme al modelo descrito anteriormente, pero adaptado al nivel de detalle correspondiente a la arquitectura. En los tres modelos (AG, AR y AO) se emplean diferentes estándares que varían en función de los servicios y sistemas que se incluyen. No obstante, además de la versión actualizada del NAF, se utilizan como recursos de trabajo la taxonomía C3 de OTAN y los estándares NISP[3] y ENI ya citados.

La Política CIS/TIC contempla una única Infraestructura Integral de Información para la Defensa (I3D) gestionada de forma centralizada, de la que forman parte los CIS permanentes y en la que se integran los CIS desplegables. Las I3D "permite integrar todas las capacidades CIS/TIC del MINISDEF y facilitar la necesaria interoperabilidad con otros sistemas de la AGE y de las organizaciones internacionales a las que pertenece España". Los objetivos de la AG CIS/TIC hacen referencia a la integración de capacidades y al establecimiento de un marco técnico alineado no solo con la Estrategia TIC de la AGE, sino también con la Estrategia de la OTAN. Entre los principios estratégicos de la Alianza, en la Estrategia C3 del año 2014, se establecía el cambio desde un modelo de entrega de capacidades a uno nuevo de provisión de servicios,

[2] C3B es la autoridad de la OTAN para la estandarización, cuenta con el apoyo del personal experto del Cuartel General de la OTAN. En agosto de 2023 el NHQC3 Staff pasó a denominarse NATO DIGITAL Staff al mando del Contralmirante Nick Wheeler.

[3] URL de acceso a la página con los estándares NISP de OTAN, https://nhqc3s.hq.nato.int/NISP/default.aspx

adoptando un enfoque integral del ciclo de vida CIS/TIC. Además de permitir un flujo de información sin discontinuidad se buscaba asegurar la interoperabilidad de Servicios CIS/TIC antes del despliegue [17].

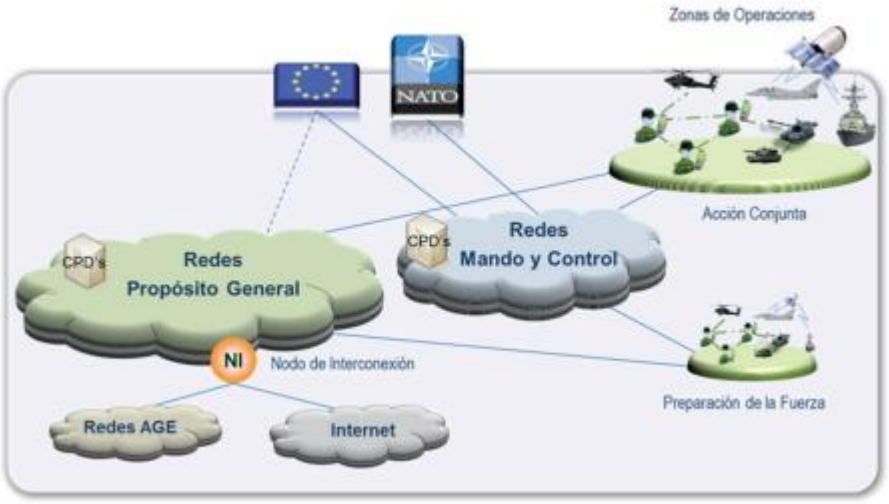

Figura 3. Situación previa a I3D [17].

La infraestructura CIS/TIC prevista por el MINISDEF proporcionará a los usuarios los servicios CIS/TIC que aseguren el tratamiento único de la información, integrando las distintas redes de telecomunicación, plataformas de información y equipos CIS/TIC. El nuevo escenario facilita la gestión centralizada de los recursos, permitiendo la clasificación de la información y la aplicación de medidas de seguridad de un modo automatizado. Al mismo tiempo la I3D permite el acceso a las redes y usuarios remotos, así como la interacción de usuarios del MINISDEF con otras organizaciones (por ejemplo, OTAN) a través de pasarelas normalizadas y aseguradas.

Se distinguen diferentes tipos de nodos: permanentes (NP), de gestión de sistemas y servicios sectoriales (NGSS), nodos de interconexión (NI), nodos desplegables (ND) y nodo de servicio compartido (SC). Los NI proporcionan la conexión e integración de los medios CIS/TIC desplegables con los medios CIS/TIC permanentes, mediante los correspondientes puntos de interconexión. Pueden ser de tres clases (I, II o III), siendo los de clase II los que proporcionan la interconexión con las redes de la OTAN, a través de conexiones fronterizas o puntos de presencia (PoP). En zona de operaciones y tomando como referencia la iniciativa FMN, la interconexión de los CIS/TIC con las redes OTAN se realiza a través de los puntos de interconexión de redes (NIP) y los puntos de interoperabilidad (IOP). A la hora de establecer los correspondientes acuerdos de interoperabilidad también se han de tener en cuenta las políticas de seguridad de la propia OTAN.

En el ámbito CIS/TIC del MINISDEF, la interoperabilidad se define como “la capacidad de los CIS/TIC del Departamento para proporcionar servicios a través de interfaces estandarizadas accesibles y aceptar servicios de otros CIS/TIC propios o de otros organismos, y utilizar los servicios intercambiados para operar de forma aislada o conjunta de manera efectiva con diversidad de CIS/TIC”. Se trata de un concepto que engloba el concepto de interoperabilidad en el ámbito de la OTAN [17].

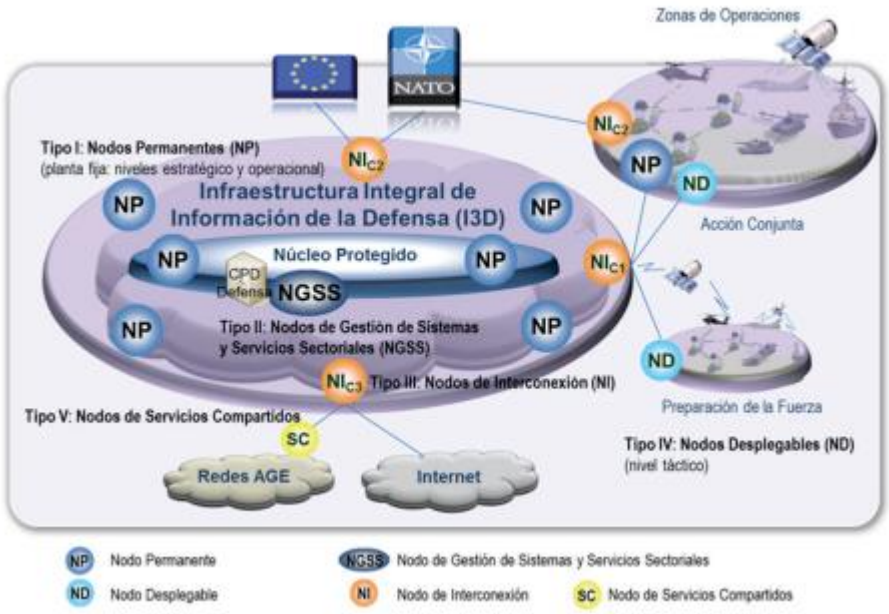

Figura 4. Estructura y tipos de nodos CIS/TIC [17].

La OTAN define la interoperabilidad como la capacidad de los aliados para actuar de manera eficiente con el fin de conseguir sus objetivos [4]. Permite que el personal, las unidades y los sistemas operen juntos, compartiendo doctrina y procedimientos comunes e intercambiando información de forma eficaz. La interoperabilidad abarca múltiples dimensiones: técnica (HW, SW, armamentos, sistemas y equipos), humana (instrucción y adiestramiento, terminología), información (elemento crítico y transversal) y de procesos. La OTAN utiliza estándares abiertos y potencia las relaciones con la industria de defensa para optimizar sus capacidades y racionalizar los esfuerzos nacionales.

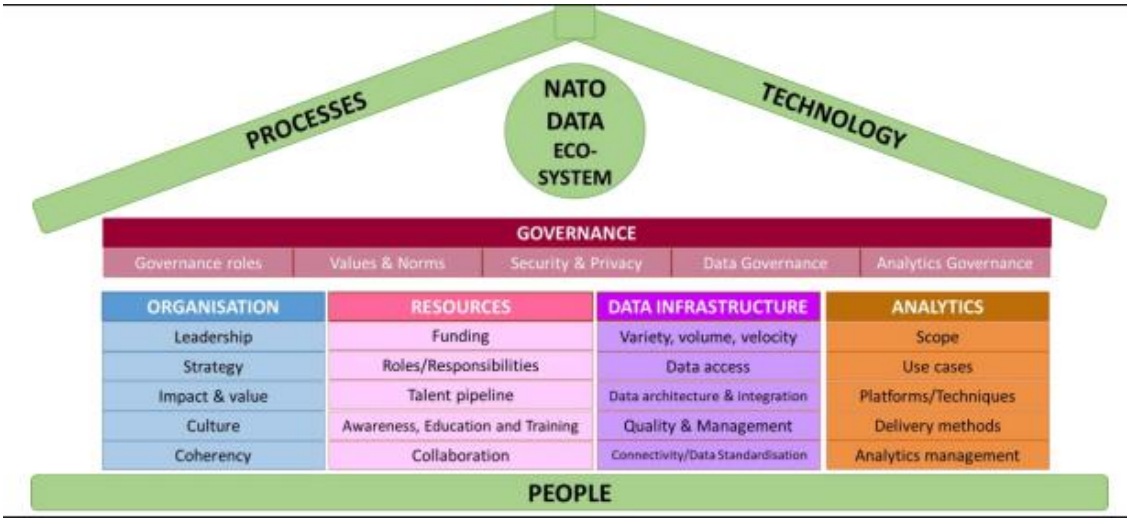

Figura 5. Interoperabilidad de los datos [4].

El NISP establece los estándares y perfiles necesarios para lograr la interoperabilidad CIS/TIC en apoyo a las misiones y a las operaciones de la OTAN. En las redes de misión que sean desplegadas bajo el paraguas de la Alianza, estos estándares serán obligatorios para los aliados. El NISP no solo es la referencia para el desarrollo de las arquitecturas sino también para todo el ciclo de vida de los CIS/TIC

de los países miembros. El Catálogo Unificado de Estándares CIS/TIC del MINISDEF (CUE) incluye los estándares del NISP (OTAN), organizados por grupos de servicios conforme a la taxonomía C3 [17].

Para asegurar la interoperabilidad de los medios CIS de las Fuerzas Armadas, el EMAD tiene entre sus cometidos la responsabilidad de implantar el concepto FMN para desarrollar y mantener la capacidad de establecer redes de misión federadas. Esta implantación se lleva a la práctica en tres ámbitos diferentes como son los medios, el adiestramiento y la gestión. En el ámbito de la gestión, además de establecerse las estructuras nacionales a nivel de gobierno, gestión y desarrollo para representar los intereses de España ante los órganos de FMN de la OTAN, se describen las responsabilidades de sus representantes y el procedimiento de intercambio de información entre ellos.

En el ámbito de los medios, el EMAD establece los requisitos e instrucciones FMN que garantizan la interoperabilidad y que se someten a los procesos de verificación, validación y demostración de forma periódica. Además de la descripción del proceso, es necesario establecer un listado de servicios consensuado con los Ejércitos y Armada, para lo cual se tendrá en cuenta el catálogo de productos establecido por CESTIC como referencia para la aprobación por parte del JEMAD de la Línea Base nacional correspondiente.

Finalmente, en el ámbito del adiestramiento se contempla el desarrollo de la doctrina FMN nacional y los ejercicios para la confirmación de la capacidad FMN. Es necesario establecer un procedimiento para demostrar esta confirmación, realizar un ejercicio de verificación, validación y confirmación de carácter anual y establecer una comunidad de conocimiento que permita el intercambio de información a través de bases de datos y repositorios para la configuración de los productos FMN por parte de los expertos.

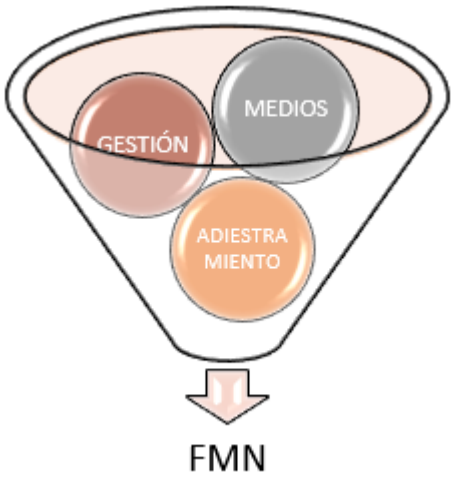

Figura 6. Áreas de trabajo FMN ESP [13].

3 LA INICIATIVA FMN DE OTAN

3.1 Antecedentes: FMN en OTAN

La OTAN no ha dejado de evolucionar para garantizar que sus fuerzas sean capaces de adaptarse a las circunstancias cambiantes del entorno operativo. Esto implica un esfuerzo continuo para disponer de fuerzas ágiles, conjuntas, expedicionarias e interoperables que permitan lograr la superioridad en el ámbito de la información y mayor eficacia en la toma de decisiones.

La OTAN se estructura en dos Mandos Estratégicos, el Mando Aliado de Transformación (ACT) y el Mando Aliado de Operaciones (ACO). El ACO se articula en tres niveles y cuenta con cuarteles generales y elementos de apoyo a nivel estratégico, operacional y táctico; ejerce el C2 de cuarteles generales estáticos y desplegables, así como de fuerzas conjuntas y combinadas en todas las misiones militares de la Alianza [25].

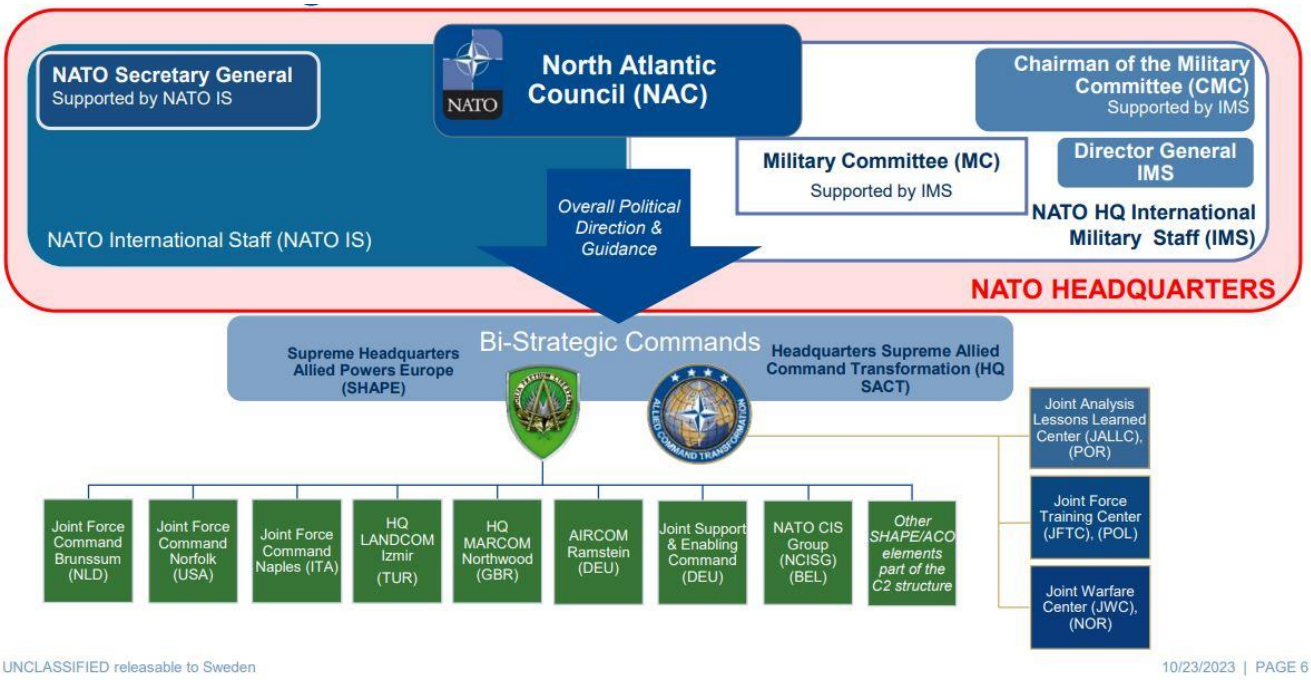

Figura 7. FMN en SHAPE (J6 *Cyber Directorate*) [26].

El Cuartel General Supremo de las Potencias Aliadas en Europa (SHAPE) es la sede estratégica, se ubica en Mons (Bélgica) y contribuye a preservar la paz, la seguridad y la integridad territorial de los países que forman parte de la OTAN en su área de responsabilidad. Su función es preparar, planificar, conducir y ejecutar operaciones militares para lograr los objetivos estratégicos de la Alianza.

El ACO es dirigido por el jefe del Mando Aliado en Europa (SACEUR), responsable ante el Comité Militar de la OTAN de la dirección y conducción de las operaciones y al mismo tiempo jefe del Mando Europeo de los Estados Unidos [26].

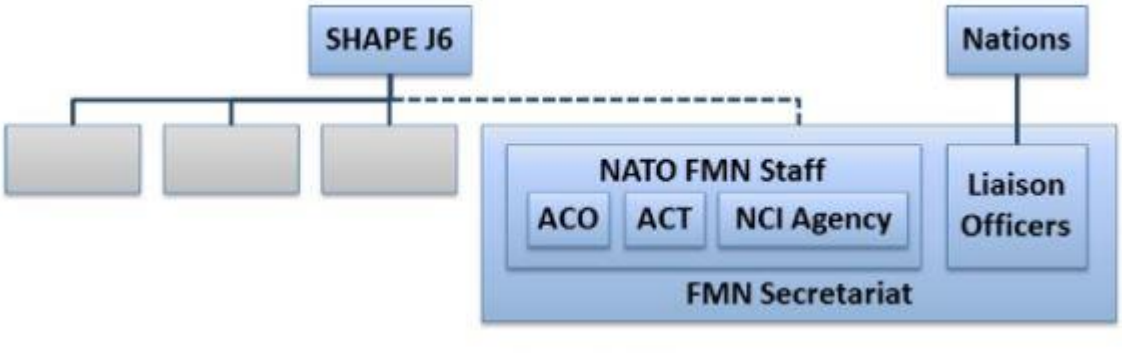

Figura 8. FMN en J6 [14].

Dentro de la estructura de SHAPE el personal se distribuye en divisiones o áreas de trabajo, siendo la división J6 Ciberespacio donde se encuentra ubicado el Secretariado FMN, del que forman parte tanto personal civil como militar. Las naciones contribuyen aportando personal para determinados puestos clave en la plantilla permanente del Secretariado, así como destacando oficiales de enlace que representan a sus respectivos países y colaboran en el trabajo diario que desarrolla FMN.

En la actualidad la iniciativa FMN se encuentra en plena evolución como consecuencia de los cambios que afectan a la OTAN. El nuevo concepto estratégico de 2022 establece como misiones principales la disuasión y defensa, la gestión y prevención de crisis y la seguridad cooperativa. El concepto de Disuasión y Defensa del Área Euroatlántica (DDA) [25] impone una profunda transformación de las estructuras de la OTAN y como consecuencia de ello será necesario disponer de unos cuarteles generales más eficientes en el desempeño de las denominadas operaciones multidominio (MDO). SHAPE seguirá contando con sus capacidades actuales y a ellas deberá sumar lo que se denominan funciones de combate a nivel estratégico: análisis y asesoramiento, planeamiento, recursos o gestión de sistemas entre otros [1].

El proceso de transformación de SHAPE supone un esfuerzo global y que afecta a todos sus componentes. Abarca aspectos culturales, materiales, organizativos, de instrucción y adiestramiento, tecnológicos o procedimentales. Es el núcleo del ACO y por tanto debe dar coherencia al planeamiento, al C2 y a la estructura de fuerzas, sea cual sea el escenario operativo [26]. En este sentido la iniciativa FMN tendrá que contribuir al nuevo cambio de paradigma que la OTAN propone en su agenda 2030. Entre las propuestas podemos destacar el fortalecimiento de la disuasión y defensa, la mejora de la resiliencia o la preservación de nuestra ventaja tecnológica.

Respecto a la innovación en Defensa en la cumbre de la OTAN de 2021 se acordó el lanzamiento de la iniciativa DIANA[4]. Su objetivo es "impulsar la cooperación transatlántica en tecnologías críticas, promover la interoperabilidad y aprovechar la innovación civil colaborando con el mundo académico y con el sector privado, incluidas las empresas emergentes". DIANA cuenta con financiación para los centros de investigación de los países de la OTAN con el fin de acelerar soluciones basadas en tecnologías disruptivas. A modo de ejemplo hay que destacar que el Portal de Tecnología e Innovación del MINISDEF

[4] *Defence Innovation Accelerator for the North Atlantic*.

ha habilitado una web de registro para inversores interesados en esta iniciativa y que de los tres desafíos piloto lanzados por DIANA uno de ellos es sobre el intercambio seguro de información.

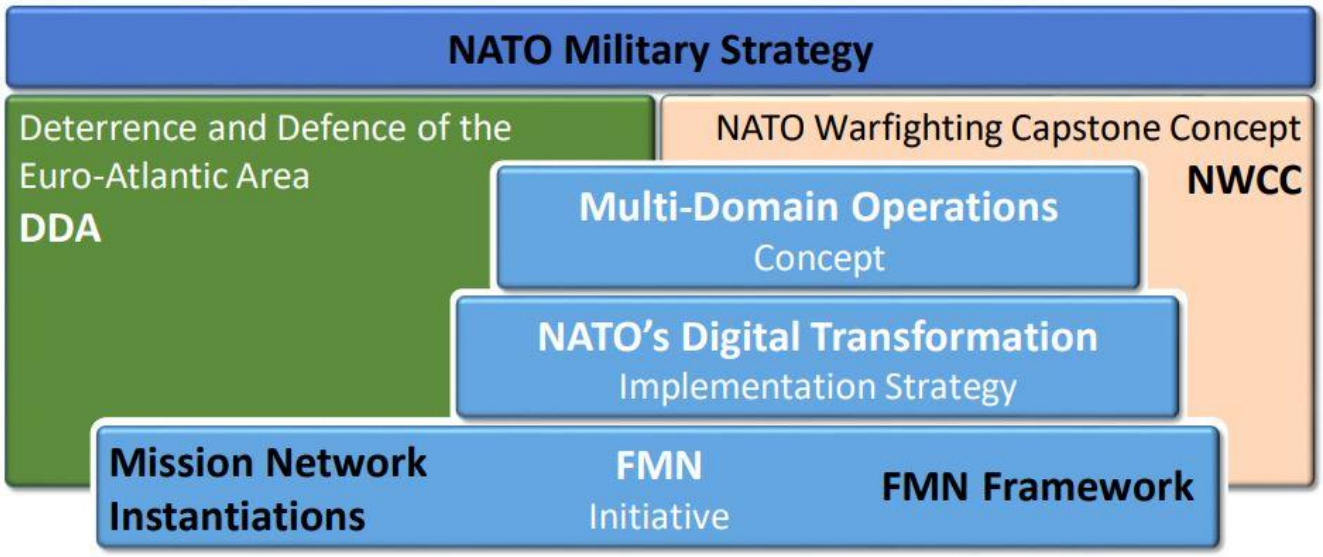

Figura 9. Contexto operativo FMN en OTAN [26].

La doctrina conjunta aliada para los CIS [27] hace referencia a los principios que debe cumplir la red de misión federada en el contexto que establece la taxonomía C3 (*Consultation, Command and Control*) de OTAN como herramienta para sincronizar y mejorar las capacidades de OTAN. Entre ellos se encuentran las conocidas características que se buscan en los sistemas como la escalabilidad, agilidad, resiliencia, y también la orientación al servicio conforme al marco FMN.

