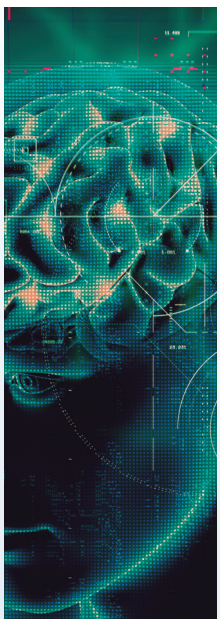
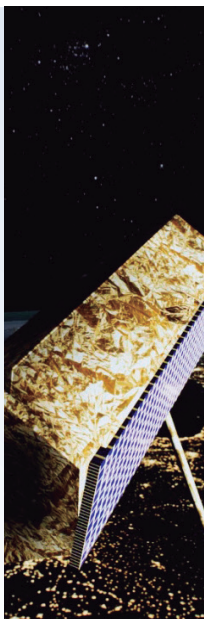
Transformación digital de las FAS para el combate multidominio





Transformación digital de las FAS para el combate multidominio

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

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

publicaciones.defensa.gob.es

cpage.mpr.gob.es

Diseño de cubierta: Irene Paloma Medina Jurado

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Paseo de la Castellana 109, 28046 Madrid

NIPO 083-23-273-2 (impresión bajo demanda)
ISBN 978-84-9091-845-6 (impresión bajo demanda)

NIPO 083-23-274-8 (edición en línea)

Depósito legal M 35303-2023
Fecha de edición: febrero de 2024
Maqueta e imprime: Imprenta Ministerio de Defensa

ÍNDICE

Introducción

Fernando Carrillo Cremades

> *«He aquí la dificultad del combate actual: desenvolverse en la esfera digital en la que estamos inmersos, y vencer en este combate».*
>
> *TG. José M. Millán Martínez*
>
> *Director del Centro de Sistemas y Tecnologías de la Información (CESTIC)*

Presente y futuro, continuidad y cambio han sido siempre las dinámicas que, equilibradas, han asegurado el éxito de las organizaciones. Y esto ha sido así porque han acertado a leer el signo de los tiempos, condición previa no solo para mantenerlas «vivas», eficaces en su momento presente, sino, a la vez, también para descifrar el horizonte, visionarlo y construir su futuro. Quienes así lo han hecho han aportado valor, han sido útiles y eficaces, manteniendo en el tiempo su relevancia y competitividad.

Disuadir o, llegado el caso, luchar y vencer. En esencia, esta ha sido siempre la misión de las Fuerzas Armadas. Cabría cuestionarse, entonces, qué nos dice ahora, para nuestra tarea diaria, una lectura sosegada del tiempo que estamos experimentando, cómo visionamos el futuro y cómo nos interpela todo ello para continuar cumpliendo con nuestra misión.

Muy pocos dudan del extraordinario desarrollo tecnológico y global que estamos experimentando en ámbitos como el de la nanotecnología, la robótica, el *big data*, la inteligencia artificial (IA), la computación cuántica o los sistemas autónomos, por enumerar solo algunos de ellos. Constituye ya una rutina la lectura periódica de noticias que informan sobre un avance, un hito más en la evolución de estas tecnologías, que hasta ahora formaban parte de la ciencia ficción. Y aunque están en sus momentos más incipientes, acertamos a identificar cómo ya están invadiendo nuestra vida cotidiana y cambiando la forma en cómo trabajamos o nos relacionamos. Nos cuesta salir del asombro, y de la incertidumbre.

Klaus Schwab, presidente ejecutivo del Foro Económico Mundial, contribuye a que podamos interpretar mejor el tiempo presente cuando afirma que:

> «[...] estamos al borde de una revolución tecnológica que modificará fundamentalmente la forma en que vivimos, trabajamos y nos relacionamos. En su escala, alcance y complejidad, la transformación será distinta a cualquier cosa que el género humano haya experimentado antes (...) nunca ha habido un momento de mayor promesa o mayor peligro...».

Y es que, hasta ahora, nunca habían convergido tecnologías digitales, físicas y biológicas. Nunca ha ocurrido, a la vez, un desarrollo a gran escala y a toda velocidad. Porque estos avances no están siguiendo un esquema lineal, como ha sido hasta ahora, sino un patrón de desarrollo tecnológico exponencial, que no tiene precedentes en la historia. Es la primera vez que los procesos de democratización de las tecnologías son tan rápidos y las posibilidades que ofrecen se muestran tan accesibles. Además, para el caso del ámbito militar, se ha producido un cambio de paradigma en el hecho de que la investigación, el desarrollo y la innovación de las tecnologías emergentes y disruptivas, provienen del ámbito civil, que ejerce de tractor, habiendo perdido el sector de la Defensa su tradicional liderazgo.

Podríamos abordar estas circunstancias con cierta lentitud, escepticismo o pensar que, al fin y al cabo, evolución tecnológica «ha habido siempre». O que, de alguna forma, estamos transitando caminos, en esencia, ya recorridos. «Es más de lo mismo», podríamos pensar. Tal vez sea así, pero tal vez no. Y la respuesta a este dilema, que no es una cuestión menor, ha de venir de desafiar de nuevo nuestra capacidad de pensamiento crítico para entender en toda su extensión y profundidad el cambio de época que parece fraguarse.

El historiador y escritor israelí Yuval Harari advierte:

> «[...] A principios del siglo XXI, el tren del progreso sale de nuevo de la estación..., y es probable que sea el último que salga de la estación llamada Homo Sapiens. Los que pierdan este tren nunca tendrán una segunda oportunidad. Si queremos conseguir un pasaje para dicho tren, debemos entender la tecnología del siglo XXI, y en particular los poderes de la biotecnología y de los algoritmos informáticos [...] los que se queden rezagados se enfrentarán a la extinción...».

En cualquier caso, todos convendrán en afirmar que, a lo largo de la historia, los ejércitos siempre han luchado por integrar en el campo de batalla los avances tecnológicos que llevaban consigo una superioridad en el enfrentamiento. Así ha sido, durante los últimos cien años, en el caso de las tecnologías de la información y todo parece indicar que las nuevas tecnologías de la cuarta revolución industrial se irán incorporando y alterarán significativamente el carácter del combate, tal y como hoy lo conocemos. El resultado previsto será la incorporación al campo de batalla de un modo de combatir diferente; las operaciones multidominio (MDO*, Multi-domain Operations*).

En efecto, estas nuevas MDO no surgen por la incorporación de los nuevos ámbitos de operación, principalmente el ciberespacial y el cognitivo, a los tradicionales ámbitos terrestre, marítimo y aeroespacial. De ser así, y a pesar de su carácter transversal, estaríamos ante unas operaciones conjuntas «ampliadas».

Las operaciones multidominio son el resultado de integrar información proveniente de un elevado número de sensores, sin que sea relevante el ámbito al que pertenecen, procesarla, analizarla, tomar una decisión y, a través de los efectores más apropiados del campo de batalla, sin que tampoco sea relevante el ámbito en el que operan, producir los efectos deseados.

El salto cualitativo más importante que se produce reside en la disponibilidad de una conciencia situacional común y completa, en la velocidad de las operaciones y en la generación de efectos como consecuencia. A destacar, entre otros, se encuentran la extraordinaria mejora en la capacidad de análisis y procesamiento de datos, en términos de calidad, cantidad, y rapidez, en la aplicación de la IA y en las posibilidades que ofrece la de hiperconectividad. Esta mayor velocidad, el «arma definitiva» según algunos autores, basada en decisiones mucho más ágiles y eficaces, no solo permitirá sobrepasar el ciclo de decisión del adversario, sino que en ella radicará, además, uno de los elementos que proporciona la capacidad de disuasión que genera este modelo de operaciones.

Se produce, por tanto, un cambio de paradigma porque el «protagonismo» principal en el combate deja de estar en el sistema de armas y el ámbito en el que se desarrolla, para desplazarse al dato, a la información, a la nube, que ahora es el punto focal. La superioridad en el enfrentamiento será, por tanto, el resultado de la Transversalidad, con mayúsculas, de todos los ámbitos entre ellos. Es la colaboración en grado superlativo, que en último término difumina sus límites.

De esta forma, es posible que se esté creando la posibilidad futura de superar la tradicional cadena letal (*kill chain*) basada, principalmente, en los ciclos de observación, orientación, decisión y acción (OODA) que cada ámbito desarrolla con un alto grado de independencia y a diferente velocidad. Es posible que se supere este modelo y se establezca una cadena letal *web* (*kill web*) multidominio que, bajo el Mando y Control de un binomio humano-máquina, genere un ciclo OODA en, desde, o a través de cualquier ámbito, o en múltiples ámbitos, e incremente en grado exponencial las opciones del comandante y su velocidad de ejecución, conectando cualquier sensor con el efector más apropiado *(any sensor, best shooter).*

Aparece entonces en el campo de batalla un nuevo «combatiente». Es el «algoritmo de guerra», resultado de la combinación de la inteligencia artificial y las capacidades militares. Es el algoritmo que está detrás de la capacidad predictiva, del comportamiento de los sistemas autónomos o de la ayuda a la toma de decisiones, entre otros. Un verdadero *game changer*. Es el algoritmo como «adversario», como «combatiente» propio, como «combatiente» aliado. Es el algoritmo a través del cual se obtiene ventaja militar.

Y todavía están por llegar nuevos y más disruptivos desarrollos tecnológicos, que continuarán requiriendo agilidad. Es necesario, como indica el documento Entorno Operativo 2035 (EO 2035), adoptar decisiones que supongan una autentica transformación que, a su vez, mantenga la experiencia acumulada, las misiones y la naturaleza de las FAS.

La transformación digital (TD) para el combate multidominio se constituye como uno de los vectores de la Transformación global referida anteriormente. Su objetivo principal no es volverse digital, no es digitalizarse, no es solo ser más eficientes en nuestra misión diaria, tal y como la desempeñamos hoy. Es también capitalizar las posibilidades del 5G, el *Big Data*, la IA, el almacenamiento y computación en la nube, o las que ofrecerán en un futuro las tecnologías cuánticas para generar nuevo valor, nuevas formas de combatir, nuevas posibilidades que no teníamos previstas. De otra forma, no es posible.

Sin embargo, aunque inicialmente pueda parecer lo contrario, la TD tiene que ver con la misión y las personas. Las tecnologías que hay que adoptar son importantes, pero el factor determinante son las personas. Las transformaciones no suceden porque se establezca una estrategia, por muy acertada y visionaria que sea. Ni porque se incorpore la última tecnología de vanguardia. Ni siquiera porque se destinen recursos suficientes. Si bien todo ello contribuye y es necesario, la transformación en las organizaciones sucede cuando las personas deciden abrazar el cambio e incorporarlo en su tarea diaria. Es decir, la transformación es real cuando las personas entienden la racionalidad del cambio y deciden transformarse, poniendo en ello toda su pasión, voluntad y compromiso. Entonces invierten una energía extra, adicional, para que el cambio suceda y marcan la diferencia. Es por ello que la TD para las MDO es, sobre todo, un proceso de gestión del cambio, en toda su complejidad, no de gestión de la mera incorporación de tecnologías.

La piedra angular de este proceso la conforma la Visión común y compartida de las MDO por parte de los máximos niveles de responsabilidad. En ella no solo se acierta a perfilar el horizonte y los objetivos a conseguir, sino que también se entiende y acepta la magnitud del cambio, colocándolo entre los asuntos relevantes y prioritarios de la agenda. De no existir este compromiso decidido, esta involucración personal mantenida en el tiempo, el proceso de TD para las MDO, que ha de ser continuo y que requiere tiempo y esfuerzo adicional, correría el riesgo de ralentizarse, volverse dificultoso y consumir un nivel extraordinario de energías.

Otro factor a considerar es la premura con la que acometer este proceso y determinar el ritmo de progreso. Algunos de los indicadores a considerar para determinar este factor podrían ser: el nivel tecnológico previsto

en los escenarios de confrontación posibles, establecido también por el potencial adversario; el nivel de desarrollo tecnológico de los sistemas de armas de incorporación previsto en las FAS; y el grado de evolución, también en términos de complejidad, de la tecnología disponible, así como su accesibilidad por el adversario. Por otro lado, a estos efectos, también es necesario considerar que los cambios de índole cultural y organizativo que llevan consigo un nuevo aprendizaje, abandonar hábitos, comportarse de forma diferente o, en esencia, salir de la zona de confort, no son ni rápidos ni fáciles. No se trata de estar atrapados por la urgencia del corto plazo, pero todo parece indicar que es necesario acelerar en lo posible el cambio e impulsar el proceso hacia las MDO y el de la TD que las hará posibles.

Sin embargo, no estamos en la línea de salida. La transformación digital en las FAS no es un camino que se inicie ahora, sino que, más bien al contrario, ya está empezando a dar sus primeros frutos. La TD para las MDO se encontraría incluida en la fase de desarrollo, ya iniciada, del Plan de Acción del MDEF para la Transformación Digital, segunda parte, que comprende los medios y servicios que afectan a la defensa, consulta política, situaciones de crisis y seguridad del Estado.

Están publicados los principales documentos de referencia. En primer lugar, el «mandato», contemplado en los principios básicos comunes de la organización de las FAS, cuando determina que «la TD de las FAS garantizará la evolución permanente y la adaptabilidad de su organización para hacer frente a los retos derivados de la era digital y de las tecnologías disruptivas». También está en vigor la Política CIS/TIC, la Política de Seguridad de la Información y la Estrategia de Gestión de la Información y el Conocimiento. También las estrategias 5G, de Explotación de la Nube y de Desarrollo, implantación y uso de la inteligencia artificial. Para el caso de las MDO son también de referencia la Visión del JEMAD de la Nube de Combate, el concepto exploratorio «Evolución de la Fuerza Conjunta hacia las operaciones multidominio» y la Estrategia Industrial de Defensa 2023, principalmente en su eje número 6.

Desde una perspectiva más tecnológica, está avanzada la implantación de la Infraestructura Integral de Información para la Defensa (I3D); el «sistema nervioso» que proporcionará la necesaria conectividad y seguridad, que podrá ampliarse en una red que integre también otros actores estatales, podrá incorporar soluciones tecnológicas avanzadas y que en julio de 2023 ya alcanzó su capacidad operativa inicial (IOC). Integrado en la I3D, se encuentra el Sistema de Mando y Control Nacional (SC2N), cuya IOC ya ha sido también declarada y en la actualidad se encuentra implantado para las operaciones que se realizan en el marco de las misiones permanentes, y también la Plataforma para la Armonización para la Gestión de la Organización (ARGO), que constituye el núcleo que permitirá la adopción

de un modelo de organización en las FAS basado en procesos de trabajo y centrado en el dato.

También está definido desde 2015 el modelo de gobernanza para el impulso y la coordinación en el MDEF de la Administración Digital y que lo constituye, principalmente, la Comisión Ministerial de Administración Digital del Ministerio de Defensa (CMAD), y su comisión permanente (CPCMAD). Sin embargo, el proceso de TD para las MDO incluye una cierta particularidad; afecta al principal «proceso de negocio», es eminentemente transversal, y se circunscribe, principalmente, a la estructura operativa de las FAS. En este sentido, dentro del modelo de gobernanza establecido, parece plausible la opción de repensar la estructura actual por si pudiera adaptarse mejor a estos rasgos distintivos.

Finalmente, es necesario establecer objetivos operativos y hoja de ruta en este proceso de TD para las MDO, y plasmarlos en iniciativas y proyectos concretos que nos permitan alcanzar la Visión establecida en origen. Es necesaria una estrategia integradora, que marque y secuencie hitos claros de transformación, asegure los recursos, y permita incrementar la velocidad de incorporación de estas tecnologías. Una estrategia que goce del compromiso de todos y esté alineada con la cultura de la organización.

De entre las líneas de acción emanadas de esta estrategia, podrían adivinarse dos de ellas. En primer lugar, la relacionada con la cultura digital, la formación, las competencias y el talento digital. De especial importancia será la capacidad para diseñar, modificar u optimizar algoritmos, de forma que se garantice la autonomía de las FAS sobre los productos o aplicaciones de *software* con IA adquiridos de la empresa privada, y permita además poder incorporar el componente innovador propio. En segundo lugar, la concerniente a la gobernanza del dato, que requiere de la máxima atención por ser la piedra angular sobre la que se construyen las MDO. Una condición *sine qua non* la constituye el impulso en el cumplimiento de los estándares que emanan de CESTIC (Centro de Sistemas y Tecnologías de la Información).

Se estima que un 85 % de las organizaciones a nivel mundial están inmersas en procesos de transformación relacionados con la tecnología digital. De ellas, las cifras de las principales consultoras en esta materia establecen que el 70 % no alcanzan sus objetivos prefijados. Como norma general, el motivo más frecuente está relacionado con la cultura y la organización, es decir, en último término, con las personas. No con la tecnología. Los desafíos culturales y de comportamiento, un pobre entendimiento de las tendencias digitales, carencias en el talento digital, una organización inadecuada, o la falta de alineación interna entre los actores más relevantes se encuentran entre los factores principales señalados.

No es casualidad, por tanto, que el primer capítulo lleve por título «Personas, cultura, organización y liderazgo», ni que a lo largo de su desarrollo se aborde la dimensión humana y organizativa que supondrán, tanto las MDO como la TD que ha de conducir a ellas. En un sugestivo y resuelto artículo, el GD Fernando Morón afronta con determinación y creatividad este desafío, ofreciendo una perspectiva que invita al debate y a la reflexión. Su trayectoria profesional en el ámbito de las tecnologías de la información y de las comunicaciones, sus responsabilidades pasadas en la gestión de la información y del conocimiento y, sobre todo, su formación humana han contribuido sin duda a su calidad.

Su trabajo se articula en dos grandes bloques. En una primera parte, se adentra en las dimensiones psicológica, emocional y social del ser humano y, como si de la fase inicial de un análisis DAFO (Debilidades, Amenazas, Fortalezas, Oportunidades) se tratase, el autor repasa las debilidades y fortalezas más relevantes, tanto desde el punto de vista de la persona, del combatiente, como del grupo al que pertenece. Una especie de «conócete a ti mismo», en alusión al célebre aforismo griego del templo de Apolo en Delfos, que resulta esencial y previo, imprescindible, para acometer con éxito este proceso de transformación. En una segunda parte, propone algunas líneas de acción para abordar la complejidad de las MDO, de nuevo con un doble enfoque en las personas y en la organización.

Acometer el cambio de paradigma que suponen las MDO, desde su complejidad intrínseca, va a depender en gran medida de cómo cada uno perciba esta realidad y la interprete. Hacernos conscientes de ello va a contribuir, entre otros, a un análisis más preciso del entorno y a una posterior toma eficaz de decisiones.

Uno de los factores que más dificulta este proceso lo constituye el hecho de que cada persona percibe e interpreta la realidad de forma diferente. Y basándose en esa interpretación decide cómo actuar o qué camino seguir. En esta interpretación no consciente, natural, por tanto, el autor pone de relieve la existencia de sesgos cognitivos, esto es, efectos psicológicos, resultado del proceso evolutivo, que nos predisponen a llegar a determinadas conclusiones de manera automática e irracional. Consecuentemente, tienen un efecto directo no solo en nuestras emociones, sino también en el proceso de cómo y por qué decidimos de una determinada manera, en ocasiones más allá de la razón y la lógica.

Otro de los factores es el mayor o menor grado de acomodación de las personas a estas dinámicas de cambio. Sobre todo, cuando, como es el caso de las MDO, llevan consigo conceptos novedosos, complejos y que desafían el entorno conocido, que hasta entonces nos proporcionaba seguridad y certidumbre. Y es en este nivel de adaptación, donde juega un papel

relevante la personalidad de cada uno, es decir, su tendencia estable a pensar, ser y sentir, fruto tanto de factores genéticos como adquiridos.

Comoquiera que los diferentes tipos de personalidad engloban a su vez diferentes rasgos, las hay que facilitan más estos procesos de transformación, mientras otras son más limitativas. Para familiarizarnos con esta identificación de rasgos, el general Morón hace referencia a dos herramientas clásicas: el indicador de *Myers-Briggs*, basado en la tipología de *Jung,* y el test de dominancia cerebral de *Herrmann*. También, y complementario a lo anterior, considera los efectos de la impronta militar, es decir, la huella que dejaron en cada uno sus primeros destinos y que, pasado el tiempo, continúa influyendo e incluso puede facilitar que, en ocasiones, intentemos resolver problemas nuevos con argumentos o herramientas que aprendimos entonces.

Tomando todo ello como base, avanza el artículo ampliando su perspectiva para situarnos en la dimensión sociocultural, como elemento también de extraordinaria influencia. No en vano, las MDO llevan intrínsecas un cambio en la actual forma de concebir las operaciones militares, con una agilidad y una complejidad inusitadas como principales factores que las definen.

Para alcanzar esta agilidad es necesario, entre otros, vencer los «silos» que generan el sesgo colectivo de «endogrupo», por el cual los miembros de un grupo tienden a favorecer y valorar de manera más positiva a su colectivo y beneficiar a las personas pertenecientes al propio grupo, en detrimento de las que no lo son. Grupos en los que, por otro lado, pone la atención el autor en el hecho de que convivan cuatro generaciones de personas que, en términos generales, perciben la realidad de forma diferente, entienden su desarrollo personal y profesional de manera distinta y en las que también tienen desigual impacto las nuevas tecnologías. Conscientes de ello, es necesario que estas generaciones se complementen entre ellas, de forma que sus fortalezas se vean potenciadas y sus debilidades reducidas.

Por otro lado, afrontar a la complejidad tampoco es tarea fácil, alertándonos el general Morón de que no percibirla en su adecuada dimensión puede convertirse en un factor limitante. Sugiere, en este sentido, la adopción del modelo «Cynefin» como herramienta para evaluar y definir las situaciones a las que nos enfrentamos y poder gestionar mejor la toma de decisiones en entornos complejos y, en ocasiones, irracionales o imprevisibles. Este modelo, muy conocido y empleado en el entorno de desarrollo de modelos ágiles, permite identificar el tipo de problema que realmente tenemos, abordarlo desde perspectivas nuevas y utilizar la estrategia más adecuada para su solución.

Porque abordar las MDO es abordar una nueva complejidad que solo es posible llevar a cabo si, en primer lugar, potenciamos e incorporamos en

el personal las habilidades que necesitan para planearlas y ejecutarlas. Habilidades que han de permitir ir más allá de los propios silos de pertenencia. Incluso más allá de las fronteras de la propia organización para, llegado el caso, poder incorporar, integrar, participantes provenientes de otras administraciones, agencias e incluso corporaciones privadas. Habilidades que le permitan generar vínculos transversales de confianza mutua, basándose en un alto grado de competencias interpersonales.

Pensamiento crítico y pensamiento sistémico constituyen dos competencias clave. El primero, muy relacionado con la lógica, la creatividad y la intuición, permite analizar y explicar situaciones de forma razonada, con una mayor apertura de mente. También revisar y adaptar nuestras afirmaciones según lo que observamos y aprendemos, sin dogmas o axiomas absolutos.

El pensamiento sistémico, en el que el autor se detiene algo más, constituye otra capacidad esencial, imprescindible, que es necesario incorporar. A través de él somos capaces de adquirir una visión de conjunto, de ver la *big picture* de una situación o problema complejo, difícil de explicar, en el que no descubrimos una relación de causalidad ni sobre el que es posible predecir su comportamiento. En definitiva, que se constituye por medio de interconexiones e interdependencias complejas de múltiples variables. Incorporar formalmente en las FAS el pensamiento sistémico a los órganos de prospectiva y a los grupos de planeamiento operativo, afirma el general, puede producir una ventaja competitiva en nuestras capacidades MDO.

También es necesario repensar la organización. La jerarquía, que forma parte de nuestro ADN, ha de ser complementada, como si de una organización híbrida se tratase, con otras estructuras más planas, principalmente en la función de Mando y Control, que faciliten la velocidad, la adaptabilidad y la creatividad. Estructuras «redárquicas» orientadas tanto a la gestión del conocimiento, para aumentarlo y difundirlo, como a la creación y a la innovación, con el propósito último de generar opciones al comandante. Este modelo de organización, por el que la información fluye a gran velocidad y puede mutar con agilidad, es más adecuado para el caso de las operaciones en la «zona gris»; además, permite integrar con facilidad y eficacia actores no militares. La forma de llegar a él propone el autor es a través de una mayor colaboración horizontal entre los mandos operativos y, quizás, con el Centro de Inteligencia de las FAS (CIFAS), que sirviera de base para acumular experiencia y extraer conclusiones válidas.

Finalmente, o tal vez lo primero, para transitar este proceso de transformación es necesario contar con un liderazgo que, más que orientado al logro, esté orientado al cambio, generando visión compartida, fomentando la creatividad, estimulando el trabajo en equipo y generando seguridad psicológica. Un líder, resalta el general Morón, que dirija la transformación

desde dentro, fomente que las ideas fluyan fácilmente, con rapidez y en sentido omnidireccional, y que todos los miembros de la organización se sientan y actúen como agentes de cambio.

Sin embargo, este líder, cuya filosofía de liderazgo del mando orientado a la misión sería la que mejor se adaptase a este modelo de operaciones, requiere de una formación y experiencias específicas en materia de MDO. Un camino que es necesario que comience a andar para, llegado el momento, introducir lo aprendido en el arte operacional.

Finaliza su artículo el general Morón incluyendo unas conclusiones que sintetizan lo tratado y ofreciendo también algunas recomendaciones, por si pudieran contribuir al cambio cultural y organizativo que las MDO llevan implícito y sobre el que, afirma, no podemos esperar, sino que estamos obligados a transformar un «avión» que está en pleno vuelo.

Por otro lado, una aproximación desde la tecnología destacaría la conectividad y la interoperabilidad como los posibilitadores que hacen posibles las MDO. Una conectividad resiliente y segura que proporcione agilidad y rapidez, conectando sensores, nodos, centros de Mando y Control y efectores.

Sin conectividad, sin una hiperconectividad resiliente y segura, no son posibles las MDO, y es por ello que el segundo capítulo centra su atención en esta capacidad habilitadora esencial. A lo largo del mismo, el capitán de navío (R) Luis Astorga lleva a cabo una aproximación «de amplio espectro» en la que se vale de su actual destino como presidente de la Organización de Comunicaciones e Información de la OTAN (NCIO) para proveer una visión complementaria desde la Alianza Atlántica. También aprovecha sus conocimientos como Doctor en Seguridad Internacional para enriquecer sus argumentos con las guerras de Armenia y Azerbaiyán, en 2020, y la actual de Ucrania.

Comienza el artículo realizando un repaso preciso de la evolución que han seguido los diferentes tipos de conectividad, de acuerdo al avance de la tecnología. Conectividad que inicialmente unía a humanos, más tarde a estos con máquinas para finalizar en la unión entre máquinas con la aparición del Internet de las cosas (IoT). Una conectividad generalizada, segura y rápida proporcionada actualmente por las redes 5G y en un futuro por las de sexta generación. Conectividad que, por otro lado, también generó en su momento la capacidad de combate en red (NEC, *Network Enabled Capability*), propiciando la transición de las operaciones centradas en la plataforma, como había sido hasta entonces, a las operaciones centradas en red.

En este sentido, aborda el autor a continuación la diferencia que percibe entre estas operaciones centradas en red y las nuevas MDO, centradas

ahora en los datos. Resalta como hechos diferenciales la incorporación de nuevos ámbitos y la posibilidad de aplicar nuevas tecnologías como la IA.

Continúa el artículo analizando cómo la evolución tecnológica de los sistemas de armas promovió la aparición de los sistemas de intercambio automático de datos como el link-11 y link-16, así como el impacto que supuso para la conducción y desarrollo de las operaciones. Las posibilidades que generaron las comunicaciones por satélite permitieron incrementar en cantidad y calidad las capacidades de enlace entra las unidades, fortalecer la coordinación, ampliar la conciencia situacional e incrementar la seguridad.

Alerta el autor, en este sentido, sobre la nueva versión que podría originarse de «niebla de la guerra» si todos los sensores, efectores y combatientes estuvieran conectados al mismo tiempo y con el mismo acceso a toda la información disponible. Analiza la relación entre un mayor volumen de información y una mejor y más precisa conciencia situacional, fruto de la mejora de la conectividad, y su impacto en los clásicos niveles de conducción estratégico, operacional y táctico.

Con relación a los límites y posibilidades de la IA, el autor realiza una interesante reflexión sobre la progresiva incorporación de la inteligencia artificial que estamos experimentando y sus límites respecto al incremento de variables, datos sobre los que basarla y, sobre todo, por el hecho de que el mundo no se rige por un principio predecible y siempre hay un lugar para el azar. La IA «no es una bola de cristal», afirma el CN (R) Astorga.

Continúa el autor su artículo levantando su mirada al horizonte para intentar responder a la pregunta sobre qué podemos esperar en las próximas décadas en el ámbito de la conectividad; congestión del espectro electromagnético, participación de operadores privados, incremento de las comunicaciones por satélite, especialmente en órbitas bajas, impacto de las tecnologías cuánticas, redes de telefonía móvil, y en los efectos en la conectividad del empleo masivo de drones.

Para el CN (R) Astorga, el futuro, pendiente siempre de lo que nos proporcione la investigación y la experimentación formal, nos traerá una conciencia situacional mejorada, enfocada principalmente en los niveles operacional y táctico, en la que la IA y la seguridad tienen una importante relevancia. Las decisiones estarán basadas en datos que «viajarán» mediante *Tactical Data Links* (TDL), el ancho de banda continuará siendo una limitación y, señala, «*no debemos prescindir de los niveles de conducción, proporcionando una conciencia situacional adaptada a las necesidades de los combatientes en el terreno*».

Muy relacionado con la conectividad, el tercer artículo aborda otro de los elementos esenciales para la planificación y conducción de MDO; la

Nube de Combate. Una primera aproximación la definiría como: una red de cobertura global dentro de un espacio de batalla que permite la gestión de la información y la prestación de servicios, con el fin último de tomar decisiones y ejecutar operaciones militares. Simplificándolo mucho, hacer posible que quien combate tenga la información correcta en el momento que la necesita.

Manuel Buesa Bueno, ingeniero de sistemas de Indra y responsable en París del proyecto FCAS nos traslada su visión sobre el importante y complejo reto que supone la concepción, desarrollo e implantación de una nube de combate para convertirla en el corazón de las MDO de la Fuerza Conjunta.

Comienza su artículo deduciendo la necesidad de contar con una Nube de Combate a la luz de los requisitos que imponen las MDO, principalmente los derivados de la centralidad del dato. De esta forma, conectividad, gestión de los datos y la información, apoyo al mando en la toma de decisiones, así como seguridad, fiabilidad y resiliencia constituyen las cuatro necesidades fundamentales derivadas de las MDO que, de manera transversal, ha de cubrir la nube de combate.

¿Qué es la nube de combate?, se cuestiona seguidamente el autor. E intenta responder a esta cuestión a través de su concepto, los elementos de su arquitectura y sus características principales. Enfoca su atención en las capacidades que genera la constitución en ella de un Sistema de Sistemas, que puede operar simultáneamente en los niveles estratégico, operacional y táctico. Una red de nodos que conforman el eje de su arquitectura y que integran comunicaciones, servicios de información y recursos de computación.

Continúa avanzando en su definición de Nube de combate, aproximándose ahora a ella desde la seguridad que requiere y los servicios que proporciona. Respecto a la primera, señala la necesidad de comenzar por la seguridad del propio dato, las políticas de acceso, la monitorización de eventos y la vigilancia activa, así como la reacción automática a las alertas. Con relación a los servicios que provee, estos son agrupados y desarrollados en el artículo de acuerdo con la taxonomía de la OTAN en: servicios de comunicaciones, servicios *core* y servicios de comunidad de interés.

Finaliza su aproximación conceptual a la nube de combate, subrayando la necesidad de establecer unos principios de arquitectura y operación específicos como base para la gobernanza. También señala algunas características de la nube como: hiperconectividad, prestaciones dinámicas, ubicuidad, resiliencia, escalabilidad, consistencia-coherencia del dato y adaptabilidad dinámica.

En una segunda parte del artículo aborda los aspectos más sobresalientes a considerar a la hora de desarrollar e implementar la nube de combate. En primer lugar, considera la necesidad de acelerar el proceso de TD en curso dentro de las FAS, haciendo de las personas el motor del proceso, evolucionando hacia un modelo que ponga el dato y la información en el centro, asegurando una inversión económica consistente y sostenida.

En segundo lugar, alerta sobre la conveniencia de, previo a los trabajos de diseño, fijar estándares de comunicación que garanticen la conectividad y estándares de diseño de servicios para permitir el intercambio de información. A partir de aquí, es posible comenzar la fase de diseño y desarrollo, atendiendo a los requisitos de la infraestructura de la nube y a los servicios de Mando y Control que soporta y que aportan el verdadero valor del sistema. Llama la atención el autor sobre la necesidad de contar, como incluye la Estrategia de explotación de la nube en el MDEF, con un entorno de desarrollo, pruebas y validación en el que un equipo multidisciplinar de personas pueda experimentar y valorar los desarrollos que se generen.

Por último, desarrolla el proceso de implementación de la Nube de Combate tanto para las nuevas plataformas o sistemas a adquirir como para las actuales, a través de un proceso de adaptación. En este sentido, considera la doble posibilidad de: federar nubes desarrolladas bajo los mismos estándares o conectar mediante pasarelas aquellas que no los comparten.

Finaliza el artículo subrayando dos aspectos que considera capitales. El primero de ellos pone el acento en los procesos de adquisición de material y la necesidad de establecer requisitos específicos que garanticen la interoperabilidad entre los sistemas conectados. El segundo se refiere a la conveniencia elaborar un plan estratégico que gobierne y guie los cambios hacia las MDO, constituya una hoja de ruta y en ella se establezcan los parámetros que definan la nube de combate que las FAS necesitan.

Sin embargo, todo el proceso de TD tratado hasta ahora requiere de una condición *sine qua non* las MDO no serían posibles. Una condición última, si no la primera. Es necesario asegurar la libertad de acción en el ámbito de operación ciberespacial. Es necesario garantizar la resiliencia y la supervivencia de los elementos físicos, lógicos y virtuales críticos que hacen posible las MDO.

Con el objetivo de contribuir a este fin, el teniente coronel Rubén Vega Bustelo, destinado en el Mando Conjunto del Ciberespacio (MCCE), ofrece su capítulo titulado «Seguridad y transformación digital para el multidominio». Su formación y experiencia dan como resultado un artículo rico en referencias y de fácil lectura y comprensión para un tema de elevada complejidad técnica.

Su aproximación a la seguridad, como no puede ser de otra forma por el destino que ocupa, mantiene un perfil eminentemente operativo, orientado a la misión de la Fuerza Conjunta. Y es que el ámbito ciberespacial es eminentemente transversal al resto y, por tanto, su seguridad, tanto física como lógica, se constituye en piedra angular para las MDO. Así, la supervivencia de la red y de la Fuerza, la seguridad de los datos, preservar el secreto de las operaciones y garantizar en último término la libertad de acción del comandante de la Fuerza Conjunta, han de constituir los primeros objetivos de protección.

En este sentido, afirma que la infraestructura digital que sustente las MDO futuras será en su momento un centro de gravedad (CoG) y, por tanto, si es controlado o destruido, las opciones de éxito se reducirán drásticamente. Basándose en esta afirmación, el autor desarrolla conceptualmente su visión de una Nube de Combate, diferenciándola de otras aproximaciones como los «servicios en la nube» o el «cloud computing». Afirma que su seguridad requiere de una aproximación holística, integrada e integradora, bajo una arquitectura coherente y flexible.

En lo referente a su diseño, el teniente coronel Vega propone una solución técnica de *Edge Computing*, que acerque la capacidad de almacenamiento y las aplicaciones a la zona de operaciones, a la línea de combate. Sus ventajas en términos de supervivencia, velocidad, capacidad de procesamiento y disponibilidad superan los retos derivados de la menor potencia computacional disponible, la menor capacidad de los enlaces y de la proximidad al adversario.

Como estrategia de seguridad de toda la arquitectura de red, el autor apuesta por la simplicidad, abandonando el concepto de seguridad perimetral para decantarse por el conocido como *Zero Trust*. Este parte de la premisa de la existencia de brechas de seguridad tras los cortafuegos, no siendo posible, por tanto, confiar en «nadie ni en nada», por defecto. A partir de aquí, el autor va desgranando los principios sobre los que se basa esta filosofía de seguridad, sus ventajas y sus propuestas para la implementación técnica del modelo.

Por otro lado, también aborda la necesidad de asegurar los enlaces, principalmente inalámbricos, que interconectan la red de nodos. De forma sucinta, se van analizando las diferentes tecnologías que proveen esta capacidad, haciendo especial referencia a la seguridad que proporcionan. Así son tratados, los *Tactical Data Link*, como topología mallada, y las tecnologías celulares, 5G y 6G y satélites, como grupo de tecnologías orientadas a la cobertura de zona.

Avanza el autor en su artículo con una sugerente reflexión sobre la necesidad de la ofensiva, la suficiencia de la defensiva y la mayor fortaleza de

una u otra a la hora de planificar y llevar a cabo operaciones en el ámbito ciberespacial, con el objetivo último de la libertad de acción. Al trasladar al ámbito ciberespacial los conceptos tácticos relativos al terreno que contempla la doctrina terrestre, concluye que la seguridad solo se puede alcanzar mediante la combinación de operaciones de infraestructura, ofensivas, defensivas y de inteligencia, vigilancia y reconocimiento. La autoridad operativa del ciberespacio debe contar, además, con las atribuciones necesarias para planear y ejecutar estas operaciones.

Como última recomendación de seguridad se subraya la necesidad de repensar el tradicional enfoque en la protección de los dispositivos, aplicaciones y redes para inclinar la balanza sobre la seguridad de los propios datos. Sobre la base de tecnologías criptográficas, herramientas de seguridad ya comercializadas o soluciones que actualmente se encuentran en desarrollo, la protección centrada en los datos (*Data Centric Security*) permite protegerlos, controlarlos y auditar su uso, no solo dentro de la organización, sino allí donde estos viajen y se almacenen.

Finaliza el capítulo definiendo el marco de integración operativa con otros poderes del Estado, a través, principalmente, de la participación del Mando Conjunto del Ciberespacio en el Consejo Nacional de Ciberseguridad, la Comisión Permanente de Ciberseguridad y del Equipo de Respuesta ante Emergencias Informáticas del Ministerio de Defensa (ESPDEF-CERT). De esta forma, se da respuesta a la Estrategia Nacional de Ciberseguridad y se contribuye a la unidad de acción en el Sistema de Seguridad Nacional, garantizando, tanto en paz como crisis, la necesaria sincronía e integración de las capacidades y operaciones militares en el ciberespacio con el resto de actores del Estado. Este entorno operativo permite la libertad de acción del mando y el empleo de las capacidades de combate multidominio de la Fuerza Conjunta.

Y estas dos últimas posibilidades, libertad de acción y empleo de capacidades, nos introducen en el último capítulo de esta publicación, que versa sobre el Mando y Control de las MDO. Porque la visión de futuro que nos permite atisbar los cambios transformacionales necesarios tanto en individuos como en organizaciones; la necesaria conectividad e interoperabilidad entre todos los elementos que intervienen de forma directa o indirecta en el campo de batalla; el elemento facilitador de la globalización del dato y de la información llamado nube de combate; y por último, el reto que implica en el entorno multidominio lograr la seguridad del mismo y de la información derivada; abren la puerta a una interesante reflexión sobre cómo sacar partido de todo ello en beneficio de la toma de decisiones, facultad intrínseca a la función de Mando y Control.

Con el objetivo de contribuir a este propósito, el comandante (en excedencia) D. Juan Ramón González Espadas ofrece su experiencia desde una

doble vertiente, como oficial y piloto de combate en su etapa de servicio activo en el Ejército del Aire y del Espacio y como *Senior Operational Advisor* en el programa *Future Combat Air System* (FCAS), su actual cometido en la empresa Airbus.

En el inicio del capítulo, con el fin de enmarcar el desarrollo de su contenido, se fija el qué debe entenderse por Mando y Control, por MDO y por control distribuido, estableciendo como escenario de referencia el Contexto Operativo (CO) 1, de Defensa Militar, contemplado en la primera revisión del documento «Entorno Operativo 2035», por ser en el que las FAS desarrollan su misión primordial.

A continuación, el autor remarca el papel del Mando y Control como piedra angular del sistema de combate futuro que englobará el conjunto de capacidades operacionales necesarias para alcanzar los objetivos militares en el escenario multidominio.

Llegado este punto, el autor plantea cuatro cuestiones: ¿Qué obliga a transformar el actual modelo de Mando y Control? ¿Qué es necesario transformar? ¿Para qué fin? Y, por último, ¿Cómo abordar la transformación?

La respuesta a la primera de las preguntas se sustenta en la identificación de tres factores: el cambio de las características del campo de batalla; el inventario cada vez más reducido de sistemas de combate; y la amenaza creciente con origen en el ámbito ciberespacial.

A renglón seguido, el autor enfrenta el qué transformar en el modelo de Mando y Control poniendo el foco de atención en tres variables: la atribución de derechos de decisión, relacionada con la delegación de autoridad; el patrón de interacciones, relacionado con los modelos de organización; y la distribución de la información, relacionada con la eficacia del modelo de gestión de la información. El análisis de estas tres variables le llevan a concluir la necesidad de migrar el modelo de Mando y Control de hoy, centrado en los diferentes mandos componentes, hacia una solución unificada de Mando y Control multidominio, que englobe y supere los actuales sistemas y que permita adaptar las variables mencionadas en función de la demanda de las operaciones militares en curso.

El proceso reflexivo llevará al lector a la tercera de las preguntas, el fin último de la transformación planteada, que en opinión del autor no es otro sino el dotarse de la agilidad para adaptar y ejecutar una cadena letal más eficaz y resistente. La escalabilidad, el alcance, la velocidad y la supervivencia de la cadena letal para lograr efectos en el espacio de batalla futuro están íntimamente ligados a un nuevo concepto de Mando y Control.

La respuesta a la última incógnita, el cómo llevar a cabo la transformación del Mando y Control, se acomete planteando diferentes actuaciones. Para

el autor, incrementar el número de nodos de Mando y Control; el empleo intensivo de las *Emerging and Disruptive Technologies* (EDT); la mejora de la interoperabilidad de los sistemas de combate; la potenciación de las operaciones desde el espacio; aumentar la capacidad de supervivencia nodal y de red; y un renovado liderazgo, pensamiento y formación del recurso humano; sientan las bases sobre las que desarrollar un Mando y Control multidominio y ágil, un nuevo concepto que el entorno operativo 2035+ exige.

Agradecimiento

Quisiera agradecer a los participantes de esta publicación la generosidad que han demostrado al compartir con los lectores sus conocimientos y experiencias. También por el tiempo dedicado a la investigación, análisis y desarrollo de sus respectivos artículos. Horas robadas al tiempo libre y al descanso. Mi gratitud se extiende a los miembros del Centro Conjunto de Desarrollo de Conceptos (CCDC) por su asesoramiento y guía en este proyecto, en especial al teniente coronel Luis Olalla Simón por su compromiso con el mismo.

Con toda seguridad, este trabajo, realizado desde la humildad de sus autores, podrá contribuir a la labor de quienes tienen asignada la misión de marcar el camino en la tarea siempre inacabada de construir unas Fuerzas Armadas de vanguardia, que continúen en el futuro prestando su mejor servicio a España; disuadir y, si preciso fuera, luchar y vencer.

> *«La victoria sonríe a quienes se anticipan a los cambios en el carácter de la guerra, no a quienes esperan para adaptarse a ellos».*
>
> *Giulio Douhet. El Dominio del Aire. 1921*

Capítulo 1

Personas, cultura, organización y liderazgo

Fernando Luis Morón Ruiz

Resumen

La transformación digital de las Fuerzas Armadas es la base que sustenta los elementos clave para las operaciones multidominio. Implica un cambio de mentalidad y en la cultura organizativa. El cambio de cultura está vinculado al modelo de organización, tipo de liderazgo y dinámicas entre las personas. Tener en cuenta la mente humana y los factores que influyen en la mentalidad militar es importante para acometer la transformación efectiva. Las operaciones multidominio implican entender qué es la complejidad y dotarse de pensamiento sistémico para tomar las decisiones correctas. También requieren un mando y control más colaborativo y nuevos modelos de organización, que permitan la participación de actores no militares, la orquestación de acciones entre dominios y ámbitos, y la ampliación del espacio de competición de las Fuerzas Armadas en la zona gris. Para ello es necesario un liderazgo transformacional y la adopción del Mando orientado a la Misión. También dotarnos de personal con las habilidades necesarias, duras y blandas, que requiere el nuevo entorno operativo. El cambio de cultura organizativa debe implicar a todo el personal y acometerse ya en todas las estructuras, con sentido práctico y de aprendizaje continuo, sin esperar necesariamente a desarrollos tecnológicos.

Palabras clave

Transformación digital, Operaciones multidominio, Sesgos mentales, Marcos de referencia, Personalidad, Mentalidad, Cultura organizacional, Diferencia generacional, Complejidad, Pensamiento sistémico, Mando y Control, Colaboración, Redarquía, Competición, Zona gris, Orquestación, Liderazgo, Seguridad psicológica, Diversidad, Mando orientado a la misión, Habilidades duras y blandas.

People, culture, organization and leadership

Abstract

The Digital Transformation of the armed forces is the foundation that contains the key elements to enable multidomain operations. It implies a change in mindset and in organizational culture. Culture change is linked to the organisation model, the leadership style and dynamics between people. To achieve effective transformation, it is important to consider the human mind and the elements that influence the military mindset. Multidomain operations require understanding what complexity is and the use of systems thinking to make the right decisions. They also require a more collaborative command and control and new organisational models that allow for the participation of non-military actors, the orchestration of actions across domains and environments, and the expansion of the military competitive space of the armed forces into the grey zone. The adoption of mission command and a transformational leadership style are required, as is the provision of people with the right hard and soft skills for the new operational domain. The change in organisational culture must involve all personnel and be implemented immediately in all the structures, with a practical approach of continuous learning, without necessarily waiting for technological developments.

Keywords

Digital transformation, Multidomain operations, Mental biases, Mental models, Personality, Mentality, Organizational culture, Generational gap, Complexity, Systems thinking, Command and Control, Collaboration, Netarchy, Competition, Grey Zone, Orchestration, Leadership, Psychological security, Diversity, Mission command, Hard and soft skills.

1. ¿Qué relación tienen la transformación digital y el combate multidominio, en el contexto humano?

El proceso en curso de TD de las FAS, además de los pilares de gestión por procesos, centralidad de los datos y racionalización de sistemas, incluye dos dimensiones adicionales: la organización y las personas, que comprenden actuaciones clave relacionadas con la formación y la promoción del uso de las nuevas metodologías y tecnologías[1].

Esto implica que, ante todo, la TD en las FAS representa un cambio en las personas y en su cultura organizativa, de manera que con la información (el dato) como referente y activo principal, todas las acciones de los miembros de la organización se alineen y converjan (mediante la gestión por procesos) para alcanzar los objetivos (la misión).

Todo ello con el soporte que proporcionan fundamentalmente las tecnologías de la información y comunicaciones (TIC) y algunas EDT como la IA.

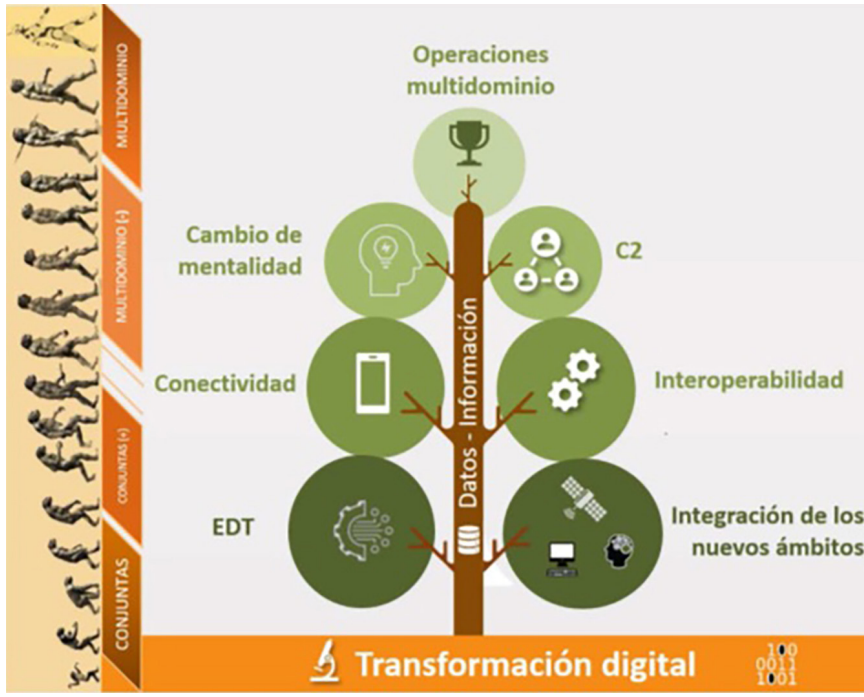


Figura 1. Elementos clave de las MDO. Fuente: Concepto exploratorio Evolución de la Fuerza Conjunta hacia las Operaciones Multidominio, EMAD, 2023

[1] Ministerio de Defensa. (2020). Instrucción 14/2020, de 15 de abril, del secretario de Estado de Defensa, por la que se aprueba la segunda parte del Plan de Acción del Ministerio de Defensa para la Transformación Digital. Apartado 5, párr. 6.

De igual manera, sobre la base de la TD se apoyarán los elementos clave de las MDO, entre los que se encuentran la integración de los nuevos ámbitos no físicos de operación (ciberespacial y cognitivo), el cambio de mentalidad, la forma de Mando y Control (de ahora en adelante C2, *Command and Control*) y cómo se gestiona la información[2]. Es precisamente la gestión de la información, acompañada de la sensorización y digitalización del campo de batalla, la que permitirá conocer la compleja situación que se presenta en las MDO, para lo que será necesario culminar la TD de las FAS[3].

Pese a lo anterior, frecuentemente asociamos la TD con algo eminentemente tecnológico —o de tecnólogos— relacionado con la eficiencia y la productividad y posibilitado por el avance de las TIC. De igual manera, tendemos a pensar que el combate multidominio consiste en una manera hipertecnológica de conducir y ejecutar las operaciones militares, basado en la superioridad que proporciona la aplicación de tecnologías disruptivas emergentes a las capacidades militares.

Estas percepciones nos pueden llevar a pensar que el elemento humano, el combatiente o el comandante quedan relegados por la tecnología en este nuevo entorno operativo de las MDO; que el papel de la iniciativa, la intuición, la estrategia y otros valores tradicionales del genio militar se subordinan al frío dictado de una IA que decide, o al menos sugiere, el mejor curso de los acontecimientos.

Tales suposiciones resultan erróneas, ya que, en general, la tecnología será un potenciador de las capacidades humanas, nunca un sustituto. Pero los medios tecnológicos, por abundantes que sean, se convierten en una fuente de dependencia e incertidumbre, en una grave vulnerabilidad, para aquel ejército o país que no acierte a diseñarlos, desarrollarlos y adaptar su operativa para integrarlos como un elemento de ventaja.

En este contexto, resulta fundamental que el componente humano de las FAS esté familiarizado con un entorno operativo, el de las MDO, caracterizado por la complejidad y la velocidad. En las MDO, los efectos en un ámbito de actuación pueden estar producidos desde otro muy diferente, con consecuencias de segundo y tercer orden difíciles de anticipar. Por ello, a pesar de la cantidad de información disponible, frecuentemente dominará la incertidumbre.

Por otra parte, la guerra siempre ha sido un enfrentamiento de voluntades, un terreno para la sorpresa, la astucia y el engaño dirigidos a las mentes

[2] EMAD. (2023, 28 de marzo). Concepto Exploratorio «Evolución de la Fuerza Conjunta hacia las Operaciones Multidominio». Párr. 49.
[3] Ibidem. Párr. 82.

para doblegar el espíritu del adversario. Precisamente en el entorno operativo multidominio, caracterizado por la interacción de las acciones en los ámbitos tradicionales de combate —característicos de la Fuerza Conjunta— con los ámbitos «no físicos» del ciberespacio y cognitivo, será donde el desempeño y adaptación del elemento humano marquen la diferencia. Mientras se aprovecha la transversalidad y omnipresencia de estos ámbitos no físicos, se intenta influir en las percepciones, sentimientos y comportamiento de los distintos actores intervinientes en el conflicto para desbordar y explotar las debilidades humanas.

Tal es la importancia del componente humano en las MDO que tres de los cuatro principios generales que cita la OTAN en su Concepto Inicial para las MDO[4], y que sirven de cimiento para el desarrollo de esta capacidad, se refieren a atributos de las personas:

- *Unidad*: que requiere colaboración, transparencia y confianza para permitir un planeamiento y ejecución armonizados de las MDO, con el beneficio de la aportación de la diversidad de perspectivas nacionales.
- *Creatividad*: que se apoya en la habilidad de analizar situaciones desde distintos puntos de vista y convertir la complejidad en sencillez. La creatividad aumenta mediante la habilidad de visualizar el contexto y dinámicas existentes, y refuerza la aptitud del comandante para orquestar las MDO.
- *Agilidad:* permite a la Fuerza aprovechar las oportunidades fugaces. Requiere iniciativa, velocidad relativa, priorización y flexibilidad de pensamiento y ejecución.

El cuarto principio de las MDO para la OTAN, *interconectividad*, tiene un componente más material y tecnológico, pero de nuevo con la finalidad de potenciar la capacidad humana: mejorar la comprensión compartida y permitir la interoperabilidad de los elementos de la Fuerza.

Conseguir educar y entrenar soldados que sepan liderar, planificar y combatir en ese entorno, adaptar nuestras estructuras operativas y nuestra cultura organizativa para ser ágiles y resolutivos en MDO al ritmo que exige el vértigo de los acontecimientos, requiere acometer una transformación profunda y real, sin esperar a los posibles desarrollos tecnológicos y adquisiciones que incrementen las capacidades materiales en ese entorno. Pero esa transformación hacia el multidominio solo es posible si, de manera simultánea, todos los componentes de las FAS interiorizan en la práctica cotidiana lo que supone la TD e incorporan los conocimientos y habilidades necesarios.

[4] OTAN. (2022, 5 de julio). *Initial Alliance Concept for Multi-Domain Operations* (NU). ACT. Párr. 19.