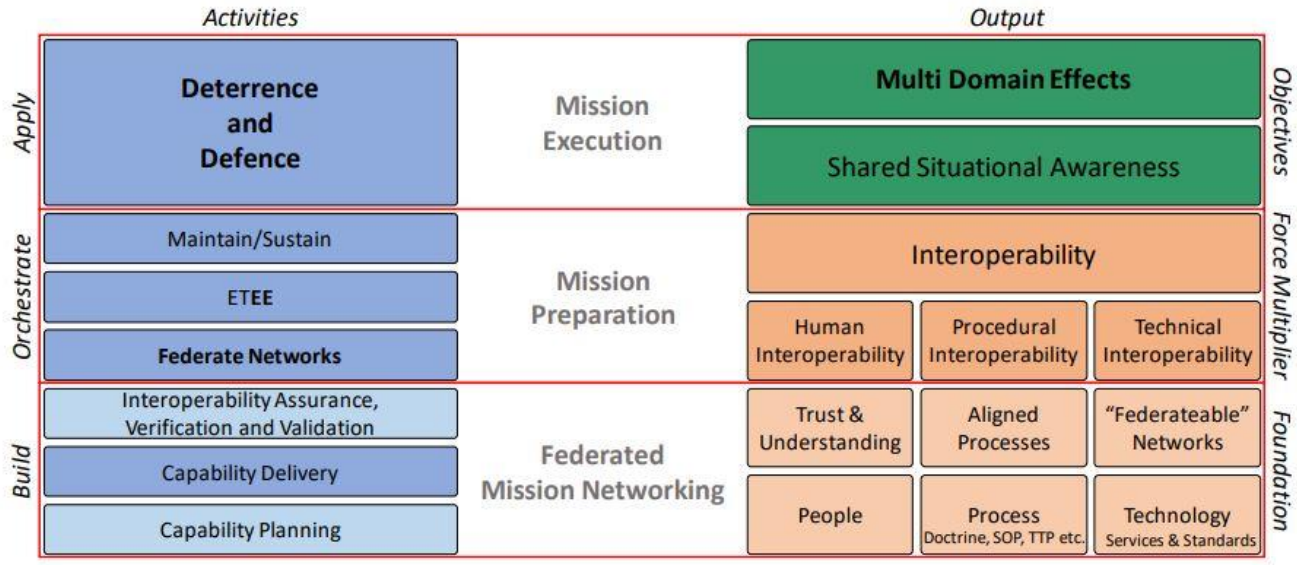

Figura 10. FMN como capacitador en las misiones [28].

Los medios CIS han de proporcionar a las fuerzas militares las capacidades C3 que permitan obtener los objetivos previstos, por ejemplo, en el ámbito de la disuasión y defensa [28]. Durante una operación multidominio se comparte gran cantidad de información que permite al Mando tener la conciencia

situacional adecuada para la toma de decisiones. Para ello las redes de misión federadas deben garantizar la máxima interoperabilidad posible no solo a nivel técnico, sino también a nivel de personal (comprensión mutua y confianza) y de procesos (doctrina, tácticas, técnicas y procedimientos). Sin la interoperabilidad no es posible conseguir los efectos óptimos deseados, incluso habiendo realizado una extraordinaria fase de planeamiento. En este sentido es necesario que todos los participantes, desde tiempos de paz, desarrollen sus capacidades orientadas al cumplimiento de los requisitos establecidos en las redes de misión federadas. La participación en ejercicios, la mejora del proceso de lecciones aprendidas o la definición de los procedimientos son parte de la iniciativa FMN para conseguir operar juntos de forma eficaz y coherente.

El Comité de Política Digital (DPC)[5] de la Alianza es un comité multinacional de alto nivel en el área C3 y se encarga del desarrollo de políticas de C3, ciberdefensa, estándares de interoperabilidad y capacidades digitales para asesorar al Consejo del Atlántico Norte (NAC). Es el motor de la transformación digital de la OTAN y permite mantener la interoperabilidad teniendo en cuenta los nuevos conceptos que surgen en OTAN como las operaciones multidominio o el *NATO Warfighting Capstone Concept* (NWCC).

El NWCC surge de la preocupación de la Alianza por mantener su ventaja sobre el adversario en el futuro, lo cual pasa por conseguir que los aliados piensen, se organicen y actúen de forma diferente a como lo hacen hoy. Partiendo de la premisa de que la victoria militar no equivale a una victoria estratégica, todo el personal involucrado en la iniciativa FMN ha de comprender los objetivos de la Alianza de cara al futuro tales como la superioridad cognitiva, la resiliencia en capas, la influencia y proyección de poder o la defensa integrada. FMN es un capacitador esencial para proporcionar un conocimiento adecuado del entorno operativo y permitir la toma de decisiones en un escenario multidominio cada vez más complejo, contribuyendo a la integración de fuerzas desde el primer día.

Para realizar su labor cuenta con el apoyo de los expertos del *NATO Digital Staff* y de varios equipos y paneles de trabajo que se dedican a un área determinada (arquitecturas, CIS marítimos, CIS aéreos, CIS terrestres, explotación de datos, etc.).

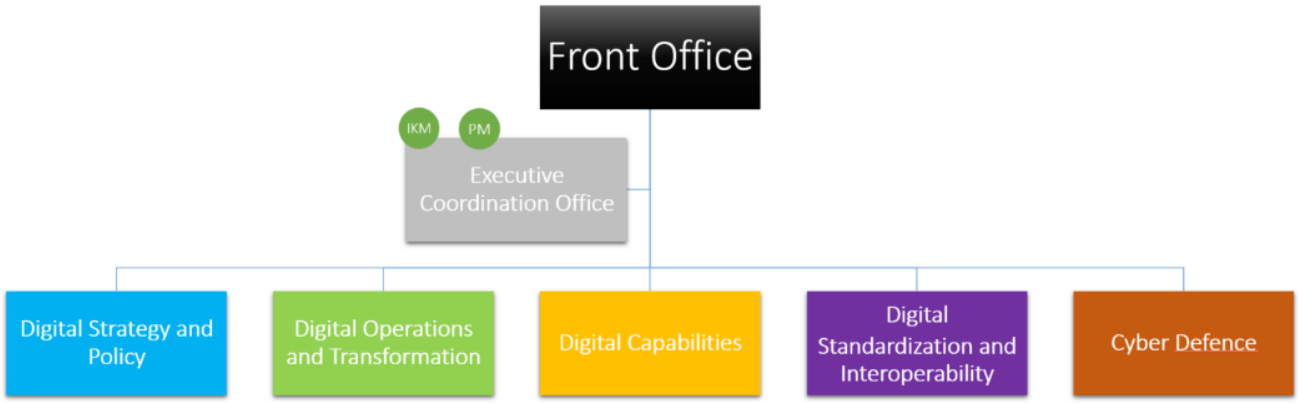

Figura 11. Áreas de trabajo del DPC [30].

[5] En diciembre de 2023 se produjo el cambio de denominación del DPC, anteriormente conocido como Junta C3 o C3 Board.

3.2 Concepto de Red de Misión Futura de 2012.

El concepto NNEC fue adoptado tras la Cumbre de Praga de 2002 y se puede definir como la capacidad de la Alianza para federar los diversos componentes del entorno operativo (redes colaborativas, servicios comunes, procesos sincronizados, sistemas nacionales y de la OTAN), desde el nivel estratégico (incluido el Cuartel General de la OTAN) hasta los niveles tácticos, a través de una infraestructura de redes e información. La infraestructura de redes e información (*NATO Information Infrastructure* o NII) es la encargada de respaldar técnicamente dicho concepto [29].

Por otro lado, la Fuerza Internacional de Asistencia para la Seguridad[6] (ISAF) fue una misión de seguridad multinacional en Afganistán que participó en la guerra entre los años 2001 y 2014. Durante los primeros años de ISAF el concepto NNEC no produjo el efecto deseado respecto a la interoperabilidad y la Alianza se vio obligada a buscar una solución. Fruto de ello en el año 2010 se desarrolló la red de misión de Afganistán (AMN) como primera instancia de red de misiones federadas para el C2 de la coalición. Su implementación se llevó a cabo en varios niveles, mediante el desarrollo de una plataforma física y distintos servicios básicos y específicos con la contribución de varios países. Con fecha 27 de septiembre de 2010 se aprobó la Directiva de Gobernanza para AMN en un contexto operativo donde la fuerza desplegada empleaba una red secreta de misión (MS) para ejercer la función de C2 [30].

La eficacia de los aliados en el cumplimiento de la misión depende de su capacidad para operar como una sola unidad y poder disponer en tiempo real de una visión común del entorno operativo. Los sistemas de C2 de la Alianza y del resto de entidades participantes en la operación deben de ser interoperables para planificar y sincronizar todas las actividades de la fuerza desplegada. Tanto el mando conjunto de la ISAF como el jefe del Mando Aliado de las Operaciones de OTAN (SACEUR) apoyaron la necesidad de una capacidad de red federada [31][32][33] de ahí que se incorporara a los requisitos de capacidades del año 2011 dentro del Proceso de Planificación de la Defensa de la OTAN (NDPP) [34].

Figura 12. Fases Proceso de Planeamiento [34].

El concepto de Red de Misión Futura fue desarrollado por orden del Comité Militar de la OTAN durante el año 2011 fruto de la colaboración entre el Mando Aliado de Transformación (ACT) y el Mando Aliado

[6] La *International Security Assistance Force* (ISAF) tuvo como antecedente una coalición de países liderada por Estados Unidos en la llamada Operación Libertad Duradera. El 31 de diciembre de 2014 la misión ISAF fue reemplazada por una nueva misión llamada *Resolute Support* o Apoyo Decidido.

de Operaciones (ACO), a partir de las lecciones aprendidas de la AMN, del informe proporcionado por el Centro de Excelencia de Mando y Control (C2CoE) y otros documentos sobre el alcance y plan de acción de FMN. Su objetivo era establecer una capacidad de red de misión federada para el intercambio de información entre la OTAN, los aliados y otras entidades no pertenecientes a la OTAN que participaran en las operaciones.

Este concepto describe tres componentes: Gobernanza, Marco FMN y Redes de Misión (*Mission Network* o MN). Se entiende por gobernanza la orientación de la iniciativa FMN a alto nivel para conseguir una gestión efectiva tanto del Marco FMN como de las Redes de Misión (MN). El Marco FMN se puede definir como una estructura integral que proporciona procesos, planes, plantillas, arquitecturas y herramientas para analizar, planear, implementar, operar, evolucionar y mejorar las Redes de Misión (MN) de la OTAN y de las naciones en entornos federados.

La MN[7] sería una instancia o entidad única, basada en la confianza y la voluntad de sus miembros, que proporciona una capacidad formada por elementos materiales (redes estáticas, redes desplegables, servicios, infraestructuras de apoyo y CIS) y no materiales (políticas, procedimientos y estándares) para la interoperabilidad en una operación o ejercicio.

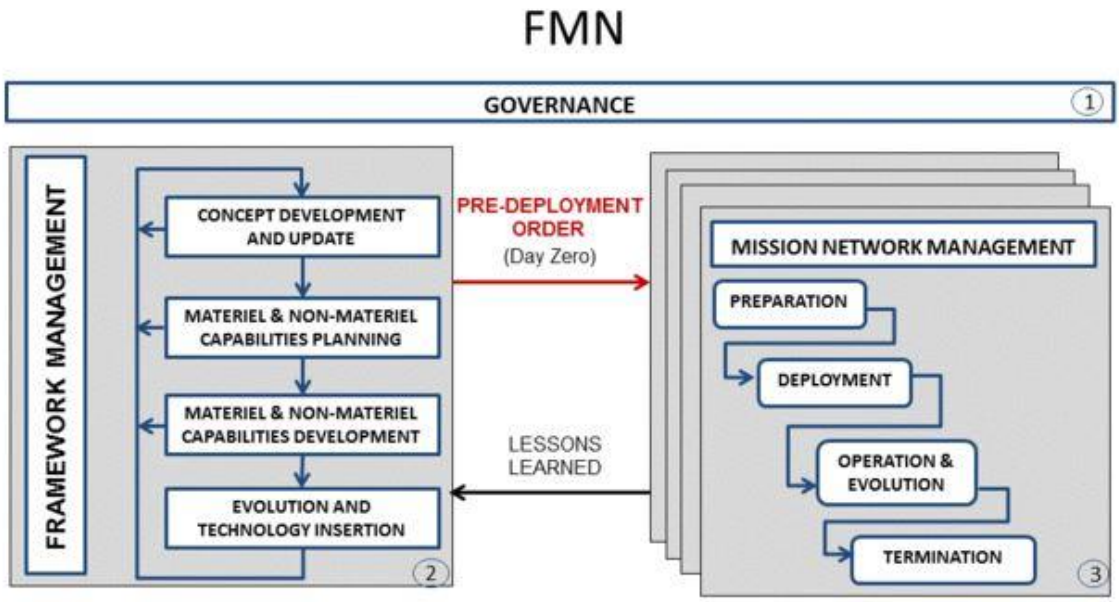

Figura 13. Componentes FMN [35].

El Proceso de Planificación de la Defensa (NDPP) contempla distintos tipos de misiones y para cada una de ellas el número de participantes puede variar. De ahí que el concepto FMN ya contemplara en el año 2012 la necesidad de responder de forma ágil a las necesidades del jefe de la Fuerza y al ritmo de batalla de cada operación. La MN tiene como objetivo proporcionar el entorno adecuado para que las fuerzas de la coalición dispongan de comunicaciones estables y seguras. Todos los participantes deben tener acceso a los sistemas de información que proporcionen datos fiables y de calidad. La MN debe estar disponible desde el comienzo de la operación, proporcionando acceso a los distintos servicios a los usuarios, los cuales requieren de una adecuada formación previa para conocer las herramientas y aplicaciones que ofrecen los sistemas y aprovechar al máximo sus capacidades.

[7] En el ámbito FMN la red de misión o MN sería una federación o asociación entre OTAN como organización, varias naciones de la OTAN y otras entidades no pertenecientes a la Alianza que participan en operaciones conservando cada una de ellas el control de sus capacidades.

Tomando como referencia los principios del concepto NNEC, FMN adoptó desde sus inicios un enfoque incremental que permitiera adaptarse a los cambios en los requisitos operativos y a la evolución de la tecnología. La reutilización de los estándares, capacidades, contribuciones de las naciones, adquisiciones colaborativas y acuerdos de nivel de servicio (SLA) permiten a FMN adaptarse a los recursos disponibles en la Alianza sin renunciar a la flexibilidad y escalabilidad que necesitan las redes de misión [29].

El concepto FMN desarrollado en 2012 se basa en el intercambio de información entre la Alianza, las naciones de la OTAN y las entidades no pertenecientes a la OTAN que participan en operaciones para constituir redes de misión federadas o MN. Uno de los elementos necesarios para establecer la red de misión en FMN son los denominados *Mission Threads* (MT). Se pueden definir como una descripción operativa y técnica del conjunto de actividades necesarias para la ejecución de una determinada misión. Una MT abarca estructuras organizativas, procesos operativos, requisitos de intercambio de información y productos de información de una tarea clave que se repite con frecuencia y que es asignada a varias Comunidades de interés (*Community of Interest* o CoI). Estas CoI comparten la información de la MN y juegan un papel clave para el análisis de los MT e identifican posibles carencias y márgenes de mejora para el cumplimiento de la misión.

En el desarrollo del concepto FMN se tuvieron en cuenta varios MT de referencia a partir de las aportaciones de las naciones, el *Allied Command Operations* (ACO) y otros elementos de la estructura de mando (NCS) de la OTAN. Estos MT están vinculados a los procesos operativos y sirven de apoyo para el desarrollo de la MN correspondiente. Los MT que se desarrollaron inicialmente estuvieron basados en una revisión de los escenarios operativos de la coalición de la Fuerza Internacional de Asistencia para la Seguridad (ISAF), de los Estados Unidos y de procesos críticos procedentes del documento MC 593/1. Entre ellos podemos destacar la gestión de servicios de red CIS, operaciones de información y efectos no letales, ISTAR, defensa aérea y antimisiles, recursos logísticos y transporte, operaciones marítimas, protección de la fuerza, CIED, conciencia situacional, maniobra y C2 [35].

Los paquetes de capacidades (*Capability Packages* o CP) engloban elementos materiales y no materiales que son implementados en los MT, tanto servicios esenciales como servicios funcionales. Entre los primeros podemos citar herramientas de almacenamiento de datos, de virtualización o de seguridad. Como ejemplo de servicios funcionales, citar los relacionados con sistemas de inteligencia, de logística y de C2. También se especifican servicios de comunicaciones que evolucionarán a medida que lo haga la tecnología, como los servicios de red (*Network Interconnection Points* o NIP o servicios de transmisión), voz, chat, correo electrónico, VTC, herramientas ofimáticas o plataformas web.

La iniciativa FMN ofrece a cada socio un nivel diferente de integración siempre y cuando cumpla con unos requisitos mínimos previamente acordados. Cada MN permite a los federados disponer de sus propios servicios, prestar servicios a otros miembros, utilizar los servicios proporcionados por terceros o seleccionar aquellos servicios que necesitan para el cumplimiento de la misión [36].

La opción A (MNE o *Mission Network Element*) o nodo es aquella en la que un miembro de la MN establece su propia infraestructura y servicios esenciales previamente certificados para su propio empleo y proporciona interconexión y determinados servicios a otros miembros conforme a los acuerdos FMN. La opción B (MNX o *Mission Network Extension*) también contempla el establecimiento de infraestructura propia, pero en este caso para proporcionar una extensión de MN, por lo que requieren de acuerdos bilaterales con un proveedor de nodo MN de la opción A. Los miembros de la opción B deben someter sus servicios a una validación de interoperabilidad conforme a los acuerdos FMN y si cuentan con los acuerdos de seguridad adecuados podrán interconectarse con las redes nacionales. La opción C (o *Hosted User*) es aquella que permite a sus miembros integrarse y utilizar el nodo o extensión proporcionado por un afiliado de la opción A o B respectivamente, mediante los correspondientes acuerdos bilaterales con el proveedor [37].

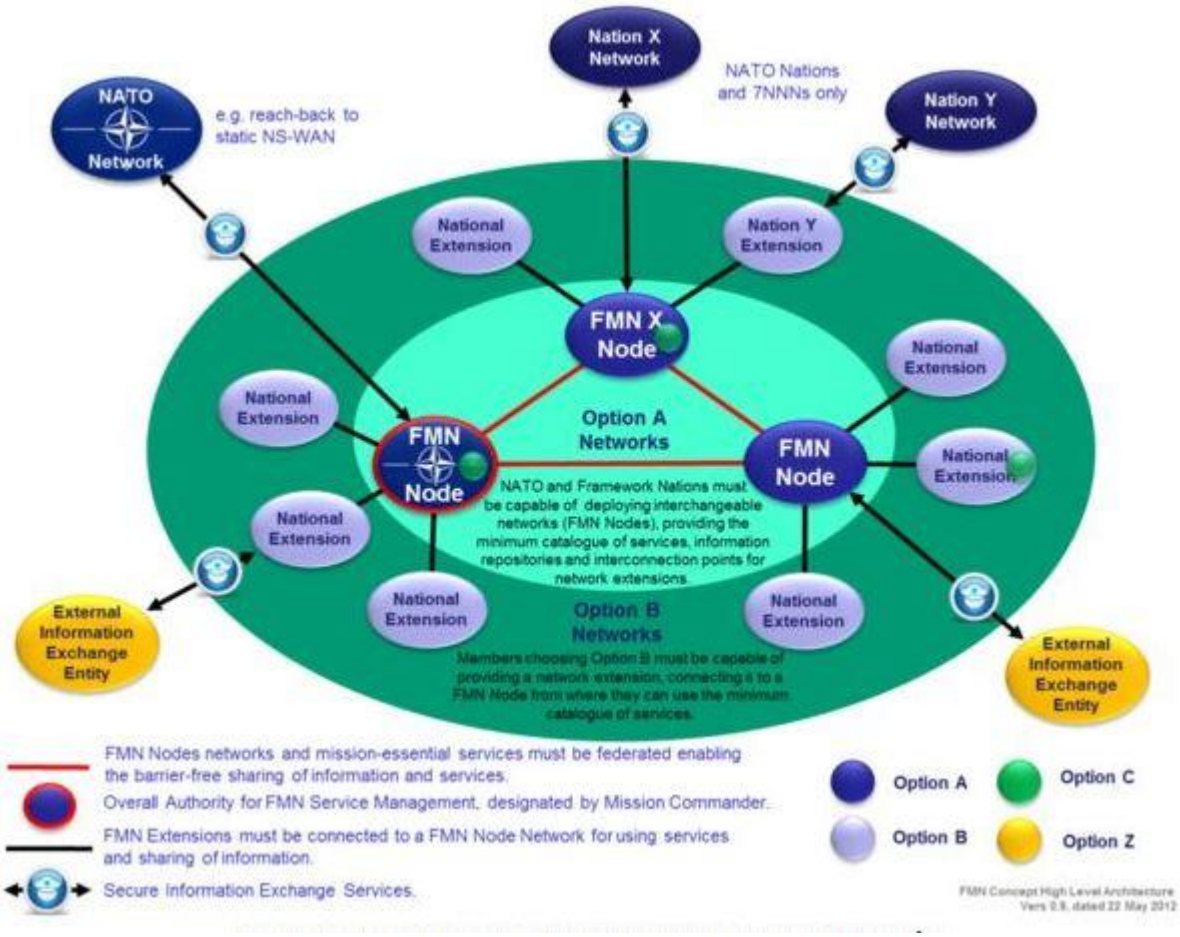

Figura 14. Niveles de integración FMN [35].

La opción Z está destinada a entidades distintas de las descritas anteriormente y permiten la interconexión a la MN para el intercambio de información previamente seleccionado. En este caso no están sujetas a todos los acuerdos marco de FMN y el resto de los socios de la red tendrán que aceptar o rechazar caso por caso las interconexiones e intercambios de información solicitados. Para ello se emplean las correspondientes pasarelas que estarán alineadas con los requisitos mínimos establecidos para el intercambio seguro de la información [34].

Desde el punto de vista operativo, en un primer momento se puso el foco de atención en las operaciones de respuesta rápida de la OTAN (*NATO Response Force* o NRF). Cada MN se desarrollaba en función de las necesidades concretas, incorporando las arquitecturas, organización, procedimientos de seguridad y tácticas, técnicas y procedimientos (TTP) adecuadas, con el fin de facilitar el intercambio de información entre todos los usuarios que participan en la misión, si bien en los primeros momentos no todos los servicios se encontraban siempre disponibles.

La MN evoluciona desde la fase de preparación, pasando por la de operación y despliegue, hasta la fase de finalización. En este ciclo es importante el proceso de lecciones aprendidas para informar a los órganos de gobierno y de gestión de FMN y conseguir la mejora continua de la red. Durante la fase de preparación, que debe durar el mínimo tiempo posible, se establece la red con los componentes disponibles que aportan los participantes en la operación.

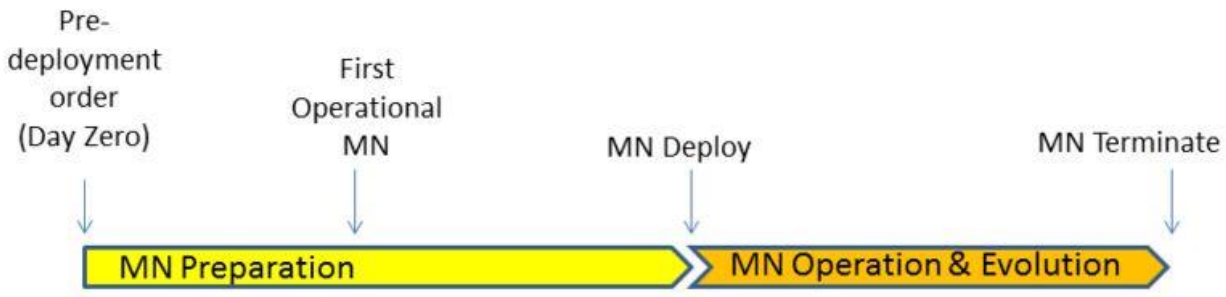

Figura 15. Línea de tiempo MN [36].

En las misiones suele haber implicados diferentes dominios y será la OTAN junto a las naciones y resto de entidades los que decidan qué información desean compartir en el dominio de información común. Es aconsejable reducir al mínimo posible el número de controles de seguridad que compliquen a los usuarios de la red el intercambio de información, lo que supone que el dominio de información común se gestione al nivel de clasificación más bajo posible.

El plan de gestión de la información de la MN describe los procesos, procedimientos y roles a lo largo del ciclo de vida de la información. Así mismo la capacidad FMN incluye procesos de gestión de la configuración y garantía de la información, con el objetivo de garantizar su confidencialidad, integridad y disponibilidad. En el Marco FMN se contempla la existencia de unas capacidades permanentes que han de mantener las naciones y la OTAN para proporcionar los requisitos iniciales de la misión. Precisamente estas capacidades mínimas que satisfacen las necesidades del Mando durante las primeras fases del despliegue es lo que proporciona la capacidad *Zero Day*.

Hay que señalar que el concepto de red de misión de 2012 establecía ya tres hitos (*Milestones)*. En el Hito 1, los participantes logran una infraestructura física separada por misión y por nivel de clasificación de seguridad. En el Hito 2 o capacidad a medio plazo, los participantes consiguen varios niveles de clasificación de seguridad con una infraestructura física separada por misión, además de proporcionar más servicios disponibles para los usuarios. Por último, en el Hito 3 o a largo plazo, la OTAN, los afiliados y otras entidades no pertenecientes a la OTAN pero que participan en las operaciones logran una infraestructura única para varias misiones y múltiples niveles de clasificación [35].

En el año 2013 se realizó el ejercicio *Steadfast Cobalt* (SFCT13) liderado por ACT y C2COE y con el apoyo de la Agencia de Comunicaciones e Información de la OTAN (NCIA). Entre sus objetivos se encontraba la mejora de la interoperabilidad de la Alianza y de los medios CIS desplegados por la fuerza NRF 14, lo cual implicaba la validación de los estándares empleados por la OTAN y por las naciones por parte del C3B en el proceso de certificación de NRF liderado por ACO. La serie de ejercicios *Steadfast* permitía comprobar el grado de implementación de los criterios NNEC con el fin de mejorar la eficacia de NRF y por ende de las misiones que llevara a cabo la OTAN [38].

3.3 El Plan de Implementación de la iniciativa FMN de la OTAN (2013-2015)

Tras la aprobación del concepto de FMN se requería el desarrollo de un plan que detallara como implementarlo teniendo en cuenta los elementos de doctrina, organización, instrucción, material, liderazgo, personal, instalaciones e interoperabilidad empleados para el análisis y el desarrollo de capacidades (método DOTMLPFI).

A partir de la doctrina desarrollada para la AMN, el futuro plan debía revisar y actualizar las políticas disponibles para alinearlas con los procesos y herramientas del Marco FMN. Se contempla la necesidad de disponer de un mecanismo que se adapte a cada MN y que sirva para implementar los principios de FMN. Además de las necesidades doctrinales, dicho plan debía proporcionar una organización que garantice la gobernanza y la gestión de FMN, tanto del Marco FMN como de las MN.

El plan también debía identificar las instalaciones necesarias para FMN y establecer la formación que necesita el personal para adquirir las habilidades necesarias. En cuanto a material, se aplicaría el principio de máxima reutilización de las capacidades existentes y se impulsaría el liderazgo para que los participantes en la iniciativa FMN asumiesen la máxima implicación. Respecto a la interoperabilidad establecería las orientaciones para la adaptación y adquisición de materiales, describiendo los requisitos técnicos y operativos para ser interoperables, conforme a la documentación sobre estándares y perfiles de interoperabilidad de la OTAN (NISP). Igualmente contemplaría la mejora de la interoperabilidad mediante la realización de pruebas de validación y verificación de los sistemas, procesos y procedimientos que contempla el Marco FMN [37].

El primer borrador del plan de implementación FMN se redactó a finales del año 2013, designando al Comité Militar (MC) como autoridad de gobernanza para la iniciativa. Tanto el ACT como el NHQC3S y algunas naciones presentaron enmiendas al texto hasta llegar a la versión definitiva, finalizada y aprobada por el MC en el año 2014, y aprobada en enero de 2015 por el Consejo del Atlántico Norte (NAC).

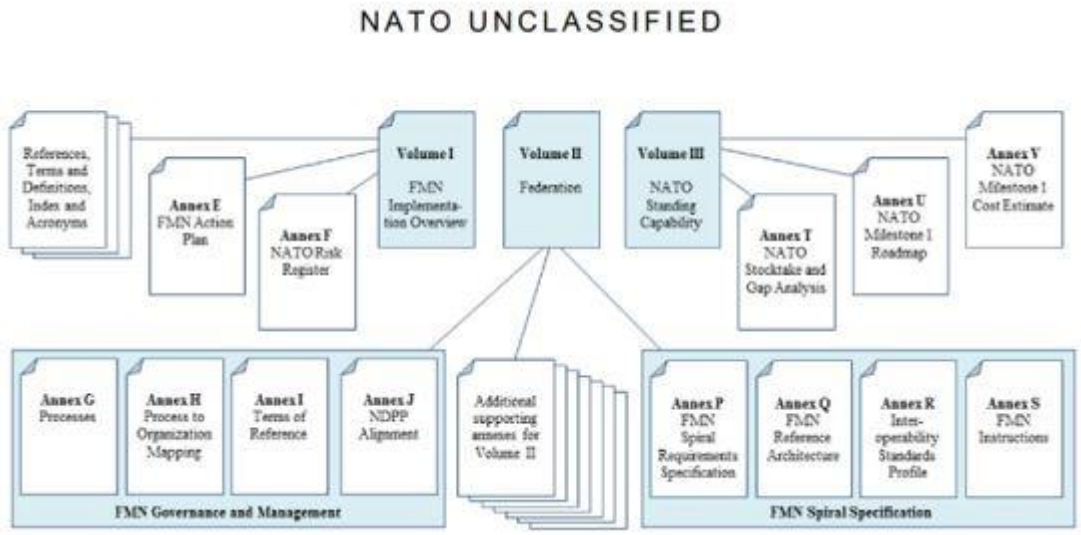

Figura 16. Plan de Implementación FMN [37].

El Plan de Implementación de FMN (NFIP) es un documento que tiene como objetivo el establecimiento de una capacidad, entendida como un conjunto de herramientas (procesos, organización, tecnología y estándares) para generar redes de misión federadas, eficaces y eficientes, que permitan mejorar tanto el C2 como la toma de decisiones en misiones y ejercicios. El plan considera que esta capacidad se debe obtener en un corto plazo para dar respuesta a cualquier tipo de misión, aprovechando los recursos disponibles. La iniciativa FMN contempla la federación como forma de lograr una economía de escala entre todos los participantes para facilitar el intercambio de información.

La versión oficial del NFIP (versión 4.0) se divide en tres volúmenes, el primero sobre la descripción general de la implementación de FMN, el segundo dedicado a la federación y un tercero sobre la capacidad permanente de la OTAN. El volumen I del NFIP recoge las tareas del MC y el enfoque genérico de la iniciativa FMN, indicando las acciones que hay que realizar para implementar la capacidad. El volumen II del NFIP se orienta a las políticas, operaciones, gobernanza, implementación técnica, gestión, verificación y validación de las partes interesadas para establecer y mantener tanto el Marco FMN como la gestión y gobernanza de la iniciativa [37].

La extensión del volumen II se debe a que describe los procesos y actividades para el gobierno, la operación y la gestión del Marco FMN. Incluye también la definición en detalle de la primera espiral FMN, así como una serie de anexos y apéndices para guiar con más detalle la implementación, desglosando las especificaciones de la Espiral 1, arquitectura de referencia, estándares de interoperabilidad, plantillas de procedimiento o plantillas de configuración. En el ámbito FMN se entiende por espiral un ciclo temporal que abarca una serie de procesos para evolucionar el nivel de madurez de la capacidad FMN.

El volumen III del NFIP se centra en el desarrollo de capacidades en el seno de la OTAN para liderar y participar en FMN. Partiendo de un análisis de las necesidades de la Alianza, establece los pasos para convertirse en un proveedor de servicios en cualquier misión o ejercicio, una hoja de ruta para alcanzar el Hito 1 (*Milestone* 1) de la OTAN y una estimación del coste previsto conforme al nivel de ambición de la Alianza. Como ya se ha indicado, la gobernanza es el elemento de FMN que proporciona el entorno adecuado para la gestión eficaz tanto del Marco FMN como de las MN. Para llevar a cabo la orientación y supervisión de alto nivel, la gobernanza se apoya fundamentalmente en dos documentos: la Directiva de Gobernanza y el Plan de Acción para la Gobernanza FMN.

Figura 17. Gobierno y gestión en FMN [37].

El MC es la autoridad de gobernanza[8] que orienta al Grupo de Gestión FMN o *Management Group* (MG) y se encarga de supervisar los progresos y posibles riesgos en el ámbito de la interoperabilidad. Para ello cuenta con el apoyo del Estado Mayor Internacional (IMS) [39].

Otras funciones desarrolladas por el MC son la supervisión del cumplimiento de los requisitos operativos de la OTAN y la coordinación de la iniciativa FMN con otros comités de alto nivel.

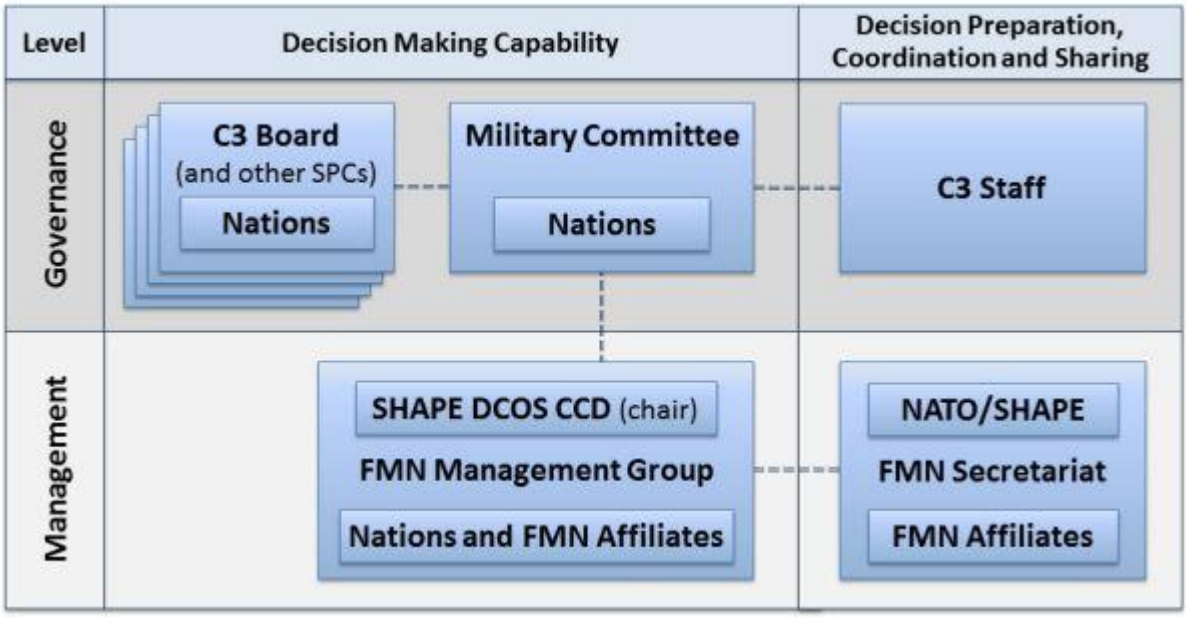

Figura 18. Estructura de gobernanza y gestión FMN [37].

El Plan de Acción de Gobernanza de FMN es utilizado por el MC para mantener la visión global y facilitar el desarrollo de la iniciativa FMN. El primer Plan de Acción para la Gobernanza se obtuvo en 2018, basado en el NFIP, se centró en el seguimiento de la implementación tanto a nivel de gobernanza como de gestión. Una vez que el Grupo de Gestión FMN se fue consolidando, el plan de acción se revisó y se focalizó en avanzar de forma decidida en los objetivos de la gobernanza [40].

[8] La Directiva de Gobernanza para FMN fue aprobada por el MC en el año 2017.

3.4 El Marco FMN

El documento que describe el Marco FMN es la Directiva de Gestión de FMN, que detalla la misión, estructura, responsabilidades y tareas de los órganos de gestión de FMN. Las dos actividades principales del Marco FMN son el Proceso Marco FMN (con sus productos y las relaciones de estos productos con los órganos de gestión) y el Apoyo del Proceso Marco FMN a la instanciación de misiones (permite reducir el tiempo necesario para conectar fuerzas durante una instancia). La Directiva no trata los acuerdos de gestión de instancias de MN pues son responsabilidad y decisión de los afiliados de FMN [41].

Para conseguir los objetivos generales de interoperabilidad *Zero Day*, mantener la disponibilidad de las fuerzas de los aliados, cumplir con los requisitos operativos establecidos y optimizar el intercambio de información para la toma de decisiones en tiempo real, la Directiva establece que la gestión de FMN es una responsabilidad compartida de todos los afiliados y su fin es garantizar que las redes de misión puedan establecerse y gestionarse de manera eficiente y eficaz.

Entre los objetivos del Marco FMN está facilitar que los afiliados creen capacidades FMN que les permitan interconectar sus fuerzas en un determinado entorno o instancia. Para ello cuenta con la estructura de gestión de FMN compuesta por el Grupo de Gestión (MG), la Secretaría FMN y sus correspondientes grupos de trabajo o *Working Groups* (WG). Los responsables de realizar las funciones de gestión de la iniciativa FMN son los afiliados y con sus representantes del MG se encargan de la toma de decisiones a nivel directivo. En el documento sobre los términos de referencia (*Terms of Reference* o ToR) del MG se recogen las condiciones para aceptar o no la asistencia de otros participantes no afiliados a las reuniones.

El MG es el organismo que toma las decisiones y asigna las tareas para conseguir los objetivos del Marco FMN. Entre sus responsabilidades está la gestión y mantenimiento del Marco FMN basado en la visión y orientación del MC [42]. También se encarga de orientar y dirigir a la Secretaría FMN y a los grupos de trabajo y de proporcionar el foro adecuado para que los afiliados decidan sobre la evolución de las capacidades FMN y las instancias de MN. Cualquier cambio que se plantee y que afecte al Marco FMN ha de presentarse de forma oficial en el MG para su acuerdo y aprobación.

El MG es igualmente el responsable de dirigir y guiar la integración de nuevos afiliados al Marco FMN a partir de la decisión del MC y conforme a una directiva sobre ampliación de afiliados FMN y al proceso de afiliación FMN. Para ello debe previamente asegurarse de que los afiliados cumplen con los requisitos de afiliación. Otra de sus misiones es dirigir la gestión de riesgos según los procesos FMN vigentes y mantener informado al MC del grado de progreso y de los objetivos alcanzados en el Marco FMN.

La Secretaría de FMN coordina las actividades del Marco FMN, realiza la gestión diaria de los procesos y es el organismo de coordinación, intercambio y preparación de decisiones. Para la gestión diaria del Proceso Marco FMN cuenta con la orientación y dirección del MG. Se encarga de sincronizar, monitorizar y coordinar actividades y procesos, informando periódicamente al MG. Dentro de la estructura de gestión de FMN, la Secretaría coordina la gestión de riesgos con el apoyo de los grupos de trabajo e informa de los riesgos críticos al MG. En el proceso de afiliación a FMN se encarga de gestionar y facilitar el proceso conforme a los documentos de referencia anteriormente citados, así como de la preparación de las reuniones anuales del MG.

La Secretaría de la FMN coordina, monitoriza y asesora a los WG cuyas misiones son las siguientes:

- El Grupo de Trabajo de Coordinación Operativa (OCWG) mantiene la coherencia entre los requisitos operativos de los usuarios y el conjunto de servicios que proporciona FMN.

- El Grupo de Trabajo de Planificación de Capacidades (CPWG), realiza la coordinación de todo el trabajo entre afiliados y resto de participantes de la iniciativa FMN para la obtención de los diferentes productos y servicios.
- La Autoridad Multinacional de Gestión de Seguridad CIS (MCSMA) se ocupa de garantizar que los requisitos de seguridad CIS para los servicios y capacidades en el Marco FMN sean adecuados y que las redes de misión basadas en FMN estén acreditadas de manera correcta.
- El Grupo de Trabajo sobre Coordinación de Cambios e Implementación (CICWG) implanta los cambios acordados en los productos y servicios y crea otros nuevos en coordinación con el CPWG. El CICWG también supervisa que los procesos, sistemas y organizaciones de los afiliados estén alineados con los principios establecidos por FMN. Y ayuda a coordinar los proyectos nacionales y de la OTAN para que las implementaciones de referencia estén sincronizadas.
- El Grupo de Trabajo de Validación y Garantía de Interoperabilidad de la Coalición (CIAV) es el organismo de la Secretaría autorizado para garantizar, validar y verificar la interoperabilidad de todas las capacidades que se agregan, modifican o eliminan en FMN.

Además de los grupos de trabajo indicados anteriormente, el NFIP contempla la creación de otros grupos de carácter temporal por si fuera necesario tratar cuestiones concretas que trasciendan de las tareas diarias que realiza la Secretaría. La representación de los afiliados FMN en los diferentes WG es lo que permite mejorar a diario en la consecución de los objetivos de la iniciativa. Además de la colaboración entre ellos, es importante mantener el contacto con las divisiones de SHAPE, con el resto de las estructuras de Mando de la OTAN, agencias, entidades y demás organismos involucrados en el ámbito de la interoperabilidad.

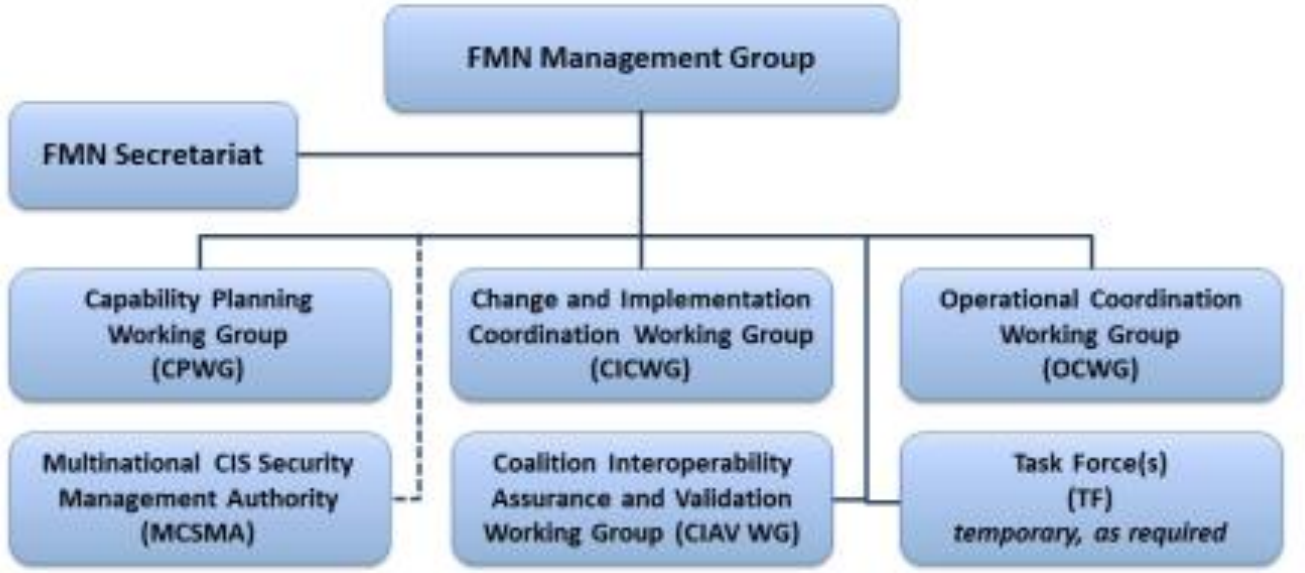

Figura 19. Estructura de gestión FMN [37].

El Proceso Marco FMN es un enfoque holístico que permite crear instancias de misión mejorando la interoperabilidad en sus tres dimensiones: personas, procesos y tecnología. El Proceso mejora de forma incremental los servicios y procedimientos disponibles para ser empleados en misiones y ejercicios. La colaboración activa de los afiliados con el resto de los organismos de la estructura FMN da como resultado estos incrementos de interoperabilidad, denominados espirales, cuyas especificaciones se emplean como guía para el desarrollo de capacidades de los miembros de la iniciativa.

Como se verá más adelante el Proceso Marco FMN basado en espirales establece unos plazos o eventos concretos para garantizar la continuidad de los resultados previstos en cada una de las fases del ciclo. Las actividades y los procesos que se realizan para obtener estos productos son interdependientes y están vinculados de forma directa a uno o varios de los objetivos del Marco FMN.

Además de la visión FMN, la Hoja de Ruta para la Gestión FMN y la Hoja de Ruta para las Especificaciones de la Espiral FMN se utilizan como guía y herramienta de planificación tanto del Proceso Marco como del desarrollo de capacidades FMN. El Proceso Marco FMN para un ciclo de vida de la espiral dura más de 7 años en los que se suceden varias fases:

- En la fase de requisitos se recopilan los requisitos de los afiliados y se identifican las capacidades para cumplir con ellos. El resultado final son los requisitos operativos que han sido priorizados por los afiliados teniendo en cuenta los requisitos de seguridad y los requisitos de capacidad asociados a ellos, dando lugar a los requisitos finales para la espiral correspondiente.

- En la fase de definición tiene lugar el análisis, integración y armonización de los requisitos definidos en la fase anterior. En principio se obtiene una propuesta de especificación de la espiral que sirva a los afiliados para el desarrollo de capacidades, de manera que los afiliados además de establecer sus objetivos individuales para la correspondiente espiral puedan actualizar sus equipos y procesos, organizar su programación y presupuestación, verificar la interoperabilidad técnica, realizar validaciones operativas. La fase finaliza con la aprobación de la versión final de las especificaciones de la espiral FMN.

- La fase de diseño se centra en las distintas opciones de implementación de capacidades una vez que las CoI trabajan en las especificaciones finales. Los afiliados buscan soluciones óptimas para sus capacidades y para ello sus expertos desarrollan productos conforme a sus objetivos individuales y a la versión final de dicha espiral.

- La fase de implementación indica los pasos que tienen que realizar los afiliados para desarrollar las capacidades de acuerdo con los diseños de la fase anterior. Se trata de una fase de transición desde la definición de procesos hasta la entrega de las capacidades. En esta fase es donde se identifican posibles candidatos para la puesta en marcha de cada capacidad y el resultado final es la implementación de capacidades conforme a los criterios establecidos en la espiral.

- En la fase de integración los afiliados integran las capacidades que han creado o modificado en sus Líneas Base (*Baseline*), y también presentan solicitudes de cambios o actualizaciones del calendario previsto. Es el momento en el que los afiliados pueden presentar una solicitud de cambio para la Línea Base FMN basada en sus verificaciones y validaciones internas.

- La fase de verificación y validación se centra en garantizar la interoperabilidad, analizando los desarrollos en su contexto operativo. Los informes elaborados por el CIAV establecen la nueva Línea Base FMN y según ella se realiza la evaluación de los logros alcanzados por los afiliados en relación con la correspondiente espiral FMN (a nivel individual y colectivo).

- La fase de uso corresponde al uso operativo de capacidades desplegables, incluyendo procedimientos y personal capacitado durante la instanciación de la red de misión o MN. Durante esta fase de dos años se llevará a cabo la confirmación de que las capacidades de los afiliados están disponibles, tomando como referencia los informes de evaluación de preparación de FMN de los distintos eventos realizados.

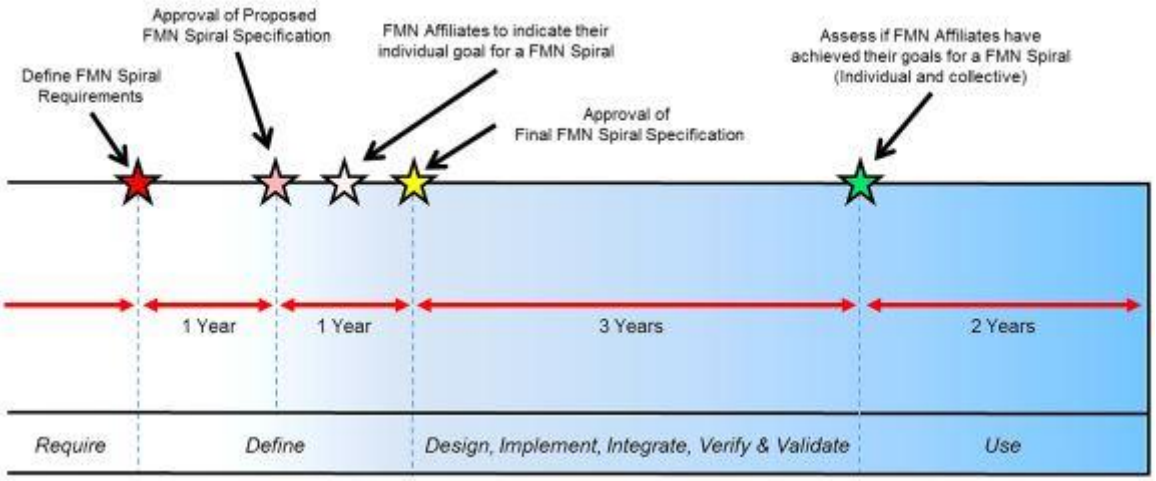

Figura 20. Ciclo de vida de una Espiral [41].

Un afiliado estará preparado a nivel FMN cuando tenga las capacidades técnicas y procedimentales validadas en un contexto operativo. El afiliado es capaz de federar servicios junto a otros participantes en una red de misión federada tal y como se indica en la espiral. Cada ciclo de vida de una espiral de FMN debe estar alineada con los procesos de planeamiento de la Defensa, con los programas de instrucción y adiestramiento de los afiliados y con el proceso de toma de decisiones para el desarrollo de capacidades. Como veremos más adelante la iniciativa FMN exige a los afiliados una gran implicación puesto que se desarrollan de forma simultánea hasta cuatro espirales.

Para representar gráficamente el ciclo de vida se emplea al Modelo en V de FMN[9] donde además del objetivo de cada fase se indica si las actividades del Marco FMN corresponden a un trabajo de grupo o bien a nivel individual realizado por cada afiliado [43].