Por tanto, será el cambio de cultura, ese elemento 100 % humano vinculado al modelo de organización, tipo de liderazgo y dinámicas entre las personas, el elemento clave a abordar de manera inmediata para acertar en la adecuada TD de las FAS hacia sus capacidades MDO. No podemos esperar; en lenguaje aeronáutico, estamos obligados a «construir el avión mientras volamos».

2. Dificultades para acometer una transformación efectiva

2.1. En el ámbito de las personas

Uno de los principales diferenciadores de las MDO respecto a las operaciones conjuntas es la gran importancia del ámbito cognitivo[5]. Para entender su importancia, es necesario considerar previamente los mecanismos básicos de la mente humana —a nivel individual y grupal— que, a pesar de los increíbles avances del hombre como especie, apenas han evolucionado desde el Paleolítico.

2.1.1. La mente humana. Sesgos y marcos de referencia

Un mecanismo arraigado en el cerebro humano, asociado a nuestra supervivencia para poder reaccionar ante potenciales amenazas, es el de inmediatamente intentar acomodar la infinidad de estímulos que recibe a modelos o patrones aprendidos. La consecuencia es que el ser humano tiende por naturaleza a filtrar la realidad, a simplificarla, aplicando continuamente etiquetas basadas en sus esquemas mentales, en un primer tipo de pensamiento predominante, el *pensamiento heurístico*, que es superficial, rápido y requiere poca energía.

Estos patrones mentales, verdaderos *marcos de referencia*[6] de nuestras percepciones y juicios, se configuran en cada individuo conforme a su temperamento, de base genética, y al carácter que desarrolla como consecuencia de su educación, cultura, entorno y vivencias. Ambos, temperamento y carácter, constituyen nuestra personalidad. Por ejemplo, el rasgo de la personalidad de nivel de *apertura mental*[7], uno de los que más afec-

[5] EMAD. (2023, 28 de marzo). Concepto Exploratorio «Evolución de la Fuerza Conjunta hacia las Operaciones Multidominio». Párr. 23 y 24.

[6] Los marcos de referencia son las estructuras de conocimiento complejo que desarrollamos a través de experiencias personales y profesionales. Cambiar la propia mentalidad requiere una reevaluación de los marcos de referencia al ser estos confrontados con nuevas informaciones.

[7] La apertura mental es la necesidad recurrente de aprender de la experiencia. Se manifiesta en una curiosidad intelectual fuerte, en la creatividad y en una relación cómoda con la novedad y la variedad.

tan a la personalidad y que, como veremos, también favorece la TD y las MDO, es fundamentalmente de base hereditaria.

Por otra parte, existe un modo de pensamiento más profundo y reflexivo que explora todas las opciones, pero que es lento y gasta mucha energía: el *pensamiento algorítmico*. Por naturaleza, nos cuesta recurrir a este tipo de pensamiento más avanzado, especialmente ante una urgencia o bajo presión.

Este estudio de los tipos de pensamiento humano, y los sesgos cognitivos que de él se derivan, le mereció en 2002 el premio Nobel de Economía a Daniel Kahneman por sus implicaciones en nuestra capacidad de juicio y en la toma de decisiones.

De entre los más de 200 sesgos documentados, quizás el más común en la conformación de esos marcos de referencia limitantes es el *sesgo confirmatorio,* por el que las creencias establecidas y los juicios son tan difíciles de cambiar. El ser humano presta una atención especial a la información que refuerza sus creencias, tendiendo a omitir el valor de la evidencia que las cuestiona.

> «No es lo que no sabes lo que te mete en líos, sino lo que das por cierto y no lo es».
>
> *Mark Twain*

A menudo, confiamos más en lo que creemos que en los datos, e inconscientemente solemos recurrir a otro tipo de autoengaño, el *razonamiento motivado*, mecanismo cognitivo que hace que las personas accedan, construyan y evalúen datos y argumentos de manera distorsionada, interpretando la información para que concuerde con sus creencias previas.

Otro de los sesgos individuales que puede impactar negativamente en el proceso de transformación es el denominado *sesgo de autoservicio*[8], o sesgo de interés personal, por el que la gente tiende a atribuirse el crédito personal de los éxitos del entorno, pero no de los fracasos, que se imputan a causas externas o a la mala suerte.

Entre los atajos mentales que empleamos con frecuencia se encuentra el *sesgo de disponibilidad*[9], por el que recurrimos a los ejemplos inme-

[8] Este sesgo también surge como resultado de un sesgo estadístico, por el que la gente piensa que en ciertas áreas es mejor que el promedio (por ejemplo, la mayoría de los conductores piensa que conduce mejor que la media).

[9] El objeto del sesgo de disponibilidad es ahorrar tiempo y energía mental, y está muy influenciado por las experiencias emocionales y las anécdotas fuertes. De esta forma, cuanto más accesible sea un suceso, más frecuente y probable lo creeremos, y cuanto más evidente nos resulte algo, más causal nos parecerá.

diatos que nos vienen a la mente para evaluar una determinada cuestión, concepto o tomar una decisión específica. Este sesgo influye sobre nuestras *intuiciones*, que están condicionadas por la información más reciente de que disponemos o aquella que nos es más familiar. Nuestra intuición no es infalible: la intuición busca esquemas en la mente, derivados de nuestra experiencia, lo que puede resultar traicionero en entornos desconocidos.

En relación con el anterior se encuentra también el *sesgo de falso consenso*, por el que la persona tiende a ver sus propios juicios y comportamiento como comunes y apropiados a las circunstancias, mientras que considera otras respuestas alternativas como improcedentes o desviadas. Todo esto puede reforzarse a nivel colectivo, en forma de *sesgo grupal*, convirtiéndose en un obstáculo ante influjos o participantes externos que pretendan aportar ideas divergentes.

2.1.2. Rasgos de personalidad

Nuestra personalidad única es una amalgama de nuestro temperamento, de carácter hereditario, y de nuestro carácter, resultado de nuestras experiencias y entorno. No se puede hablar de personalidades mejores o peores, pero sí se sabe que hay unas con rasgos más susceptibles hacia determinados sesgos cognitivos que otras, y que no todas se desenvuelven igual en procesos de transformación o entornos complejos y de incertidumbre. Tampoco todos los tipos de personalidad tienen la misma aproximación hacia la cooperación, que es una de las claves de las MDO.

Una de las clasificaciones más populares de los tipos de personalidad sigue siendo la del psicólogo Carl Jung. Conocer los rasgos específicos de nuestra personalidad, saber nuestras predisposiciones mentales y, por lo tanto, en qué áreas cognitivas y emocionales podemos tener carencias o incluso auténticos ángulos muertos resulta muy relevante tanto para el autoconocimiento como para nuestro desempeño en la propia organización, ya que la personalidad influye en los sentimientos, reacciones y actitudes frente a distintas situaciones.

Basado en la tipología de Jung se desarrolló el indicador de Myers-Briggs (MBTI)[10], que mediante un test evalúa cuatro dicotomías con dos externos cada una: extraversión (E) o introversión (I); intuición (N) o sensación (S); pensamiento (T) o sentimiento (F) y juicio (J) o percepción (P). El MBTI da como resultado hasta 16 tipos de personalidad, agrupados en cuatro siglas, con el porcentaje de cada rasgo característico.

[10] MBTI: del inglés *Myers-Briggs Type Indicator*.

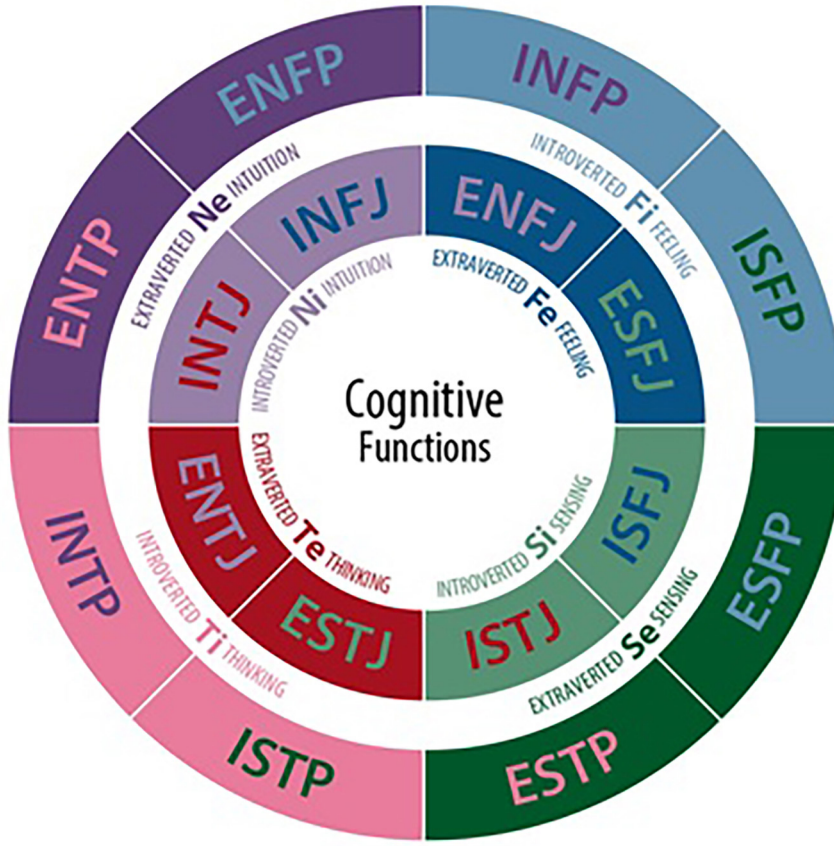


Figura 2. Los 16 tipos de personalidad del indicador Myers-Briggs. Fuente: Creative Commons CC0

Lo anterior resulta importante en las organizaciones, ya que determinados perfiles de rasgos muy acentuados pueden ser óptimos para unos puestos o resolver problemas determinados y nefastos para otros[11]. Es por esto por lo que Ejércitos como el norteamericano emplean este tipo de test para asesorar a sus líderes sobre las fortalezas y debilidades de su personalidad para cada contexto.

Otra herramienta similar y de más fácil aplicación, empleada por el Departamento de Liderazgo del Ejército de Tierra, es el test de dominancia cerebral de Herrmann. De nuevo, perfiles muy sesgados hacia el exceso

[11] Por ejemplo, sin que se pueda hablar de absolutos, perfiles con valores extremos en tipos como el ESTJ (controlador detallista) y ESTP (dominador carismático) tienden a juicios y reacciones muy distintos al ENFP (innovador e integrador) o el INTP (perfeccionista reflexivo).

de control o la rigidez normativa pueden adaptarse peor en procesos que requieran un extra de apertura y creatividad.

Es importante tener en cuenta que, como resultado de nuestra cultura y sistema educativo, en nuestra sociedad las personalidades del tipo «organizador» y «experto» resultan predominantes (en torno a un 70 %), y que estas mentalidades se acomodan mejor a estructuras organizativas burocratizadas, con un mayor componente reactivo ante la novedad y el cambio. Pese a nuestra tendencia natural de seleccionar y aproximarnos a los más iguales a nosotros, ser conscientes de esta inclinación nos debe estimular también a buscar lo diferente, nuestro complementario, fomentando así la diversidad en los equipos y, con ello, una mayor apertura de mente colectiva para la resolución de los problemas.

En cualquier caso, este tipo de herramientas son útiles para el autoconocimiento y el desarrollo personal, pero no resultan válidas en procesos de evaluación y selección. Todas las personalidades son, en principio, válidas y la fortaleza de la organización se basará en la diversidad y complementariedad de sus componentes y de su capacidad de cooperar en equipo.

2.1.3. La mentalidad militar

Los ejércitos han basado tradicionalmente su funcionamiento en la jerarquía, en la disciplina, la planificación y el control. Su preparación permanente se realiza sobre la base de tácticas, técnicas y procedimientos que se depuran y ensayan hasta conseguir automatismo y sincronización en las reacciones ante una situación dada. Es la fórmula que mejor ha funcionado y para la que ciertos tipos de personalidad, con sus marcos mentales asociados, han resultado generalmente más aptos.

Así, perfiles más inclinados hacia el control y la organización, con rasgos más conservadores, suelen encajar bien con los valores tradicionales de la cultura militar, ya que esto puede resultar decisivo para que el ruido del combate no distraiga a los que están empeñados en el mismo.

Un factor relacionado con lo anterior puede ser la impronta: las carreras de los militares son frecuentemente un reflejo de los destinos por los que estos han ido pasando. El fenómeno de la impronta se produce principalmente en los primeros destinos y empleos, que son los que parecen dejar una huella más profunda y duradera.

La impronta puede tener una influencia significativa en las decisiones tomadas en etapas posteriores ante situaciones novedosas, por la tendencia a resolver todos los problemas, en los distintos niveles, con los mecanismos y marcos mentales incorporados previamente. Este fenómeno tiene dimensión internacional, como nos advierte la cultura militar anglosajona con el conocido aforismo «Si eres un martillo, todo lo que ves son clavos».

Afortunadamente, en el modelo de FAS español, esta impronta inicial, más que una limitación, se constituye por lo general en una fortaleza de la mentalidad militar dominante, gracias al enriquecimiento que suponen la diversidad de destinos y medidas como el fomento de la movilidad y rotación, enfoques conjunto e interarmas, cursos comunes a las FAS, como los de Estado Mayor o Inteligencia, segundas trayectorias profesionales y, en general, la multitud y variedad de experiencias derivadas de la participación en misiones internacionales, que permiten que el militar evolucione a lo largo de su carrera y fomentan la diversidad y la perspectiva. Esta fortaleza del militar español, tan apreciada en el extranjero, resulta positiva para la capacitación en las MDO, ya que los mandos que son más abiertos y menos rígidos en sus marcos de referencia son más adaptativos y propensos a hacer mejores juicios y valoraciones ante situaciones complejas.

2.2. La cultura en las FAS ante la transformación necesaria para las MDO

Como hemos visto, conceptos como unidad, cohesión, jerarquía y disciplina son básicos y necesarios en las FAS. También sabemos que determinados perfiles de personalidad suelen encajar mejor en la mentalidad militar tradicional. En ese escenario, los sesgos inconscientes se podrían llegar a consolidar en un *sesgo colectivo de endogrupo* o de pertenencia. El problema surge si, con el paso del tiempo, este efecto se hace acumulativo y consolida una cultura subyacente determinada, donde los marcos mentales dominantes hagan que el pensamiento colectivo se uniformice y la organización como tal pierda diversidad y perspectiva, con aversión al cambio, pasando a «mirar por el retrovisor» en lugar de adaptarse a lo que el presente y el futuro le requieren.

> «Lo único que hay más difícil que introducir una idea nueva en la mente de un militar es sacar una vieja».
>
> *Basil H. Liddell Hart*

Existen también otros factores organizacionales que pueden contribuir a la inercia, al cambio de mentalidad, dificultando la acción correctiva a los procesos de pensamiento erróneo. Uno de ellos, especialmente relevante en las organizaciones jerárquicas, es *la distancia al poder.*

En las culturas organizacionales, que se basan en una distancia menor al poder, los miembros establecen relaciones llamadas «entre iguales», más que relaciones entre superiores y subordinados. De este modo, los subordinados se encuentran más cómodos y trabajan con la expectativa permanente de contribuir al proceso de toma de decisiones de los superiores.

En organizaciones con una cultura de mayor distancia al poder sus componentes están necesariamente sometidos a unas relaciones de poder más absoluto. Los superiores ostentan el poder con relación a su situación en la jerarquía. Se produce una distribución estable del poder que pone orden en entornos inciertos y caóticos. Este modelo organizacional tiende a reducir la capacidad de los subordinados de cuestionar decisiones, así como la posibilidad de aumentar los puntos de vista alternativos.

Esto nos llevaría a pensar que una cultura de alta distancia al poder contribuye a una mayor efectividad en situaciones adversas, acallando cualquier potencial conflicto o disidencia. Sin embargo, esto no es necesariamente así en entornos de gran complejidad y dinamismo, que requieren un ciclo de decisión y flujos de información superiores para mantener la iniciativa y estar abiertos a nuevas ideas.

> «Cuanto más poder le des a un solo individuo frente a la complejidad y la incertidumbre, más probable será que tome malas decisiones. Como consecuencia, hoy en día hay muy buenas razones para que las empresas traten de pensar más allá de la jerarquía».
>
> James Surowiecki en su libro *Sabiduría de los grupos* (2004)

En este campo, la evolución y adaptabilidad experimentada por las FAS españolas en los últimos años, con su participación destacada en el escenario internacional en el marco de las Organizaciones Internacionales de Seguridad y Defensa de las que España forma parte, y en estrecho contacto con Ejércitos de países aliados, ha sido más que notable. No obstante, para dotarse de capacidades MDO, se requerirá expandir la cultura actual hacia la convivencia de las estructuras orientadas al control con otras de menor distancia al poder. Estas redes alternativas, más dinámicas, ágiles y flexibles (concepto de redarquía)[12] se orientan principalmente hacia el conocimiento y la colaboración, por lo que resultan aún más aptas para el modelo de C2 y tipo de liderazgo específicos del escenario multidominio.

2.2.1. La diferencia generacional

En las organizaciones actuales conviven cuatro generaciones con marcadas diferencias en cuanto a sus vivencias, habilidades y formas de pensar: los *baby boomers*, nacidos entre 1945 y 1964; la generación X, con nacidos

[12] Véase el apartado 3.3. Necesidad de nuevos modelos de organización.

desde 1965 hasta 1981; generación Y o *millennials*, nacidos entre 1982 y 1997; y los *centennials* o generación Z, nacidos entre 1997 y 2010.

Esta diversidad, sin duda potencialmente enriquecedora, presenta importantes paradojas y retos para las FAS. En la era de la información, las dos generaciones que copan la dirección son «inmigrantes digitales», mientras que los nacidos después de 1980 son verdaderos «nativos digitales» que viven inmersos en la sociedad de Internet y no conciben la vida sin tecnología.

Esta «brecha digital» también comporta diferencias ideológicas. Los inmigrantes digitales recibieron una educación basada en la responsabilidad, respeto y obediencia a la autoridad, conformando una cultura basada en el esfuerzo y el sacrificio, con miras laborales generalmente a largo plazo. Los jóvenes nativos digitales son creativos, flexibles y multitarea; prefieren el trabajo —e incluso las relaciones— a distancia, son autodidactas, con espíritu innovador y pragmático, aunque no son tan fáciles de fidelizar como sus generaciones precedentes. Las perspectivas laborales de los jóvenes son, por lo general, más temporales, ya que su compromiso va en función a su proyecto profesional, ligado a un beneficio y motivación personales. Una de las claves para su retención es que se sientan parte de un entorno que privilegie la participación y valoración de sus aportaciones.

Las nuevas tecnologías proporcionan a los militares más jóvenes (nativos) el acceso a información y a servicios de organizaciones fuera de su cadena de mando. Están más acostumbrados a experimentar y trabajar según «redes de conocimiento» más abiertas e informales y entienden que este acceso, y las relaciones que se desarrollan a partir del mismo, pueden ser beneficiosas para el cumplimiento de sus cometidos. Los «inmigrantes» están más habituados a emplear procedimientos definidos, son más estructurados y, por lo general, se muestran más reactivos a experimentar de forma natural los nuevos servicios que la tecnología ofrece.

Ambas mentalidades presentan fortalezas y debilidades, por lo que el papel del liderazgo será clave para complementar cada una con lo mejor de la otra y cohesionar el conjunto. Los «nativos» deben incorporar los valores de los «inmigrantes» y viceversa, de una forma positiva y constructiva; es decir, integrar la experiencia, la perseverancia y la orientación al largo plazo con la espontaneidad, el impulso y la creatividad. De igual manera, los jefes deben liderar los esfuerzos que se marquen hacia la TD y convertirse en un ejemplo para los demás en la utilización y máximo aprovechamiento de la tecnología. El reto no es menor: los líderes actuales (inmigrantes digitales) tienen que acertar a comprender o adivinar cómo crear las FAS en la que los nativos se van a desenvolver en el futuro.

2.2.2. ¿Qué entendemos por «complejidad» en los problemas de las MDO?

La realidad de las MDO es tremendamente compleja y dinámica, de modo que lo que antes parecía fácil de controlar ahora se antoja incluso imposible de conocer. No percibir en su adecuada dimensión la complejidad es un factor limitante.

Para entender mejor cómo la complejidad en el entorno operativo de las MDO representa un reto para el planeamiento, conducción y ejecución de las operaciones militares, conviene utilizar un modelo que nos sirva de referencia para sistematizar los distintos tipos de problemas a que se enfrentan los comandantes.

El marco *Cynefin*[13] establece cuatro entornos de complejidad y desorden creciente, que definen cuatro tipos de problemas y cuatro maneras distintas de abordarlos:

- *Dominio de lo simple o claro* (*Known knowns, best practices*): en el que los problemas tienen una única solución, dentro de un rango de posibilidades conocido. En este entorno se aplican relaciones causa-efecto, y es al que tiende la mente humana, por su linealidad. El proceso típico de resolución de problemas en este entorno es *detectar-clasificar-responder*.
- *Dominio complicado* (*Known unknows*, *good practice*): en este entorno puede haber varias soluciones a un problema. Es el caso, por ejemplo, de un diagnóstico médico por el que, ante unos síntomas determinados, pueden existir diversas causas o enfermedades. Los entornos complicados son el terreno para los expertos, y en ellos se sigue el proceso *detectar-analizar-responder*. El entorno complicado sigue siendo un entorno controlado y predecible, aunque las posibilidades de errar aumentan en función de la calidad de los expertos que intervienen o de las dinámicas de cooperación que existan.
- *Dominio complejo* (*Unknown unknowns*, soluciones emergentes): en él las fuentes de posibles causas aumentan, por lo que ya resulta un entorno impredecible. Las relaciones causa-efecto solo se conocen *a posteriori*, ya que cada elemento ejerce influencia sobre todos los demás (relaciones sistémicas). Un ejemplo ilustrativo de este dominio es cuando los tripulantes del Apolo XIII lanzan el famoso mensaje «*Houston, tenemos un problema»,* que automáticamente mueve la

[13] Dave Snowden, experto en estrategia y entornos complejos, creó en 1999 el modelo *Cynefin* como marco conceptual para ayuda en la toma de decisiones. *Cynefin* ayuda a conceptualizar conceptos abstractos para poder describir, entender y clasificar mejor una serie de situaciones o contextos, como a los que se enfrentan organizaciones en entornos de complejidad. También es útil para explicar la transformación cultural y digital que estamos viviendo.

situación al dominio complejo. Aquí se utiliza la experimentación[14] como metodología para avanzar, y el patrón es *probar-detectar-responder*. La decisión irá más enfocada a tratar de sacar hipótesis, validar las que se puedan y aprender.

- *Dominio caótico* (*Unknownables*): el más difícil de gestionar, ya que presenta situaciones demasiado confusas para esperar una respuesta basada en conocimientos. Es imposible intentar establecer una relación causa-efecto, porque no existe. Un ejemplo de este entorno fueron los ataques del 11 de septiembre, o la pandemia del covid-19. Aquí la pauta es *actuar-detectar-responder*, en la se actúa con una toma de decisiones instantánea y según el resultado que se percibe, en un aprendizaje continuo, se responde de nuevo y sucesivamente.

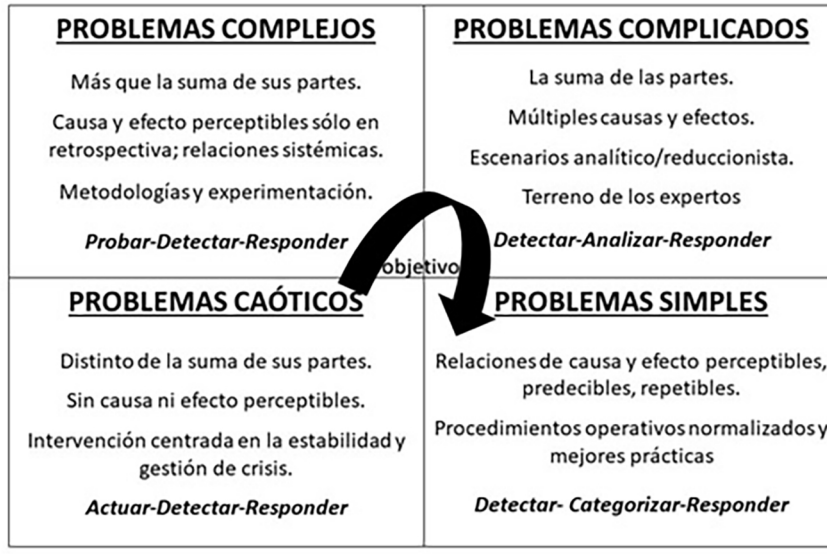


Figura 3. Modelo Cynefin de entornos de complejidad.
Fuente: elaboración propia a partir del modelo de David Snowden

El objetivo ante los problemas que plantean las MDO será, por tanto, que conforme aumente nuestro conocimiento, nos desplacemos «en sentido de las agujas del reloj» de lo caótico a lo complejo, a lo complicado y a lo simple. Para lograrlo se requiere seguir un método formal de pensamiento sistémico.

[14] En este tipo de entornos la participación de expertos no asegura que se llegue a una solución aceptable, por lo que suele ser más acertado trabajar con expertos en metodologías que con expertos en soluciones.

2.2.3. ¿Las MDO implican cambios en el modelo de C2?

La complejidad de las MDO y la necesaria integración que ha de existir entre la actuación de la Fuerza Conjunta en los ámbitos tradicionales y los nuevos ámbitos de operación (aeroespacial, ciberespacial y cognitivo) hace cada vez más difícil comprender cómo «mandar» o, más precisamente, cómo «pedir» efectos. Esto implica que el Mando deberá entender las posibilidades que ofrecen las capacidades de la Fuerza y otros elementos no militares en estos ámbitos, los efectos que se pueden generar en todos ellos y el modo de hacerlo[15].

Operar en estos nuevos escenarios multidominio implica necesariamente cambiar la forma de pensar. Hemos de pasar de tratar de «dominar» el campo de batalla a actuar con agilidad: lograr ventanas de ventaja temporal, aprovechables desde cualquier ámbito y contribuir a alcanzar los efectos deseados en ámbitos diferentes. Esta será la transformación o evolución más importante[16].

En esa línea, la OTAN, en su «Concepto inicial para las MDO», enfatiza la necesidad de cambios en el modelo de C2:

> «Las MDO exigen un enfoque más ágil interámbitos en las interelaciones de apoyo (*supporting/supported*) para el C2. Resulta crítica una colaboración más amplia entre los Comandantes y actores no militares. La futura cultura MDO deberá desarrollarse de manera que promueva la interacción e integración de equipos intergubernamentales y civiles (*multi-agency*)»[17].

El C2 de fuerzas heterogéneas constituirá un reto añadido a las MDO. La mentalidad de colaboración y la adaptabilidad, con el apoyo de la técnica para tener una perspectiva común, serán claves para gestionar la complejidad y la diversidad. Las MDO de OTAN deben incorporar la complejidad de ejércitos de naciones individuales que puedan operar a través de múltiples ámbitos, orquestando y deconflictando según se requiera, y emplearán la ventaja técnica para explotar los datos de todas las fuentes que permita una conciencia situacional común (COP)[18] de los cinco ámbitos[19]. También se asociará y colaborará más activamente con actores no militares para obtener deconflictación, coordinación y sincronización más amplios.