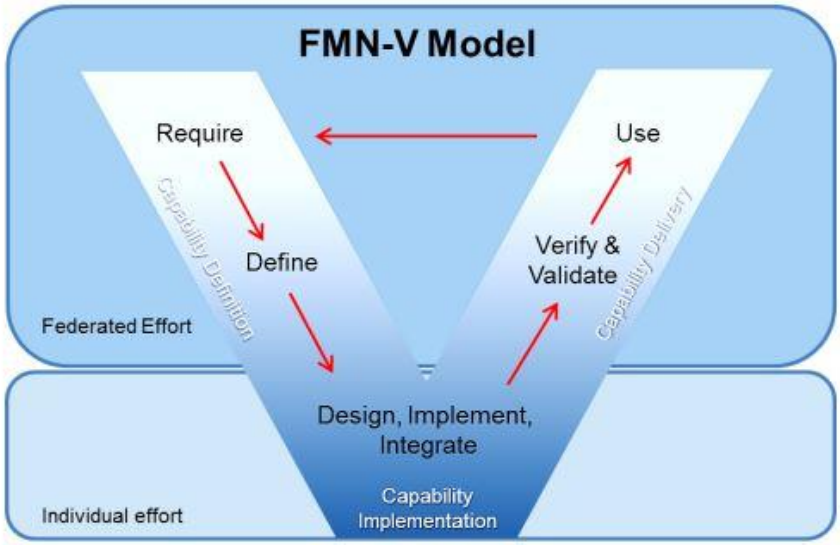

Figura 21. Modelo en V [41].

[9] El Modelo en V de FMN se basa en la ISO/IEC/IEEE 15288:2015, Sistema de Procesos de Ciclo de Vida y en el AAP-48, Sistema de Procesos para el Ciclo de Vida de OTAN.

Otro elemento que forma parte del Marco FMN es el Apoyo del Proceso Marco FMN a la instanciación de redes de misión. Para conseguir una red de misión federada es necesario que los afiliados que participen en ella establezcan los correspondientes acuerdos de gobernanza y de gestión. Al mismo tiempo, la MN se beneficia de todos los productos que se obtienen a lo largo del ciclo en V descrito.
.
Para la creación de la MN hay dos documentos especialmente importantes, la *Baseline* o Línea Base de la espiral y las instrucciones de incorporación, membresía y salida del Marco FMN (documento JMEI) que se actualizan de forma periódica. Estas referencias no solo impulsan la creación de MN, también optimizan los tiempos y mitigan los riesgos de implementación en la configuración de las capacidades de los afiliados. Estos productos serán desarrollados en la parte práctica que se centra en el papel de los afiliados y en cómo FMN potencia su eficacia operativa.

El Marco FMN favorece la identificación de deficiencias en la MN al contemplar no solo la preparación, operación y finalización de la red, sino que incorpora las lecciones aprendidas que sirven para retroalimentar el ciclo. Se trata de mantener todo el contacto posible entre el Marco FMN, los afiliados y la instancia o MN específica que se desarrolla.

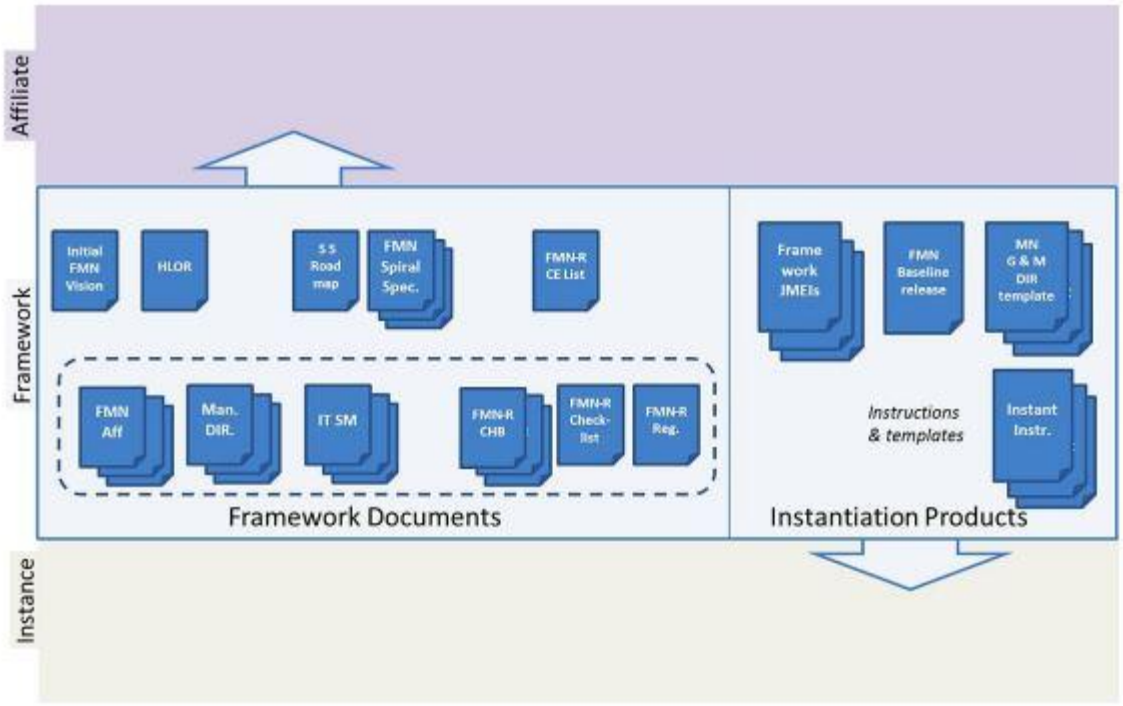

Figura 22. Interacción Marco, afiliados y MN [41].

La monitorización del MG es fundamental para identificar los cambios y adaptarse a las nuevas necesidades de FMN y de la OTAN. Mediante indicadores de desempeño que se definen en la Hoja de Ruta de la Gestión FMN se miden los resultados del Marco FMN en relación con sus objetivos y la visión FMN [44]. Los informes emitidos por el MG al MC contribuyen a evaluar el progreso de los afiliados y deben incluir no solo los riesgos actuales y potenciales de la iniciativa FMN sino también las correspondientes acciones de mitigación.

PRODUCTOS DEL MARCO FMN E INTERACCIÓN ENTRE LOS ORGANISMOS DE GESTIÓN				
FASE	**PRODUCTO**	**RESPONSABLE**	**APOYO**	**OBSERVACIONES**
	Visión FMN	Secretariado	WG	Según sea necesario
	Hoja de Ruta de la Gestión FMN	Secretariado	WG	Anual
REQUISITOS	**Hoja de Ruta de las Especificaciones de la Espiral**	CPWG	OC WG MCSMA WG	Anual
DEFINICIÓN	**Propuesta de Especificación de la Espiral**	CPWG	OC WG MCSMA WG CIAV WG	Para cada Espiral
DEFINICIÓN	**Especificación Final para la Espiral+**	CPWG	OC WG MCSMA WG CIAV WG	Para cada Espiral
DEFINICIÓN	**Objetivos de los afiliados para la Espiral**	Secretariado	Afiliados	Para cada Espiral
DEFINICIÓN	**Criterios de Preparación FMN**	Secretariado	CIC WG OC WG CIAV WG	Para cada Espiral
DISEÑO		Afiliados		Según sea necesario
IMPLEMENT.		Afiliados		Según sea necesario
INTEGRACIÓN	**Petición de cambios a la *Baseline***	Afiliados	CIAV WG CIC WG	Según sea necesario
VERIF. Y VALID.	**Informes AV&V**	CIAV WG	CIC WG OC WG	Según sea necesario
VERIF.Y VALID.	**Evaluación de la *Baseline***	CIC WG	CIAV WG	2 veces al año
USO	**JMEI**	CIC WG		Para cada Espiral
USO	**Instrucciones para la Instanciación**	Secretariado	WG	Para cada Espiral
USO	**Informe de valoración de la consecución de objetivos de la Espiral FMN**	CIC WG		Para cada Espiral
USO	**Informe final de valoración sobre la disponibilidad FMN**	Afiliados	Secretariado	Un informe por evento realizado

Tabla 2. Productos FMN [45].

Ya se han citado anteriormente dos herramientas que son fundamentales para la gestión del Marco FMN además de la visión de la iniciativa. Concretamente la Hoja de Ruta de Gestión y la Hoja de Ruta de Especificaciones de la Espiral. Como vemos en el cuadro resumen de productos desarrollados durante el ciclo de vida de la espiral, estos documentos están presentes desde el comienzo e implican a la mayoría de los organismos que forman parte de la estructura.

La Hoja de Ruta de Gestión o *Roadmap* de Gestión FMN, contribuye a mejorar la calidad y sincronización de las actividades del Proceso Marco anteriormente descrito. Permite a su vez que el MG disponga de una visión más completa del Marco FMN para su mejor supervisión y la posterior toma de decisiones. También es un documento útil para los afiliados y aspirantes a ingresar en FMN a la hora de preparar el desarrollo de capacidades y el resto de las actividades que se realizan en el Marco FMN [45].

El *Roadmap* de gestión se compone de tres elementos, el Ciclo de vida de la Espiral FMN, el Plan a 10 años para sincronizar y dirigir las actividades del Marco FMN y un Cronograma con los eventos principales para determinar las tareas y los plazos que permitan cumplir con los objetivos de la visión FMN. Para obtener la hoja de ruta vigente ha sido necesario sintetizar el NFIP (principalmente el volumen II que recoge los procesos en detalle) y actualizarlo teniendo en cuenta los resultados tras la revisión integral del Proceso Marco FMN. Una de las conclusiones fue la necesidad de modificar el ritmo de batalla de FMN y aumentar la fase de desarrollo e integración en un año más, lo cual quedó documentado en el Proceso Marco Optimizado (OFP) [46].

En el ciclo de vida de la espiral FMN se representan gráficamente las relaciones que mantienen el MG, la Secretaría, los distintos WG y los afiliados a lo largo del tiempo que dura cada espiral, desde su fase de requisitos hasta la fase de uso. El gráfico muestra los flujos de información, los intercambios de productos y los resultados previstos conforme a las actividades establecidas en el Marco FMN. Otro de los anexos del *Roadmap* de gestión FMN es el Plan a 10 años en el que como su propio nombre indica, se representan para cada una de las reuniones semestrales del MG, los productos clave que desarrollan cada uno de los WG, la tarea principal de la Secretaría en cada año del Plan, y en qué fase están los afiliados para cada una de las cinco espirales que hay en marcha simultáneamente.

El último anexo, el Cronograma, proporciona un plan a nivel estratégico donde se identifican hasta 6 fases (en el periodo de 2020 a 2030) que se sincronizan con los Hitos 1, 2 y 3 establecidos por la Alianza (a nivel de desarrollo de políticas, fuerzas y capacidades) y con las correspondientes espirales (desde la actual Espiral 4 hasta la 10). Para ello se identifican también una serie de condiciones decisivas que van jalonando el correspondiente gráfico hasta alcanzar los objetivos de la visión FMN.

La Hoja de Ruta de la Especificaciones de la Espiral FMN *(FMN Spiral Specification Roadmap)* es un documento que establece el desarrollo de capacidades operativas a diez años para la implementación de las espirales. Recordemos que este desarrollo es incremental y que cada espiral establece los pasos donde en un periodo de tiempo (cronograma) se alcanzan unos objetivos previamente definidos por los afiliados. De ahí la importancia del nivel de ambición (LoA o *Level of Ambition*) y la sincronización de todos los implicados a la hora de obtener unos resultados positivos en cada implementación [43].

Las espirales permiten a su vez adaptarse a posibles cambios sobrevenidos como consecuencia de nuevas necesidades operativas o misiones.

Fruto de la experiencia derivada de la red AMN implementada en la misión ISAF de Afganistán se establecieron los objetivos para la Espiral 1 FMN. En lugar de realizar un desarrollo de capacidades completo se trató de alinear los procesos y las configuraciones de los sistemas de los componentes de la red para conseguir federar el C2, la gestión de la información y del campo de batalla, los servicios *Core* (servicios fundamentales como el registro o la autenticación), la colaboración distribuida, las comunicaciones, la seguridad CIS y la gestión y el control de los servicios (SMC).

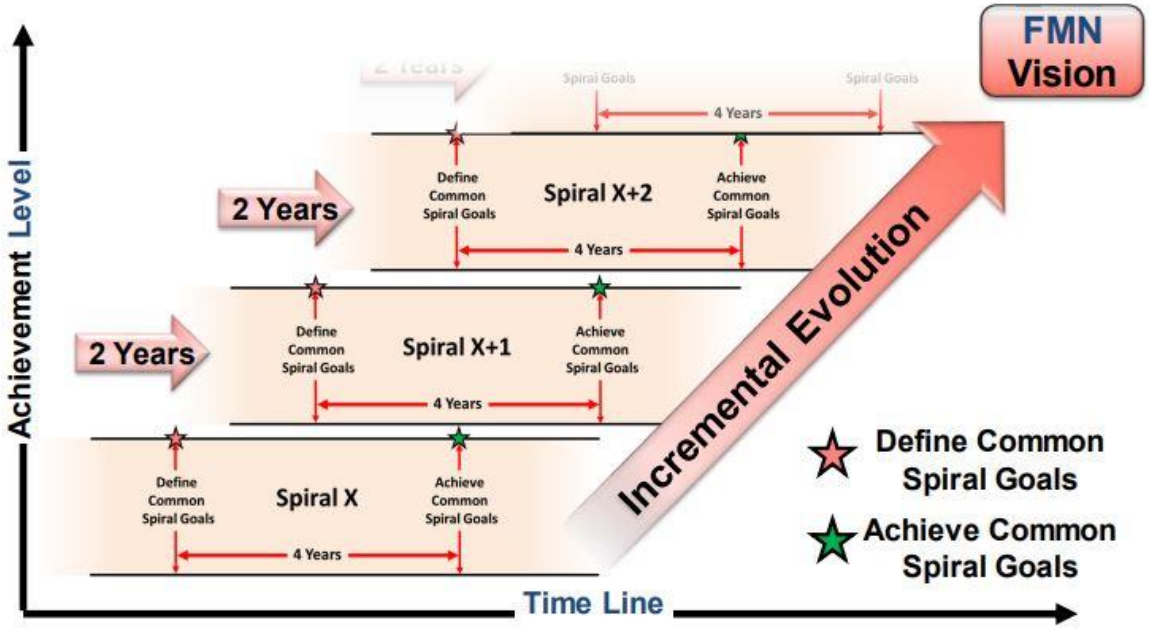

Figura 23. Evolución incremental [43].

La Espiral 2 incorporó nuevas actualizaciones que mejoraban las capacidades de la Espiral 1 y estableció además nuevas capacidades como la del conocimiento del entorno operativo en los diferentes dominios[10], la capacidad de la vigilancia e inteligencia conjunta o la mejora del SMC.

Además de actualizar las capacidades ya obtenidas en las anteriores espirales, la Espiral 3 pretendía avanzar hacia los Hitos 2 y 3 del NFIP de OTAN, es decir lograr una capacidad con una única infraestructura para todas las redes de misión desplegadas y para sus correspondientes niveles de seguridad. Se establecía como objetivo el implementar el concepto *Protected Core Networking* (PCN) que permite un acoplamiento entre los dominios de información y la infraestructura de transporte para la prestación de servicios de alta disponibilidad [47] [48].

El concepto y la visión FMN establecen los objetivos estratégicos que sirven de punto de partida para la definición de los requisitos operativos de las redes de misión federadas por parte del OCWG. A la hora de traducir esas necesidades operativas en unos requisitos específicos para una CoI, se obtienen las denominadas *Swimlanes*[11]. La división en líneas de acción facilita la colaboración de los distintos grupos de trabajo, permite identificar posibles obstáculos y aclarar responsabilidades durante el proceso. Cada espiral tiene unos objetivos que sirven de guía para las *Swimlanes* y para todo el personal implicado en el desarrollo de capacidades, desde el personal que forma parte de las unidades operativas hasta los expertos técnicos [49].

[10] *Common Operational Picture* o COP formada por *Recognized Environmental Picture* o REP, *Recognized Maritime Picture* o RMP, *Recognized Land Picture* o RLP y *Recognized Air Picture* o RAP.
[11] El término procede de los diagramas de flujo de procesos donde visualmente (como las calles de una piscina olímpica) se distinguen las tareas y responsabilidades de cada subproceso de un proceso de negocio.

Los objetivos que se establecen en cada espiral tienen un efecto directo en la mejora de capacidades (*Capability Enhancements* o CPE) del Modelo en V de FMN. Los CPE son importantes porque transforman los requisitos operativos elaborados por el OCWG en mejoras de carácter técnico y a nivel de procedimientos.

El CPWG, encargado de su elaboración, juega un papel armonizador para garantizar el cumplimiento de la interoperabilidad en sus tres dimensiones, teniendo en cuenta también los requisitos de seguridad.

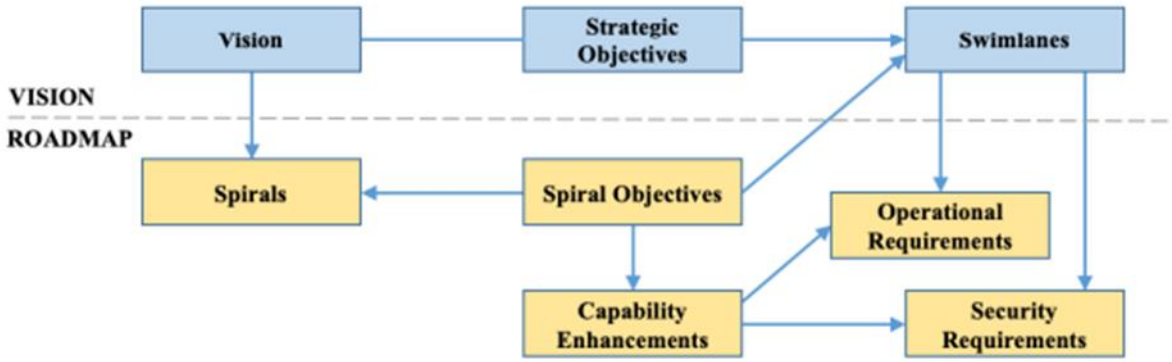

Figura 24. Visión de *Swimlanes* [43].

Los requisitos de seguridad detallan las medidas de seguridad CIS que se deben implementar en las redes de misión y son elaboradas por el MCSMA WG, incorporando toda la información técnica necesaria para garantizar la seguridad de los servicios correspondientes a cada espiral. Los requisitos de seguridad tienen un carácter transversal por lo que es importante que el personal que se dedica a ellos esté en contacto directo y de forma periódica con los responsables de la definición de requisitos operativos y CPE.

En cuanto al documento de especificaciones de la espiral, recoge las Instrucciones de Procedimiento (PI) e Instrucciones de Servicio (SI) donde el personal técnico describe de forma detallada las actividades a realizar por los afiliados FMN para federarse con el resto de los participantes en las tres dimensiones que abarca la interoperabilidad. El documento, elaborado por el CPWG, incorpora otros anexos de carácter técnico relacionados con la arquitectura y estándares FMN. En su elaboración también participan el resto de los grupos de trabajo, incluido el CIAV.

State	Spiral 1	Spiral 2	Spiral 3	Spiral 4	Spiral 5	Spiral 6	Spiral 7	Spiral 8
Operational and Security Requirements	---	---	Mar 2017	Nov 2018	Nov 2020	Nov 2022	Nov 2024	Nov 2026
Proposed Specifications	---	May 2017	Apr 2018	Apr 2019	Nov 2021	Nov 2023	Nov 2025	Nov 2027
Final Specifications	Apr 2015	Nov 2017	Nov 2018	Nov 2020	Nov 2022	Nov 2024	Nov 2026	Nov 2028
Emerging operational use	2016	2018	2021	2023	2025	2027	2029	2031
Preferred operational use	2017-2018	2019-2021	2022-2023	2024-2025	2026-2027	2028-2029	2030-2031	2032-2033

Tabla 3. Marco temporal [43].

4 PARTE PRÁCTICA DEL TFM: IMPACTO DE FMN EN LAS REDES DE MISIÓN DE LOS AFILIADOS

4.1 España como afiliado en FMN

Nuestro país cuenta con una larga experiencia en el ámbito de FMN puesto que logró federar una red de misión nacional (AMN-ESP) en la misión de ISAF. En el año 2016 solicitó de manera formal incorporarse a la estructura FMN aliada como afiliado[12], lo que implica el compromiso de seguir sus normas y estándares cuando se despliegue una red de misión, ya sea en operaciones o ejercicios. En aquel año SACEUR solicitaba a los afiliados que adoptasen las medidas necesarias para cumplir con los requisitos de la Espiral 1, aprovechando los ejercicios de certificación *Steadfast Cobalt* que realizaban las unidades de la eNRF[13].

Desde que España expresó entonces su intención de afiliarse a FMN como MNE (*Mission Network Element*) no ha dejado de adquirir conocimientos gracias a más ejercicios (como por ejemplo la serie *Trident Juncture*), lo que obligó a la creación de las estructuras FMN nacionales[14] en el MINISDEF con responsabilidades en los diferentes ámbitos que afectan a la iniciativa FMN.

La estructura FMN nacional está formada por los organismos del MINISDEF que tienen responsabilidades en alguno de los ámbitos que afectan a los requisitos, es decir a la gestión, a los medios o al adiestramiento FMN. Dicha estructura, que debe estar coordinada con la estructura aliada para garantizar la coherencia y sincronización entre las actividades y productos obtenidos, se compone del Comité FMN, la Oficina FMN-ESP, sus grupos de trabajo y el Laboratorio FMN-ESP.

El Comité FMN dirige, coordina y controla todas las actividades para la implementación de la capacidad FMN en las Fuerzas Armadas, en coordinación con las estructuras aliadas. Para planear y coordinar dicha implementación cuenta con la Oficina FMN-ESP como órgano de apoyo. Para facilitar todo el proceso, España cuenta con varios grupos de trabajo:

- Un grupo de trabajo de organización, coordinación e implementación que realiza el seguimiento y coordina todas las actividades que realizan el resto de los grupos. También realiza la gestión de riesgos y de los asuntos relacionados con el proceso de afiliación.
- El grupo de trabajo de operaciones garantiza la coherencia entre los requisitos operativos que establece la estructura aliada y la priorización de las capacidades FMN nacionales para su empleo en operaciones. Está involucrado en la definición y desarrollo de los *Mission Threads* (MT) que se implementan posteriormente en operaciones y ejercicios, con un enfoque más orientado en los requisitos de intercambio de información y en la obtención de la interoperabilidad conjunta. Su presidente es el representante en el OCWG de la estructura FMN aliada.
- El grupo de trabajo de definición define como su nombre indica los aspectos técnicos necesarios para el desarrollo de arquitecturas, servicios y productos FMN. También realiza las acciones oportunas para alinear las especificaciones técnicas de la espiral FMN con las configuraciones técnicas y los estándares de interoperabilidad nacionales. Su presidente es el representante nacional en el CPWG de la estructura FMN aliada.

[12] Carta del JEMACON para la afiliación de España a FMN, de 3 de febrero de 2016.
[13] OTAN notificó la confirmación parcial de la capacidad FMN nacional a través de la participación en el ejercicio STCO.
[14] Guía Estructura FMN-ESP. EMAD. Mayo 2015.

- El grupo de trabajo de obtención, tras compilar los requisitos operativos, técnicos y de seguridad, los transmite a los órganos responsables de la definición, obtención y evaluación de los sistemas de C2 que se podrían emplear en una red de misión federada. Además de la definición de los servicios FMN y de mantener el catálogo nacional de capacidades, se encarga de la identificación de posibles desviaciones respecto de los requisitos iniciales y de la gestión de cambios para su resolución. Su presidente es el representante en el CICWG de la estructura FMN aliada.
- El grupo de trabajo de validación y verificación efectúa el seguimiento para asegurar que la capacidad FMN nacional se ajusta a los requisitos. Su presidente es el representante en el CIAVWG de la estructura FMN aliada.
- Finalmente, el grupo de trabajo de seguridad es el responsable de la definición de los requisitos de seguridad de los componentes de la capacidad FMN. A su vez se encarga de comunicar los requisitos, estándares y procedimientos necesarios a los organismos nacionales de acreditación de seguridad de los sistemas CIS y al grupo de trabajo de obtención para la coordinación global de todos los requisitos. Su presidente es el representante en el MCSMAWG de la estructura FMN aliada.