---

15 EMAD. (2023, 28 de marzo) Concepto Exploratorio «Evolución de la Fuerza Conjunta hacia las Operaciones Multidominio». Párr. 68.

16 *Ibidem*. Párr. 67.

17 OTAN. (2022, 5 de julio). *Initial Alliance Concept for Multi-Domain Operations* (NU). ACT. Párr. 29.

18 COP: en inglés *Common Operating Picture*.

19 Para la OTAN los cinco dominios operacionales son la tierra, el mar, el aire, el espacio ultraterrestre y el ciberespacio.

El desarrollo e implementación futuros de las MDO requerirá un énfasis mucho más amplio en la colaboración que las operaciones conjuntas, y necesitará que los comandantes desarrollen una nueva mentalidad y un estilo de liderazgo adaptativo[20].

Tal es el énfasis que la OTAN pone en la colaboración en su concepto para las MDO que, además de utilizar el término «orquestar» en referencia a la acción del comandante a través de un C2 más difuso, llega a acuñar el término C3 para describir el mando, control y colaboración como una Función Conjunta de la máxima utilidad al considerar las MDO[21].

Conseguir implementar una verdadera cultura de colaboración, unido a la disponibilidad de la información que proporciona la visión compartida común, es lo que permite formas avanzadas de C2 descentralizado.

Figura 4. Relación entre problemas (según el marco Cynefin) y modelo de C2 para el entorno VUCA (Volátil, Incierto, Complejo y Ambiguo) de las MDO. Fuente: elaboración propia

Este tipo de C2 es el empleado por el modelo de liderazgo del «mando orientado a la misión» (*mission command*), que es el que, mediante el propósito compartido, la confianza y la iniciativa de los escalones subordinados, mejor se adapta a la complejidad y agilidad de las MDO.

[20] OTAN. (2022, 5 de julio). *Initial Alliance Concept for Multi-Domain Operations* (NU). ACT. Párr. 46.
[21] *Idem.*

3. Medidas en el ámbito de las personas para la transformación hacia las MDO

El Plan de Acción para la TD del Ministerio de Defensa incorpora dimensiones en el ámbito de las personas y de la organización. Estas medidas[22] serán el fundamento sobre el que posteriormente se tendrán que ampliar las capacidades humanas con relación a las MDO mediante otras actuaciones sobre el resto del personal de las FAS.

3.1. Incorporación de las habilidades correctas en el personal

El personal será un elemento clave en la aplicación de las MDO, no solo por la naturaleza tan especializada de los nuevos ámbitos y la tecnología emergente, sino también por la necesidad de comandantes, planificadores y operadores que puedan pensar y actuar a través de múltiples ámbitos. Por lo tanto, además de la fuerte demanda de especialistas de dominio, el personal militar necesitará creatividad para pensar en nuevas formar de aumentar la conciencia multidominio, por ejemplo, para efectuar la decepción o generar sorpresa[23].

Por una parte, disponer de expertos en áreas específicas (*hard skills*) será crítico para el enfoque de abajo a arriba que identifique los problemas, inicie los requisitos y asesore sobre las soluciones a la conectividad entre ámbitos y asuntos de interoperabilidad. Esto resultará especialmente importante a nivel táctico para que los subordinados ejecuten el propósito del comandante a través del mando orientado a la misión, conectando sensores y actuadores a través de los cinco ámbitos[24].

Por otro lado, se necesitarán líderes competentes en entornos tecnológicos y digitales, capaces de tener en cuenta el impacto que sus decisiones tendrán en todos los ámbitos de la operación. La formación en liderazgo debe, por tanto, orientarse a promover un cambio de mentalidad y premiar, además de las clásicas *soft skills*, el conocimiento técnico, la innovación, la creatividad y la capacidad de establecer vínculos de confianza mutua. También deben valorarse positivamente las actitudes críticas constructivas con el propio sistema, que contribuyan a adaptar la Fuerza Conjunta al entorno en el que opere[25].

---

22 Ministerio de Defensa. (2020). La Instrucción 14/2020, de 15 de abril, del Secretario de Estado de Defensa, por la que se aprueba la segunda parte del Plan de Acción del Ministerio de Defensa para la Transformación Digital desarrolla siete actuaciones en el ámbito de las personas (atención a usuarios, control, comunicación, formación, etc.).

23 OTAN. (2023, 10 de marzo). *Alliance Concept for Multidomain Operations*. Párr. 33.

24 *Ibidem*. Párr. 34.

25 EMAD. (2023, 28 de marzo). Concepto Exploratorio «Evolución de la Fuerza Conjunta hacia las Operaciones Multidominio». Párr. 72 y 73.

El éxito de las MDO también se facilita mediante la participación de personal heterogéneo que aporte diversidad y perspectiva. Para ello se deben ampliar los modelos de personal vigentes para generar una fuerza militar que pueda ejecutar las MDO. Contemplar la diversidad podría aportar perfiles de personal que previamente no eran considerados aptos para la milicia por las características físicas o culturales que se requerían para el servicio de las armas. Esto requerirá un cambio de mentalidad, pero puede ayudar a crear equipos con habilidades multidominio con una mezcla flexible de personal de uniforme y no uniformado[26].

Por lo tanto, entre las competencias más necesarias de cara a obtener capacidades MDO se encuentran habilidades duras, como el dominio de las competencias técnicas digitales. De ellas, el pensamiento crítico y el pensamiento sistémico son habilidades formales, que requieren método y formación definidos. También se requieren otras habilidades más blandas, relacionadas con las competencias interpersonales humanas (como la inteligencia social, gestión de las emociones, escucha activa, empatía y saber promoverlas en el entorno de trabajo). Ambas conjuntamente permiten la construcción de la seguridad psicológica[27] y la confianza necesarias para que se dé el mando orientado a la misión y ser efectivos en las MDO. Para que la cultura organizativa interiorice la importancia de estas habilidades se requiere un liderazgo transformador.

3.2. Necesidad de incorporar el pensamiento sistémico (systems thinking) en las FAS

Para decidir y resolver, primero hay que entender. Y entender es sinónimo de modelizar de manera suficientemente fiel. Solo así se puede entender la complejidad. Para ello es necesario el empleo de métodos y herramientas formales, como la dinámica de sistemas.

El método sistémico de resolución de problemas, como respuesta más completa ante la complejidad, no es algo nuevo en los Ejércitos. Conceptualmente, se emplea en el planeamiento OTAN[28] aunque

[26] OTAN. (2023, 10 de marzo). *Alliance Concept for Multidomain Operations*. Párr. 35.
[27] Véase el apartado 3.4.1. Liderazgo para la Transformación.
[28] La *Comprehensive Operations Planning Directive* (COPD) contempla en el estudio del Área de Interés la existencia de «Sistemas Complejos Adaptativos», y recurre al Análisis de Sistemas para determinar las relaciones e influencias entre ellos. OTAN. (2021, 15 de enero). *Comprehensive Operations Planning Directive* COPD. Versión 3.0 (NU), pp. 2-10, 2-11. La *Allied Joint Doctrine for the Planning of Operations* (AJP-5), menciona el «Análisis Sistémico de Sistemas» (*SoSA, System of System Analysis*) en el apartado de interacción de sistemas, interdependencias, influencias y vulnerabilidades. OTAN. (2019, mayo). *Allied Joint Doctrine for the Planning of Operations* (AJP-5), Ed. A, Version 2. pp. 4-7.

difícilmente se llega a aplicar con rigor científico en los planes y operaciones militares.

> «Una buena parte de los errores en el proceso de planeamiento se originan en la etapa Inicial (análisis de la misión, definición del problema), al tomar como base del análisis lo que se piensa como un hecho cierto, cuando no es más que una opinión subjetiva y, por tanto, discutible».
>
> PDC-5 Doctrina «Planeamiento de las Operaciones», julio 2023. Parr. 155.

Un ejemplo histórico que ilustra esta paradoja es el fracaso, incluso la hilaridad, que causó el general norteamericano Stanley McCrystal, al presentar de forma gráfica en 2009 una aproximación sistémica al problema operativo en Afganistán. El objetivo de su mensaje era ilustrar, de una manera científica, que la estrategia militar estaba errada desde el principio, al no tener en cuenta las interacciones de los distintos actores y los efectos de segundo y tercer orden de las acciones que se realizaban. En su lugar, la reacción que se obtuvo fue la de «matar al mensajero»: los militares se dedicaban más a hacer «platos de espagueti en *PowerPoint*» que a ganar la guerra.

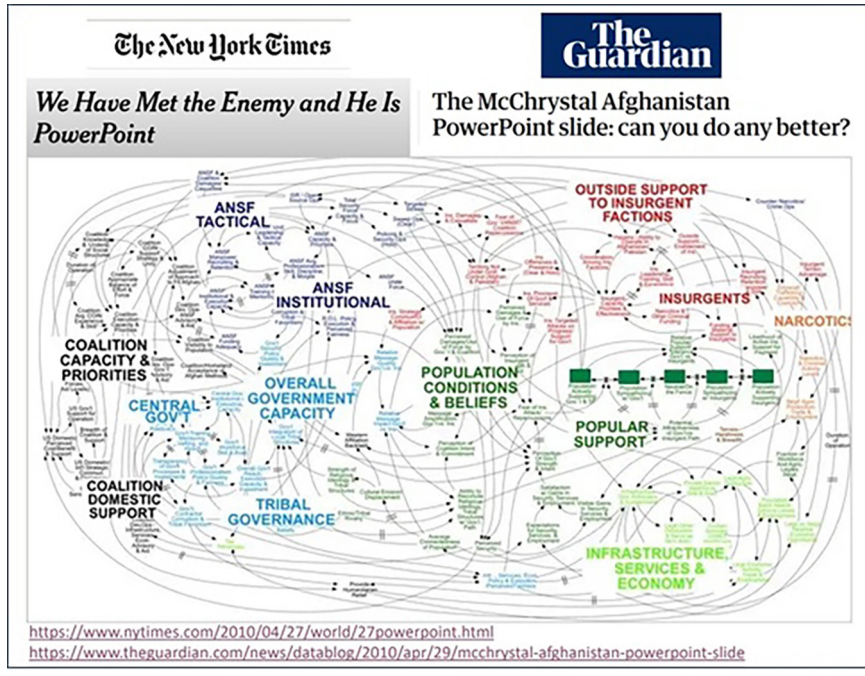


Figura 5. Representación de estrategia militar en Afganistán por general McChrystal y reacción en prensa. Fuente: The New York Times y The Guardian

Pretender desenvolverse con agilidad e iniciativa en los entornos complejos de las MDO sin desarrollar previamente la cultura y el método para abordar este tipo de problemas de manera sistémica es un riesgo. De nuevo, la mentalidad de transformación digital, por su orientación al dato único objetivo, la perspectiva común, acceso transversal a la información, y la claridad de las interacciones a través de los procesos que proporciona, es un habilitador necesario para poder adquirir progresivamente técnicas de pensamiento sistémico, que serán imprescindibles para diagnosticar correctamente los actores e interdependencias presentes en una MDO. Esta perspectiva permitirá a los comandantes decidir la mejor estrategia a seguir y saber «orquestar» acciones teniendo en cuenta no solo el impacto perseguido, sino también sus efectos en derivadas de segundo y tercer orden.

El *pensamiento sistémico (systems thinking)* es una disciplina para ver totalidades. Es un marco de interrelaciones, para ver patrones de cambio en vez de «instantáneas estáticas», con el nivel de detalle suficiente para el propósito que se persiga. En el entorno complejo de las MDO definir correctamente el problema, su contorno y «radiografía» cambiantes, puede ser la parte más compleja para su resolución, ya que muchos de los problemas a que se enfrente el comandante serán problemas «blandos» (el problema muta con cada solución que se adopta)[29].

> «Hoy el pensamiento sistémico se necesita más que nunca porque la complejidad nos abruma. Quizá por primera vez en la historia, la humanidad tiene capacidad para crear más información de la que nadie puede absorber, para alentar mayor interdependencia de la que nadie puede administrar y para impulsar el cambio con una celeridad que nadie puede seguir. Esta escala de complejidad no tiene precedentes. Nos rodean ejemplos de "fallos sistémicos"».
>
> *Peter Senge,* 1990

Volviendo al modelo *Cynefin*, en pensamiento sistémico se habla de caos en aquellos sistemas que muestran una hipersensibilidad a las condiciones iniciales. Por otro lado, se habla de complejidad para referirse a un sistema cuando no son fácilmente conocidos sus mecanismos o comportamiento. El pensamiento sistémico y los modelos mentales que permite generar ayudan a entender el comportamiento de esos sistemas considerados complejos o caóticos, pero que son tan comprensibles y predecibles como cualquier otro cuando se han modelizado correctamente.

[29] Existen problemas «más duros» (con soluciones exactas como, por ejemplo, interceptar un misil balístico) y otros problemas «más blandos» (como «estabilizar y democratizar Afganistán») en los que no hay solución perfecta, ni estable, ni atemporal. Casi todos los entornos intensivos en el ser humano, como la Defensa, representan problemas «blandos». Existen modelos específicos para su diagnóstico y conocer su evolución, como la *Soft Systems Methodology*, de Peter Checkland.

Incorporar formalmente en las FAS el pensamiento sistémico a los órganos de prospectiva y en apoyo a los grupos de planeamiento operativo puede generar una ventaja competitiva en nuestras capacidades MDO.

3.3. Necesidad de nuevos modelos de organización

La TD tiene mucho que ver con cómo se comparte la información. El cambio de paradigma, del clásico «necesidad de conocer» al «necesidad de compartir» es necesario para las MDO. La estructura organizativa condiciona el flujo de la información. Los modelos jerárquicos orgánicos son imprescindibles para la gestión y el control, pero en ellos la información se compartimenta y su flujo se ralentiza.

> Comparándolo con los métodos de planeamiento paralelo y secuencial, el planeamiento colaborativo permite desarrollar productos mucho más coherentes y armonizados, en todos los niveles.
>
> • Su principal ventaja estriba en su mejor gestión de la información, lo que reduce la duración de los procesos de planeamiento y mejora los resultados.
> • Sus principales inconvenientes son: la posible aparición del *pensamiento de grupo* y la *ilusión* de un «nivel de mando único», que desincentive la aplicación de las herramientas de *pensamiento crítico y creativo*; [...] así como el riesgo de adoptar las herramientas de la información sin una *metodología correcta* de trabajo colaborativo [...].
>
> PDC-5 Doctrina «Planeamiento de las Operaciones» julio 2023. Párr. 88.

Por eso, en las organizaciones transformadas digitalmente es habitual que las *estructuras orgánicas* se adapten y simplifiquen, conviviendo con otras dos más dinámicas, flexibles y transversales, con estructuras de red *(redarquía)*[30]: Una *red de conocimiento*, orientada a mantener la perspectiva común, aumentar y difundir el conocimiento, alinear y motivar, orientada al desarrollo de las personas y a la gestión del talento. Y una *red de creación*

[30] Redarquía es un cambio de paradigma organizacional. Apuesta por un modelo organizativo colaborativo que emerge en la era de la agilidad, aumentando la capacidad de adaptación y colaboración de toda la estructura, con la finalidad de coordinar los esfuerzos de los miembros de la organización para alcanzar los objetivos marcados. La redarquía se basa en una estructura en red, en la conectividad, dejando paso a la iniciativa y colaboración de las personas que forman parte de la organización. Se centra en el futuro y en las nuevas oportunidades que este presenta. Se basa en la confianza y en el valor añadido, y entiende a los empleados como agentes movilizadores del cambio. *Fuente:* https://www.randstad.es/contenidos360/cultura-empresarial/la-redarquia-un-nuevo-modelo-organizativo-emergente/ (consulta: 1 de noviembre de 2023).

e innovación, más operativa, que explora, analiza y moviliza para generar resultados concretos con agilidad e impacto.

Esta organización dual se corresponde en parte con la adoptada en las FAS, con estructuras orgánica y operativa, más otra transversal de carácter funcional. Pero la TD, con su orientación a procesos, datos y servicios, obliga a una adaptación en cómo se gestiona la información entre estas estructuras, que también será necesaria para dotar de capacidades MDO a las FAS[31]. En la actualidad, el poder de una organización se mide por la velocidad con que fluye la información dentro de ella. Este factor está directamente relacionado con la agilidad con la que la propia organización, como un todo, es capaz de reaccionar ante los cambios en su entorno. Las estructuras orgánica, operativa y funcional de las FAS presentan dinámicas y culturas organizativas distintas entre sí, que es necesario aproximar mediante el alineamiento e interdependencia de sus procesos y la adopción del modelo colaborativo en red: La redarquía es la estructura natural de la era digital.

Quizás el principal cambio de paradigma que nos orienta hacia las MDO es la necesidad creciente de las FAS de estar capacitadas para actuar en la zona gris y en la zona de competición del espectro de los conflictos, en coordinación con actores e instrumentos distintos al poder militar[32]. Ante la cada vez más difusa frontera entre los conceptos de paz, conflicto y guerra, el solape cada vez mayor entre seguridad interior y exterior, la dificultad creciente de discriminar combatientes y no combatientes, militares y civiles, actores estatales y no estatales en los conflictos asimétricos, de naturaleza híbrida, en la zona gris y ante operaciones de influencia que estamos presenciando, nuestras FAS deben adaptarse ya, y de manera continua, para ser capaces de planificar, conducir y ejecutar con éxito operaciones en el amplio abanico de las MDO, conscientes de que esta capacidad y eficacia permanentes serán a su vez la mejor medida de disuasión para evitar la agresión y escalada ante potenciales adversarios (García Cantalapiedra, 2019).

El problema anterior nos obliga a adaptar nuestra organización para incorporar capacidades permanentes en áreas de prospectiva, seguimiento y planeamiento relacionadas con las MDO y a revisar también nuestro proceso para generar estructuras operativas *ad hoc* capaces de responder ante los nuevos retos operativos con la suficiente agilidad y eficacia, ante la imprevisibilidad y rapidez con que surgen los acontecimientos.

---

[31] Una acertada gestión de la información permitirá acelerar el ritmo de batalla y afrontar ciclos de planeamiento, decisión y ejecución más cortos. Será, por tanto, un pilar sobre el que se sustenten las MDO. EMAD. (2023, 28 de marzo). Concepto Exploratorio «Evolución de la Fuerza Conjunta hacia las Operaciones Multidominio». Párr. 56.

[32] Ibidem. Párr. 151.

Esto afecta también a la preparación de la Fuerza: En el contexto complejo y dinámico de las MDO, nuestro paradigma ha de pasar de «conocer para cambiar» a «cambiar para conocer». Adaptando el aforismo anglosajón, para las MDO hemos de convertir nuestro concepto tradicional de adiestramiento, del *train as you fight*, entrénate como te gustaría luchar, al *fight as you train*, o lucha mientras te entrenas, con mentalidad cotidiana de combate en todos los puestos[33] y el foco permanentemente fijado en la misión principal de las FAS, para propiciar una cultura de experimentación, aprendizaje y adaptación permanentes que, alineada con el proceso de TD, elimine burocracias innecesarias (entendidas como los elementos del proceso que no aportan valor) en aras de la máxima eficacia, flexibilidad y agilidad del conjunto[34].

3.3.1. Evolucionando hacia las MDO desde la práctica

La creación de la Fuerza Conjunta representó en su momento un modelo de éxito de cómo las FAS saben reorganizarse.

A menor escala, otro ejemplo ilustrativo de cómo las FAS pueden transformar su organización para responder a nuevas misiones fue en su día la creación de los Mandos Operativos para las misiones permanentes. Esta adaptación exitosa también transformó las estructuras orgánicas de los Ejércitos y Armada, aumentando las interacciones con la estructura operativa y la aproximación del adiestramiento específico con la preparación, conducción y ejecución de operaciones militares. Si bien los Mandos Operativos permanentes adolecen en la actualidad de carácter multidominio, propiciar una colaboración transversal creciente entre ellos —especialmente con el Mando Conjunto del Ciberespacio— y quizás con el Centro de Inteligencia de las FAS, siempre bajo la «orquestación» del Mando de Operaciones, constituiría no solo un refuerzo a la eficacia de su misión específica, sino también una fuente incremental de aprendizaje y experiencia en capacidades MDO sobre la que aplicar el proceso de lecciones aprendidas y mejores prácticas (LAMP) de las FAS, en beneficio del conjunto.

El «Concepto inicial de la OTAN» establece que las MDO se caracterizan por poder requerir de forma dinámica la incorporación de actores no militares en las estructuras de planeamiento y ejecución (otros elementos de

[33] Conscientes y sensibilizados de que en tiempo de paz ya se es objetivo de operaciones de espionaje e influencia en la zona gris, a través del ciberespacio, redes sociales, etc. y que la transición a las MDO puede ser inmediata.

[34] El modelo de organización de las FAS estará en línea con el proceso de transformación digital del Ministerio de Defensa. Será capaz de efectuar ágilmente los ajustes organizativos precisos. Todos los componentes de las FAS se integrarán en la gestión de procesos de carácter conjunto. Gobierno de España (2020). RD 521/2020, de 19 de mayo, por el que se establece la organización básica de las FAS. Art. 2 y 3.

la administración, organizaciones, operadores civiles, expertos, etc.)[35]. Es necesario que las FAS se familiaricen progresivamente con esos formatos, creando los mecanismos de integración de actores civiles en los procesos de las FAS y practicando los procedimientos resultantes, ya que no será posible improvisarlos de manera efectiva y oportuna ante una crisis.

Otro ejemplo positivo en esa misma dirección fue la creación y desarrollo de la Unidad Militar de Emergencias (UME), y su capacidad de integrarse en estructuras de mando y ejecución civiles, hacer transferencia de autoridad mutua en función del nivel de la emergencia, cooperar con el resto de Ejércitos, la Armada, y otros actores (por ejemplo, compañías de transporte) para adaptar la mejor respuesta a la evolución de los acontecimientos.

En este sentido, las experiencias de la UME y también de los Ejércitos y Armada ante las cada vez más frecuentes y sorpresivas operaciones militares de apoyo a autoridades civiles (Balmis y Baluarte ante la pandemia del covid-19, tormenta Hermine, emergencia volcánica en la Palma, incendios, inundaciones, etc.) se podrían entender como actuaciones de las FAS con un embrionario carácter multidominio (en cuanto a estructuras de mando, colaboración con otros actores, importante componente en el ámbito cognitivo, etc.) cuyas lecciones aprendidas se podrían aglutinar, por tanto, en mejores prácticas y acciones correctoras que nos permitiesen aumentar progresivamente nuestra mentalidad, capacidades y organización hacia las MDO.

La necesidad de la Fuerza Conjunta de integrarse con otros elementos de poder distinto del militar y ampliar su espacio de competición para hacer frente a amenazas híbridas en la zona gris del espectro de los conflictos implica un mayor grado de trabajo cotidiano con empresas, proveedores de servicios y otros actores, y un cambio en la cultura de Defensa hacia una concepción más participativa e integrada, que requiere progresivas adaptaciones organizativas, procedimentales y normativas, con cambios en el marco legal de actuación de las FAS, cuya puesta en marcha será a su vez un elemento de credibilidad y disuasión.

3.4. Modelo de liderazgo que se requiere

3.4.1. Liderazgo para la transformación

Más de la mitad de los proyectos de TD están fracasando por la reactividad al cambio imperante en la propia cultura de la organización. El papel del líder,

[35] OTAN. (2023, 10 de marzo). *Alliance Concept for Multidomain Operations*. Párr. 12: "For brevity within the definition, all the non-military Instruments of Power (IoP), commercial entities and other stakeholders are described as 'non-military', and the importance of 'synchronisation' with these entities is stated but not meant to imply any form of military primacy".

especialmente al más alto nivel, resulta, por tanto, esencial para que la transformación efectiva se produzca. La TD no es algo delegable, o fracasará.

En la dicotomía entre modelos de liderazgo transaccional (orientado al logro) y liderazgo transformacional (orientado al cambio), este último será el deseable en los más altos niveles de la jerarquía de las FAS, por ser el que mayor impacto genera en el clima y cultura de la organización.

El estilo de liderazgo debe adaptarse a la evolución de la situación, para lograr estimar e impulsar lo que demanda el nuevo contexto. Tanto en el proceso de TD de las FAS como en la generación de capacidades MDO, por su comunalidad y ser el primero habilitador de lo segundo, los estilos de liderazgo más adecuados son:

- El *visionario*: que dirija y ejemplifique el cambio, consiguiendo movilizar a la gente hacia una visión y propósito compartidos.
- El *asociativo*: que cree armonía y vínculos emocionales, construyendo relaciones que motiven y resuelvan disputas.
- El *preparador* o *coach*: que genere conciencia, promoviendo el desarrollo del personal y equipos para que sean capaces de pilotar el cambio.

Otros estilos de liderazgo más transaccionales y voluntaristas pueden dirigir y controlar la obtención de resultados a corto plazo, pero, al ser menos participativos, es posible que no logren la motivación y visión compartidas para que el cambio real se produzca.

Una de las habilidades del líder transformador para crear el clima y cultura propicios al cambio es saber generar *seguridad psicológica*[36]. Un clima de seguridad psicológica, plasmado en medidas y dinámicas concretas, permite aprovechar el talento y experiencia de todos los miembros de la organización, aumenta la cohesión, el nivel de compromiso y la confianza entre los miembros del equipo; y permite generar una cultura de debate constructivo, basada en la lealtad y el respeto mutuos, para poder encontrar soluciones creativas y más completas a problemas complejos.

Por lo tanto, podemos sintetizar que el liderazgo necesario para la transformación es un *liderazgo creativo*. El liderazgo creativo en las FAS debe entenderse como la parte del ejercicio del Mando que mediante el liderazgo persigue generar la transformación y evolución desde dentro, fomenta que las ideas fluyan fácilmente y con agilidad en todas las direcciones y

[36] La seguridad psicológica se refiere a la sensación de bienestar psicológico que experimentan los miembros de un equipo cuando sienten que pueden expresarse libremente sin miedo a ser juzgados o rechazados por sus ideas, opiniones o preguntas, especialmente por parte de sus supervisores. Está relacionada con la productividad, creatividad, resiliencia y capacidad de retención de las organizaciones.

consigue que todos los componentes de la organización se sientan partícipes y actores del cambio.

3.4.2. Liderazgo para el planeamiento y conducción de las MDO

Si las MDO se basan en la cooperación y la coordinación/orquestación de actividades, el mejor modelo de liderazgo será aquel que consiga el mayor nivel de compromiso de todos sus miembros en esa dirección.

Por lo tanto, será la filosofía de liderazgo del *mando orientado a la misión* (MoM) la que mejor se adapte a esta transformación y, a su vez, a la complejidad y dinamismo que requiere el C2 de las MDO.

El MoM, que fomenta la decisión y ejecución descentralizados sobre la base de la confianza, mediante la aplicación de una «iniciativa disciplinada» en torno al propósito del comandante, es el modelo de liderazgo del Ejército de Tierra y uno de los cuatro pilares sobre los que se sustenta su transformación hacia el Ejército 2035 (no es extraño que otro de sus pilares sea precisamente la transformación digital). Al ser una filosofía de liderazgo conocida y de la que existe abundante información, no se desarrolla en este capítulo (Borque *et al.,* 2015).