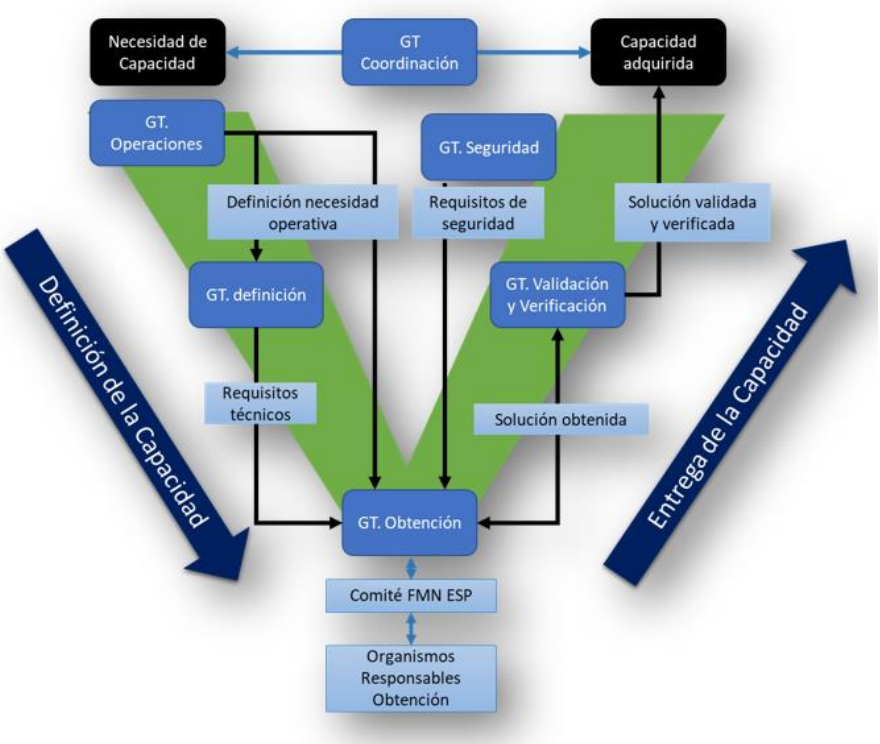

Figura 25. Modelo en V, FMN-ESP [37].

Al igual que ocurre en la estructura aliada, las relaciones entre los diferentes grupos de trabajo se definen siguiendo el Modelo en V donde se parte de una necesidad operativa, se define la capacidad, se entrega la capacidad para las correspondientes pruebas y una vez validada y verificada se considera como adquirida conforme a FMN.

Los requisitos que han sido desarrollados por los grupos de trabajo de operación y definición, con la colaboración del grupo de seguridad, serán entregados al grupo de obtención para que identifique los sistemas en los que es necesario implantar los requisitos FMN y se encargue de su seguimiento, informando al Comité FMN de la evolución y de los cambios que se hayan acordado.

Para realizar las validaciones y verificaciones, el grupo de trabajo responsable se apoya en el Laboratorio FMN-ESP conectado a la red internacional de laboratorios CV2E (*Coalition Verification and Validation*

Environment). El Laboratorio puede comprobar y certificar la interoperabilidad nacional y OTAN antes de un ejercicio o misión, verificando el cumplimiento de los requisitos operativos y de seguridad.

Uno de los objetivos de España como afiliado para la implantación FMN es la redacción, difusión, actualización y custodia de la doctrina FMN. Las publicaciones nacionales se estructuran en tres niveles:

- Nivel 1 o máximo nivel, donde encontramos la doctrina FMN nacional y la Línea Base nacional dirigida por el EMAD.
- Nivel 2, donde se incluye el Plan de Acción FMN-ESP y es dirigido por el MCCE.
- Nivel 3, en el que se elaboran el resto de los documentos, desde instrucciones técnicas a procedimientos u otros trabajos realizados por los Grupos de trabajo de la estructura nacional. Los presidentes de los distintos grupos son los encargados de la dirección de su elaboración.

El procedimiento general para la elaboración de esta documentación comienza con la detección de una necesidad operativa por parte de cualquiera de los organismos implicados. Una vez evaluada la situación por los miembros del grupo correspondiente se elaborará una propuesta para que se apruebe por el EMAD. El siguiente paso será la asignación de responsabilidades a los diferentes elementos de la estructura (Comité, Laboratorio, Oficina, WG) para la elaboración del documento. Finalmente se tramitará por parte del responsable y en coordinación con el grupo de trabajo que lidera el proyecto la propuesta de validación final para la aprobación del órgano de gobierno FMN-ESP (EMAD).

4.2 El papel de los afiliados en el Proceso Marco FMN

El objetivo de los integrantes de la iniciativa FMN, como sabemos, es el empleo del Marco FMN para que los afiliados puedan desarrollar sus capacidades y poder operar conectados en un red de misión federada desde el primer día del despliegue con el máximo nivel de interoperabilidad.

Tras la propuesta de las especificaciones de la espiral los afiliados disponen de información sobre los posibles riesgos de cara a la fase de desarrollo de capacidades y pueden decidir su nivel de ambición para dicha espiral. Una vez aprobada la versión final de las especificaciones de la espiral[15] en desarrollo, los afiliados cuentan con dicho documento como referencia para sincronizar todos los procesos que permiten la evolución y disponibilidad de las capacidades FMN.

La Línea Base FMN está formada por los diferentes elementos de configuración (*Configuration Elements* o CI)[16] de las capacidades CIS y de comunicaciones que han sido aprobadas por los afiliados para el entorno FMN. Este producto permite disponer de una instantánea actualizada de las capacidades disponibles, para evaluar el grado de cumplimiento para el alistamiento FMN[17] de los afiliados en función de las especificaciones de la espiral y del nivel de ambición declarado.

La mejora incremental en la que se basan las espirales se puede apreciar en el aumento de capacidades FMN disponibles para los participantes en la instanciación de redes, incluyendo requisitos mínimos según el tipo de afiliado (A, B, C según se pretenda proporcionar una MNE, una MNX o simplemente ser un participante, capacidades para uso común de todos los integrantes de la MN o capacidades iniciales para empleo individual).

[15] En noviembre de 2023 el *Management Group* en su reunión número 16 celebrada en Mons (Bélgica) ha aprobado las especificaciones para la Espiral 5.
[16] Un CI o elemento de configuración es cualquier componente que necesita ser administrado para brindar un servicio de TI
[17] *FMN-Readiness Criteria Checklist*, abarcan requisitos técnicos, de procedimientos y operativos. Se extraen de las especificaciones de la Espiral FMN correspondiente y también de los procedimientos y plantillas acordados para instanciar una red de misión (MN).

El grupo de trabajo CICWG tiene entre sus responsabilidades la definición y mantenimiento de la gestión de servicios de las redes de misión y establecer el marco para la arquitectura de los servicios IT. Respecto a esta arquitectura, el CICWG establece un repositorio denominado arquitectura *As is* donde los afiliados pueden hacer sus contribuciones para mejorarla [50].

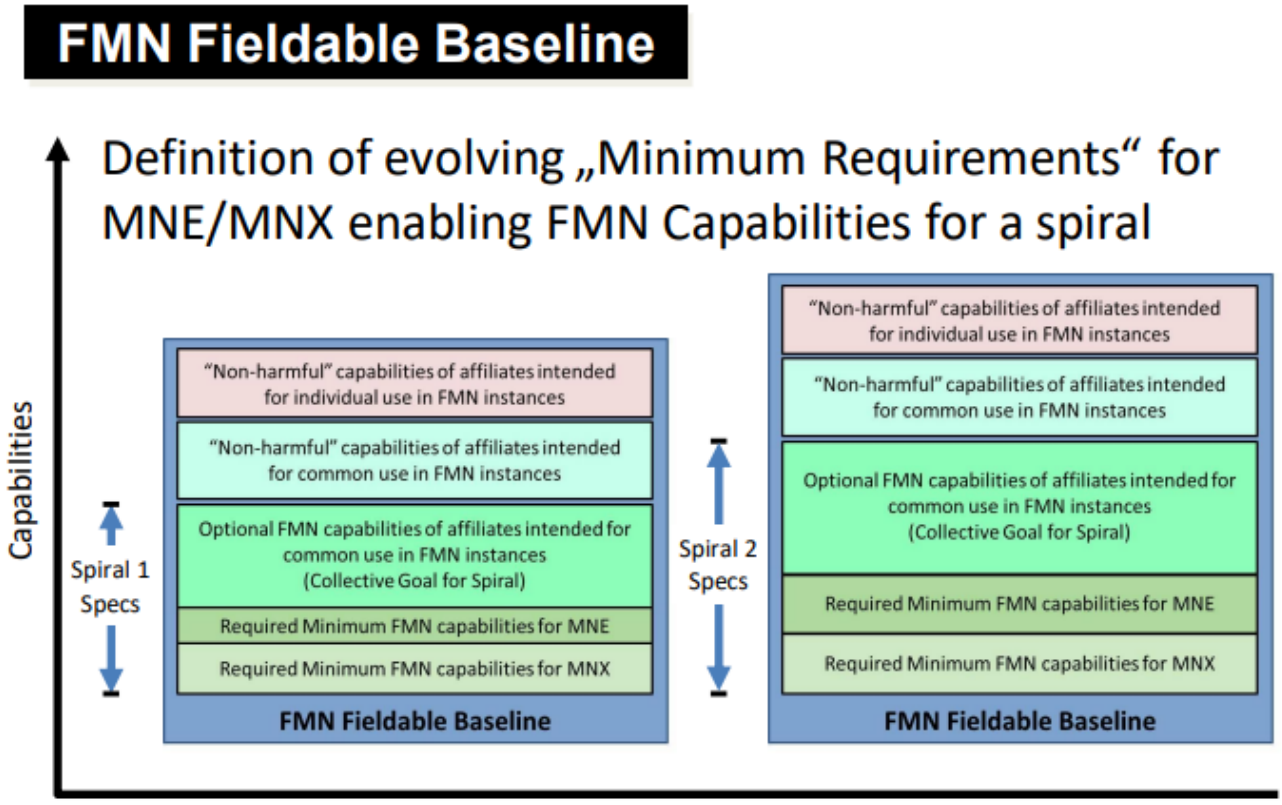

Figura 26. Mejora incremental de capacidades [51].

Otra de sus misiones es la gestión y mantenimiento de la Línea Base FMN y de las instrucciones para la incorporación, membresía y salida del marco FMN (documento JMEI). El CICWG identifica y valora también posibles riesgos durante las fases de implantación de la espiral y apoya a los afiliados para que puedan alinearse de forma completa de cara a su confirmación como *FMN-Readiness*.

El Proceso Marco FMN, a través del CICWG, facilita la participación de los afiliados a la hora de proponer cambios a la Línea Base de la espiral, lo que mejora la operatividad en el entorno FMN. La gestión de cambios asegura que los métodos, procesos y procedimientos estándar empleados para cualquier cambio se llevan a cabo de forma eficiente y buscando un equilibrio entre la mejora planteada y el riesgo asociado a dicho cambio.

Un cambio es cualquier modificación que afecta al CI y que puede tener un impacto en los servicios CIS. El afiliado que considera que hay que realizar algún cambio eleva una solicitud formal denominada *Request for Change* o RFC con los detalles del cambio propuesto para el CI de la *Baseline* [51].

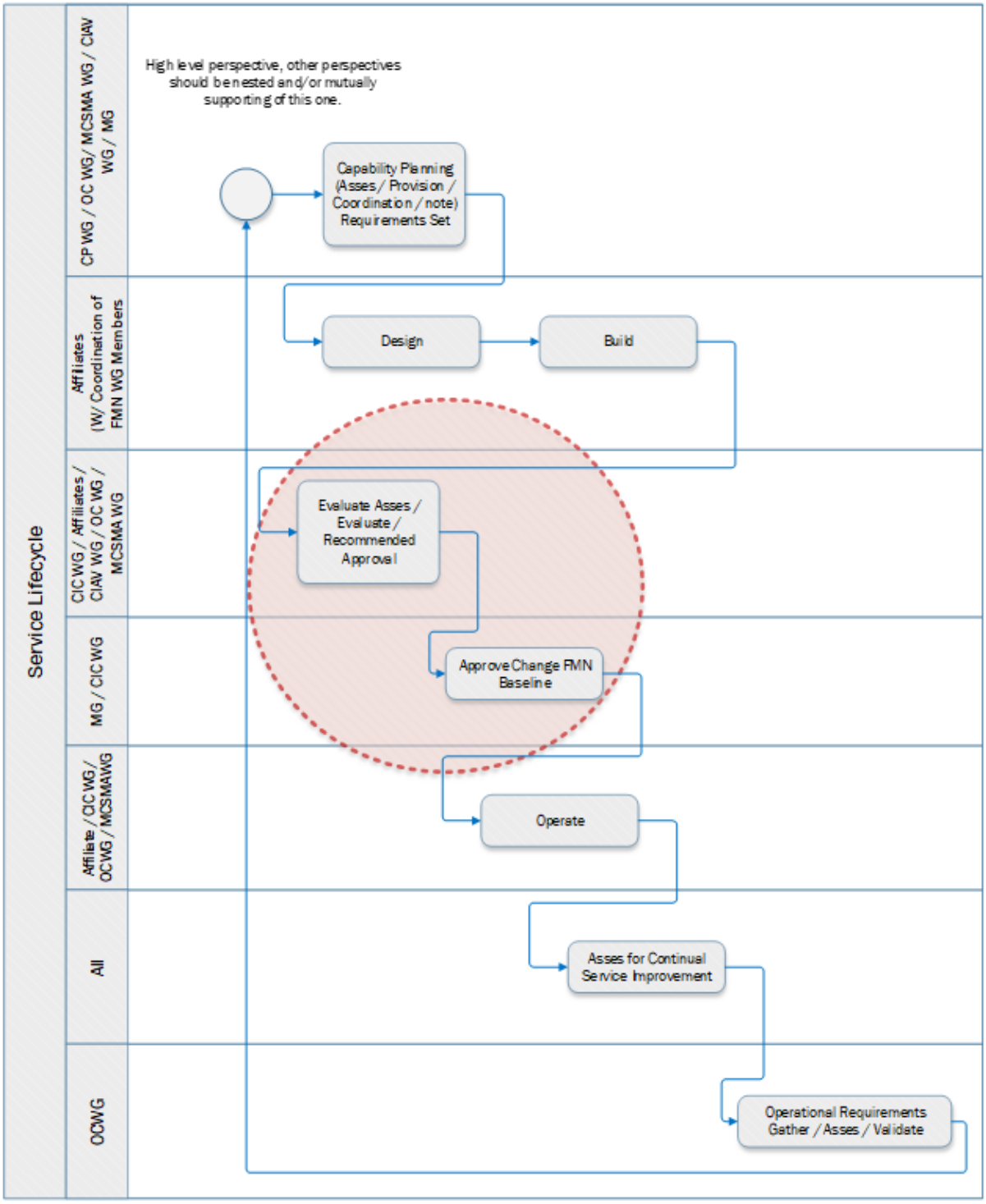

Figura 27. Ciclo de vida de los servicios y afiliados [51].

Pero ¿qué proceso sigue la propuesta de solicitud de cambio o RFC que traslada un afiliado al CIC?
En primer lugar, el CIC se encarga de revisar que la propuesta es correcta desde el punto de vista técnico y si fuera necesario solicita al afiliado información adicional (RFI). Antes de que se realice la reunión para la aprobación oficial de los cambios en el *Change Advisory Board* o CAB (foro donde se reúnen los representantes de los afiliados y los expertos de los grupos de trabajo CIC y CIAV), la solicitud podría ser revisada por el CIAV que se encargaría de valorar el impacto del cambio y el análisis de riesgos y determinar si es necesario realizar algún test de validación y verificación previo. En caso positivo y tras

la realización de las pruebas correspondientes, CIAV emitiría un informe adjunto a la RFC con el resultado correspondiente.

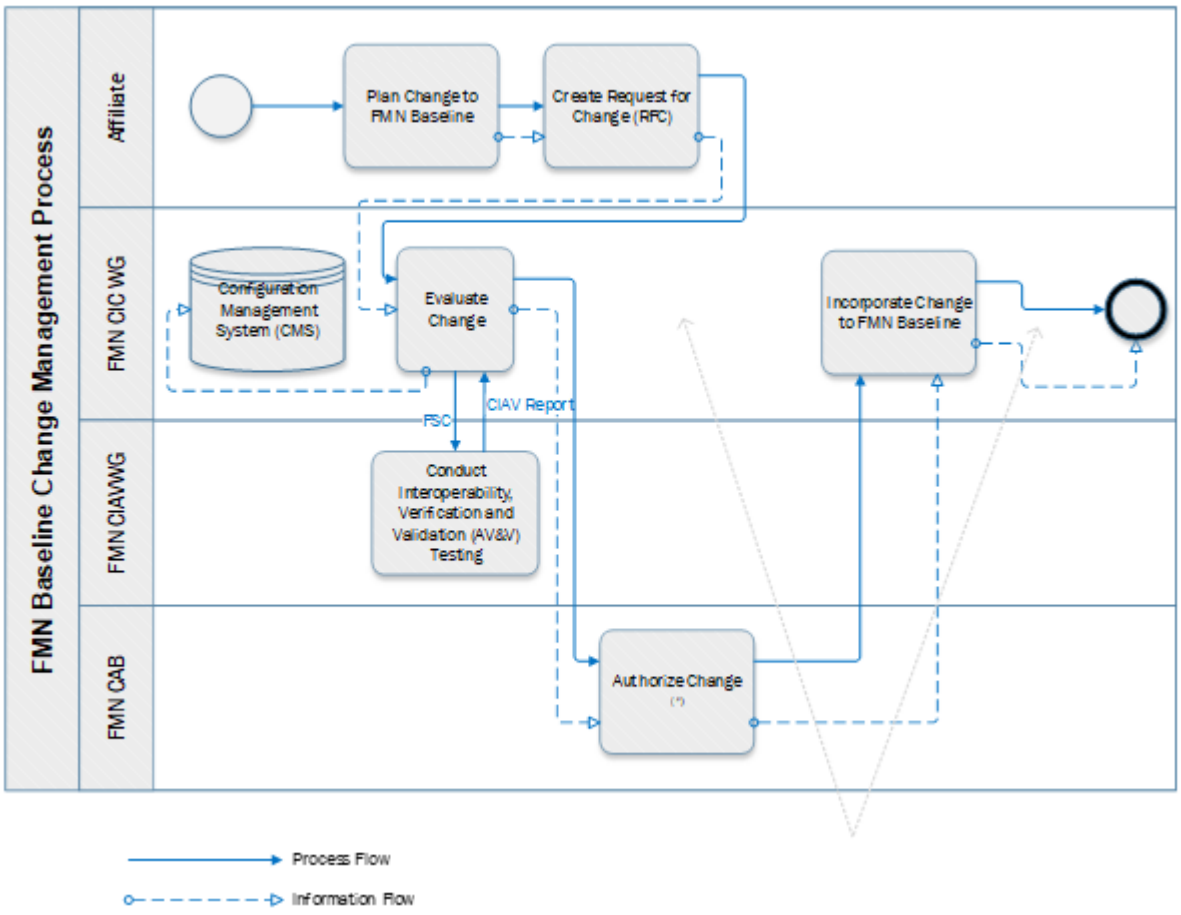

Figura 28. Gestión de cambios [51].

Durante la reunión del CAB, si la RFC no cumple con los requisitos para su inclusión en la *Baseline* será rechazada para que el afiliado la vuelva a plantear o bien la cancele por no ser viable. En el caso de que todos los participantes en el proceso de gestión de cambios hayan dado su visto bueno, la RFC consigue el estatus de aprobada por el CAB y se puede incluir en la Línea Base FMN [51].

En el año 2021 el *Management Group* aprobó una actualización de las instrucciones de incorporación, afiliación y salida para la *Mission Network* (JMEI de MN). Contienen un "conjunto de publicaciones que brindan orientación sobre gobernanza y gestión, procedimientos, servicios, infraestructuras y atributos de datos necesarios para que las MN proporcionen un entorno operativo para que los participantes de la misión puedan compartir información de forma segura y confiable". Es una documentación muy importante para los afiliados porque trata todas las fases del ciclo de vida de la MN, desde que se establecen los requisitos operacionales hasta las instrucciones para la creación de la MN, con el objetivo final de proporcionar orientación, plantilla y formularios para la planificación, implementación y operación de la MN.

Por lo tanto, la JMEI *Baseline* 3.0 recomienda a los participantes de las redes de misión las tácticas, técnicas y procedimientos (TTP) para la federación de sus redes nacionales. Dicha referencia sirve para el establecimiento, operación y mantenimiento de la MN al proporcionar instrucciones técnicas y plantillas de configuración que describen la arquitectura y el nivel mínimo de interoperabilidad de los

servicios de la red. Precisamente el objetivo final de la MN es conectar servicios para intercambiar información [49].

El documento JMEI puede emplearse a nivel estratégico, operacional y táctico, junto a otros documentos operativos como la doctrina conjunta aliada (AJP-6) o la doctrina nacional. Consta de cuatro volúmenes, el primero sobre el proceso de incorporación, el segundo sobre la membresía, el tercer volumen trata sobre el proceso de salida y el cuarto contiene instrucciones técnicas. No es posible describir en este TFM sobre la iniciativa FMN todos y cada uno de los aspectos que abarca el documento si bien haremos una breve reseña de algunos de los formularios que contienen los diferentes volúmenes.

El primero de ellos, el de incorporación a FMN, tiene dos anexos de los cuales el primero es una lista de verificación de configuración de la MN y el segundo contiene diferentes formularios para el proceso de incorporación. Entre ellos podemos destacar la plantilla de carta de adhesión a la MN, la declaración de cumplimiento (*Statement of Compliance*, SoC) de MN o el formulario de aprobación para operar MN (documento final de autorización o ATO). El volumen sobre membresía contiene seis anexos, destacando el primero de ellos que trata sobre el contexto operativo y proporciona una hoja de ruta estratégica, un plan de acción y los requisitos mínimos para los servicios FMN. El resto de los anexos detallan la arquitectura de la MN, la gestión y operación de servicios (catálogo, cambios, implementación, IKM) y finalmente uno sobre requisitos de seguridad de la comunidad FMN (CSRS).[18]

El tercer volumen dedicado al proceso de salida detalla una lista de verificación para la desconexión de la MN e incluye un apéndice sobre el mantenimiento del registro operativo de la MN. El último volumen está dedicado a las instrucciones técnicas para los diferentes servicios (de comunicaciones, audio y vídeo, DNS, DTS, certificados digitales, autenticación web, mensajería, enlace de datos, información geoespacial, etc.).

Figura 29. Proceso de obtención [49].

Tal y como vemos la iniciativa FMN proporciona a los afiliados todo tipo de referencias detalladas tanto a nivel operativo como a nivel técnico lo que sirve a cualquier componente que participa en la

[18] *Community Security Requirements Statements*.

instanciación de redes de misión, desde personal dedicado al planeamiento hasta expertos en desarrollo de arquitecturas.

Otro ejemplo del apoyo de la iniciativa FMN al planeamiento operativo de los afiliados es el anexo de configuración de los CIS de la MN. Alineado con la directiva de planeamiento (COPD) de ACO, el documento detalla los procesos CIS para el despliegue, empleo, operación y protección de las redes de misión federadas. Partiendo de la premisa de que la configuración de los CIS es una responsabilidad nacional, este anexo se desarrolla por un grupo de expertos o grupo de planeamiento CIS que trabaja de forma coordinada con el resto de los grupos que planean la MN.

Se trata de un planeamiento cooperativo a nivel operacional donde en cada fase hay una contribución de los CIS para la federación de las redes de misión. En la fase de desarrollo del plan operacional, desde la obtención del CONOPS hasta la obtención del OPLAN, el Grupo CIS proporciona varios documentos tomando referencias como por ejemplo la JMEI *Baseline* 3.0.

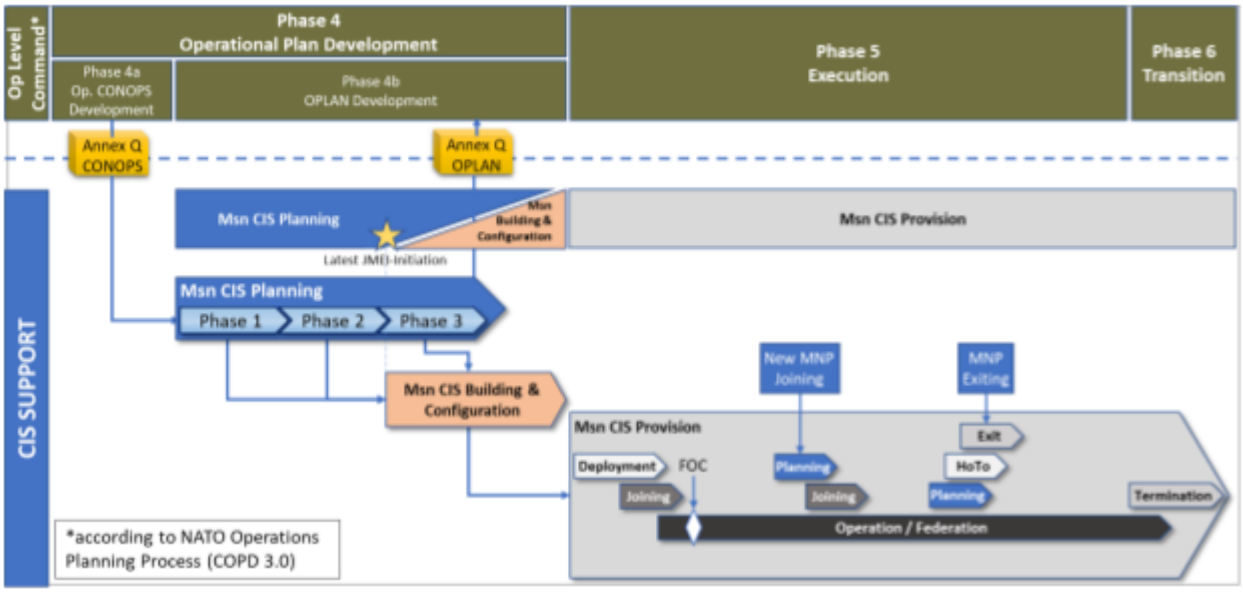

Figura 30. Contribución FMN a planeamiento [49].

En el caso de que no exista un grupo de planeamiento CIS permanente, durante las fases 3 y 4 del COPD es necesario establecer una estructura CIS que coordine con el resto de los grupos el planeamiento de las redes de misión. Lo ideal sería que hubiera representantes de los distintos componentes de la MN en cada grupo, no obstante, lo que sí se cumple es que la J6 es la que lidera el *CIS Planning Group* a nivel operacional.

Además de un secretariado para apoyar al grupo directivo y coordinar las tareas de planeamiento, se establecen varios grupos de trabajo. Hay un grupo de coordinación que se encarga de que el planeamiento sea coherente con los objetivos del Mando y de proporcionar las capacidades operativas que se requieren en la *Joint Operational Area* (JOA) de la coalición. Su principal contribución al grupo de planeamiento CIS es el ATO para la operación de la MN.
Otras contribuciones destacadas de estos grupos son el desarrollo de requisitos de intercambio de información (*Information Exchange Requirements* o IER), la definición de indicadores para las pruebas de AV&V, la definición de los indicadores para los procesos de gestión de servicios y control (SMC) y los volúmenes I, II y III de la JMEI, el volumen IV de la JMEI así como la valoración de riesgos (*Security Risk Assessment* o SRA), la declaración de cumplimiento (SoC) y los procesos de acreditación para la red.

4.3 La participación de los afiliados en la implantación de la Espiral 3 de FMN.

Como ya se expuso al hablar de la Hoja de Ruta de la Especificación de la Espiral, las espirales mejoran las redes de misión de forma incremental mediante actualizaciones de las capacidades ya implementadas y añadiendo otras nuevas. Para respaldar el desarrollo de arquitecturas, la definición de requisitos y la planificación de capacidades de la OTAN, el empleo de la taxonomía C3 tiene un carácter muy relevante. La versión 7.0 de la taxonomía C3 incluye la mejora de productos publicados con anterioridad, como la taxonomía de servicios de Comunidad de Interés (CoI), servicios de comunicaciones, servicios básicos, productos de información o aplicaciones de usuario, así como nuevos productos como la taxonomía de capacidades y la de datos C3.

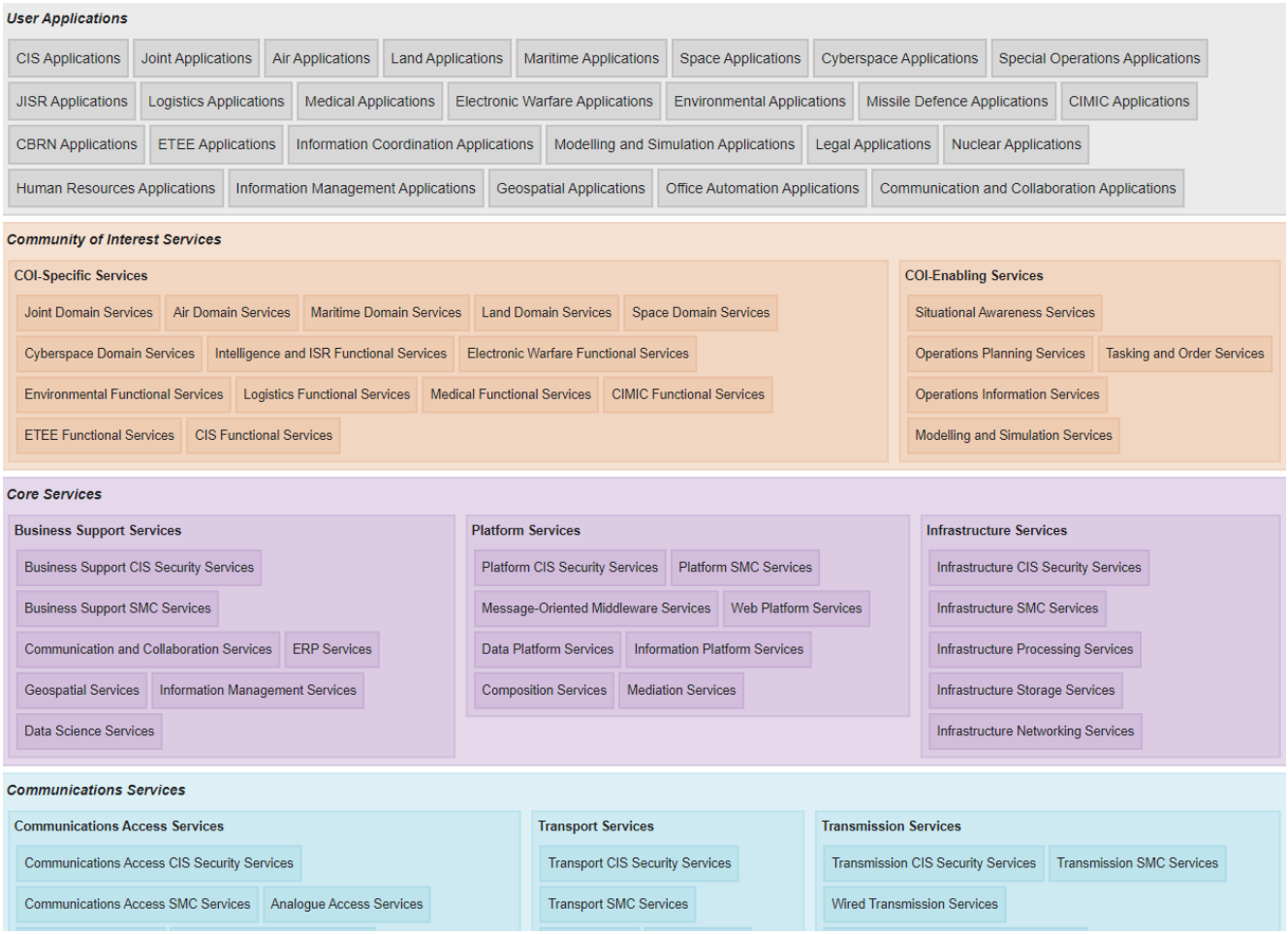

Figura 31. Tipos de servicios y aplicaciones [50].

La taxonomía de los servicios básicos o *Core Services* representa aquellos servicios principales que proporcionan las funcionalidades técnicas para que las capacidades comunes y genéricas no tengan que ser implementadas por aplicaciones individuales u otros servicios (servicios de soporte empresarial, servicios de plataforma y servicios de infraestructura). La taxonomía de servicios de comunicaciones o *Communication Services* representa un conjunto de servicios técnicos centrados en la interconexión de sistemas y mecanismos para la transmisión de datos conforme a los parámetros de calidad establecidos. Se distinguen tres categorías principales, servicios de acceso a las comunicaciones, servicios de transporte y servicios de transmisión.

Los servicios CoI representan un conjunto de servicios técnicos proporcionados a los CIS, centrados en uno o varios grupos colaborativos de usuarios, con objetivos, intereses o misiones compartidos. Están orientados principalmente a respaldar las aplicaciones de los usuarios y el consumo de servicios y se distinguen dos categorías, los servicios específicos CoI y los de habilitación. Los primeros son los que corresponden a los servicios funcionales o *Functional Services* que proporcionan funcionalidades a los usuarios en apoyo a ejercicios y operaciones. Por otra parte, los de habilitación son similares a los servicios básicos en su función de proporcionar elementos que sirven para el desarrollo de los servicios de dominio específicos, pero se diferencian de los *Core Services* en que no proporcionan capacidades genéricas, sino que están orientadas a procesos C3 y servicios específicos para un determinado grupo o CoI.

Actualmente la Espiral 3 FMN se encuentra en su fase de empleo operativo por parte de los afiliados, incorporando mejoras en los servicios esenciales, de comunicaciones y los servicios CoI. Esto permite a los afiliados que despliegan una red de misión federada disponer de sistemas CIS con las mismas funcionalidades que tienen en sus entornos nacionales, lo que redunda en una mayor interoperabilidad para todos los miembros de la coalición. Concretamente se ha conseguido optimizar el C2 incorporando nuevas funcionalidades para el intercambio de información en los distintos dominios y en el ámbito ISR o de inteligencia [48].

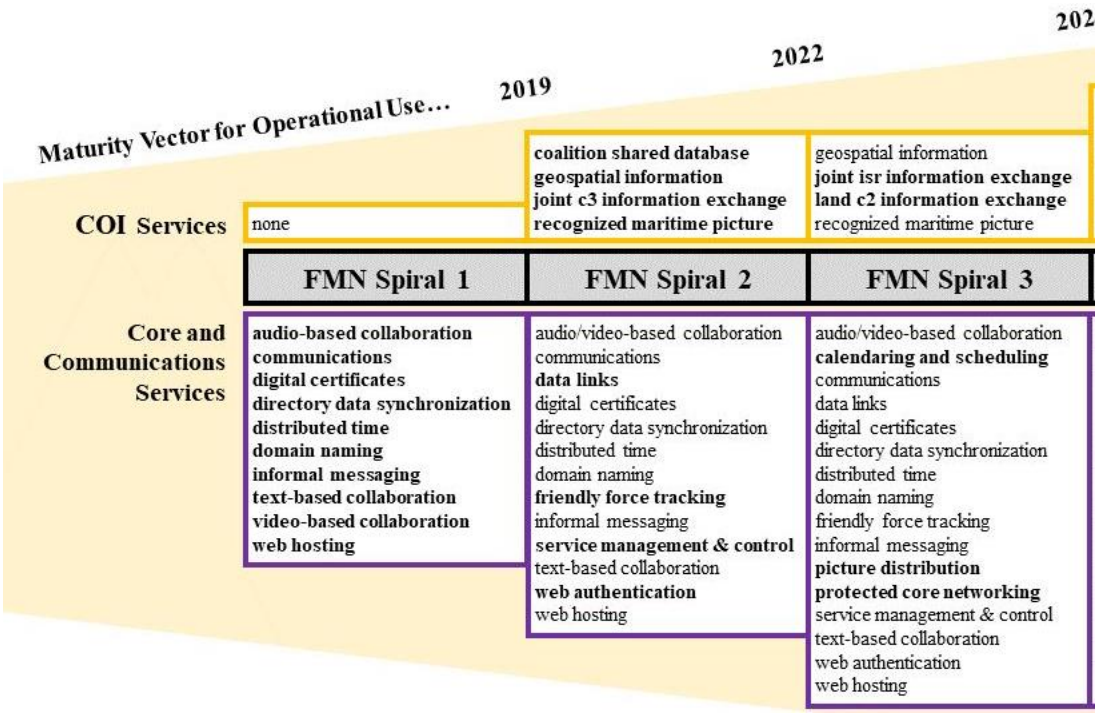

Figura 32. Evolución de las espirales de FMN [48].

Tras la aprobación de las especificaciones de la Espiral 3 en el año 2018, se han ido implementando las instrucciones de servicio (SI) y procedimentales (PI) en los sistemas de C2 de las redes de misión federadas. Entre las primeras y como más destacadas podemos señalar las SI de *Data Link*, *Domain Network Service*, *Friendly Force Tracking* o FFT, chat, certificados digitales o mensajería. Entre las procedimentales o PI destacan las de seguridad CIS, gestión de la información, gestión y control de servicios o colaboración distribuida [47].

La labor de FMN en apoyo a los afiliados sirve para mejorar la implementación de las redes de misión en los diferentes ejercicios. Tanto el Secretariado FMN como los diferentes grupos de trabajo proporcionan la documentación de referencia elaborada por personal experto procedente de todas las naciones

participantes. Su apoyo durante el proceso de gestión de cambios contribuye a reducir las diferencias entre la *Baseline* y los objetivos individuales propuestos para la instanciación de redes de misión. La colaboración del CICWG y del CIAVWG con los expertos nacionales en la preparación de los ejercicios es fundamental para conseguir un resultado óptimo. En cualquier caso, el éxito de la iniciativa FMN descansa en la implicación de los afiliados durante todas las etapas del ciclo de desarrollo e implementación de las espirales.

El proceso de gestión de cambios a la *Baseline* ha ido evolucionando de manera que los afiliados dispongan de más información y capacidad para interactuar con los organismos responsables de su dirección y coordinación. La tendencia reciente respecto a la participación de los afiliados FMN en el proceso de cambios en la Espiral 3 es positiva puesto que la contribución respecto a las espirales anteriores ha ido aumentando, situándose hoy día en un 63% (24 afiliados de los 38 que pertenecen a la iniciativa). Se puede apreciar que hay un aumento de RFC aprobadas entre la celebración de las últimas dos reuniones del *Management Group* o MG.

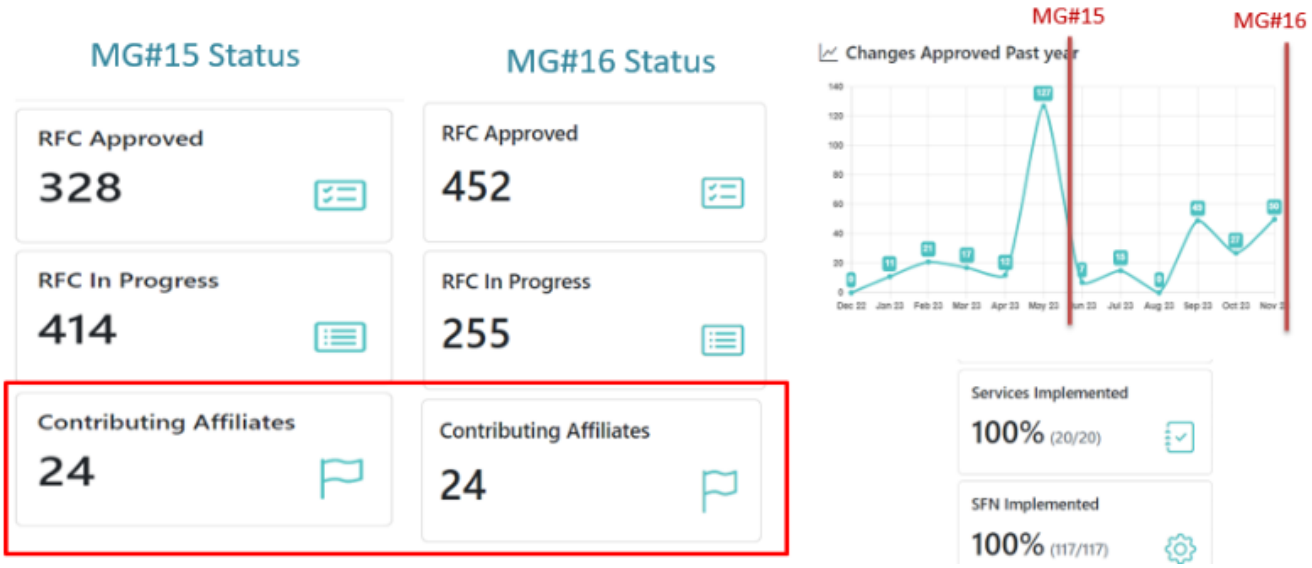

Figura 33. Evolución proceso gestión de cambios [51].

Los servicios donde ha habido un mayor aumento de RFC aprobadas son principalmente los de colaboración basada en audio y video, los de tiempo distribuido, de mensajería informal y de web hosting. Al mismo tiempo se ha agilizado el proceso y se ha conseguido que el número de RFC en fase de estudio haya disminuido. A finales del 2023 se ha constatado que la implicación de los afiliados en la implementación de productos de la FMN *Baseline* ha ido en aumento para todos los servicios, en la inmensa mayoría de ellos se ha duplicado el número de participantes.

Podemos destacar los servicios de comunicaciones, los de autenticación web y el esfuerzo colectivo realizado para alcanzar los objetivos de *Protected Core Networking* o PCN. La mayor implicación la vienen realizando los países afiliados en la opción A (MNE) mientras que el 75% de los países que han optado por la opción C no han participado en el proceso de gestión de cambios.

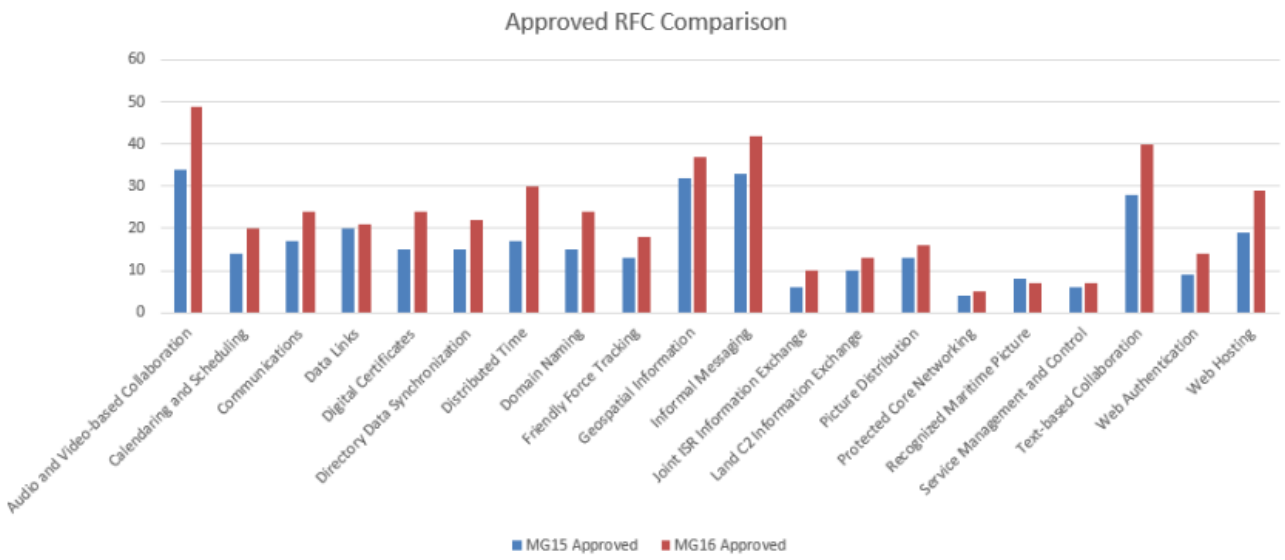

Figura 34. RFC aprobadas en MG 15/16 por servicios [52].

Aunque ha habido una mejora notable en la participación de los afiliados desde el comienzo de la iniciativa FMN, los datos estadísticos señalan que el número medio de participantes en la implementación de un servicio es de 12, siendo el servicio de colaboración basado en texto en el que han participado un mayor número de ellos (un total de 20).

Existen diferentes eventos propuestos por el ACT de OTAN para fomentar la interoperabilidad, uno de ellos es el *TIDE Sprint*[19], punto de encuentro del ámbito militar, académico y de la industria para el desarrollo de conceptos, requisitos y especificaciones de interoperabilidad. De carácter bianual, la fortaleza de TIDE reside en su poder de convocatoria para reunir durante una semana a un elevado número de expertos. En su última edición de otoño de 2022 se puso el foco en la gestión del espacio de batalla multidominio, la transformación digital y la seguridad centrada en el dato (DCS). Pero de los diez temas de la agenda, uno fue la verificación y validación de interoperabilidad y otro las redes de misión federadas (FMN), lo que pone de manifiesto la relevancia de la mejora de la interoperabilidad para la OTAN y sus miembros.

Otro de los eventos que forma parte de la iniciativa *Interoperability Continuum* de OTAN es el *TIDE Hackathon*. Surge de la necesidad de agilizar los procesos de transformación y adquisición de la Alianza en un entorno complejo y muy dinámico. Los *TIDE Hackathon* promueven soluciones innovadoras que tengan en cuenta el impacto de las tecnologías emergentes y disruptivas en la interoperabilidad. El objetivo de este evento que involucra a grupos de expertos en un entorno altamente competitivo es "demostrar cómo las EDT (tecnologías disruptivas y emergentes) pueden mejorar la interoperabilidad multidominio entre los sistemas de C2 de una red de misión"[20].

Pero sin lugar a duda el ejercicio más importante en el ámbito de la interoperabilidad es el ejercicio CWIX (Exploración, experimentación y evaluación de interoperabilidad de la Coalición), aprobado por el MC de OTAN y enfocado al ámbito técnico y operativo. Tiene como objetivo probar y mejorar la interoperabilidad de los sistemas C4ISR nacionales y de la Alianza, con especial atención a los desplegados en NRF y estructuras similares. La dirección y gestión de CWIX corresponde a ACT, pero la ejecución se realiza en varias sedes nacionales de forma simultánea que comparten una red de pruebas

[19] *Think-Tank for Information Decision and Execution*.
[20] https://www.act.nato.int/our-work/exercises/coalition-warrior-interoperability-exercise/

común[21]. La principal sede donde se ejecuta el ejercicio CWIX es el Centro de Entrenamiento de Fuerza Conjunta (*Joint Force Training Centre* o JFTC) de Bydgoszcz (Polonia).

Los ejercicios CWIX permiten a las naciones experimentar, probar y eliminar riesgos de sus sistemas desplegables antes de llevar a cabo sus misiones. Por un lado, contribuyen a la mejora del C2 antes de los ejercicios *Steadfast Cobalt* y *Trident Juncture*, por ejemplo, a conseguir la interoperabilidad entre las radios tácticas móviles de las fuerzas desplegadas. CWIX aborda igualmente la interoperabilidad de los procedimientos a emplear en las capacidades presentes y futuras. Las pruebas sirven para reducir los tiempos de despliegue, minimizar posibles errores y también para fomentar la innovación de los participantes, con propuestas alternativas que incorporan tecnologías emergentes. Se trata por tanto de contribuir al objetivo de la OTAN de mantener su ventaja estratégica.

Events / Schedule		CWIX ESC	TIDE Sprint Fall	CWIX IPC	CWIX MPC	TIDE Hackathon	CWIX FCC	TIDE Sprint Spring	CWIX Execution
2024	Date	19-22 Sep 23		14-17 Nov 23	23-26 Jan 24	19-23 Feb 24	9-12 Apr 24	18-22 Mar 24	3-21 Jun 24
	Location	Prague, CZE		Thessaloniki, GRE	Odense, DNK	Place TBD, NDL	Bydgoszcz, POL	Dresden, DEU	Bydgoszcz, POL
2025	Date	17-20 Sep 24	Date TBD	12-15 Nov 24	28-31 Jan 25	24-28 Feb 25	18-21 Mar 25	07-11 Apr 25	2-20 Jun 25
	Location	Place TBD, NOR	Virginia Beach, USA	Place TBD, ROM	Slagelse, DNK	Location TBD	Bydgoszcz, POL	Location TBD	Bydgoszcz, POL
2026	Date	16-19 Sep 25	Date TBD	11-14 Nov 25	27-30 Jan 26	23-27 Feb 26	17-20 Mar 26	13-17 Apr 26	8-26 Jun 26
	Location	Place TBD, NLD	Virginia Beach, USA	Place TBD, CZE	Location TBD	Location TBD	Bydgoszcz, POL	Location TBD	Bydgoszcz, POL
2027	Date	Date TBD	Date TBD	Date TBD	Date TBD	Date TBD	Date TBD	Date TBD	Date TBD
	Location	Location TBD	Virginia Beach, USA	Location TBD	Location TBD	Location TBD	Location TBD	Location TBD	Location TBD

Tabla 4. Calendario *Interoperability Continuum* [43].

En el caso particular de España y dentro de los objetivos del Plan de Acción FMN-ESP, el EMAD es responsable de evaluar la disponibilidad operativa de las unidades y el grado de alistamiento (*FMN-Readiness*) de los Ejércitos y de la Armada. Con este fin se realiza el ejercicio V2CN FMN (Ejercicio de Verificación, Validación y Confirmación Nacional) con el que se comprueba el cumplimiento de los requisitos técnicos, operativos y la capacidad FMN de España. En sus inicios el ejercicio se centró en el adiestramiento técnico de los participantes (ha contado con la participación de personal de Portugal) y ha ido evolucionando con el objetivo de permitir una ejecución remota y la participación de otros afiliados FMN, convirtiéndose así de forma oficial en un ejercicio de confirmación de capacidades FMN.

El ejercicio V2CN se realiza antes del ejercicio *Steadfast Cobalt* (ejercicio de ACO) y del ejercicio CWIX (ejercicio de ACT) y sirve de preparación para la participación de nuestras unidades en los ejercicios de certificación de OTAN y también como foro de conocimiento para la implementación de servicios y obtención de lecciones aprendidas. España participa en los ejercicios CWIX a través de sus unidades militares y también a través del mundo empresarial. Así por ejemplo en el año 2021 estuvo presente con

[21] Red clasificada *Combined Federated Battle-Lab* (CFBL)

la instalación y operación de un nodo[22] desde la Base de Retamares (Madrid)[23], en el que se realizaron varios test a los diferentes servicios FMN de la espiral en uso. O más recientemente, durante el pasado mes de junio de 2023, la empresa RFE participó en dos áreas del ejercicio CWIX23. Por un lado, en el área de las comunicaciones, con una solución denominada GESCOMET VCS para la gestión de las comunicaciones del programa Dragon 8X8 de España. Por otro lado, en el área de la simulación, con una propuesta para las comunicaciones tácticas de los simuladores de carros de combate *Steel Beast* y VBS4, que también integra la simulación en gafas de realidad aumentada[24].