> «El cambio de mentalidad para las MDO permitirá disponer de mandos intuitivos, deseosos de experimentar posibles sinergias, sin temor al fallo y predispuestos a promover cambios de gran calado en aspectos de personal, impulsar nuevos métodos de adiestramiento o propugnar modificaciones relevantes en la organización. En definitiva, más preparados para operar en los nuevos entornos».
>
> EMAD. (2023, 28 de marzo). Concepto exploratorio «Evolución de la Fuerza Conjunta hacia las Operaciones Multidominio». Párr. 74.

Pero adoptar el MoM no es condición suficiente para el éxito en las MDO. El abanico de conocimientos que requiere este nivel es significativo, y se requerirá el entrenamiento adecuado para que comandantes y personal clave entiendan las capacidades, oportunidades y limitaciones de los cinco ámbitos, lo que implica una modificación de nuestra actual enseñanza militar. El tacto y las habilidades diplomáticas serán igualmente importantes, teniendo en cuenta el requisito de las MDO de incrementar la colaboración. Esto ayudará a desarrollar los cimientos de experiencia y confianza que se requieren para delegar la necesaria autoridad para que las MDO tengan éxito[37].

[37] OTAN. (2023). *Alliance Concept for Multidomain Operations*. 10 de marzo de 2023. Párr. 36.

Los futuros líderes de las MDO también deberán evolucionar en su aplicación del arte operacional[38]. El arte operacional deberá adaptarse para encapsular los cinco dominios e integrar capacidades de un rango más amplio de actores contribuyentes, manteniendo la misma filosofía y principios fundamentales[39]. Esto requerirá un esfuerzo doctrinal y de formación, con un incremento significativo de las oportunidades de adiestramiento del personal, tanto a nivel nacional como internacional (OTAN, UE, etc.) tal como comienzan a hacer otros países.

Figura 6. En las FAS de los EE. UU. se realiza desde hace años el curso de Estratega Conjunto Multidominio, de un año de duración, con un carácter eminentemente práctico, para capacitar a sus líderes en el asesoramiento, planeamiento y conducción de las MDO. Fuente: Joint All Domain Strategist > Air University (AU) > ACSC Article Display (af. edu)

Las MDO, además de por su vertiginosa complejidad, se caracterizan por su incertidumbre. Aquellos líderes con las mentes más abiertas estarán mejor capacitados para gestionar situaciones contradictorias: Serán más imaginativos, solicitando puntos de vista alternativos y se mostrarán más propensos a debatir con aquellos con perspectivas diferentes. En este punto, conviene tener en cuenta el papel de la experiencia y la intuición.

Ningún líder tendría éxito si no confiara en la experiencia acumulada a lo largo de su carrera, pero esto requiere una matización en las MDO: nuestra intuición se basa en nuestras experiencias y aprendizajes pasados, por lo que, en un entorno poco familiar, nos puede llevar a encasillar de una manera rápida las situaciones para focalizar la atención en lo importante e

[38] OTAN. (2020). *Allied Joint Doctrine*, AJP-01(F) RD, p. 41.
[39] OTAN. (2023). *Alliance Concept for Multidomain Operations*. 10 de marzo de 2023. Párr. 37.

ignorar lo accesorio. Conocemos y valoramos a grandes líderes militares del pasado por lo acertado de su intuición, pero esto es en parte efecto de un nuevo sesgo de disponibilidad por nuestra parte, ya que omitimos selectivamente a otros tantos grandes militares que por seguir su intuición cometieron sonoros fracasos. Este lado oscuro de la experiencia puede cegarnos y generar la falsa sensación de que sabemos lo que en realidad ignoramos. De nuevo, el pensamiento crítico de un equipo diverso que sabe colaborar, con metodologías formales de trabajo, unido a la perspectiva común sobre datos objetivos que propugna la TD serán la mejor protección del líder contra ese error de percepción y sus consecuencias.

Saber gestionar la incertidumbre requiere actitud positiva ante lo inesperado, flexibilidad y agilidad mental, apertura de miras y la disposición permanente a aprender. El aprendizaje y la adaptación continuos deben ser características del liderazgo para las MDO. Muy ligado con la gestión de la incertidumbre está la gestión de la frustración. Para ello, es necesario tener paciencia, principios sólidos, visión a largo plazo y, sobre todo, saber trabajar en equipo y formar equipos, con facilidad para establecer conexiones, y desarrollar proyectos con un enfoque multidisciplinar e innovador (García Cantalapiedra, 2020).

> «El desarrollo de una filosofía de mando que abarque una cultura de aprendizaje y adaptación requiere Comandantes que sean a la vez abiertos de mente y capaces de aprender de sus propios fallos. El conocimiento del propio Comandante, sus habilidades analíticas y el clima de mando que promueva determinarán el nivel de comprensión que se consiga».
>
> OTAN. (2020). *Allied Joint Doctrine*, AJP-01(F) RD. C-3

La cita doctrinal anterior incide en una de las características principales de los líderes militares del siglo XXI: el autoconocimiento y la autorregulación. Ante la presión y saturación cognitiva que generan las MDO, fenómenos como el cansancio no reconocido y el sesgo de pérdida cuando la situación es adversa afectan negativamente a la valoración del riesgo y a la calidad de la decisión. Por el contrario, un líder equilibrado, sereno y reflexivo, que conoce sus fortalezas y debilidades, y las admite dejándose complementar, es el mejor antídoto ante la incertidumbre.

> «Se mide la inteligencia del individuo por la cantidad de incertidumbre que es capaz de soportar».
>
> *Emmanuel Kant*

Pero el ejercicio del liderazgo tradicional se enfrenta a otro reto en la era de la información y en las MDO: cada vez más, el jefe ya no podrá estar físicamente presente para transmitir personalmente su impronta, inspirar y motivar. Por razones de ubicuidad, dispersión, seguridad, etc., se incorpora un tipo complementario de *liderazgo remoto*, que requiere que el líder sea capaz de ejecutar múltiples roles de forma simultánea. El modo de trabajo y relación a distancia, además de resultar un imperativo operacional derivado de los nuevos escenarios, también es el entorno familiar y de preferencia de las generaciones de nativos digitales, lo que representa una oportunidad para el líder si acierta a alternar la rigidez estructural de la jerarquía con un estilo más orientado hacia su poder de influencia y la capacidad de generar confianza, que permita delegar parte de sus funciones a través de un liderazgo compartido, para generar la iniciativa y dinamismo del modelo del MoM y la orquestación coordinada de actividades que requieren las MDO.

4. Conclusiones

El multidominio es un nuevo contexto para las operaciones que va más allá de lo conjunto, y que requiere cambios en la manera de pensar tradicional en lo que respecta a organización de la Fuerza y áreas de operaciones. Las FAS necesitan entender mejor las amenazas y oportunidades del entorno multidominio, y actualizar sus capacidades para poder realizar MDO. Para ello es preciso impulsar desde el más alto nivel el cambio cultural necesario para pasar de las operaciones conjuntas a las operaciones multidominio, y generar requisitos de nuevas capacidades desde escalones inferiores que permitan abordar las deficiencias que limiten la transformación hacia las MDO[40].

Además de la interoperabilidad técnica, para operar eficazmente en el multidominio, es necesario alcanzar un adecuado nivel de interoperabilidad semántica y organizativa, que permita a todos los elementos de la Fuerza Conjunta comunicarse, compartir información y, si es necesario, romper fronteras organizativas para conseguir los efectos deseados[41].

La TD de las FAS es la base sobre la que se apoyan los elementos clave de las MDO, como el cambio de mentalidad, la forma de C2 y cómo se gestiona la información. Estos elementos clave son de naturaleza humana, por lo que deben gestionarse internamente. El éxito en las MDO descansa

[40] OTAN (2022, 22 de julio). *Initial Alliance Concept for Multi-Domain Operations* (NU). ACT. Párr 5.
[41] EMAD. (2023, 28 de marzo). Concepto exploratorio «Evolución de la Fuerza Conjunta hacia las Operaciones Multidominio». EMAD. Párr. 126.

esencialmente en la superioridad de la información y en la agilidad para tomar la mejor decisión con objeto de obtener ventaja sobre un adversario[42].

El cambio de cultura organizativa es quizás el mayor reto por abordar para la TD hacia las MDO. Para ello es importante ser conscientes del efecto de los sesgos y marcos de referencia mentales, tanto individuales como grupales, que aplicamos en la toma de decisiones, y su impacto en los procesos de transformación. Esto implica instaurar mecanismos que permitan desarrollar el autoconocimiento, la autorregulación y el pensamiento crítico. Contar con los perfiles de personalidad y habilidades adecuados en puestos clave facilita el clima y dinámicas necesarios de apertura, diversidad y colaboración para que el cambio sea compartido y la transformación se produzca. El papel que desempeñe el liderazgo al más alto nivel resulta determinante.

Las generaciones que intervienen en el proceso de TD presentan diferencias en cuanto a mentalidad y capacidades digitales que no son excluyentes, sino complementarias. De nuevo es necesario que el liderazgo propicie que tanto nativos como inmigrantes digitales sean cocreadores y copartícipes del mismo proceso de transformación.

Para que el personal esté capacitado para la TD y las MDO es necesario adaptar la formación en las FAS para:

- Dotarnos de habilidades «duras» que incorporen competencias digitales y en las tecnologías asociadas a este tipo de operaciones. Para ello, los centros de formación y adiestramiento deberán adaptar sus currículos al mismo ritmo que esas tecnologías y la organización militar potenciará las trayectorias profesionales que permitan captar y mantener el talento digital.
- Orientar la formación en liderazgo a promover un cambio de mentalidad que premie, además de las habilidades blandas clásicas, la innovación, la creatividad, la capacidad de establecer vínculos de confianza mutua y las actitudes críticas constructivas con el propio sistema, que contribuyan a adaptar la Fuerza Conjunta al entorno en el que opere.

La experimentación y el *wargaming* son herramientas indispensables para que la Fuerza Conjunta evolucione hacia las MDO. La utilización de ejercicios como marco de experimentación es una práctica que habrá que adoptar de manera gradual, asumiendo que se pueden cometer errores. Se trata de estar preparado para fallar lo antes posible, aprender y avanzar[43].

[42] EMAD. (2023, 28 de marzo). Concepto exploratorio «Evolución de la Fuerza Conjunta hacia las Operaciones Multidominio». EMAD. Párr. 51.
[43] EMAD. (2023, 28 de marzo). Concepto exploratorio «Evolución de la Fuerza Conjunta hacia las Operaciones Multidominio». EMAD. Párr. 51.

De igual manera, el adiestramiento colectivo es un capacitador clave de las MDO y debe mejorarse para incluir escenarios que incorporen un mayor nivel de complejidad. La creación de entrenamiento que mezcle lo virtual y la realidad para generar realismo multidominio es esencial para el desarrollo de una fuerza con capacidades MDO[44].

La redarquía es el modelo organizativo de la era digital. Se basa en la conectividad y la cooperación, y es el que mejor se adapta a la perspectiva, agilidad e iniciativa que requieren las MDO y su modelo de liderazgo. La TD facilita la comunicación en red, y esta además ayuda a comprometer y fidelizar a los nativos digitales. La redarquía implica simplificar y hacer converger las dinámicas de las actuales estructuras orgánica y funcional en las FAS, y aproximarlas a la operativa para una mayor capacidad de respuesta, adaptabilidad y flexibilidad del conjunto.

El C2 de las MDO se basa en la orquestación de acciones interámbitos, implica interacción e integración con actores no militares y se basa en la cooperación y adaptabilidad. El modelo de liderazgo que mejor se adapta a este tipo de C2 es el MoM o *mission command*, basado en el propósito compartido, la iniciativa y la confianza. El MoM tendrá su aplicación principal en el nivel táctico de conducción de las operaciones, mientras que la orquestación y coordinación de acciones se darán fundamentalmente en los niveles operacional y estratégico.

Las FAS deben participar activamente en la consecución de los tres objetivos que marca la Estrategia de Seguridad Nacional (ESN-21) respecto al planeamiento estratégico integrado[45]. Participar en el primer objetivo de avanzar en el modelo de gestión de crisis supone adoptar un enfoque anticipatorio y centrar la toma de decisiones en el análisis de hechos y datos objetivos[46]. Para ser efectivos en las MDO y disminuir la incertidumbre es necesario entender realmente lo que significa la complejidad, e incorporar métodos formales de análisis y resolución de problemas complejos, como el pensamiento sistémico (*systems thinking*) en apoyo al planeamiento militar.

Participar en desarrollar la capacidad de prevención, disuasión, detección y respuesta de España frente a estrategias híbridas (tercer objetivo de planeamiento estratégico integrado de la ESN-21) supone que la Fuerza Conjunta debe actuar en un contexto de seguridad en el que las amenazas

[44] OTAN. (2022). *Initial Alliance Concept for Multi-domain Operations* (NU). ACT. 5 de julio de 2022. Párr. 39.
[45] EMAD. (2023, 28 de marzo). Concepto exploratorio «Evolución de la Fuerza Conjunta hacia las Operaciones Multidominio». Párr. 46.
[46] Gobierno de España. (2021, cap. 4). Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021 (ESN 21).

convencionales se alternan con el uso combinado de vectores económicos, tecnológicos, diplomáticos y de información, entre otros, como elementos de presión y desestabilización[47].

Lo anterior implica que, para abordar las MDO en todo su espectro, la Fuerza Conjunta debería desarrollar una organización capaz de planear, dirigir y ejecutar actividades por debajo del umbral del conflicto y en el ámbito cognitivo, y estudiar el papel que desempeña frente a la manipulación informativa y por parte de agentes extranjeros, en apoyo a otros instrumentos de poder del Estado.

Para ello, será necesario ampliar el espacio de competición de las FAS para hacer frente a las actividades en la zona gris, ya que el mayor empleo de esta zona en los conflictos por parte de adversarios y competidores refuerza la idea de que las MDO también deben realizarse por debajo del umbral del conflicto armado, lo que exigirá una mayor integración con el resto de instrumentos de poder del Estado[48].

Por lo tanto, aunque el rápido avance de las EDT imprime un carácter de urgencia en el desarrollo de capacidades multidominio, la definición de un marco legal y ético para contrarrestar y generar efectos, especialmente en el ámbito cognitivo, resulta tan crítico como desarrollar la propia tecnología[49].

5. Posibles recomendaciones hacia las MDO

De manera no exclusiva, algunas de las acciones que se pueden acometer para propiciar el cambio de mentalidad y cultura organizativa de las FAS, desde la TD hacia las MDO, son:

- Respecto a la TD / orientación al dato:
  - Sin esperar a un modelado de procesos formal externo, revisar con espíritu crítico los procesos de trabajo y flujos de información cotidianos, ensayando nuevos procedimientos y eliminando las etapas que no aporten valor. Romper la inercia del «siempre se ha hecho así».
  - Fomentar la reutilización de productos vs. su reelaboración, a todos los niveles (por ejemplo, en lugar del método tradicional de envío de estadillos y datos de control parciales al escalón superior, que los refunde y a su vez los eleva, etc., hacerlos de forma concurrente y en tiempo real

[47] Gobierno de España. (2021, cap. 4). Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021 (ESN 21).
[48] EMAD. (2023, 28 de marzo). Concepto exploratorio «Evolución de la Fuerza Conjunta hacia las Operaciones Multidominio». EMAD. Párr. 45.
[49] OTAN. (2022, 5 de julio). *Initial Alliance Concept for Multi-Domain Operations* (NU). ACT. Párr. 12.

en una plataforma colaborativa) de manera que la información no se fragmente y haya una única fuente de información unívoca, en tiempo real, y accesible por todos.

- Fomentar la parametrización de valores objetivos en los informes en apoyo a la decisión, en lugar de utilizar elementos de juicio subjetivos (alto, bajo, etc.) que permitan establecer métricas y, por tanto, ver la evolución y tendencias de lo medido, hacer comparativas y tomar medidas correctoras.

- Respecto a la formación y capacidades:
  - Fomentar el autoconocimiento y autorregulación (fundamentos psicológicos, comunicación, etc.), con apoyo de los departamentos de psicología, liderazgo y asistencia técnica de las FAS.
  - Incluir el pensamiento crítico en los programas de formación (detección de sesgos, heurísticas y falacias lógicas).
  - Desarrollar la capacidad formal de pensamiento sistémico (*systems thinking*) para el análisis y modelado de problemas complejos en apoyo a los procesos de planeamiento y decisión, inicialmente a modo de *think tank* (por ejemplo, en el Centro Superior de Estudios de la Defensa, o sobre departamentos de asistencia técnica de los Ejércitos/Armada). En función de los resultados de las primeras experiencias, valorar su inclusión en programas de formación y extensión a los Grupos de Planeamiento Operativo.
  - Valorar la posibilidad de diseñar y programar un curso MDO.
  - Valorar la especialización de determinados cuarteles generales y unidades en aspectos MDO, a modo de unidades de referencia[50].
  - En el planeamiento y conducción de las operaciones actuales incluir diversidad (multinacional, actores civiles, perfiles heterogéneos), método formal de análisis y resolución de problemas complejos y nuevos ámbitos que proporcionen opciones de respuesta no convencionales.

- Respecto a desarrollar conciencia de operaciones conjuntas a las MDO:
  - Aprovechar las operaciones de asistencia a autoridades civiles en tiempo de paz como experiencias MDO, ya que constituyen un buen entrenamiento para sistemas, conectividad, uso de la comunicación e influencia, estructuras de mando y procedimientos con otros actores no militares. Entender estas operaciones con mentalidad de aprendizaje

[50] Como ejemplo, el Ejército norteamericano ya ha creado tres *Multi-Domain Task Force* con orientación regional.

de un contexto MDO de «baja intensidad» e incorporar a nivel general las acciones correctoras derivadas del proceso de lecciones aprendidas puede favorecer la creciente capacidad MDO de las FAS. Se aprende mientras se practica.

- De igual manera, experimentar y validar progresivamente los conceptos de las MDO en las misiones permanentes de las FAS, propiciando una mayor integración de otros Mandos Operativos[51] y elementos de poder distintos del militar[52] en su conducción y seguimiento; incluyendo en el planeamiento acciones en todos los ámbitos, físicos y virtuales, con creciente participación en el cognitivo. Sin la familiarización progresiva desde tiempo de paz con este tipo de operaciones será muy difícil ser resolutivos y ágiles en caso de conflicto, dado que las agresiones multidominio se producirán frecuentemente desde la zona gris. Estas prácticas permitirían también desarrollar reglas de enfrentamiento, normativa y el marco jurídico adecuado para realizar MDO, tanto en el ámbito de la preparación de las FAS como en escenarios potenciales de zona gris. Todo ello, además de desarrollar la capacidad MDO, contribuiría eficazmente a la disuasión.

[51] Fundamentalmente el ciberespacial y de inteligencia.

[52] Diplomático, FCSE, mediático, operadores de telecomunicaciones y del espacio, etc.

Capítulo 2

Operaciones multidominio. Conectividad

Luis Francisco Astorga González

Resumen

El artículo revisa, desde un punto de vista conceptual, la previsible evolución de las comunicaciones en el campo de batalla que, previsiblemente, van a incorporar nuevas tecnologías y conceptos para acelerar el ciclo OODA (Observar, Orientar, Decidir, Actuar) y facilitar efectos multidominio. La guerra en Ucrania y el uso efectivo para C2 de sistemas civiles, como redes de telefonía o satélites de baja órbita terrestre, abren la posibilidad de combinar, en escenarios futuros, sistemas civiles y militares para mejorar la resiliencia y ampliar los anchos de banda. El proceso de los datos acumulados en la nube con inteligencia artificial será una herramienta imprescindible, especialmente a nivel táctico, para disponer de un ciclo OODA eficaz contra adversarios con capacidades equivalentes.

Palabras clave

Multidominio, OODA, Telefonía, Satélites, Inteligencia artificial, Ucrania, NEC.

Multi-Domain Operations. Connectivity

Abstract

The article reviews, from a conceptual overview, the evolution of battlefield communications over the next two decades, which is expected to incorporate new technologies and concepts to accelerate the OODA (Observe, Orient, Decide and Act) cycle and facilitate multidomain effects. The war in Ukraine and the effective use of civilian systems for command and control, such as telephone networks and low-Earth orbit satellites, open up the possibility of combining civilian and military systems in future scenarios to improve resilience and increase bandwidth. The processing of data accumulated in the cloud by Artificial Intelligence will be an essential tool, especially at the tactical level, to achieve an effective OODA cycle against adversaries with equivalent capabilities.

Keywords

Multidomain, OODA, Telephone networks, Low-Earth orbit satellites, Artificial intelligence, Ukraine, NEC.

1. Introducción

La OTAN define las MDO como la integración efectiva de fuerzas conjuntas, defensa integrada aérea y antimisil, operaciones cibernéticas, mando control y comunicaciones, sistemas de inteligencia, indicios y alertas, guerra electrónica, capacidades espaciales y capacidades nucleares[1].

En la doctrina de la Alianza, ser capaces de definir una arquitectura multidominio constituye la base para el empleo efectivo futuro de la Fuerza. Siguiendo con definiciones de la doctrina OTAN, el instrumento de poder militar tiene que ser capaz de actuar decisivamente en todos los ámbitos de operación de manera sincronizada y en coordinación con otros instrumentos de poder, tales como el poder político, el económico, etc. Para ello las fuerzas de la Alianza deben contar con alta capacidad y disponibilidad, ser interoperables y tienen que ser capaces de crear efectos decisivos para combatir las amenazas, tanto las simétricas como las asimétricas, en los ámbitos de operación físicos, virtual y cognitivo.

El análisis prospectivo de escenarios realizado por la Alianza justifica la necesidad de esta arquitectura multidominio. La evaluación de los conflictos futuros indica que la superioridad de la que ahora dispone la Alianza va a verse retada por adversarios con un gran potencial de adaptación. Es por ello que la OTAN estima que la capacidad de llevar a cabo MDO es un paso en la dirección correcta para mantener una disuasión creíble y, si fuera necesario, vencer en conflictos venideros.

Vivimos en la era de la conectividad y de los datos. Hay miles de millones de personas que tienen un teléfono móvil, con el que acceden a posicionamientos GPS, navegación, compras, líneas aéreas, redes sociales, juegos, trabajos científicos y técnicos, etc. La conducción autónoma sin asistencia humana es ya técnicamente posible y empresas multinacionales coordinan su producción y sus transportes a través de Internet. El mundo se ha transformado y se ha vuelto digital y conectado en las tres últimas décadas. Y esto, como no podía ser menos, ha transformado igualmente las operaciones militares. En este sentido, hace más de dos décadas que se empezó a gestar la doctrina de combate en red, NEC (*Network Enabled Capability*). Uno de los «padres» de la idea, el Almirante Cebrosky, hablaba de la nueva economía que facilitaba Internet y asociaba esa misma revolución a las operaciones militares:

> «The [...] military could use battlefield sensors to swiftly identify targets and bomb then. Thousands of warfighters would act as a single, self-aware coordinated organism. Better communications would

[1] OTAN. (2023). *Alliance Concept for Multi-Domain Operations*. NATO ACT.

> let troops act swiftly and with accurate intelligence, skirting creaky hierarchies. It would be a revolution in military affairs unlike any seen since the Napoleonic age. And it would not take hundreds of thousands of troops to get a job done – that kind of massing of forces would be replaced by information management. [...] computer networks and the efficient flow of information would turn the chain saw of a war machine into and scalpel». (Cebrowsky and Gartska, 1998)[2]

Con el concepto NEC las operaciones militares se estructuraban alrededor de la red, de tal forma que los actores tenían acceso a sensores y armas disponibles de manera distribuida. El modelo sostiene que la superioridad de la información que ofrece la red permite al ciclo de decisión OODA[3] (observar, orientar, decidir, actuar) que sea más rápido que el del enemigo y, por ello, se obtiene ventaja en los niveles táctico, operacional o estratégico. En el NEC se pretendía pasar de las operaciones centradas en las plataformas a las operaciones centradas en la red; el concepto multidominio da un paso adicional, apartándose aún más de las plataformas, en cierto sentido «del mundo físico», e intenta que las operaciones se centren en los datos.

Cómo se gestionan los datos y la información que una multitud de sensores conectados pueden proporcionar es uno de los problemas del combate en red. Si todo el mundo accede a todos los datos disponibles en la red podemos simplemente encontrarnos en una nueva versión de la niebla de la guerra definida por Clausewitz: estaríamos ahogados en una nube de datos que no seriamos capaces de filtrar y que finalmente nos llevarían a tener un ciclo OODA más lento que el de nuestro adversario.

De vuelta a la doctrina, para hacer esta transición desde la red hacia los datos necesitamos acometer una profunda transformación digital en la Alianza. Esta será la clave para poder orquestar y sincronizar las actividades de los diferentes instrumentos de poder y así obtener efectos multidominio, asegurar la interoperabilidad, mejorar el conocimiento del entorno y facilitar la consulta política y la toma de decisiones basadas en datos. Datos que requieren una política común de gobierno y una gestión que garantice la seguridad de esos datos a través de la Alianza[4].

Este trabajo pretende analizar, de una manera conceptual, cómo los avances en conectividad que permite la tecnología actual contribuyen a facilitar las MDO. Cómo puede ser el escenario del campo de batalla del futuro y

[2] Citado por: Walker, G. H., Stanton, N. A., y Jenkins, D. P. (2009). *Command and control: The sociotechnical perspective*. CRC Press.

[3] Alumbrado por el coronel de la Fuerza Aérea de los EE. UU John Boyd.

[4] OTAN. (2023). NATO's digital transformation implementation strategy [en línea]. Disponible en: https://www.nato.int/cps/en/natohq/news_214878.htm

cómo hay que diseñar el intercambio de información —y los medios técnicos— para alcanzar los objetivos perseguidos. Cuáles son los riesgos y cuáles los límites a los que de momento nos enfrentamos.

2. Conectividad: ¿qué ha cambiado?

Hemos mencionado ya cómo las posibilidades que ofrecía Internet hace dos décadas anticipaban entonces una importante transformación futura del campo de batalla, pasando de «la guadaña al bisturí». La aparición de Internet con sus enormes posibilidades de intercambio de información permitió construir una *Common Operational Picture,* en tiempo útil, mucho más rica y completa que en el pasado.

Hay un cambio de paradigma en las comunicaciones, que empezó con Internet, pero cuyo crecimiento es exponencial: hasta muy recientemente los mensajes se intercambiaban entre humanos. Incluso con Internet, una buena parte de las comunicaciones tenían como destino final a personas. Esto está cambiando masivamente y cada vez tienen más importancia los mensajes entre máquinas, que permiten llevar a cabo decisiones preprogramadas —automáticas— sin necesidad de intervención humana. Esta tendencia está cada vez más presente en nuestra vida diaria; las luces de un centro comercial se encienden o se apagan automáticamente, dependiendo de las señales que proporciona un sensor. Pero esa decisión de encender o no las luces —o de activar unas escaleras mecánicas— puede ser más compleja que la simple determinación del nivel lumínico e introducir otros elementos, como horarios comerciales, movimiento, etc. Podemos incluso crear un sistema que aprenda y que decida cuándo es pertinente que las escaleras mecánicas no arranquen, incluso cuando un usuario se aproxima, considerando por ejemplo una combinación de ahorro energético y satisfacción de los usuarios, de forma que la decisión de arrancar o no las escaleras ya no dependerá de un algoritmo prefijado —por complejo que este sea—, sino de cómo aprende el sistema para maximizar esos parámetros.

En este proceso de comunicaciones entre máquinas es muy relevante la aparición de Internet de las cosas (IoT), y el rol que ya juega el aprendizaje maquina (ML, *machine learning*) en nuestra vida cotidiana. Hay decenas de miles de millones de dispositivos enlazados a través de IoT: sensores en fábricas, vehículos, *wearables*, domicilios, etc. Todos estos dispositivos generan ingentes cantidades de datos que deben ser procesados —o descartados— y analizados de forma automática sin intervención humana. Y ello porque solo es posible procesar esta ingente cantidad de datos si se hace de manera automática y solo es posible transformarla en decisiones si lo hacemos a través de lo que denominamos IA —en este caso ML (Mishra y Tyagi, 2022)

Las máquinas, para aprovechar las capacidades que ofrece el IoT, necesitan comunicación ubicua, ultrarrápida y ultra confiable (Di Francesco y Karlsson, 2018), algo que ya pueden proporcionar, por ejemplo, las redes 5G. Pero incluso este paradigma está ya empezando a cambiar: el estándar de las redes 6G va a desplazar el análisis inicial de los datos desde la nube al *Edge Computing*, limitando las necesidades de intercambio de datos, que empieza a anticiparse como masivo. Y las necesidades son siempre crecientes, hasta el punto de que «el ancho de banda disponible no es suficiente, nunca lo ha sido y nunca lo será» (Nielsen. 1998)[5].

Siguiendo a los clásicos —en particular a Clausewitz— la naturaleza de la guerra es inmutable, pero la forma cambia según las circunstancias. Las operaciones militares siempre han estado condicionadas en gran medida por las posibilidades y limites que permiten las comunicaciones. Cuando los Ejércitos crecieron de forma exponencial a comienzos del siglo XIX —fruto de la revolución en las operaciones militares que alumbró la *levée en masse* de Napoleón—, se hizo imposible, para los generales al mando, el control de diferentes escenarios: los alemanes inventaron entonces el *mission command* y aparecieron de manera natural los distintos niveles de conducción militar que utilizamos en Occidente hoy en día: táctico, operacional y estratégico. Niveles de conducción que demostraron su utilidad en las guerras mundiales del siglo XX y que fueron, en cierto sentido, olvidados durante los años cincuenta y sesenta del pasado siglo y recuperados, especialmente en Occidente, tras los análisis efectuados a consecuencia del fiasco que los Estados Unidos sufrieron en Vietnam.

Pero la pertinencia de esos niveles de conducción fue de nuevo puesta en cuestión a finales del pasado siglo, con la aparición del concepto NEC: para los abanderados del combate en red, las posibilidades de la técnica y las modernas comunicaciones ofrecían a los comandantes de los teatros una *situational awareness* (una conciencia de la situación) que eliminaba la necesidad de la división por tres niveles de conducción y permitía pasar del nivel estratégico al táctico.

En mi artículo «La esencia de la guerra y el concepto NEC» (Astorga, 2011: 11-32) ponía en cuestión la desaparición de los niveles de conducción por la introducción del combate en red, pese a lo apuntado por el almirante Cebrowsky, al que antes hemos citado. De manera sintética, porque la niebla de la guerra no desaparece con la mejora de las comunicaciones y porque más datos no ayudan *per se* a tomar mejores decisiones en entornos complejos y cambiantes contra adversarios equivalentes (*peer competitors)*. Como señala Friedman en su artículo «making NEC worthwhile» (Friedman,

[5] De acuerdo con la ley de Nielsen sobre el ancho de banda, las necesidades de los usuarios crecen un 50 % anualmente, medido entre 1983 y 2023.

2004: 14-18), en realidad con el concepto NEC intentábamos realizar la guerra basada en la COP, una *common operational picture* supuestamente casi perfecta y, sobre todo, mucho mejor que la del adversario. Pero tener una buena COP ayuda a tomar mejores decisiones, especialmente a nivel táctico y en acciones que requieran una reacción muy rápida – por ejemplo, en guerra aérea- pero no es garantía de que cuando las decisiones son del nivel operacional o estratégico, una COP perfeccionada mejore sustancialmente ese proceso.

Pero ya no hablamos de NEC; con las MDO abandonamos la aproximación «centrada en la red» (*network centric approach*) para pasar a una aproximación centrada en los datos (*data centric approach*). Y es legítimo entonces preguntarse sobre cuál es la diferencia entre ambos conceptos; al fin y al cabo, lo que intercambiamos entre unidades o sistemas son datos en ambos casos. Es natural dudar de si hablamos del mismo «perro con distinto collar». Haremos ese análisis más adelante; sin embargo, es conviene señalar desde ahora cuáles son, a mi juicio, las diferencias principales entre ambos casos.

En primer lugar, los ámbitos son diferentes. No solo consideramos los clásicos ámbitos físicos (terrestre, marítimo, aeroespacial) y los no tan clásicos (cibernético), sino que también incluimos un nuevo ámbito: el de información o cognitivo.

En segundo lugar, disponer de los datos adecuados en el lugar adecuado —normalmente la nube— nos permite en teoría analizar esos datos con herramientas de IA y tomar decisiones que mejorarán no solo la velocidad del ciclo OODA, sino, sobre todo, la calidad de nuestras acciones.

3. Comunicaciones, Mando y Control (C3)

Como hemos ya apuntado, el desarrollo de las comunicaciones en la milicia ha evolucionado desde el intercambio de mensajes entre personas hasta la automatización de mensajes entre máquinas. Durante milenios fueron la voz o el texto escrito los medios usados por los generales y sus subordinados para proporcionar órdenes o intercambiar información; solo muy recientemente —en los últimos dos siglos— primero el telégrafo y luego la radio ampliaron el alcance del intercambio de mensajes, reduciendo extraordinariamente los tiempos; en otras palabras, acelerando el ciclo OODA.

La creciente complejidad de los sistemas de armas y la necesidad de una gran velocidad de reacción, especialmente en la guerra aérea, promovieron la aparición de los sistemas de intercambio automático de datos, tales como link 11 o link 16. Estas redes —con limitaciones— facilitaban disponer

de una *Recognised Air Picture* (RAP) común y la coordinación de asignación de blancos entre distintas unidades. Se diseñaron incluso herramientas informáticas que realizaban esa asignación de blancos, buscando la mayor eficiencia posible: batir al mayor número de enemigos a la mayor distancia en el mínimo tiempo, herramientas que, al menos en mi limitada experiencia con la del grupo de combate de la Armada instalada en el portaviones Príncipe de Asturias, nunca funcionaron demasiado bien.

Estos intercambios de datos se realizaban a nivel táctico; hasta hace pocos años los enlaces con los niveles operacional o estratégico se realizaban fundamentalmente por radio, especialmente en la mar y en el aire, pero también en tierra, en escenarios alejados de los centros de decisión de nivel superior. En la mayor parte de las marinas de guerra de Occidente, la mensajería formateada con los estándares del ACP 127 ha sido, durante mucho tiempo, el principal medio de C2 que usaban los niveles estratégico y operacional con las fuerzas desplegadas. Y dadas sus limitaciones, la filosofía de *isión command*, a la que antes hemos hecho referencia, resultaba particularmente adecuada para el empleo de esas fuerzas.

La aparición del satélite de comunicaciones militares y su expansión durante los años 90 del pasado siglo, cambió la relación de los mandos operacionales con las fuerzas desplegadas. Las comunicaciones seguras por teléfono en tiempo real eran posibles, así como el intercambio no solo de mensajería formal, sino de mensajería informal (correo electrónico) e imágenes y documentos complejos. La información que antes se distribuía en texto empezó a almacenarse en servidores de datos organizados siguiendo una estructura de hiperenlaces como el de las páginas web de Internet. Y a medida que el ancho de banda fue creciendo, la complejidad de los intercambios de datos entre las unidades desplazadas y los mandos operacionales lo fueron haciendo también; no solo en lo relacionado con los aspectos operativos de la misión, sino también en lo relacionado con la propia administración burocrática de la unidad desplegada.

El empaquetado y transmisión de los datos tácticos a través del satélite —la RAP, video, etc. Alteró de nuevo la relación entre mandos operacionales o estratégicos— y las fuerzas desplegadas. Los comandantes operacionales disponían, al menos en teoría, de la misma información que sus fuerzas y los medios para ejercer el mando táctico en tiempo útil[6]. La evolución de las comunicaciones por satélite generó una dinámica diferente entre los niveles de conducción de operaciones militares, al facilitar una sinergia

[6] «Tiempo real» se relaciona con la presentación instantánea de información mientras ocurren los eventos, mientras que «tiempo útil» se refiere al período durante el cual la información es relevante y valiosa para la toma de decisiones, independientemente de si se presenta en tiempo real o con cierto retraso.

—de nuevo, al menos en teoría— más eficaz entre lo táctico, lo operacional y lo estratégico. Esa revolución tecnológica amplió la conciencia situacional, al ofrecer una transferencia en tiempo útil de información desde el terreno de operaciones hasta el mando estratégico, permitiendo una toma de decisiones en los niveles superiores más instruida. La coordinación se fortaleció, habilitando la colaboración en tiempo útil entre líderes estratégicos y comandantes en el terreno, permitiendo modificaciones ágiles en el diseño operacional según cambiaban las circunstancias.

Otras ventajas que aportó el uso las comunicaciones por satélite fueron: la mejora de la seguridad de las comunicaciones, posibilitando el intercambio de datos clasificados entre niveles; la optimización de la planificación conjunta; y la mejora del apoyo logístico en aspectos muy diversos, desde la solicitud de repuestos y munición hasta la telemedicina o la asistencia técnica de forma remota.

Pero los satélites militares con comunicaciones en alta frecuencia han sido solo un jalón en el camino. En las últimas dos décadas se ha observado un cambio acelerado en el panorama de las comunicaciones inalámbricas, con diversas tendencias tecnológicas que han redefinido la forma en que las personas se comunican y acceden a la información. Estas tendencias no solo han tenido un impacto en la vida cotidiana, sino que también posibilitan la transformación de la manera en la que operamos en el campo de batalla. La evolución constante de las comunicaciones móviles, catalizada por avances como la llegada de la tecnología 5G y la proliferación del IoT, abre enormes posibilidades sobre cómo las fuerzas militares pueden aprovechar y beneficiarse de estos avances tecnológicos. De igual manera, la aparición de proveedores comerciales de comunicaciones a través de satélites de baja órbita, como Starlink, que ofrece internet con un buen ancho de banda y a precios muy competitivos, amplía las posibilidades de los enlaces de datos de las fuerzas desplegadas que, hasta la fecha, dependían en gran medida de satélites geoestacionarios.

Resulta imprescindible mirar a la industria y a las aplicaciones en el ámbito civil, porque han ido a la vanguardia, adoptando y adaptando de forma muy ágil innovaciones tales como el 5G. Esta quinta generación de redes móviles ha revolucionado la velocidad, la capacidad y la latencia de las comunicaciones inalámbricas, abriendo nuevas posibilidades para aplicaciones de alta demanda de datos, al permitir la conexión de dispositivos en tiempo real con una eficiencia sin precedentes. Al mismo tiempo, el IoT ha llevado a una proliferación de dispositivos conectados que abarcan desde electrodomésticos inteligentes hasta sensores industriales, creando una red de interconexión global que genera y comparte datos constantemente.

¿Cómo aplicar de manera efectiva estas innovaciones al ámbito militar? Hay muchas opciones y posibilidades, que se tienen que ajustar a las

condiciones tácticas y operacionales. El despliegue de redes inalámbricas tácticas, que utilicen la tecnología 5G para transmitir datos en tiempo real entre unidades en el terreno, está siendo ya explotada; hay empresas españolas ofreciendo soluciones punteras y el Ministerio de Defensa ha asignado varios contratos para redes militares 5G. Pero esto puede y debe combinarse con satélites de baja órbita, los clásicos geoestacionarios militares o civiles, radio —definida por *software*— en todo el espectro de frecuencias e incluso láser direccional.

Nos vamos a encontrar, por tanto, en un campo de batalla hiperconectado, un intercambio de datos, información y órdenes realizados a través de multitud de medios, lo que va a permitir acelerar el ciclo OODA. Gracias, entre otras razones, al uso de IA y su aprovechamiento de los datos incorporados a la Nube de Combate. En ese sentido, es importante conocer los límites que hoy presenta la IA, qué se puede esperar de ella y, sobre todo, qué es lo que no puede proporcionar.

4. Inteligencia artificial y datos: límites y posibilidades

Hemos afirmado que vamos a comunicar nuestros sistemas de forma masiva y acumular datos en la nube para acelerar el ciclo OODA. La IA es la herramienta que nos va a permitir procesar esa ingente cantidad de datos y transformarla en decisiones y órdenes a los distintos escalones de la cadena. Por ello es necesario detenerse en una cuestión fundamental: ¿Cuán inteligente es de hecho la IA? La respuesta a esta pregunta es sencilla: cero. El nombre «inteligencia» lleva a confusión; el término «inteligencia artificial» parte de la idea de los padres del concepto en los años cincuenta del pasado siglo, que creían que con la evolución de la computación sería posible replicar el mecanismo de funcionamiento del cerebro humano en un sistema electrónico (Agrawal *et al.*, 2018).

Casi setenta años después de la famosa conferencia de Dartmouth[7] en la que se acuñó el término, no estamos más cerca de lograr esa replicación. La IA no es más que un conjunto de algoritmos y sistemas de procesos que permiten predecir de manera precisa —más de lo que es capaz de hacer un ser humano— qué va a suceder en determinados sistemas. La IA es fundamentalmente un pronosticador. Un pronosticador muy bueno... en ciertas condiciones. En otras, es completamente inútil. Y además puede ocurrir que haga un pronóstico correcto y, sin embargo, nos lleve a conclusiones y a acciones completamente erróneas.

[7] El proyecto de investigación estival en Dartmouth, EE. UU., en 1956, fue un *workshop* de seis semanas considerado como el evento fundador de la inteligencia artificial como campo de estudio.

Analicemos algunas frases que se oyen de manera repetida: «con los datos adecuados la IA podrá predecir el futuro». «Sabremos quién será el próximo presidente de los EE. UU., cómo evolucionará la economía mundial o cómo será la sociedad del futuro» —un poco en la idea de la trilogía de La Fundación, una de las famosas novelas del prolífico escritor de ciencia ficción y divulgador científico Isaac Asimov.

Conviene hacer algunas reflexiones sobre todo esto. Si un avión viaja de Bruselas a Madrid podemos hacer un pronóstico bastante bueno de cuándo va a salir y a llegar. No necesitamos IA para hacerlo, es añadir a la hora de salida la distancia dividida por la velocidad del avión. ¿Podemos mejorar ese pronóstico? Podemos incorporar, por ejemplo, el día que se viaja —cuánto tráfico hay ese día en la ruta—, el volumen de aviones operando en los aeropuertos de salida y llegada, la distancia a la parada de taxis o al aparcamiento, el funcionamiento del aeropuerto, etc. Si hemos acumulado los datos apropiados durante el tiempo suficiente, podemos entrenar una red neuronal para que nos proporcione un pronóstico mejor. Algo muy útil para la operativa de una compañía aérea, que va a tener una idea más precisa de cuál es el tiempo real que necesitan sus aviones. Pero ¿qué ocurre si hay un accidente en Bruselas y se cierran las pistas? No está en nuestros datos, no forma parte del modelo, por lo que la predicción de la IA para ese día de la operativa de los aviones sería totalmente errónea.

Imaginemos que tenemos una compañía multinacional de detergentes, con fábricas en diversas partes del planeta, que compra las materias primas que consume en todo el mundo y que vende sus productos de forma global. ¿Cómo optimizar la producción maximizando beneficios? Los precios de las materias primas varían dependiendo de donde se compren, al igual que el precio del transporte, la demanda de los diferentes mercados, el coste de la energía, etc. Podemos introducir un número muy elevado de variables: los datos disponibles y el uso de mecanismos de IA nos permiten resolver un problema de optimización que sería muy difícil de realizar de otra manera, incluso con regresiones multivariante. No obstante, de nuevo, este mecanismo, extraordinariamente útil para la compañía, no puede anticipar que habrá una guerra en una frontera por la que pasan sus materias primas; *la IA no es una bola de cristal*.

Podemos pensar que es un problema de incrementar el número de variables que incorporamos; que si tuviésemos datos suficientes podríamos también haber pronosticado el conflicto en esa frontera. Lo que genera de nuevo dos importantes condicionantes; el primero, cuáles son los límites del sistema. Si no hay límites, el número de variables es infinito. El segundo, cuáles son los datos acumulados de las variables que pretendemos usar. Si no hay datos pasados, no hay posibilidad de que la IA pronostique el futuro.

Pero hay algo todavía más importante que fija los límites de la predicción: si el universo es o no es determinista. En el siglo XVIII el matemático francés Pierre Simón Laplace, influenciado por los descubrimientos de Galileo o Newton, afirmaba: «Si se conociera la velocidad y la posición de todas las partículas del Universo en un instante dado, se podría predecir su futuro por el resto de los siglos» (Hennessey, 2007: 128-159). Hemos considerado al universo como determinista durante siglos, pero ya no es así.

El matemático Edward Lorenz, con la famosa teoría del caos, ilustrada en el famoso «efecto mariposa»[8], cuestionó la afirmación de Laplace, al demostrar cómo variaciones infinitesimales en las condiciones iniciales del sistema llevaban a estados finales muy diferentes. Además, la mecánica cuántica nos ha hecho entender que el mundo cuántico está indeterminado:

> «[...] no es posible predecir (en función de un conjunto de causas precedentes) qué valores de la medida producidos en el colapso de una partícula van a hacerse realidad. Las interacciones de los sistemas cuánticos entre sí y de estos con los macroscópicos van creando continuamente multitud de incertidumbres en la evolución del universo. En este sentido la evolución del mundo no refleja una partitura preestablecida, sino que es «creativa», al elegir continuamente unos valores precisos de entre un conjunto de posibilidades superpuestas que nunca llegarán a ser realidad» (Monserrat, 2009).

En otras palabras: la predicción de cualquier IA, por avanzada que esté, tendrá límites, porque el mundo no es determinista. Sin descender a la mecánica cuántica, en sistemas caóticos —por ejemplo, la sociedad humana— variaciones a las condiciones iniciales del sistema pueden llevar a condiciones finales muy diferentes. Y en todo caso, solo si disponemos de información suficiente del pasado sobre las variables relevantes del proceso, podremos pronosticar el futuro, en aquellos casos en los que sea posible. No siempre lo es. Conocer cuántas veces ha salido cara al lanzar una moneda no ayuda a saber si saldrá cara o cruz en el siguiente lanzamiento.

¿Por qué esta larga disertación sobre datos e IA al hablar de conectividad en el futuro campo de batalla? Pues, precisamente, porque es importante entender que muchas de las decisiones que se tomarán en el campo estratégico o incluso operacional no las puede tomar una IA o un conjunto de herramientas de IA, analizando una ingente cantidad de datos (Payne y Warbot, 2021). En el nivel táctico, sin embargo, la recopilación de datos y su análisis con herramientas de IA, que proporcionen decisiones en tiempo útil, pueden cambiar el ciclo OODA, acelerándolo de forma muy notable.

[8] «El aleteo de las alas de una mariposa se puede sentir en el otro lado del mundo».

Para aprovechar las capacidades que la IA ofrece es necesario estudiar bien los «casos de uso», su aplicabilidad, la tecnología a emplear o los datos disponibles. Con el uso de la IA no nos vamos a enfrentar a un problema complejo, sino a un montón de problemas diferentes que habrá que valorar de forma separada; no para todas nuestras necesidades tácticas u operativas el uso de IA podrá proporcionar soluciones.

5. Prospectiva tecnológica en conectividad

Podemos, hasta cierto punto, intentar anticipar algunas de las tendencias tecnológicas que van a tener impacto en el campo de batalla en las dos próximas décadas y que ya se empiezan a ver en la guerra en Ucrania. La OTAN referencia algunas de ellas en su EMSS (*Electromagnetic Spectrum Strategy*)[9]. Un estudio interesante sobre tendencias tecnológicas, que incluye computación y comunicaciones en el periodo 2020-2040, es el de Michael O'Hanlon (2019). Hay mucha literatura al respecto, pero poca variación en la estimación de que la hiperconectividad, la IA y las tecnologías cuánticas van a dominar el escenario tecnológico militar en la primera mitad de este siglo.

¿Qué nos vamos a encontrar en las próximas décadas? Congestión del espectro, con conflictos crecientes entre las frecuencias de uso civil y militar, demanda masiva de conectividad en cualquier lugar y a cualquier hora, uso masivo de drones, sistemas autónomos y armas inteligentes de gran precisión (Singh, 2023), guiadas con o sin intervención humana, aprovechando datos de múltiples sensores, radar, ópticos, de detección electromagnética pasiva, ubicados en tierra, mar, el aire o el espacio. La explotación de la información que proporcionan estos sensores, combinada con las armas de precisión disponibles, está ya haciendo muy difícil la guerra de maniobra. En cierto sentido, hemos vuelto a la Primera Guerra Mundial, cuando la ametralladora confinó en el frente Occidental a los soldados en trincheras sin que hubiera avances significativos durante años. Los combates en ciudades como Bajmut, en donde los avances se miden en centenas de metros, parecen retrotraernos a ese escenario de hace un siglo.

Respecto a las comunicaciones, dos elementos en cierta medida inesperados han cobrado gran protagonismo en las operaciones de las FAS de Ucrania. Uno son las redes de telefonía móvil. Ucrania ha hecho uso de redes 3G y 4G para sus operaciones militares, algo que ha negado a los rusos al impedir cualquier servicio de *roaming* procedente de Rusia o Bielorrusia (Milevski, 2022). Es previsible que en el futuro las fuerzas en

[9] Emitida en febrero de 2019.

combate utilicen las redes comerciales disponibles, también en el 5G y en el futuro 6G, además del despliegue de su propia infraestructura.

El otro elemento disruptivo han sido las comunicaciones por satélite, especialmente a través de aquellos de baja órbita terrestre (*Low Earth Orbit*, LEO). Estas comunicaciones están siendo fundamentales para proporcionar C2 y para diseminar inteligencia y llevar a cabo el *targeting*. Lo más relevante y el cambio de tendencia que muestran estos satélites es la importancia de los operadores privados (Chabert, 2023: 145-56). Al igual que en el caso de la telefonía, los operadores privados no solo pueden complementar a las redes militares, sino que permiten enmascarar las comunicaciones militares en ellas. Ucrania no es ni mucho menos un estándar en capacidades militares comparado con países punteros de la Alianza, pero el núcleo de sus comunicaciones militares en la guerra se fundamenta en redes civiles y especialmente en los servicios de Starlink, la compañía de internet basada en satélites LEO[10]. El intercambio de mensajes, video, chat, etc., a través de los terminales de Starlink ha permitido, según algunos analistas, reducir el tiempo de *targeting* de 20 minutos a un minuto (Rahaman Sarkar, 2023). Ucrania dispone de varios miles de terminales de Starlink y ante las amenazas de la compañía de interrumpir el servicio, ha solicitado que el coste —unos 400 millones anuales— sea cubierto por la ayuda de Occidente (McLeary, 2022). Es también muy relevante para las aplicaciones militares de este tipo de satélites, dadas sus características —un número elevado de satélites en azimuts diferentes, transmisiones en multifrecuencia, antenas de orientación electrónica— el que resulte muy complejo perturbar sus comunicaciones. Anticipando el futuro, la explotación en la próxima década de tecnologías cuánticas disminuirá mucho el tamaño de las antenas y las potencias necesarias en los enlaces[11]. Esto facilitará la reducción de la huella electromagnética de las comunicaciones militares y hará previsiblemente su detección y perturbación más compleja.

Rusia, que no dispone, como hemos señalado, de acceso a las redes de telefonía en Ucrania, ni tampoco a satélites de comunicaciones LEO, como Starlink, está experimentando enormes problemas de C2, que ejerce fundamentalmente a través de radios cifradas en UHF/VFH.

[10] Starlink dispone de unos 4.000 satélites en órbitas a 550 km de altura, lo que permite una latencia de 25 ms.

[11] U.S. Army CCDC Army Research Laboratory Public Affairs. (2020, marzo 19). Army scientists create innovative quantum sensor. Disponible en: https://www.army.mil/article/233809/army_scientists_create_innovative_quantum_sensor#:~:text=In%202018%2C%20Army%20scientists%20were%20the%20first%20in,Army%20Combat%20Capabilities%20Development%20Command%E2%80%99s%20Army%20Research%20Laboratory

Sus deficientes comunicaciones condicionan sus operaciones, pero es relevante analizar, además de C2, alguna otra de las funciones operacionales clásicas, como por ejemplo el apoyo de fuegos. Si nos centramos en la artillería, en la que los rusos tienen, según la mayoría de los analistas, con ventaja de uno a diez en cantidad, la experiencia de más de un año de guerra prueba que están en franca desventaja ante los sistemas HIMARS de artillería ucraniana y el uso de munición guiada. La combinación de un conjunto de capacidades: recolección de inteligencia, comunicaciones con gran ancho de banda en tiempo útil, rápido proceso de los datos, un *targeting* ágil y el uso de armas de alta precisión, es lo que ha proporcionado a los ucranianos un OODA mucho más rápido que el ruso. Las comunicaciones permiten acelerar el ciclo, pero sin la inteligencia y las armas de precisión las comunicaciones *per se* no proporcionarían la ventaja a las tropas ucranianas que la sinergia con otras capacidades está ofreciendo.

Otro elemento que está resultando disruptivo son los vehículos autónomos no tripulados, especialmente los aéreos. Los drones están resultando los actores clave del conflicto en Ucrania, de igual manera que lo hicieron en la guerra en Armenia por Nagorno-Karabaj, pero a una escala completamente diferente. Según algunas fuentes, Ucrania está perdiendo alrededor de diez mil drones al mes (Freedberg Jr., 2023), derribados por medios cinéticos o por guerra electrónica.

Para la Alianza Atlántica los vehículos autónomos van a mejorar las capacidades actuales en, por ejemplo, detección, identificación y asignación de blancos; van a expandir y mejorar las capacidades multidominio agregando datos de fuentes diversas, contribuyendo así a generar una COP aumentada; y van a permitir nuevas capacidades, tales como los enjambres (*swarms*) y las actividades anti-enjambres[12].

Las comunicaciones con los drones de subida (*uplink)* y descarga o bajada (*downlink)* se efectúan por medios inalámbricos. A mayor frecuencia en el enlace se dispondrá de más ancho de banda, el enlace puede ser más direccional y el dron usar antenas más pequeñas, pero el alcance es inversamente proporcional a la frecuencia. El uso de satélites LEO para los enlaces con los drones es una opción que parece muy prometedora. De hecho, se ha empleado en Ucrania. Fuentes de Starlink señalaron en la primavera de 2023 que Ucrania había estado usando sus satélites para controlar drones y que han tomado medidas para evitarlo (Roulette, 2023) —sin especificar cuáles son esas medidas—, ya que la compañía no quiere que su red se utilice para operaciones ofensivas.

[12] CNAD. (2023). Allied applications of autonomous systems for military capabilities. NATO.