Como resultado de la participación y mejora obtenida en los diferentes ejercicios, sobre todo en CWIX, los diferentes participantes obtienen un grado de disponibilidad FMN. En la siguiente tabla se puede apreciar en la columna de la izquierda un listado con algunos de los servicios que implementa la Espiral 3 y el resto de las columnas hacia la derecha corresponden al porcentaje en el que el afiliado (se han suprimido las nacionalidades a las que corresponde cada columna con el porcentaje por servicios) ha completado el proceso de validación y verificación establecido en FMN en cada servicio. El nivel alcanzado refleja el resultado obtenido por el afiliado en los test FMN de CIAVWG y en los ejercicios CWIX. Aquellos productos que consiguen estar al 100 por 100 serán incluidos posteriormente en la FMN *Baseline*.

	SP3	SP3	SP3	SP3	SP3	SP3
Audio and Video-based Collaboration	0 %	0 %	43 %	0 %	100 %	25 %
Calendaring and Scheduling		0 %	75 %	0 %	100 %	0 %
Communications	0 %	0 %	100 %	0 %	100 %	100 %
Data Links	0 %	100 %	0 %	75 %	80 %	0 %
Digital Certificates	0 %	0 %	75 %	0 %	0 %	89 %
Directory Data Synchronization	0 %	0 %	0 %	0 %	100 %	50 %
Distributed Time	0 %	0 %	100 %	0 %	33 %	67 %
Domain Naming	100 %	86 %	0 %	0 %	0 %	75 %
Friendly Force Tracking	0 %	0 %	100 %	57 %	57 %	0 %
Geospatial Information	100 %	0 %	0 %	67 %	100 %	100 %
Informal Messaging	0 %	0 %	60 %	0 %	100 %	100 %
Joint ISR Information Exchange	100 %	0 %		0 %	0 %	100 %
Land C2 Information Exchange	0 %	0 %	30 %	80 %	85 %	0 %
Picture Distribution	0 %	0 %		100 %	100 %	0 %
Protected Core Networking		0 %	0 %	0 %		100 %
Recognized Maritime Picture	0 %			100 %	0 %	0 %
Service Management and Control		0 %	100 %	0 %	100 %	
Text-based Collaboration	57 %	29 %	100 %	43 %	29 %	0 %
Web Authentication	0 %	100 %	100 %	0 %	0 %	0 %
Web Hosting	75 %	0 %	100 %	0 %	0 %	100 %

Tabla 5. Implementación de la Espiral 3 FMN en países opción A [48].

En estos momentos el número de participantes en la iniciativa FMN es de 38, incluyendo a la Alianza como un afiliado más. Hay 16 miembros de la opción A (MNE, como España) de los cuales uno de ellos no es todavía miembro de la OTAN (Suecia). Seis países son de la opción B (MNX) de los cuales uno de ellos no es miembro de la OTAN (Austria). A la opción C corresponden dieciséis países de los que cuatro no son naciones OTAN (Australia, Irlanda, Nueva Zelanda y Suiza). Ucrania, Moldavia, Georgia y Azerbaiyán tienen el estatus de país observador junto a otras entidades y organismos como el Estado

[22] ESP ARMY SC2NET - FMN CS

[23]https://ejercito.defensa.gob.es/unidades/Valencia/rt21/Noticias/2021/El_Regimiento_de_Transmisiones_21_avanza_en_la_interoperabilidad_ejercicio_CWIX21.html

[24] https://club.camaramadrid.es/rfe-ejercicios-otan-cwix2023/

Mayor de la Unión Europea (EUMS). Aquellos países que cuenten con un espónsor pueden iniciar su solicitud para afiliarse a la iniciativa FMN tal y como han hecho recientemente Japón o Corea del Sur de la mano de los Estados Unidos. De los 38 afiliados a FMN, un total de 25 contribuyen aportando oficiales de enlace al Secretariado FMN, lo cual refuerza la plantilla permanente.

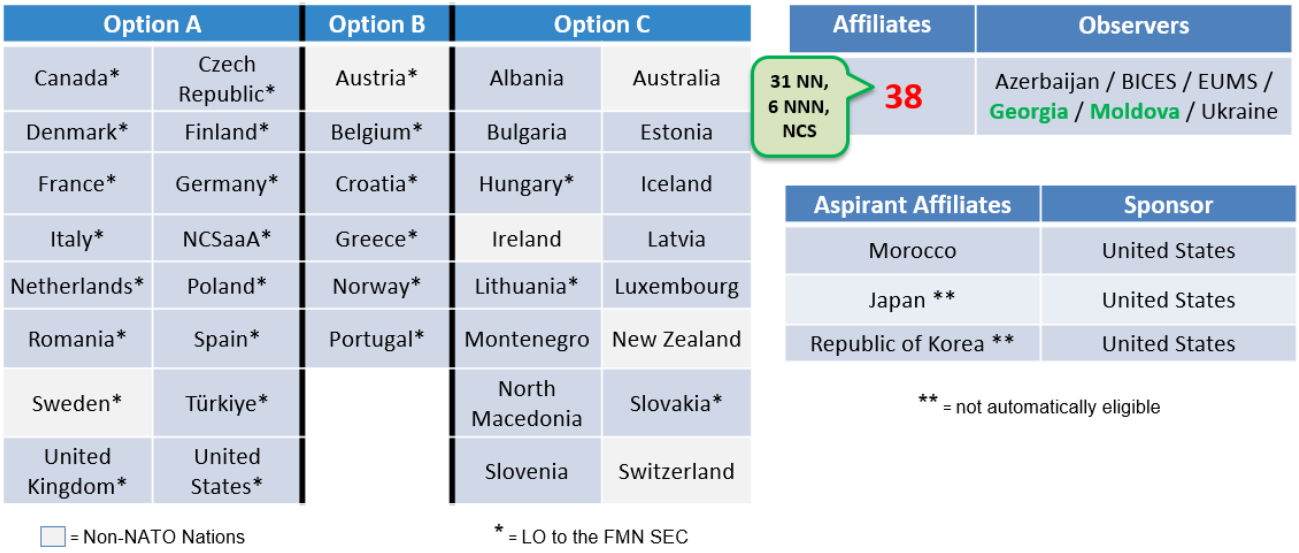

Figura 35. Distribución de los afiliados a FMN por opciones [60].

4.4 Contribución de las futuras espirales a la eficacia operativa de los afiliados

La actividad de los afiliados no se detiene durante la fase de empleo de la Espiral 3 en el despliegue de redes de misión federadas. Como se ha comentado de forma simultánea la iniciativa FMN está desarrollando nuevas especificaciones para las futuras espirales y otras se encuentran en plena revisión para conseguir obtener la versión definitiva. En el caso concreto de la Espiral 4, los afiliados se encuentran trabajando en sus procesos nacionales de adquisición y solicitud de cambio. Además, la comunidad FMN ha decidido adelantar la fase de empleo y durante el año 2024 se desplegarán redes de misión en Espiral 4, de ahí la importancia de que los afiliados realicen una buena revisión de sus objetivos individuales y aprovechar los resultados obtenidos en los ejercicios realizados.

Entre los objetivos de la Espiral 4 FMN se encuentra la mejora de la interoperabilidad del servicio de habilitación de CoI, proporcionando a la federación la capacidad de compartir información y aumentar la conciencia situacional (SA) entre los diferentes dominios (por ejemplo, con la mejora de la información geográfica del *Tactical Data Link* marítimo y aéreo). Se mejora igualmente la ciberseguridad con nuevos requisitos técnicos para un mayor número de servicios y también la gestión de riesgos de la seguridad de los CIS, mediante la compartición de información y procedimientos optimizados para la acreditación de las redes [52].

En cuanto a la interoperabilidad del servicio específico de CoI, en el ámbito terrestre, se mejora la respuesta de los CIS tácticos multinacionales con ayuda de la estandarización técnica de productos de información. A nivel táctico, desde las unidades tipo brigada hasta pelotón, se implementan requisitos para el intercambio de información de unidades en movimiento que permitan el C2 eficaz. También se mejora el intercambio de información para el mando y control marítimo [53].

La Espiral 4 incorpora nuevas actualizaciones de las capacidades ya presentes en la Espiral 3 (FFT, PCN, SMC) y establece otras nuevas como la de distribución superpuesta[25] para las redes. En general se producen mejoras en los servicios para el C2 y gestión del espacio de batalla (por ejemplo, en el desarrollo de la simbología), en el proceso de *targeting* conjunto, en la gestión de la información y en la definición de procesos e intercambio de productos de inteligencia, apoyo sanitario y CIMIC (cooperación cívico-militar).

El número de instrucciones de servicio (SI) ha ido aumentando en cada espiral (20, 23 y 26 en las espirales 3, 4 y 5 respectivamente). La validación técnica de las SI se realiza en los eventos organizados por el grupo de trabajo CIAV de FMN. La validación operativa de las especificaciones FMN (*Procedural Instructions* o PI) se realiza en ejercicios con escenario operativo, como el JC2A organizado por CIAV y sobre todo en el ejercicio CWIX.

Service Instructions (SI) - Espirales FMN		
Spiral 3	**Spiral 4**	**Spiral 5**
COI-Specific		
		Air C2 Information Exchange
		Fires Information Exchange
Joint ISR Information Exchange	Joint ISR Information Exchange	Joint ISR Information Exchange
Land C2 Information Exchange	Land C2 Information Exchange	Land C2 Information Exchange
	Land Tactical C2 Information Exchange	Land Tactical C2 Information Exchange
Recognized Maritime Picture	Maritime C2 Information Exchange	Maritime C2 Information Exchange
COI-Enabling		
Data Links	Data Links	Data Links
Friendly Force Tracking	Friendly Force Tracking	Friendly Force Tracking
	Ground-to-Air Information Exchange	Ground-to-Air Information Exchange
Picture Distribution	Overlay Distribution	Overlay Distribution
Core Services		
Audio and Video-based Collaboration	Audio and Video-based Collaboration	Audio and Video-based Collaboration
Calendaring and Scheduling	Calendaring and Scheduling	Calendaring and Scheduling
Digital Certificates	Digital Certificates	Digital Certificates
Directory Data Synchronization	Directory Data Synchronization	Directory Data Synchronization
Distributed Time	Distributed Time	Distributed Time
Domain Naming	Domain Naming	Domain Naming
Geospatial Information	Geospatial Information	Geospatial Information
Informal Messaging	Informal Messaging	Informal Messaging
Service Management and Control	Service Management and Control	Service Management and Control
Text-based Collaboration	Text-based Collaboration	Text-based Collaboration
	Virtualized Processing	Virtualized Processing
Web Authentication	Web Authentication	Web Authentication
Web Hosting	Web Hosting	Web Hosting
Communications		
Communications	Communications	Communications
		Communications Transport
Protected Core Networking	Protected Core Networking	Protected Core Networking
20	**23**	**26**

Tabla 6. Incremento de Servicios [43].

Cada año y con suficiente antelación el Secretariado FMN recibe diferentes propuestas de apoyo procedentes de los afiliados para el despliegue de las redes de misión. Durante el año 2024 seguirá un calendario para la implementación y prueba de los nuevos servicios aprovechando diferentes ejercicios o despliegues de las unidades alistadas para las diferentes estructuras operativas. Concretamente se prevé

[25] *Overlay distribution*, en la arquitectura genérica de C2, es una infraestructura de comunicaciones que permite la conectividad y la compartición de información entre los nodos de la red.

dar apoyo al planeamiento y ejecución de los ejercicios *Federated Cloud* y *Steadfast Cobalt* y a los despliegues de NRF o eFP (*Enhanced Forward Presence*) entre otros [54].

Durante el año 2024 los afiliados trabajarán para mitigar las carencias de la Espiral 5 y poder incorporar sus objetivos individuales. El objetivo principal de la Espiral 5 es completar las capacidades de la Espiral 4 para alcanzar el Hito 2 de interoperabilidad, para lo cual se han desarrollado 71 capacidades distribuidas en servicios *Core* genéricos (12), servicios *Core* de habilitación (25), de comunicaciones (10), y servicios federados para las CoI (24). Estando previsto su fase de empleo operativo en misiones y ejercicios a partir de 2028, la Espiral 5 contiene también en sus especificaciones mejoras para dar los primeros pasos en la implantación de la estrategia de seguridad centrada en el dato. Sin perder de vista el objetivo de compartir información procedente de todos los dominios para el planeamiento y preparación de actividades, el esfuerzo se centra en evolucionar desde el concepto de seguridad en la red a la seguridad en el dato [55].

El Hito 3 de interoperabilidad FMN está previsto para el año 2030 con la Espiral 6, cuyo objetivo es que los afiliados puedan desplegar y operar redes de misión centradas en el dato (*Data Centric*). La previsión es que solo algunos afiliados estarán en condiciones de implementar esta capacidad debido a la entidad y complejidad de los cambios propuestos. Esto supondrá un mayor esfuerzo a la hora de disponer de una red federada operativa y segura que de soporte a las funciones de combate que realizan todos los afiliados. La futura red de misión será más dinámica en cuanto al tratamiento de los datos y requerirá el establecimiento de un entorno más seguro mediante el control de accesos y de identidad.

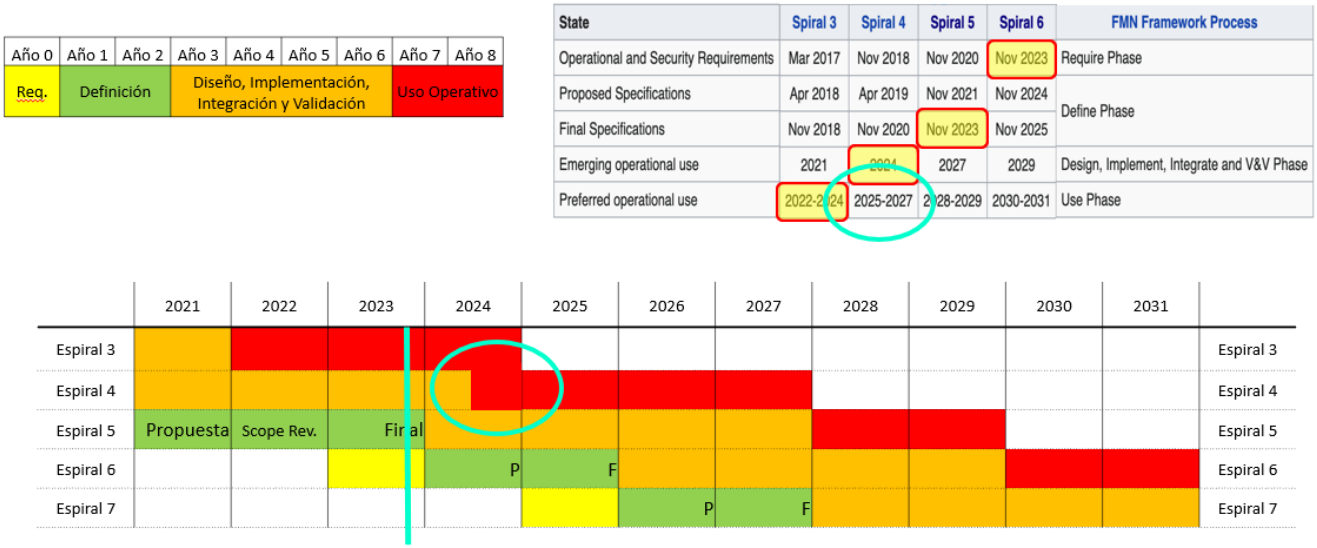

Tabla 7. Calendario para Espirales FMN [43].

Como parte de la mejora de capacidades que requieren las MDO y de cara a poder contribuir a la implantación del Hito 3, durante el año 2024 los afiliados trabajarán en la revisión de las especificaciones de la Espiral 6. Los grupos de trabajo FMN nacionales propondrán soluciones operativas para implementar la seguridad de la tecnología 5G o potenciar el empleo de las comunicaciones HF con nuevos servicios y protocolos. La iniciativa FMN contribuye en todo momento a la consecución de los objetivos de la espiral, entre los que se encuentran la planificación logística de las operaciones, el desarrollo de un entorno que permita el intercambio de información eficaz en las operaciones tierra-aire, la adecuación de los servicios de gestión y control a las nuevas redes, el apoyo para explotar las capacidades del dominio espacial que tienen algunos afiliados y potenciar el uso compartido de la información con participación de entidades civiles [56].

Si bien el calendario para las Espirales 7 y 8 está definido, los objetivos de estas espirales no lo están aún. En línea con las últimas propuestas ya en marcha, el futuro de las redes de misión federadas seguirá basado en la política de *Zero Trust*, es decir, poder contrarrestar las amenazas externas e internas asumiendo que siempre hay riesgos en la red. Se trata de garantizar el intercambio y la seguridad de los datos procedentes de aplicaciones, servicios y redes en cualquier situación (cuando se almacenan, se explotan o se transfieren). A su vez, la iniciativa FMN contribuye a mejorar las capacidades que requieren las operaciones multidominio como por ejemplo el proceso de adquisición de objetivos o *targeting*, el C2 en el ciberespacio o el desarrollo de instrucciones de servicio específicas para CoI de carácter multinacional que operen a nivel táctico.

En cuanto a la seguridad centrada en el dato o DCS, supone una ruptura con el enfoque estático basado en la red que aportará mejoras en varios aspectos. Por un lado, en la compartición de información, porque refuerza el principio de necesidad de conocer y facilita el intercambio automatizado entre dominios y entre comunidades de interés (CoI). Para ello se recurre a un enfoque estandarizado mediante el etiquetado de datos al nivel de detalle requerido, lo que favorece el trasvase de la información entre dominios sin la intervención humana [57].

La implantación de DCS también permitirá mayor agilidad operativa, al emplear estándares y tecnologías aprobadas para la gestión de la seguridad de la información. Admite la aplicación de reglas de acceso concretas a los datos protegidos mientras los usuarios están en movimiento o durante períodos donde las comunicaciones son de baja calidad. También permite controlar los datos en entornos CIS más dinámicos y complejos, donde la transición a nubes públicas o híbridas requieren una mayor granularidad en las medidas de seguridad, o donde el intercambio de información con los participantes de la red federada está sujeto a acuerdos que son susceptibles de cambios o modificaciones. Con DCS se facilitará el uso de servicios de alojamiento compartido y también la escalabilidad pues es posible cambiar la infraestructura y los procesos sin tener que modificar la solución de seguridad [58].

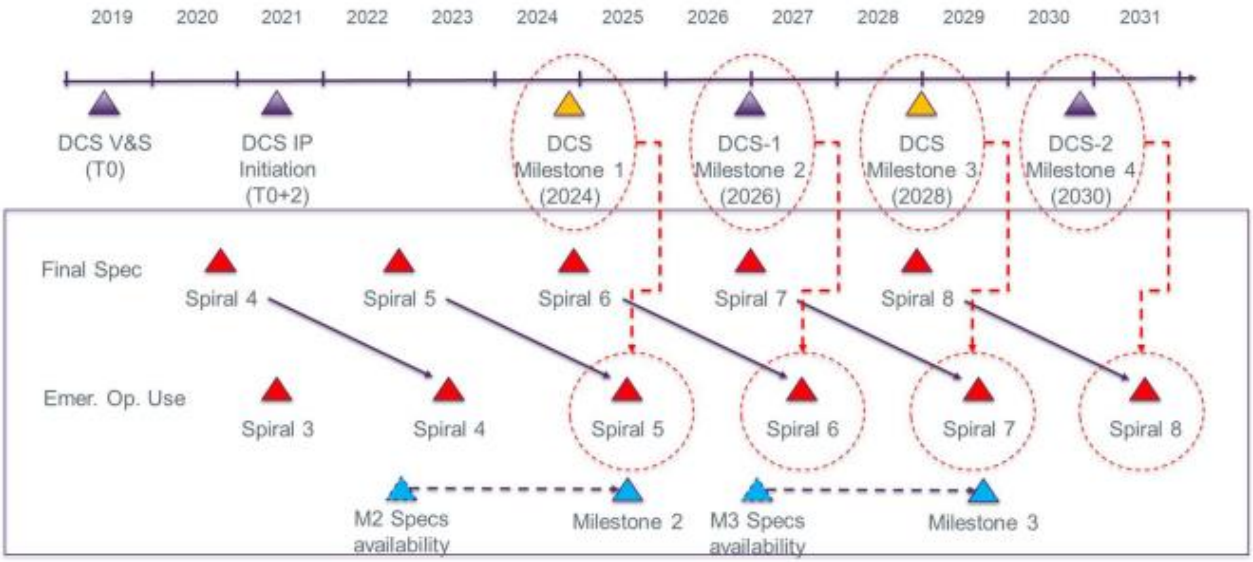

Figura 36. DCS en espirales FMN [59].

En cuanto a la seguridad, la protección de la información supone el control de acceso granular a nivel de objeto (atributos del sujeto, recurso y contexto). DCS también proporcionará una capa adicional de protección (defensa en profundidad) y reduce la probabilidad de exfiltración de datos al estar protegidos durante todo el ciclo de vida. A medida que la tecnología evolucione con la inteligencia artificial o la computación cuántica, las amenazas a los protocolos de seguridad y criptográficos también lo harán, de ahí la ventaja que supondrá DCS para poder realizar una reconfiguración ágil y dinámica de las medidas de seguridad [59].

En definitiva, la implantación de DCS para las redes de misión FMN contribuirá a superar algunas de las restricciones actuales a la hora de compartir datos sensibles entre los afiliados [57].

Como se ha descrito en los párrafos anteriores, durante los próximos años se prevé alcanzar una mayor eficacia operativa y seguridad en las redes de misión federadas. Para que los afiliados alcancen sus objetivos en el desarrollo de capacidades FMN es necesario eliminar cualquier discrepancia entre sus objetivos individuales y las especificaciones técnicas de la espiral, de ahí la importancia de optimizar los procesos de implementación y prueba de los servicios FMN tanto nacionales como multinacionales [60].

La perspectiva de los afiliados es que se debería simplificar el proceso de gestión de cambios o RFC. Respecto a los test para probar los servicios a implementar, se necesita clarificar los requisitos para considerar un ejercicio de prueba como un evento oficial FMN. Una vez que una aplicación ha sido probada y se considera que cumple con los requisitos FMN, sería aconsejable no tener que volver a realizar nuevas pruebas sobre esa capacidad si no suponen una verdadera mejora operativa para los afiliados. En general, es necesario una mayor participación de personal en las fases de experimentación y sacar el máximo provecho a los recursos disponibles incorporando a nuevos actores implicados (agencias, academia e industria).

En cualquier caso, la contribución de FMN a las espirales está alineada con los objetivos de la OTAN y seguirá ayudando a los afiliados, dentro de su nivel de ambición, a avanzar hacia la interoperabilidad desde el primer día y a la consecución del Hito 3, que incluirá el intercambio completo de información y una mayor seguridad a todos los niveles.

5 CONCLUSIONES

FMN supone para la OTAN un capacitador de primera magnitud para la consecución de sus objetivos y se encuentra alineada con el Concepto Estratégico de 2022 y con la Agenda 2030. La iniciativa FMN aborda la interoperabilidad en todas sus dimensiones y desde el primer día del despliegue, lo que redunda en el cumplimiento de las misiones OTAN en un escenario cada vez más complejo. Uno de los principales retos de FMN de cara al futuro es su adaptación al nuevo entorno operativo, donde la transformación digital iniciada hace ya años se une a unas operaciones multidominio que requieren mejorar el intercambio de información para optimizar el proceso de toma de decisiones.

La iniciativa FMN cuenta ya con una larga trayectoria y el número de participantes ha ido aumentando de forma paulatina. De los datos analizados en el TFM se puede confirmar que la mayoría de los afiliados han incrementado su participación y han mejorado su estatus FMN dentro los niveles de ambición que se habían marcado. Durante los últimos años y a la vista de los resultados obtenidos, una de las principales preocupaciones de FMN ha sido seguir impulsando todo tipo de medidas para mitigar las carencias identificadas. El personal sigue siendo el recurso más valioso de la OTAN y también de FMN, por lo que hay que fomentar la participación de expertos de todos los ámbitos que contribuyan al desarrollo e implementación de las nuevas tecnologías emergentes y al análisis de posibles riesgos.