Una de las vulnerabilidades de los drones es la perturbación de sus comunicaciones o de las señales de navegación GPS. Además de a los ataques cinéticos —con munición— son también vulnerables a los haces direccionales de radiofrecuencia, que vuelven inoperante su electrónica si no está adecuadamente protegida. Hay un equilibrio entre el coste y la complejidad de proteger la electrónica de los drones ante ataques de pulsos electromagnéticos, que en el conflicto ucraniano se ha resuelto en favor de la cantidad. Como hemos señalado, Ucrania está perdiendo en combate más de cien drones al día.

Los drones dependen en la actualidad del control de sus operadores —y, por tanto, de sus enlaces inalámbricos con ellos—, pero esto va a cambiar en el futuro. Ucrania está siendo el laboratorio a gran escala del uso de drones en conflictos convencionales, pero a raíz de la guerra del 2020 entre Armenia y Azerbaiyán, la *US Navy* hacía las siguientes reflexiones en su estrategia tecnológica para sistemas autónomos[13]:

> «In the fall of 2020, Azerbaijan decisively defeated Armenia in a 44-day conflict. Despite both sides' modern air defenses precluding traditional (manned) air combat, Azerbaijani employed superior unmanned air systems (UAS) in multiple ways. Kinetically, they used UAS as targeting assets for loitering munitions and weaponized UAS to directly strike tanks, radars, etc. In the Information Warfare domain, UAS live-streamed footage of Armenian losses, enabled viral videos on social media, and supported a devastating propaganda campaign. While UAS were not the sole contributor to the overall decisive victory, this yet again illustrates the highly disruptive potential of unmanned systems—and signals what the future potentially holds as these unmanned systems become IAS».

En la estrategia de la *US Navy* los drones dotados de IA cumplirán funciones diversas, pero una de ellas es como portadores de armas. Lo que implica que en determinadas circunstancias tomarán decisiones autónomas para el uso de esas armas. Sin entrar a valorar los problemas y dificultades éticas que va a generar esta autonomía en el uso de armamento letal, el que los drones incorporen IA posibilitará, para algunas plataformas, la reducción de sus comunicaciones y por ello mejorarán su resiliencia y discreción. En todo caso, y a la vista de las prometedoras reducciones en el tamaño de las antenas que posibilita la tecnología cuántica, para las futuras comunicaciones con drones, en escenarios fuera del alcance de las redes 5G o 6G, el uso de satélites LEO parece un medio ideal, dadas las bajas latencias, los amplios anchos de banda y la resistencia a la perturbación que ofrecen estas constelaciones.

[13] Department of the Navy. (2021, julio). *Strategy for intelligent autonomous systems.*

Aunque ya se están realizando algunas pruebas prometedoras con el intercambio de claves de encriptación cuántica o la transmisión de información, aprovechando las propiedades de partículas entrelazadas cuánticamente, no es probable que estas tecnologías disruptivas vayan a estar disponibles a medio plazo[14]. Lo que sí parece es que las tecnologías cuánticas podrían revolucionar los sensores, las antenas, la computación y la transmisión de datos. Estamos solo empezando a vislumbrar las posibilidades que la trasposición de los principios de la mecánica cuántica ofrece a la ingeniería y a los ingenios militares. En ese esfuerzo de I+D+i[15] en aplicaciones cuánticas, que vamos a efectuar con nuestros aliados para continuar disponiendo de ventaja tecnológica en el campo de batalla, hay que considerar que no tenemos capacidad tecnológica e industrial para hacerlo solos. De nuevo, como en el pasado, habrá que buscar nichos tecnológicos para capacidades específicas que contribuyan a nuestro desarrollo industrial, pero con la conciencia de que la armazón de las futuras capacidades probablemente dependerá, en gran medida, de la cooperación con nuestros aliados y, en particular, con los Estados Unidos.

6. Intercambio de datos

Para anticipar cómo se puede diseñar la estructura de comunicaciones futura, hay que hacer algunas suposiciones sobre cómo las tendencias tecnológicas que antes hemos apuntado van a condicionar las posibilidades operativas en la próxima década:

- No habrá prácticamente ningún soldado o vehículo occidental que no lleve un dispositivo personal de comunicaciones que al menos proporcione su posición, el denominado *Blue Force Tracking*. Muy probablemente ese dispositivo se usará, además, para transmitir y recibir información y órdenes.
- El espectro de comunicaciones usará todas las frecuencias y modulaciones disponibles y hará uso de comunicaciones y medios civiles para complementar las capacidades militares. Redes desplegables en 5G y 6G, satélites geoestacionarios y LEO, enlaces tácticos de datos, redes de área en baja potencia, etc. El aprovechamiento de todo el espectro y medios disponibles será una necesidad para afrontar la gran demanda de ancho de banda.
- La seguridad y resiliencia de las redes de comunicaciones será un requisito imprescindible para operar en escenarios de alta intensidad contra adversarios equivalentes. Sin esa resiliencia en los sistemas de enlace

14 Science & Technology Organisation (STO) (2021, Nov.) *Quantum Review*.
15 Investigación, Desarrollo, Innovación.

—y también de posicionamiento— no se conseguirá obtener un ciclo OODA más rápido que el del adversario.

- La información obtenida de los múltiples sensores disponibles se transmitirá por diversos sistemas y medios a la Nube de Combate, lo que permitirá generar una COP que dará una conciencia situacional mejorada. Esto facilitará la toma de decisiones tácticas y, en algunos casos, operacionales.
- El uso de herramientas de IA permitirá el adecuado proceso e integración de los datos recibidos en tiempo útil y enviados a la nube. La COP generada en la nube con estas herramientas posibilitará la toma de decisiones tácticas a una velocidad a la que los humanos no somos capaces. Esa capacidad la van a tener también los sistemas autónomos, lo que aumentará su resiliencia y reducirá las necesidades de conectividad para su control.
- Independientemente del ancho de banda disponible, sin disciplina y priorización de los datos a intercambiar, se puede llegar a saturar las redes, que pueden ser incapaces de gestionar y transmitir la gran cantidad de datos que generarán los dispositivos IoT y los múltiples sensores desplegados en el campo de batalla.
- Los sistemas autónomos, sobre todo aéreos, pero también terrestres, marinos y submarinos, cada vez tendrán más importancia, en sus roles como plataformas de sensores y como portadores de armas. Aunque el uso de IA permitirá reducir la intervención humana en su control, las necesidades de ancho de banda *up/down link* para el intercambio de datos crecerán de forma muy significativa.

Bajo estos supuestos, ¿Cómo organizar las comunicaciones inalámbricas? ¿Tiene que llegar todo a la nube? ¿Con qué frecuencia debemos intercambiar datos? ¿Cómo hacemos llegar a los combatientes la COP que ellos necesitan? ¿Qué pasa en un entorno de negación del uso del espectro electromagnético, en el que puede no haber acceso a la nube?

Disponemos ya de algunas respuestas doctrinales a estas preguntas. La OTAN, hoy en día y en el nivel táctico, lleva a cabo sus comunicaciones de datos con TDL, fundamentalmente con los protocolos Link 16 y Link 11 (este último reemplazado progresivamente por Link 22). La visión de la OTAN para estos enlaces tácticos hasta el año 2040[16] sostiene que la base de sus comunicaciones tácticas serán el Link 16, el Link 22 y el *Joint Range Extensión Application Protocol* (JREAP), que básicamente facilita la transmisión de los mensajes más allá del horizonte, encapsulando los mensajes a través del protocolo IP y, por ejemplo, enlaces satelitales en SHF.

[16] OTAN. (2023). Bi-Strategic Commands Data link Strategy. Junio.

La visión que propone la estrategia TDL es clara:

> «Reliable, secure, information rich, interoperable NATO TDL will be a key enabler for effective Multi-Domain Operations (MDO) in the foreseeable future. The Alliance will continue developing and implementing new cutting-edge data link technologies to maintain the information advantage against any potential adversary in the tactical and operational levels».

En el nivel táctico y operacional, los enlaces TDL van a continuar siendo el mecanismo de transmisión de datos para la OTAN hasta el año 2040. El núcleo lo formará el Link 16 con capacidades mejoradas, con *Link* 22 como complemento, que deberá haber sustituido al *Link* 11 completamente para el año 2025[17].

La voluntad de tomar decisiones basadas en datos (*data driven decisions*), ayudados por herramientas de IA, es explícita en los documentos doctrinales de la OTAN. El *digital backbone* es la herramienta de conectividad —por medios diversos, alámbricos o inalámbricos— que permitirá recolectar los datos disponibles, almacenarlos en un lugar (virtual) y procesarlos de forma que la Alianza pueda realizar MDO, disponer de una adecuada conciencia situacional, asegurar la interoperabilidad, garantizar que se pueden realizar las consultas políticas adecuadas y que se tomen decisiones basadas en la explotación de los datos disponibles.

¿Esta voluntad de disponer de los datos en la nube quiere decir que el sensor de temperatura del motor de un carro de combate Abrahams debe de formar parte de la COP? ¿Y con qué frecuencia mediríamos la temperatura del motor? ¿Cada segundo? ¿Cada minuto? ¿Cuán relevante es el dato y la frecuencia de medición, incluso para las aplicaciones de mantenimiento, que cada vez monitorizan más en tiempo real el estado de los sistemas? La transmisión de estos datos, muchos de ellos a través del IoT, podría saturar el ancho de banda disponible e impedir la transmisión de datos verdaderamente relevantes para las operaciones. En este sentido, y volviendo a señalar que el ancho de banda disponible en servicios móviles nunca es suficiente, es lógico anticipar que en entornos tácticos tendremos que gestionar el ancho de banda disponible, con prioridades similares a las de criterios de calidad de servicio (QoS-*Quality of Service*), para asegurar que los datos importantes llegan a la nube y viceversa.

¿Qué información necesitan los comandantes tácticos sobre el terreno? El capitán de una compañía de infantería, el general que manda una brigada mecanizada, el jefe de un grupo de artillería, el comandante de un escuadrón de caza... ¿Van a acceder a la COP completa, a una parte de ella, o

[17] *Ibidem.*

solo a las órdenes que vienen del escalón superior? ¿Permite la tecnología eliminar la división por niveles de conducción y por ello terminar con el *mission command*?

Mi opinión, por las mismas razones que expuse hace ya una década en mi artículo «La esencia de la Guerra y el concepto NEC» (Astorga, 2011: 11-24), es que no debemos prescindir de los niveles de conducción y que hay que proporcionar COP adaptadas (*tailored)* a las necesidades de los combatientes sobre el terreno. En todo caso, la respuesta a estas preguntas solo las puede proporcionar la investigación y la experimentación formal[18], un camino que debemos ya empezar a recorrer, de forma nacional y también multinacional.

No hemos discutido en este análisis cómo generar efectos multidominio a nivel estratégico, especialmente en el dominio cognitivo, al entender que se sale del alcance de este trabajo, que está centrado en conectividad. Sabemos que el hecho de que buena parte de la población mundial lleve un teléfono inteligente en el bolsillo permite el uso de técnicas de manipulación cognitiva que en el pasado no eran posibles. Es fundamentalmente la emoción la que permite llevar a cabo técnicas de manipulación muy efectivas, que alteran la percepción de esa opinión pública a la que, hoy en día, es posible acceder de forma masiva. Esa manipulación en determinados casos puede producir efectos estratégicos. En mi artículo «Manipulación cognitiva en el siglo XXI» (Astorga, 2021:15-43) analicé el fenómeno y sostuve la necesidad de considerar el terreno cognitivo como un ámbito de operación, como así se realizó anteriormente en la doctrina española (PDC-01A) y la conveniencia de sincronizar las actuaciones en ese ámbito con la estrategia general, en línea con la estrategia multidominio de la OTAN. Sin embargo, no creo que estemos en la próxima década en condiciones de sincronizar efectos a nivel estratégico entre el ámbito de operación cognitivo y los demás ámbitos de manera automática o semiautomática, por muchos datos de los que dispongamos, con el uso de herramientas de IA, por las razones que antes se expusieron al analizar las limitaciones de la IA.

Por lo que, al menos en el nivel estratégico, el conflicto —la guerra— seguirá siendo un arte, no una ciencia, durante mucho tiempo.

7. Conclusiones

El campo de batalla del futuro será tecnológico. El uso de sistemas autónomos, armas inteligentes y la explotación de los datos recogidos por múltiples sensores y tratados con IA facilitarán disponer de un ciclo OODA

[18] OTAN. (2023). *Final report of NIAG Study Group 263 on Command and Control Capabilities in support of Multi Domain Operations (Multi Domain C2).*

acelerado. Pero será imprescindible contar con comunicaciones seguras, con bajas latencias y amplios anchos de banda que permitan los intercambios de información en tiempo útil entre las plataformas de sensores y armas y la nube.

La experiencia de la guerra en Ucrania, con el uso masivo de drones y el intercambio de información de C2 por múltiples vías, incluyendo sistemas civiles de telefonía y proveedores de internet vía satélite, apunta a la extensión de los medios de C2 y a una cierta difusión de las líneas entre medios específicamente militares y civiles.

Las redes en 5G (y su futuro reemplazo, 6G), parecían liderar el panorama de las futuras comunicaciones militares junto con los clásicos enlaces de datos tácticos como Link 16 o Link 22. Sin embargo, la experiencia del conflicto en Ucrania muestra que otras alternativas, tales como los satélites LEO pueden contribuir de manera muy significativa a incrementar alcances, anchos de banda e incluso la resiliencia de las comunicaciones tácticas.

Los avances tecnológicos, que ya se apuntan, pueden resultar disruptivos. Sensores, computación y comunicaciones cuánticas han dejado de ser ciencia ficción, son reales ya en laboratorio y en experimentación, por lo que probablemente su traslado a la producción industrial se va a efectuar en los próximos años. Es necesario estar atento para incorporar esta tecnología, en coordinación con nuestros aliados, en el momento adecuado, para no colocarnos en una posición de inferioridad frente a nuestros adversarios.

Por último, y respecto al empleo de la IA, la forma en la que seamos capaces de incorporarla, especialmente en los niveles táctico y operacional, determinará si nuestro futuro ciclo OODA es más veloz o no que el de nuestros adversarios.

Capítulo 3

La Nube de Combate

Manuel Buesa Bueno

Resumen

Las operaciones multidominio suponen un reto por la complejidad que representan las interacciones entre los diferentes ámbitos de operación. Un conocimiento transversal de la situación y la capacidad de operar desde diferentes dominios de forma simultánea aumentará las probabilidades de éxito en la operación.

La Nube de Combate se presenta como una solución técnica para potenciar la interoperabilidad entre los elementos de la Fuerza de todos los dominios, resultando, así como un medio para impulsar el combate colaborativo.

La implementación de la Nube de Combate requerirá de cambios en el seno de las Fuerzas Armadas y de un plan específico para su desarrollo e implementación.

Palabras clave

Combate Colaborativo, Sistema de Sistemas, Multidominio, Interoperabilidad, Transformación digital, Nube Federada, Superioridad de la información, Dato en el centro, Nube de Combate.

The Combat Cloud

Abstract

Multi-domain operations are challenging because of the complexity of the interactions between the different domains. Cross-domain situational awareness and the ability to operate from different domains simultaneously will increase the chances of a successful operation.

The Combat Cloud is presented as a technical solution to enhance interoperability between force elements across all domains, resulting in a means to drive collaborative combat.

The implementation of the Combat Cloud will require changes within the armed forces and a specific plan for its development and implementation.

Keywords

Collaborative Combat, System of Systems, Multidomain, Interoperability, Digital Transformation, Federated Cloud, Information superiority, Data-Centric, Combat Cloud.

1. La necesidad de la Nube de Combate en el Combate Multidominio

Los escenarios multidominio plantean un nuevo reto para las FAS y, para afrontarlos con éxito, se requerirá potenciar las capacidades colaborativas entre ámbitos de operación. La Nube de Combate (de ahora en adelante «NC») se presenta como una solución para cubrir esta necesidad, el objetivo de este capítulo es aterrizarla para identificar cuáles son las claves de esta solución.

1.1. El reto de los escenarios multidominio

La doctrina para el empleo de las FAS define los cinco ámbitos de operación (de ahora en adelante «ámbitos») que se consideran en las MDO. Es conocido también que en estos ámbitos no se opera de manera aislada y que unos ámbitos tendrán efectos sobre otros. De esto se deriva que, para poder tener un entendimiento completo de lo que sucede en el espacio de las operaciones, es necesario aplicar un enfoque transversal que abarque los diferentes ámbitos. Ya no hay batallas separadas en un mismo conflicto, el enfrentamiento es único, aunque parezca que predomine un dominio.

El nivel de interacción e interdependencia entre ámbitos se va incrementando conforme lo hacen los avances tecnológicos en materias como la IA, las nuevas tecnologías de comunicaciones o la computación en la nube, por nombrar algunos. La irrupción tecnológica multiplica las capacidades de los ámbitos cibernético y cognitivo, lo que progresivamente conllevará una mayor influencia sobre los ámbitos más tradicionales (terrestre, marítimo y aeroespacial), dibujando así un escenario cada vez más complejo que desorientará a las fuerzas que no estén preparadas para afrontarlo, al dificultar y bloquear su capacidad para tomar decisiones.

Un reto fundamental al que se enfrentan las FAS es el de entender las implicaciones de este escenario y cómo deben prepararse para afrontarlo en el futuro. Se debe convertir el riesgo que supone permanecer estáticos ante estos cambios, en la oportunidad que supondría explotarlos de manera conjunta con una gestión anticipada del camino necesario que permita un proceso de transformación ordenado.

1.2. La información como eje de las MDO

Habrá enfrentamiento en todos los ámbitos, pero todos girarán en torno a un dominio central que es el de la información. El éxito en estos escenarios complejos estará del lado del que disponga de los medios para tener la superioridad en la información en la batalla. Esta ventaja permitirá tener

un mayor conocimiento de lo que está sucediendo, además de ofrecer la capacidad de confundir a un adversario desinformado.

Poner la información en el centro de las operaciones convierte a los datos en un activo crítico y a los procesos que transforman ese dato en información en una necesidad. Será crítico recoger datos de los ámbitos cognitivo y ciberespacial e integrarlos con los datos obtenidos del resto de ámbitos. Los procesos de análisis de datos transversales y la fusión y correlación de estos serán los que permitan obtener una información que dé claridad en la toma de decisiones e identificar y anticipar todas las maniobras cognitivas y cibernéticas del adversario.

No es suficiente con tener los medios para obtener información bien integrada y de calidad para tener superioridad sobre el enemigo si no se obtiene y gestiona de manera ágil. La tecnología nos va llevando a un ritmo de batalla donde los ciclos de toma de decisión y actuación son cada vez más cortos, la velocidad a la que se completan los bucles que recorren el camino del dato a la información es crítica y el que esta información fluya de manera rápida por el teatro de operaciones es más crítico aún.

La posesión de información en tiempo útil habilita a los mandos intermedios distribuidos por el campo de batalla para tomar decisiones que agilizan las operaciones, reduciendo los tiempos de reacción de la fuerza. Una de las consecuencias de situar a la información en el eje central de la misión y que todo gire en torno a ella, es la posibilidad de tener un C2 más distribuido.

Todo trata de saber lo que hay que hacer en el momento adecuado y en el sitio preciso. El objetivo es que la información nos permita movernos en la batalla a mayor ritmo que el enemigo.

1.3. La Nube de Combate como solución habilitadora de las MDO

Es prioritario disponer de una solución tecnológica que habilite este enfoque transversal en los distintos ámbitos, que ejerza de eje en las operaciones y las articule proporcionando capacidades en estas cuatro necesidades fundamentales:

- *Conectividad*: la base de la integración entre los ámbitos es la comunicación. Todos los elementos que forman parte de la batalla deben tener la posibilidad de conectarse con el resto, tanto si son sensores, efectores, sistemas de procesamiento de datos o unidades de C2. Las comunicaciones deben ser estables y soportar entornos hostiles donde el oponente trate de anularlas.
- *Gestión de los Datos y la Información*: esta necesidad se centra en la gestión del ciclo de vida completo de los datos y en el proceso que los

convierte en información y conocimiento para la toma de decisiones. Los datos y la información generada por todos los sistemas conectados desde los diferentes ámbitos deben ser accesibles de manera transversal y se deben gestionar bajo una misma política que incluya su priorización, almacenamiento, encriptado y destrucción. La recopilación, el uso y el intercambio de datos e información que se va haciendo debe ajustarse a las necesidades de la misión en cada momento.

- *Soporte a la autoridad en la toma de decisiones*: el volumen de información que se genera en estos escenarios es muy elevado y la tendencia de crecimiento es exponencial, puesto que cada vez habrá más puntos de entrada de datos. A la necesidad de digerir grandes cantidades de datos e información se suma la complejidad de tomar decisiones que pueden afectar a varios ámbitos simultáneamente, bien de manera directa o a través de efectos colaterales.

  Para facilitar el proceso de toma de decisiones en este contexto tan complejo, será necesario contar con que generen propuestas y alternativas de actuación adecuadas al perímetro de influencia de cada autoridad responsable de la toma de decisiones.

- *Seguridad, fiabilidad y resiliencia*: la solución que va a contener todos los datos y la información de la misión debe considerar la seguridad como máxima prioridad desde la fase de diseño. Además, debe ser fiable y estar preparada para operar en escenarios hostiles donde el adversario tratará de denegar su operación.

Todas estas necesidades deben cubrirse de manera transversal de forma que todos los elementos desplegados en los diferentes ámbitos queden orquestados bajo una solución tecnológica. A esta solución nos referimos como NC.

2. ¿Qué es la Nube de Combate?

Este capítulo describe la NC desde su concepto, los elementos de su arquitectura y sus características principales.

2.1. Concepto de Nube de Combate

No se debe confundir el concepto de la NC con la aplicación en exclusiva de un determinado tipo de tecnología, como puede ser la 5G[1]; como tampoco debe hacerse con los dominios de computación, por ejemplo, el *Cloud Computing*[2], que tiene un nombre similar, pero se centra en dar solu-

[1] Estándar de comunicaciones de quinta generación.
[2] Tecnología de computación en la nube.

ciones relativas a la computación. Ambas son tecnologías clave que utiliza la propia NC. La terminología de la nube es amplia y las acepciones de cada término pueden variar en función del contexto en el que se referencien.

El concepto de la NC está asociado al valor que se ofrece hacia la maximización y consecución de los objetivos de la Fuerza Conjunta por explotación sinérgica de sus recursos, al aplicar de forma combinada estas y otras tecnologías, asegurando la prestación del servicio colaborativo en los escenarios multidominio.

La NC es una solución tecnológica que habilita la interoperabilidad entre plataformas y proporciona un sistema de información distribuido único donde se integran y procesan conjuntamente todos los datos recopilados por los sensores y sistemas conectados desde cualquier dominio. La aplicación de esta tecnología sobre el teatro de operaciones permite disponer de esta información para la toma de decisiones en el lugar donde se necesita y en el momento que se precise, mejorando de manera notable las capacidades de C2.

2.2. Un Sistema de Sistemas que opera en los niveles estratégico, operacional y táctico

Los recursos y sistemas conectados a la NC se comportan como un «sistema único» o Sistema de Sistemas (SoS)[3] como se conoce técnicamente en el ámbito de la Ingeniería de Sistemas.

Cada plataforma dispone de sus capacidades individuales de las que debe disponer en todo momento, aunque no esté conectada a otras plataformas. Cuando múltiples plataformas se integran en un SoS el efecto resultante no es solo una suma de capacidades de los sistemas que lo componen, sino que se produce un efecto sinérgico donde aparecen capacidades emergentes que surgen de la colaboración de varios sistemas y en el que el todo es mayor que la suma de las partes. Estas capacidades que se orquestan en el seno de la NC tienen el potencial de conferir superioridad táctica sobre el enemigo basada en la Superioridad en Información.

El Sistema de Sistemas constituido en la NC puede operar simultáneamente en todos los ámbitos operacionales y en los tres niveles de la estructura operativa de las FAS:

- *Nivel estratégico:* la NC proporcionará información para facilitar la selección de los objetivos estratégicos y la manera más eficiente de acometerlos. Esto incluye el soporte en el dimensionado de la Fuerza y planeamiento de las misiones, prediciendo los posibles comportamientos y las opciones de reacción del enemigo.

[3] SoS: del inglés *System of Systems*.

- *Nivel operacional:* la NC permite planear y ejecutar las operaciones haciendo uso de las capacidades del sistema de sistemas. Dispondrá de herramientas de planeamiento y simulación de la misión que generarán las opciones del uso más efectivo de la Fuerza. Este análisis dará soporte al planeamiento de la misión y al rol de cada sistema dentro de las actividades que se ejecutan de manera conjunta y sincronizada.

  Los algoritmos de la NC que simulan y ayudan a planificar las operaciones son los mismos que se van a ejecutar en la práctica durante la misión, lo que lleva a una mayor coherencia entre el proceso de planeamiento y la ejecución.

- *Nivel táctico*: en el nivel táctico la NC proporciona servicios de C2 que permiten integrar y diseminar la información en toda la extensión del teatro de operaciones, habilitando la toma de decisiones en los puntos más cercanos al despliegue de los efectos.

  Cuando la NC opera en el nivel táctico, lo hace junto con la perspectiva del nivel operacional; dispone de información de los objetivos globales de la misión y de la situación táctica de cada sistema, sin importar el ámbito desde donde opere. Esta visión transversal permite ofrecer soporte a la toma de decisiones, identificando desviaciones en el plano táctico con respecto al cumplimiento global de la misión y proponiendo alternativas de manera instantánea como reacción a cualquier amenaza imprevista.

2.3. Arquitectura de la Nube de Combate

La NC puede considerarse como un macrosistema de información construido a partir de la suma de los recursos que integran la Fuerza Conjunta y que asiste de forma personalizada a los diferentes roles de operación que integran la cadena de mando. Trasladado a la arquitectura de la NC, las plataformas, sistemas y personal se traducen en una red de nodos que integran comunicaciones, recursos de computación y servicios de información.

La estructura base de la NC está formada por todos los nodos que se interconectan en una topología de malla. A esta infraestructura se conectan los sensores, efectores, usuarios asociados y, en general, cualquier recurso que pueda aportar o requerir información que pueda impactar a la actuación conjunta de la Fuerza.

2.3.1. Los nodos

Los nodos son el eje de la arquitectura de la nube, proporcionan una infraestructura global de comunicaciones, ejecutan los procesos asociados a las actividades colaborativas y gestionan los recursos técnicos para llevarlas a cabo de manera eficiente.

La configuración de los diferentes tipos de nodos es el resultado de las restricciones SWaP[4] de las plataformas que los integran y de sus requerimientos de movilidad que, al fin y al cabo, son, a su vez, el resultado del ámbito en el que operan y propósito al que sirven:

- *Nodos de alta movilidad*, cuyas plataformas integradoras se encuentran en la zona de operaciones más próxima al enemigo. Estos nodos tendrán mayor número de sensores, efectores y usuarios conectados; en cambio, la capacidad de cómputo será reducida, el tipo de datos que use será más táctico, de validez efímera y consumo rápido.
- *Nodos semi-desplegables*, como pueden ser puestos tácticos avanzados. Dispondrán de mayor capacidad de proceso que los anteriores y tendrán asociados un menor número de sensores y efectores.
- *Nodos fijos*, ubicados en localizaciones estratégicas en entornos seguros (normalmente territorio aliado). Estos nodos, en cambio, tendrán gran capacidad de cálculo y acceso a bases de datos con información de inteligencia permanente.

La NC definirá cuáles son las mínimas características que se requieren para que un componente de la Fuerza pueda ser un nodo de la nube.