Desde el punto de vista de la organización, el Marco FMN ha conseguido mantener una estructura más estable para monitorizar los procesos y trabajos en marcha, gracias al trabajo del Secretariado FMN. Los diferentes grupos de trabajo están dando mayor coherencia a los procesos del ciclo de vida de las espirales, con especial énfasis en el desarrollo de arquitecturas para poder alinear FMN con la implantación de DCS en las redes de misión. También se ha hecho hincapié en fortalecer todos los grupos de trabajo con expertos que aporten sus conocimientos y den continuidad a los desarrollos, tanto a nivel nacional como internacional, buscando posibles sinergias que permitan seguir avanzando en los distintos temas de interés. El aprovechamiento del recurso humano y la labor de los oficiales de enlace y personal destinado en la estructura permanente ha dado mayor impulso para aumentar la calidad en las tareas diarias y productos del Marco FMN.

Otro objetivo que se ha conseguido es optimizar el formato de las reuniones que se realizan tanto a nivel de gobierno como de gestión. Las reuniones del MG son de vital importancia para consolidar diferentes asuntos que son consensuados por los representantes nacionales, por lo que se requiere un trabajo previo bien hecho y una priorización de los asuntos a tratar a dicho nivel. El trabajo diario de la estructura FMN en las reuniones presenciales y a distancia que tienen establecidas en sus calendarios también ha mejorado, permitiendo la participación no solo de los expertos de dicho grupo, sino también de personal de otros ámbitos que aportan otros puntos de vista pero que son claves para la coherencia de los productos obtenidos.

En línea con lo anterior, la mejora de la eficacia operativa también ha sido posible al disponer de un portal web de referencia en el ámbito de la interoperabilidad, donde se recogen los productos a obtener por cada organismo implicado en FMN. También el empleo de TIDEPEDIA como herramienta oficial para crear temas de estudio, de debate y para el desarrollo de eventos y documentación, permite a los participantes aportar soluciones o correcciones de cualquier asunto relacionado con FMN. La facilidad para acceder y utilizar estos recursos facilita a los diferentes grupos de trabajo estar en contacto diario y al corriente de cualquier cambio que afecte a FMN en general y a los eventos de su área de responsabilidad en particular.

Respecto a la coherencia en el ciclo de vida de la espiral, las Espirales 3 y 4 ya han supuesto una mejora en cuanto a la trazabilidad entre los requisitos operacionales y las capacidades desarrolladas. En este sentido la colaboración dentro de FMN entre los grupos se ha fortalecido a la vez que se ha potenciado la

colaboración con otras entidades. Entre los organismos con los que FMN seguirá manteniendo acuerdos de cooperación podemos destacar el *Consultation, Command and Control Board* (C3B), el *Joint Intelligence, Surveillance and Reconnaissance Integration Group* (JISR IG), el *Military Committee Standardization Boards* (MC SB) o la *Conference of National Armaments Directors* (CNAD). Uno de los retos seguirá siendo alinear las políticas y doctrinas nacionales con las capacidades FMN consensuadas.

En general se ha mejorado el Marco FMN para que los productos que cada grupo de trabajo va desarrollando respecto a cada espiral estén perfectamente alineados, intentando dar mayor protagonismo a la fase de pruebas. Los productos FMN como la *Baseline*, las JMEI y los formatos de referencia se han mejorado para que los participantes de la iniciativa FMN dispongan de una guía más completa y clarificadora para la instanciación de las redes de misión. Para realizar el seguimiento de los avances que cada afiliado va haciendo respecto a la validación y verificación de los servicios de cada espiral se ha puesto en marcha dentro del portal web FMN un apartado que recopila información actualizada sobre el proceso de gestión de cambios, que junto al proceso de lecciones aprendidas permite potenciar el ciclo de vida de la espiral y mejorar la calidad de los productos finales y futuros.

En resumen, se ha podido comprobar que el marco FMN es un auténtico potenciador de la eficacia operativa y que permite avanzar en los objetivos de la OTAN a través de la interoperabilidad en sus tres dimensiones, personas, procesos y tecnología. El éxito futuro dependerá en gran medida de la voluntad de los afiliados para seguir contribuyendo a fortalecer la estructura FMN, aprovechar los recursos disponibles y fomentar la participación en todos los foros orientados a mejorar el despliegue de redes de misión federadas para ejercicios y operaciones.

6 BIBLIOGRAFÍA

[1] *NATO Strategic Concept 2022, NATO Summit in Madrid, 2022.*

[2] MCM-0038-2005/0032-2006, *Development of a NATO Network-Enabled Capability (NNEC).*

[3] Concepto de información en red del JEMAD, 2007.

[4] *NATO Enterprise C3 Interoperability Directive*, AC/322-D (2019) 0031(INV). Portal web CoI FMN OTAN, 2019.

[5] *NATO Warfighting Concept* (*NWCC*), *Allied Command Transformation* (ACT), 2023.

[6] Concepto de Empleo de las FAS, 2017.

[7] Entorno operativo 2035, catálogo de publicaciones, MINISDEF, 2019.

[8] Panorama de las tendencias geopolíticas. Horizonte 2040. IEEE, 2019.

[9] Conceptos para el Combate 2035. MADOC, 2019.

[10] PDC-01(A) Empleo de las Fuerzas Terrestres, 2018.

[11] PD2-001 Funciones de Combate, 2013.

[12] Manual Convergencia de Capacidades. *The US Army in MDO*, 2020.

[13] Nota Conceptual sobre Operaciones Multidominio, CCDC (EMAD), 2020.

[14] Operaciones multidominio en la OTAN, *Allied Command Transformation* (ACT), 2023.

[15] MARTÍNEZ-VALERA, G.; El enfrentamiento avanzado, las operaciones multidominio. *Global Strategy Reports*, 2022.

[16] *The US Army in Multi-Domain Operations 2028*. *US Army*, 2018.

[17] AG CIS/TIC del MINISDEF, 2017.

[18] PÉREZ MARTÍNEZ, F.; La transformación digital en los nuevos escenarios de conflicto: del campo de batalla digital al campo de batalla inteligente. ACAMI, 2023.

[19] MILLÁN MARTÍNEZ, J.M., Transformación digital en el Ministerio de Defensa: El viaje inaplazable. Revista Española de Defensa, 2022.

[20] LLOPIS SANCHÉZ, S.; Las telecomunicaciones tácticas militares: vanguardia de la transformación digital del campo de batalla. ACAMI, 2021.

[21] *PO 0191, NATO´s Digital Transformation Implementation Plan Strategy*, 2023.

[22] Requisitos Operativos de Intercambio de Información de los CIS del ET. MADOC, 2015.

[23] Directiva de Planeamiento Militar, 2017.

[24] Arquitectura de referencia de los CIS desplegables del ET v.1.0, 2019.

[25] MCM-0067-2020 (NS), *Concept for the Deterrence and Defence- of the Euro -Atlantic Area.*

[26] SH/COM/SAC/WC/20210817/2 (NS) *SACEUR´s AOR-Wide Strategic Plan*, 2023.

[27] *Allied Joint Doctrine for Communication and Information Systems Edition A Version 1.*

[28] AJP-01, *Allied Joint Doctrine*. *Ed F*, 2022.

[29] *NATO* N*etwork Enabled Capabilities* (*NNEC*): F*easibility Study v.2.0*, 2005; *Vision and Concept*, 2006; *Management Approach to NNEC* (*MAN*), 2007; *Roadmap*, 2007; *Compendium of NNEC-Related Architectures;* 2007.

[30] MC 0593-2020 *Minimum Level of C2 Service Capabilities in Support of Combined Joint NATO Led Operations.*

[31] Memorando de COMISAF a SACEUR *Future Coalition Network*, 2011.

[32] Memorando del comandante JFC Brunssum a SACEUR respaldando la Red de Misiones de la Coalición Futura, 2011.

[33] Memorando de SACEUR a COMISAF. La Red de Misiones del Futuro, 2011.

[34] Requisitos de capacidad mínima de la OTAN, Anexo 1 de AC/281-N(2012)0003(R), 2012.

[35] *Future Mission Network Concept, version 2.0,* 2012.

[36] *FMN Mission Network (FMN) Concept, version 2.0*. Portal web CoI FMN OTAN, 2012.

[37] *NATO Federated Mission Networking Implementation Plan (NFIP) V.4.0*. Portal web CoI FMN OTAN, 2014.

[38] ACT-NNEC-SFCT-2013/01, *NATO Network-Enabled Capability* (*NNEC*) *Compliancy Analysis of Exercise Steadfast Cobalt*, 2013.

[39] MC 0648 (*Final*), *Military Committee Federated Mission Networking (FMN) Governance Directive*, Portal web CoI FMN.

[40] MCM-0194-2016 *Revision 1, Military Committee Federated Mission Networking Governance Action Plan*, Portal web CoI FMN.

[41] SH/CCD J6/FMN/137/16-313769. Management Directive, *Version 2.0*. Portal web CoI FMN, 2018.

[42] C-M(2012)0096, *Military Committee Advice on the Future Mission Network* (*FMN*) *Concept*, 2012.

[43] *FMN Spiral Specification Roadmap.* Secretariado FMN, 2022.

[44] SH/CCD J6/FMN/063/18-320466, *FMN Vision, Version 3.1*, Portal web CoI FMN OTAN, 2018.

[45] *FMN Management Roadmap, version 2.0.* Portal web CoI FMN OTAN, 2023.

[46] *NATO Architecture Framework V.4.0.* Portal web CoI FMN OTAN, 2020.

[47] F*MN Spiral 3 Reference Architecture*. Secretariado FMN, 2018.

[48] *FMN Spiral 3 Specification Planning*. Secretariado FMN, 2022.

[49] *NATO Term NSO*, versión digital, 2023.

[50] *Federated Mission Networking (FMN) Architecture Management Plan*. Portal web CoI FMN OTAN, 2018.

[51] *FMN Baseline Change and release Management Process*. Anexo A del S*ervice Management Document, version 3.0.* Secretariado FMN, 2022.

[52] *FMN Spiral 4 Specification Planning*. Secretariado FMN, 2022.

[53] MC 0640-2018 de OTAN, *Minimum Level of CIS Capabilities at Land Tactical Level.*

[54] ACO *Directive* 080-122 (NS) *Allied Reaction Force*.

[55] *FMN Spiral 5 Specification.* Secretariado FMN, 2023.

[56] MCM-0004-2023, *Alliance Concept for Multi-Domain Operations.*

[57] *Final report of NIAG Study Group 267 on DCS,* 2021.

[58] *DCS IP 2 0 - Volume IV Annex B - Benefits and DOTMLPFI Analysis,* 2022.

[59] *NIAG Study Group 267 on Data Centric Security*, 2022.

[60] *FMN MG Guidance for Capability Development in Spirals 4, 5 & 6, version 5.* Secretariado FMN, 2023.

ANEXO I: TÉRMINOS Y ACRÓNIMOS

A2/AD	*Anti-access / Area Denial*
ACO	*Allied Command Operations*
ACT	*Allied Command Transformation*
ADM	Armas de destrucción masiva
AG	Arquitectura Global
AGE	Administración General del Estado
AMN	*Afghanistan Mission Network*
ATO	*Authorization to operation*
AV&V	*Assurance, Verification and Validation*
C2	*Command and Control*
C2COE	Centro de Excelencia de Mando y Control
C3B	*Consultation, Command and Control Board*
C4ISR	*Consultation, Command, Control, Computers, Intelligence, Surveillance and Reconnaissance*
CAB	*Change Advisory Board*
CI	*Configuration Elements*
CIAV	*Coalition Interoperability Assurance and Validation Working Group*
CICWG	*Change and Implementation Coordination Working Group*
CIMIC	*Civil Military Cooperation*
CIO	*Chief Information Officer*
CIED	*Counter-Improvised Explosive Devices*
CIS	Sistemas de Telecomunicaciones e Información
CNAD	*Conference of National Armaments Directors*
CoI	*Community of Interest*
COP	*Common Operational Picture*
COPD	*Comprehension Operational Planning Directive*
CONOPS	*Concept of Operations*
CP	*Capability Packages*
CPE	*Capability Enhancement*
CPWG	*Capability Planning Working Group*
CSRS	*Community Security Requirements Statement*
CV2E	*Coalition Verification and Validation Environment*
CWIX	*Coalition Exploration Experimentation Evaluation Interoperability Exercise*
DCS	*Data Centric Security*
DDA	Defensa del Área Euroatlántica
DIANA	*Defence Innovation Accelerator for the North Atlantic*
DNS	*Domain Name System*
DTS	*Distribution Time Service*
DPC	*Digital Policy Committee*
DT	*Digital Transformation*
EDT	*Emergents Disruptive Tecnologies*
eFP	*Enhanced Forward Presence*
EMAD	Estado Mayor de la Defensa
ENI	Esquema Nacional de Interoperabilidad
EUMS	Estado Mayor de la Unión Europea
HF	*High Frecuency*

FAS Fuerzas Armadas
FFT *Friendly Force Tracking*
FMN *Federated Mission Networking*
GESCOM Gestor de Comunicaciones del ET
I3D Infraestructura Integral de Información para la Defensa
IA Inteligencia Artificial
IEEE Instituto Español de Estudios Estratégicos
IER *Information Exchange Requirements*
IKM *Information and Knowledge Management*
ISAF *International Security Assistance Force*
ISTAR *Intelligence. Surveillance, Targeting Adquisition and Reconnaissance*
JFTC *Joint Force Training Centre*
JMEI *Joining, Membership and Exiting Instructions*
JOA *Joint Operational Area*
MC *Military Committee*
MCCE Mando Conjunto del Ciberespacio
MCSMA *Multinational CIS Security Management Authority*
MDO *Multidomain Operations*
MINISDEF Ministerio de Defensa
MG *Management Group*
MN *Mission Network*
MNE *Mission Network Element*
MNX *Mission Network Extension*
MT *Mission Thread*
NAC *North Atlantic Council*
NAF *NATO Architecture Framework*
NCIA *NATO Communications and Information Agency*
NCS *NATO Command Structure*
NDPP *NATO Defence Planning Process*
NDS *NATO Digital Staff*
NHQC3S *NATO Headquarters C3 Staff*
NIAG *NATO Industrial Advisory Group*
NII *NATO Information Infrastructure*
NISP *NATO Interoperability Standards and profiles*
NFIP *NATO Framework Implementation Plan*
NNEC *NATO Network Enabled Capability*
NRF *NATO Response Force*
NWCC *NATO Warfighting Capstone Concept*
OCWG *Operational Coordination Working Group*
OISD Organizaciones Internacionales de Seguridad y Defensa
OPLAN *Operations Plan*
OTAN Organización del Tratado del Atlántico Norte
OFP *Optimized Framework Process*
PCN *Protected Core Networking*
PI *Procedural Instruction*
RAP *Recognized Air Picture*
REP *Recognized Environmental Picture*
RFC *Request for Change*
RFI *Request for Information*
RLP *Recognized Land Picture*
RMP *Recognized Maritime Picture*

SA	*Situational Awareness*
SACEUR	*Supreme Allied Commander Europe*
SC2N	Sistema de Mando y Control Nacional
SDN	*Software Defined Network*
SDR	*Software Defined Radio*
SI	*Service Instruction*
SHAPE	*Supreme Headquarters Allied Powers Europe*
SLA	*Service Level Agreement*
SMC	*Service Management and Control*
SoC	*Statement of Compliance*
TDL	*Tactical Data Link*
TF	*Task Force*
TFM	Trabajo Fin de Máster
TTP	Tácticas, Técnicas y Procedimientos
VUCA	Volatilidad, Incertidumbre, Complejidad y Ambigüedad
WG	*Working Group*

ANEXO II: ESPIRAL 2 FMN

Detalle de objetivos según el Plan de Acción Nacional FMN-ESP (MCCE, EMAD):

Instrucciones de Servicio

- Instrucción para colaboración audio y video.
- Instrucción para *Coalition Shared Database* (CSD).
- Instrucción para comunicaciones.
- Instrucción para *data links*.
- Instrucción para certificados digitales.
- Instrucción para sincronización de directorios.
- Instrucción para sincronización de tiempos.
- Instrucción para *Domain Name Server* (DNS).
- Instrucción para *Friendly Force Tracking* (FFT).
- Instrucción para información geoespacial.
- Instrucción para mensajería.
- Instrucción para intercambio de información C3.
- Instrucción para *Recognized Maritime Picture* (RMP).
- Instrucción para gestión de servicios.
- Instrucción para chat.
- Instrucción para autenticación web.
- Instrucción para servicios web.

Instrucciones procedimentales

- Instrucción para seguridad CIS.
- Instrucción para colaboración distribuida.
- Instrucción para gestión de la información.

- Instrucción para información *Joint Intelligence, Surveillance and Reconnaissance* (JISR).
- Instrucción para *Recognized Environmental Picture* (REP).
- Instrucción para gestión de servicios.
- Instrucción para s*ituational awareness*.

ANEXO III: ESPIRAL 3 FMN

Detalle de objetivos según el Plan de Acción Nacional FMN-ESP (MCCE, EMAD):

Instrucciones de Servicio

- Instrucción para colaboración audio y video.
- Instrucción para *calendaring y scheduling*.
- Instrucción para comunicaciones.
- Instrucción para *data links*.
- Instrucción para certificados digitales.
- Instrucción para sincronización de directorios.
- Instrucción para sincronización de tiempos.
- Instrucción para *Domain Name Server* (DNS).
- Instrucción para *Friendly Force Tracking* (FFT).
- Instrucción para información geoespacial.
- Instrucción para mensajería.
- Instrucción para intercambio de información JISR.
- Instrucción para intercambio de información de C2 terrestre.
- Instrucción para distribución de imágenes.
- Instrucción para redes de núcleo protegido.
- Instrucción para *Recognized Maritime Picture* (RMP)
- Instrucción para gestión y control de servicios
- Instrucción para chat.
- Instrucción para autenticación web.
- Instrucción para servicios web.

Instrucciones procedimentales

- Instrucción para C2 de misiones MEDEVAC.

- Instrucción para C2 de misiones navales.
- Instrucción para seguridad CIS.
- Instrucción para colaboración distribuida.
- Instrucción para gestión de la información.
- Instrucción para información *Joint Intelligence, Surveillance and Reconnaissance* (JISR).
- Instrucción para *Recognized Environmental Picture* (REP).
- Instrucción para gestión y control de servicios.
- Instrucción para *situational awareness*.

ANEXO IV: ESPIRAL 4 FMN

Detalle de objetivos según el Plan de Acción Nacional FMN-ESP (MCCE, EMAD):

Instrucciones de Servicio

- Instrucción para colaboración audio y video.
- Instrucción para *calendaring y scheduling*.
- Instrucción para comunicaciones.
- Instrucción para *data links*.
- Instrucción para certificados digitales.
- Instrucción para sincronización de directorios.
- Instrucción para búsquedas sincronizadas.
- Instrucción para sincronización de tiempos.
- Instrucción para *Domain Name Server* (DNS).
- Instrucción para *Friendly Force Tracking* (FFT).
- Instrucción para información geoespacial.
- Instrucción para mensajería.
- Instrucción para intercambio de información JISR.
- Instrucción para intercambio de información de C2 terrestre.
- Instrucción para intercambio de información de C2 marítima.
- Instrucción para distribución de imágenes.
- Instrucción para redes de núcleo protegido.
- Instrucción para *Recognized Maritime Picture* (RMP)
- Instrucción para gestión y control de servicios
- Instrucción para chat.
- Instrucción para procesamiento virtualizado.
- Instrucción para autenticación web.
- Instrucción para servicios web.

Instrucciones procedimentales

- Instrucción para C2 de misiones aéreas.
- Instrucción para C2 de misiones terrestres.
- Instrucción para C2 de misiones MEDEVAC.
- Instrucción para C2 de misiones navales.
- Instrucción para seguridad CIS.
- Instrucción para intercambio de información cívico-militar.
- Instrucción para comunicaciones.
- Instrucción para colaboración distribuida.
- Instrucción para gestión de la información.
- Instrucción para colaboración distribuida.
- Instrucción para gestión de la información.
- Instrucción para información *Joint Intelligence, Surveillance and Reconnaissance* (JISR).
- Instrucción para *targeting* conjunto.
- Instrucción para *Recognized Environmental Picture* (REP).
- Instrucción para gestión y control de servicios.
- Instrucción para *situational awareness*.
- Instrucción para comunicaciones tácticas.

ANEXO V: ESPIRAL 5 FMN

Enumeración de objetivos establecidos en las especificaciones de la Espiral 5 de FMN **según el Plan de Acción Nacional FMN-ESP (MCCE, EMAD):**

- Mejorar la capacidad de apoyo médico y de telemedicina.
- Mejorar la federación de las capacidades forense y de contramedidas NRBC
- Mejorar el conocimiento del entorno (*Situational Awareness*) proporcionando capacidades adicionales para construir y difundir, de forma semi-automatizada y estructurada, elementos de los siguientes componentes de la COP:
    - *Recognized CBRN Picture*,
    - *Recognized Cyberspace Picture*.
- Mejorar las capacidades de *targeting* conjunto.
- Seguir avanzando hacia los Hitos 2 y 3 definidos en el volumen I del NFIP de la OTAN:
    - Permitiendo el intercambio semiautomático de información (mensajería, chat, *web hosting*) entre varios niveles de clasificación dentro de la federación.
- Permitir el intercambio automatizado de datos de simulación en apoyo de múltiples procesos operativos, educativos y de formación.
- Mejorar la capacidad de defensa de la red.
- Mejorar las capacidades forense y de contramedidas NRBC
- Mejorar JISR proporcionando capacidades iniciales para compartir productos como:
    - Difusión de la explotación.
    - Procesamiento federado.
- Mejorar las capacidades de infraestructura de audio, vídeo y medios de comunicación.
- Mejorar las capacidades geoespaciales mediante la prestación de apoyo inicial a los servicios *geo-whiteboarding*.
- Mejorar la resiliencia y redundancia del intercambio de información a nivel táctico a través de la federación de la sincronización de archivos.
- Mejorar la capacidad de defensa de red, incluyendo todas las operaciones basadas en red.
- Proporcionar capacidades iniciales para firmar digitalmente.

- Mejorar la gestión de la información incorporando capacidades de archivado masivo de datos.
- Mejorar la colaboración distribuida proporcionando capacidades de comunicaciones unificadas y colaboración.
- Mejorar las capacidades de apoyo al intercambio de información cívico-militar.
- Mejorar la gestión y el control de los servicios proporcionando capacidades iniciales para federar:
    - Gestión de niveles de servicio,
    - Gestión de la disponibilidad.

La fase de requisitos tendrá lugar entre los años 2019 y 2020, la fase de definición los años 2021 y 2022, la fase de diseño, implementación, integración, verificación y validación será durante los años 2023, 2024 y 2025 y su fase de uso y confirmación será durante los años 2026 y 2027. Durante el año 2028 irán dando paso a las especificaciones de la Espiral 7 FMN.

ANEXO VI: ESPIRAL 6 Y 7 FMN

Enumeración de objetivos establecidos en las especificaciones de la Espiral 6 y 7 de FMN **según el Plan de Acción Nacional FMN-ESP (MCCE, EMAD):**

- Seguir avanzando hacia los Hitos 2 y 3 definidos en el volumen I del NFIP de la OTAN:
    - Permitiendo el intercambio semiautomático de información (mensajería, chat, *web hosting*) entre la federación e Internet en apoyo del intercambio de información cívico-militar.
- Mejorar la capacidad de defensa de la red.
- Mejorar las capacidades de apoyo a la interconectividad de la red incluyendo sistemas no tripulados y robótica.
- Mejorar el conocimiento del entorno (*situational awareness*) proporcionando capacidades adicionales para construir y difundir, de forma semi-automatizada y estructurada, elementos de la *Recognized Space Picture*.
- Mejorar el conocimiento del entorno (s*ituational awareness*) de una manera cada vez más automatizada y estructurada, a fin de proporcionar una COP conjunta.
- Mejorar la gestión de la información proporcionando capacidades para apoyar la explotación de la Internet de las cosas (IoT), *Big data* y computación cognitiva.
- Mejorar los procesos de análisis y toma de decisiones mediante la inclusión de la Inteligencia Artificial (IA).
- Mejorar la gestión y el control de los servicios proporcionando capacidades iniciales para federar:
    - Gestión de capacidades.

La fase de requisitos tendrá lugar entre los años 2021 y 2022, la fase de definición los años 2023 y 2024, la fase de diseño, implementación, integración, verificación y validación será durante los años 2025, 2026 y 2027 y su fase de uso y confirmación será los años 2028 y 2029. Durante el año 2030 irán dando paso a las especificaciones de la Espiral 7 FMN.

Partiendo de los avances obtenidos con la Espiral 6 y actualizando las capacidades obtenidas en las espirales previas, con la Espiral 7 se pretende alcanzar los siguientes objetivos:

- Seguir avanzando hacia los Hitos 2 y 3 definidos en el volumen I del NFIP de la OTAN

La fase de requisitos tendrá lugar entre los años 2023 y 2024, la fase de definición los años 2025 y 2026, la fase de diseño, implementación, integración, verificación y validación será durante los años 2027, 2028

y 2029 y su fase de uso y confirmación será los años 2030 y 2031. Durante el año 2032 se irán dando paso a las especificaciones de la Espiral 7 FMN.