Los nodos se conectan y desconectan de la red de manera dinámica según va cambiando el contexto de la misión. Esto supone un reto para la seguridad, puesto que se debe poder hacer de manera ágil. Para lograr ese objetivo es necesario establecer los principios y arquitectura de seguridad desde la fase de concepto donde se empieza a dar forma a la NC.

2.4. Seguridad de la Nube de Combate

La infraestructura de la NC se debe construir bajo unas directrices de seguridad que garantice la ciberresiliencia. Todos los nodos que se conecten a ella deben cumplir con los requisitos de seguridad que se establezcan en ellas.

El dato es el recurso clave de la NC. La seguridad de la nube debe empezar por el propio dato, que además de ser encriptado se debe etiquetar para que permanezca identificado en todo momento y se pueda controlar su uso. La NC es conocedora de los servicios que se van ejecutando en los nodos conectados durante la misión, de los tipos de datos que se van a requerir y a qué nodos pueden ser solicitados (CSA)[5]. Esto permite ajustar las políticas de acceso de los servicios exclusivamente a los datos que necesita, lo que presenta una doble ventaja: por un lado, limita el acceso a la información de

[4] Tamaño, peso y consumo de potencia, del inglés *Size, Weight and Power*.
[5] Conciencia situacional en el espacio Cíber, del inglés *Cyber Situational Awareness*.

un nodo que eventualmente pudiera tener una brecha de seguridad y, por otro, permite detectar comportamientos sospechosos al identificar accesos a datos que no se correspondan con las necesidades de los servicios en curso.

La monitorización de los eventos que suceden en la nube debe ser continua, realizando de esta manera un análisis del comportamiento de los nodos en tiempo real, identificando cualquier situación sospechosa que pueda suponer un riesgo para la red. En el caso de detectarse un nodo infectado, los servicios de seguridad de la nube analizarán el tipo de amenaza y ajustarán las políticas de seguridad de manera global para así protegerse de ese tipo de amenaza y aislar el nodo infectado. La NC debe tener la capacidad de ejercer una seguridad adaptativa en la red que le permita modificar la configuración de seguridad de los nodos y los datos dinámicamente adaptándose al contexto cibernético de la misión en cada momento.

La NC dispondrá de una vigilancia activa que se aplicará a todos los servicios que se ejecuten (*self-protection*)[6]. Sobre cada uno de ellos se aplicará una protección que analizará tanto el comportamiento del servicio como el contexto del comportamiento. Esto incluye garantizar que los accesos al servicio y desde el servicio sean seguros.

La NC reaccionará de manera automática a las alertas sobre anomalías que se detectan sin necesidad de intervención humana, sobre la base de unas políticas y reglas predefinidas, implementando las acciones de corrección necesarias según la amenaza detectada (*self-healing*)[7].

Los servicios de ciberseguridad deben aplicarse sin ralentizar los procesos que se ejecutan en la nube. Esto supone un reto por la cantidad de cómputo que hay que desplegar en tiempo real para mantener la seguridad activa. Una arquitectura de seguridad implementada de forma nativa en la nube facilitará que pueda distribuirse la carga de cómputo entre los distintos nodos y ejecutarla de manera ágil.

2.5. Servicios de la Nube de Combate

La NC proporciona sus capacidades a través de servicios. Los servicios de la nube se pueden clasificar siguiendo las directrices marcadas por la C3 Taxonomy[8], que agrupa los servicios técnicos en tres tipologías: Servicios de Comunicaciones, Servicios *Core* y Servicios COI[9].

---

6 Término técnico de ciberseguridad relativo a la autoprotección de los servicios en ejecución.

7 Término técnico de ciberseguridad relativo a la capacidad de tomar acciones correctivas sin intervención humana.

8 OTAN (2021, septiembre). *Consultation, Command and Control Board*.

9 Del inglés *Community Of Interest*.

2.5.1. Servicios de Comunicaciones y Servicios *Core*

El primer objetivo de la NC es establecer una red de comunicaciones donde tanto las funciones específicas de cada plataforma como aquellas de aplicación/interés común a varias plataformas puedan conectarse e intercambiar información en un entorno seguro. Estas funciones se constituirán como servicios que se encargarán de garantizar que los flujos de información y la ejecución de servicios de C2 se puedan llevar a cabo de manera estable y eficiente. Haciendo referencia a la C3 *Taxonomy* de la OTAN, estos serían los servicios clasificados como Servicios *Core* y Servicios de Comunicaciones.

Sobre los Servicios de Comunicaciones y Servicios *Core* se despliega la capa de Servicios COI, que son los que realmente aportan valor a la actividad de la Fuerza.

2.5.2. Servicios COI

En la actualidad, los enlaces tácticos de datos, como el Link-16, están diseñados para intercambio de datos en crudo, pero no tanto para el intercambio de la información/conocimiento que se genera tras su tratamiento. Que la NC habilite una arquitectura de intercambio de información orientada a servicios significa que, en lugar de intercambiar datos para que cada sistema produzca de forma privativa sus propios productos de información elaborada, se ponga a disposición de terceros la propia capacidad del sistema para producir dicha información.

La definición del formato de la información que se requiere para el servicio se hace a través del contrato de servicios, que termina siendo el estándar de comunicación para intercambiar información relacionada con un determinado servicio.

Esto permite definir servicios para cubrir necesidades concretas de usuario, definiendo libremente los datos e información que se solicitará en cada servicio.

Póngase como ejemplo que se dispone de un radar capaz de hacer *tracking* a una amenaza previamente detectada y se quiere disponer de esa funcionalidad en otras plataformas que no tienen esa capacidad. Se podría acordar un contrato de servicio para trasferir la información de *tracking* generada por el radar que permita exponer su funcionalidad interna diseñada a medida en una funcionalidad potencialmente utilizable por cualquier plataforma de la red. A esa funcionalidad «estandarizada» se le conoce como servicio, y facilitaría que cualquier sistema de la red pueda hacer *tracking radar* de una amenaza sin necesidad de disponer de esa capacidad de manera propia.

Si se dispone de un grupo de plataformas y sistemas de diferentes ámbitos integrados en la NC con diferentes capacidades y todos ellos estandarizan su funcionalidad a través de servicios, sería lo equivalente a tener todas las capacidades en cada una de las plataformas. Si se hace un ejercicio de abstracción, de lo que disponemos es de un sistema de información; no es necesario centrarse en la plataforma, no es necesario centrarse por dominio, nos centramos directamente en el fin, que es la información en sí, no en quién la está generando.

La concatenación de diferentes capacidades granulares dispersas en el ecosistema permite construir dinámicamente nuevas capacidades fruto de la colaboración. Se pueden generar nuevos servicios más complejos que utilicen de manera sincronizada los servicios nativos de las plataformas de la nube.

Estos servicios más complejos, que solamente se pueden disponer en un contexto de sistema de sistemas, generan información más completa y facilita la interdependencia entre diferentes plataformas para habilitar el combate colaborativo. Bien orquestada, la combinación de capacidades y efectores simultáneos desde diferentes ámbitos puede ser un elemento sorpresa difícil de gestionar por el adversario.

Estos Servicios de C2 se pueden solicitar desde cualquier parte de la red, bien directamente por un usuario o bien por otro servicio de más alto nivel. La localización concreta de la ejecución de los servicios es agnóstica del usuario, viene resuelta por los Servicios *Core* de la NC. Se buscará siempre el nodo más apropiado para la ejecución de cada servicio, considerando, además de criterios técnicos, cuál es el contexto de la misión en ese momento.

2.6. Características de la Nube de Combate

Algunas características que ayudan a complementar el concepto de la NC:

- *Hiperconectividad:* todos los nodos deben estar conectados entre sí. Incluso perteneciendo a diferentes ámbitos, se deben comunicar bajo el mismo estándar y deben poder acceder a cualquier servicio disponible en la red. Las comunicaciones serán más ágiles y se eliminarán los cuellos de botella. Debe extenderse a plataformas actuales, futuras y de otros países aliados.
- *Prestaciones dinámicas:* la NC no se limita a un número fijo de nodos, sino que crece y decrece conforme entran y salen plataformas. Cuantos más sistemas conectados, de más capacidades dispone el sistema de sistemas resultante.

- *Ubicuidad:* la información está accesible desde todos los nodos de la nube, debe poder estar donde se requiera habilitar una autoridad militar.
- *Resiliencia*: la NC utilizará la arquitectura distribuida de nodos para hacer asignaciones dinámicas de recursos redundados y, así, garantizar alta disponibilidad de uso incluso en entornos con conectividad limitada.
- *Escalabilidad*: la orientación de la nube a servicios que, una vez estandarizados, pueden ser ejecutados en cualquier plataforma compatible con la NC, permite agilizar la creación de nuevos servicios que puedan ser de interés para los usuarios de la nube.
- *Consistencia y coherencia del dato*: al disponer de toda la información de forma ubicua, se puede fusionar y generar una única fuente de verdad que luego se disemina por todo el teatro de operaciones, de manera que todos los sistemas tengan la misma información y esta esté referenciada de la misma manera, lo que facilitará la coordinación de acciones colaborativas.
- *Adaptabilidad dinámica*: la NC es una arquitectura dinámica que puede cambiar de tamaño, bien porque entren y salgan nodos de la red, o bien porque se divida en varias partes debido a las circunstancias de la misión. La nube tendrá la capacidad de adaptarse y sincronizar sus sistemas conforme se producen los cambios, sin perder la capacidad de gestionar y ejecutar sus servicios.

2.7. Gobernanza de la Nube de Combate

Para mantener el orden dentro de un ecosistema tan complejo, con elementos tan heterogéneos, se necesitan unos principios de arquitectura y operación específicos a los que se acojan todos los nodos que quieren formar parte de la red. Estos principios deben ser especificados previamente a partir de una estrategia definida por el gestor de la nube. Se deberán seguir las directrices en cuanto a seguridad marcadas por las políticas de la nube y se deberá seguir el marco de trabajo que define la NC para el intercambio de Servicios de C2.

La NC, por su parte, proporcionará protección, seguridad y los servicios de infraestructura que garanticen el correcto uso de los recursos técnicos y la adecuada gestión del ciclo de vida de los datos.

3. Principios para la concepción de la Nube de Combate

Este capítulo tiene el objetivo de dar una visión de los aspectos más importantes que hay que tener en cuenta a la hora de desarrollar e implementar la NC. Son tan importantes los aspectos técnicos para tener la capacidad de crear una solución, como los aspectos estratégicos que definan cómo debe ser esa solución.

3.1. La transformación digital como base sobre la que construir la Nube de Combate

Para que la NC pueda operar de manera satisfactoria es necesaria una base técnica y una cultura digital orientada al dato que ahora mismo no se dispone.

3.1.1. Completar el proceso de transformación digital

Es necesario disponer de un cierto nivel de digitalización para poder integrar la NC dentro de una estructura y que esta sea operativa. Lo mismo sucede con las tecnologías disruptivas como la inteligencia artificial o el *big data*. Es contraproducente adoptarlas sin disponer de una base de digitalización adecuada en el seno de la organización que las quiera explotar. Un salto antes de tiempo sin disponer del contexto adecuado para explotar estas tecnologías sería costoso e ineficiente.

El proceso de transformación digital de las Fuerzas Armadas sigue su curso, pero todavía queda mucho camino por recorrer. La tecnología está fragmentada y, en algunos casos, obsoleta; existen carencias tecnológicas críticas y los datos, el elemento más importante de la transformación digital, siguen almacenados de manera desestructurada en silos a los que es difícil acceder de manera global.

3.1.2. Las personas como motor de la transformación

Como se ha explicado en detalle en el capítulo 1, el ritmo en el proceso de TD es lento en organizaciones grandes y segmentadas que arrastran la inercia de modelos de trabajo que llevan décadas implantados. El ritmo no lo marcará la aparición de la tecnología, sino que va a venir marcado por las personas que forman parte de la organización. Cualquier impulso que se le quiera dar al proceso debe ser poniendo a las personas en el foco. Algunas claves:

- *Objetivos claros y transparencia:* estos procesos de cambio pueden ser abrumadores por la velocidad a la que va avanzando la tecnología. Las opciones de digitalización nunca se terminan. A las personas se les deben fijar objetivos concretos a los que se quiere llegar, explicar por qué se necesita alcanzarlos, y qué se necesita cambiar para lograrlos.
- *Objetivos comunes y coherentes*: los objetivos deben estar alineados por todas las FAS y, en aquellos que son transversales como el caso de la NC, deben ser objetivos únicos, y el plan para alcanzarlos a lo largo de la organización debe ser coherente.
- *Participación directa de las personas:* se debe promover la innovación, la creatividad y la diversidad de pensamiento de las personas para

que aporten al proceso de transformación digital. Debe ser un proceso abierto, ágil y flexible que permita involucrar a todos los actores. La creación de grupos multidisciplinares para identificar ideas de uso a partir de necesidades del día a día facilitará el proceso y será aceptado de manera más rápida por todos.

- *La industria como soporte del proceso*: la industria debe apoyar durante todo el proceso a la organización, buscando la manera más sencilla y útil de aterrizar las soluciones tecnológicas al usuario.

3.1.3. El dato en el centro

Uno de los principales objetivos de la TD es evolucionar a un modelo digital centrado en el dato. El objetivo es pasar de un proceso de intercambio de datos farragoso, lento y difícil de explotar a un modelo en el que todos los datos son accesibles y se pueden usar para lo que se necesita, dónde se necesita y cuándo se necesita.

Esta necesidad estratégica es el eje central de la política CIS/TIC, cuya finalidad se define para «proporcionar al Ministerio de Defensa un conjunto de directrices comunes globales y únicas que, basadas en los principios de la propia política, permitan que la información, por su carácter estratégico, sea fiable y accesible con la debida protección, en todo momento y lugar, para cualquier usuario que la precise, conforme a su perfil autorizado, y a los requisitos de dicha información».[10] Esto implica un cambio de paradigma que afecta de manera esencial a todos los procesos de las FAS.

Para evolucionar a este nuevo modelo que permita poner la información en el centro de los procesos de las FAS, es necesario desarrollar cuatro aspectos fundamentales para potenciar el uso de los datos:

- *Propósito y clasificación de los datos*: todos los datos que se almacenen deben tener un propósito. Se recogen muchos datos y no todos tiene valor o se deben agrupar con otros datos para que lo tengan. Es necesario conocer qué tipos de datos se necesitan explotar y etiquetarlos según el uso que se les vaya a dar.
- *Estandarización de los datos*: todos los datos de la nube deberán estar disponibles para ser explotados por las herramientas o servicios de cualquier sistema conectado a la nube. Implica definir estándares para que la compatibilidad sea global. Estos estándares se aplicarán tanto a los datos como a los metadatos, y serán definidos por la organización responsable de las FAS, considerando requisitos técnicos e industriales.

[10] Ministerio de Defensa. (2017). *Política de los Sistemas y Tecnologías de la Información y las Comunicaciones*. Marzo.

- *Accesibilidad a los datos*: los datos deben ser accesibles de manera ágil desde cualquier lugar desde donde se necesiten. Esto implica disponer de una infraestructura de comunicaciones que proporcione conectividad a todos los sistemas de la nube. Todos los datos guardados deben estar correctamente indexados para que puedan ser localizados por los servicios que los necesiten.
- *Seguridad de los datos*: una de las claves en la especificación de los datos es hacerlos seguros desde el diseño. No debe suponer ningún riesgo sacar los datos de los silos actuales para abrirlos a la nube.

Es necesario elaborar una estrategia sobre los datos transversal a toda la organización de las FAS, que parta de un análisis de los datos que se van a necesitar y cómo se van a explotar en el futuro; que genere un catálogo con todos los datos donde se describa cómo es el dato, dónde está guardado o quién lo ha generado; que defina y establezca un marco de gobierno para gestionarlos y controlarlos; que establezca estándares para garantizar la consistencia entre los datos y las herramientas que los explotan y que asegure que se obtiene el mayor beneficio de ellos.

Existen dos actuaciones generadas desde el Plan del Ministerio de Defensa para la Transformación Digital, que materializan la necesidad de poner el dato en el centro:

- «Crear una Plataforma para la Gestión y el Gobierno de los Datos Maestros del MDEF[11]».
- «Identificar los Datos Maestros del MDEF y crear un Catálogo de Datos Maestros[12]».

Estas actuaciones son necesarias para poder implementar la NC. Se debe impulsar utilizando como motor lo que se quiere conseguir y para qué, incluyendo en el proceso a las personas que van a explotar los datos para cubrir las necesidades operacionales requeridas en cada caso.

3.1.4. La inversión necesaria para la transformación digital

Todos los procesos de transformación necesitan de una inversión consistente y sostenida. Si las intenciones se sostienen con recursos (y se dispone de una estrategia correctamente elaborada), se llegará a resultados que permitan a las FAS estar en una posición donde poder implementar las nuevas tecnologías que están llamadas a cambiar la manera de afrontar los conflictos.

[11] Ministerio de Defensa. (2020, julio). *Plan del Ministerio de Defensa para la Transformación Digital*, p. 115.
[12] *Ibidem*, p. 117.

La inversión debe ser inteligente, se debe aprovechar la ventaja de afrontar estos cambios en un momento en el que ya han sido ejecutados por muchas organizaciones y existen multitud de herramientas para allanar el camino. Se deben aprovechar los desarrollos técnicos que ya llevan tiempo implementados con éxito en el ámbito civil.

Las FAS y la industria nacional deben estar sincronizados en este proceso y mantener una hoja de ruta común a largo plazo para garantizar la consistencia de las soluciones que se van dando en cada paso. Se debe identificar dónde están los *gaps* tecnológicos y realizar las inversiones oportunas para reforzar el tejido empresarial en tecnologías estratégicas para la Defensa y para otros sectores.

Se debe aspirar a tener un control nacional de las infraestructuras críticas de Defensa que van a sostener nuestra arquitectura de nube. El propósito es tener soberanía nacional y control en la aplicación de las tecnologías clave. En el contexto de la NC se incluyen: la computación en la nube, las tecnologías de comunicaciones, las nuevas tecnologías de explotación de datos como *big data* o la IA y, por supuesto, todas las aplicaciones relacionadas con la ciberseguridad.

La inversión en España en TD (tecnologías de la información, capacidades digitales, infraestructura y ciber seguridad) durante el año 2022 fue del 0,4 % del presupuesto destinado a Defensa, por detrás de otras naciones como Reino Unido (8,3 %), Francia (6,8 %) o Alemania (2, 6%), datos extraídos del International Institute for Strategic Studies (IISS).

Son números modestos teniendo en cuenta la importancia de la TD para las FAS. Teniendo en cuenta, además, que la inversión en este apartado tiene un impacto muy positivo en la industria nacional, mejorando sus capacidades, impulsando la innovación y el talento, generando empleo de calidad y creando productos tecnológicos de gran demanda internacional. Todo esto a la vez que se avanza hacia la autonomía estratégica nacional.

En términos puramente económicos hay que resaltar que el retorno de inversión para el Estado es ampliamente positivo. Existen estudios que concluyen que el conjunto de actividades relacionas con la Defensa presenta un efecto multiplicador de retorno económico por el que, por cada euro invertido, se generan de media 2,5 euros.[13]

3.2. Constitución de la Nube de Combate

El objetivo de la NC es crear un marco único de colaboración donde todos los sistemas puedan conectarse formando un sistema de información distribuido.

[13] Según un estudio realizado por la consultora Kearny a partir de datos publicados en los *Cuadernos de Política Industrial de la Defensa*.

Esto se consigue a través de la creación de una infraestructura común donde todas las plataformas puedan operar entre ellas hablando el mismo lenguaje, y de unos Servicios de C2 que den soporte a la toma de decisiones y permitan desplegar las capacidades colaborativas.

En este capítulo se escribe sobre las consideraciones más importantes que hay que tener en cuenta para la fase de diseño y desarrollo de la NC.

3.2.1. Complejidad de la NC en comparación con las nubes civiles

Implementar una NC conlleva importantes retos en comparación con lo que supone implementar una nube convencional, debido a que estas nubes civiles se instalan sobre entornos controlados donde:

- Los nodos son estáticos y están alojados en instalaciones seguras.
- Disponen de capacidad de cómputo escalable, sin limitación de capacidad de procesamiento.
- Las comunicaciones son estables, con velocidades de trasmisión de datos elevadas y predecibles.
- Los equipos y sistemas de comunicación son estándares.

Una NC tiene características que precisarán de soluciones innovadoras en campos como las comunicaciones o la computación. Entre sus características principales destacan las siguientes:

- Nodos desplegados en entornos tácticos hostiles, algunos de ellos con mucha movilidad, con ataques directos tanto al medio físico como el cíber.
- Capacidades de cómputo limitadas a las restricciones de SWaP de las plataformas.
- Las comunicaciones son inestables, no siempre disponibles entre todos los nodos, con diferentes velocidades de trasmisión en función del contexto (en muchas ocasiones muy reducidas).
- Se mezclan diferentes tecnologías de comunicaciones y sistemas de información, dependiendo del tipo de dominio y de la plataforma.

3.2.2. La necesidad de definir estándares antes de acometer el diseño de la NC

En las nubes instaladas en entornos controlados es más sencillo establecer una normativa de diseño común y crear una infraestructura de red con un modelo predefinido. En el caso de la NC la infraestructura global es heterogénea y estará formada por nubes con diferentes características, por lo que es más complejo adoptar un modelo ya preestablecido por la industria.

Se necesita algo más específico que dé solución a las diferentes configuraciones posibles de las NC.

Para garantizar la interoperabilidad dentro de cada NC y entre las diferentes NC es necesario fijar estándares de comunicación que garanticen la conectividad y estándares de diseño de servicios para permitir el intercambio de información. Estos estándares definirán cómo debe ser la gobernanza de la red, la gestión de políticas y los recursos, los accesos a los servicios, los requisitos para entrar en la red, etc.

Si no se establece este marco común de diseño y desarrollo, las nubes que se vayan gestando desde los diferentes ámbitos de las FAS se irán creando con sus propios estándares, sin la posibilidad de interoperar de manera efectiva con otras nubes. Todo esto haría inviable el proyecto de NC nacional multidominio.

No es necesario crear nuevos estándares, las tecnologías de la nube llevan tiempo desarrolladas y ya existen estándares consolidados que se pueden fijar como marco de referencia. Un buen ejemplo, que se empieza a usar como referencia en los grupos NIAG[14], es el NIST.SP.500-332[15] que propone un estándar de referencia para nubes federadas (o «nube de nubes»).

Una vez que tenemos los estándares definidos para usarlos como marco de referencia, se puede comenzar el diseño de la NC. Se identifican dos fases en el proceso de constitución de la NC: una primera fase de diseño y desarrollo y una segunda fase de implementación.

3.2.3. La infraestructura de la NC

Dos retos técnicos importantes que tiene que afrontar la NC son:

- Proporcionar una capa de servicios que permita abstraerse del problema que supone una nube desplegada en un contexto táctico hostil con las características que se exponían el apartado 3.2.2; y
- Crear un entorno eficiente para la computación de los Servicios de C2 y la distribución de la información.

La infraestructura de la NC será la encargada de proporcionar la solución específica que se necesita para cubrir estos dos retos.

Por tanto, el objetivo principal de la infraestructura de la NC es proporcionar una capa que gestione las comunicaciones y que provea de los servicios que permitan una correcta ejecución de las funciones colaborativas en

[14] Del inglés *NATO Industrial Advisory Group*.
[15] Del National Institute of Standards and Technology.

la NC, todo ello garantizando la seguridad de la información a la que le va a dar soporte.

Estos servicios, que en la C3 *Taxonomy* de la OTAN se les conoce como Servicios de Comunicación y Servicios *Core*, constituyen la infraestructura de cada nube. Cada NC de cada sistema de armas o dominio tendrá sus servicios de infraestructura adaptados a las condiciones de la capa física y al entorno táctico de cada uno. Al estar desarrollados bajo los mismos estándares, tendrán un lenguaje común que les permitirá interoperar.

Los servicios de infraestructura son técnicos, y para desarrollarlos no es necesario disponer de los Servicios de C2 ni de las capacidades operacionales a implementar. Esto permite desacoplar esta fase de la necesidad de disponer de los requisitos operacionales de la NC.

3.2.4. Servicios de Mando y Control

Estos servicios son los que aportan valor a la misión proporcionando información para la toma de decisiones y la orquestación del combate colaborativo. Se desarrollan a partir de una necesidad operacional y podrán ser utilizados por todos los sistemas conectados a la NC. Los servicios de la NC se van creando y van evolucionando constantemente al ritmo que van apareciendo nuevas necesidades operacionales.

Estos servicios hacen uso de la capa de infraestructura como base sobre la que se ejecutan, abstrayéndose de la gestión de su ejecución.

Se deben definir para un uso estandarizado cuáles son las interfaces de uso para cada servicio, los «contratos de servicio», para permitir así su empleo por todos los sistemas conectados a la NC. Todos los servicios desarrollados, que sigan los estándares definidos por la NC y que dispongan de un contrato de servicios acordado para uso común, pasarán a formar parte de un catálogo de servicios colaborativos de la NC.

3.2.5. La importancia de disponer de capacidades de análisis operacional y de CD&E[16]

Seleccionar la solución técnica más adecuada en la que materializar la NC requiere de un análisis complejo donde valorar diferentes conceptos técnicos y operacionales.

Para poder realizar este análisis las FAS se deben de dotar de capacidades de análisis operacional para escenarios multidominio y de un entorno de desarrollo de conceptos y experimentación (CD&E).

[16] Del inglés *Concept Development and Experimentation*.

Los servicios de la nube dan soporte directo al C2 por lo que su desarrollo va a estar muy ligado a los conceptos operacionales que se decidan desplegar[17]. Durante el proceso de experimentación sobre las posibles soluciones se deben considerar al mismo tiempo conceptos técnicos y conceptos operacionales, buscando la mejor solución dentro de ese binomio[18].

Las FAS se deben dotar de un espacio de desarrollo que disponga de laboratorios y equipos con los que poder experimentar diferentes conceptos bajo distintos contextos tácticos y donde poder valorar parámetros técnicos de cada desarrollo, como pueden ser: las velocidades de trasmisión en diferentes entornos, la protección frente a ataques cibernéticos, las latencias y tiempos de ejecución, la estabilidad y resiliencia de la nube, el correcto desempeño y la calidad adecuada de los Servicios de C2, etc.

Además de los laboratorios de desarrollo y medios para la experimentación, para poder disponer de las capacidades de análisis operacional y CD&E se necesita un equipo multidisciplinar con formación y amplia experiencia en ámbitos como: el operacional, el de las tecnologías de la información, el de ciberseguridad, el de desarrollo del *software* y *hardware*, etc.

Esta necesidad está recogida en la *Estrategia de explotación de la nube en el Ministerio de Defensa*[19], donde se anuncia la «constitución de un grupo de trabajo permanente para la implantación y empleo de la tecnología de nube en el seno de la estructura de Gobierno de los CIS/TIC del Ministerio, y dependiente del Comité de Sistemas de Información del MDEF[20]». Este equipo de trabajo debe incluir expertos de la industria, que estén en todo momento dando soporte para encontrar la solución que mejor cubra las necesidades, y sea técnicamente viable implementar en las plataformas, desde donde se va a desplegar.

3.2.6. La importancia de disponer de un entorno de pruebas y validación

La solución madurada en un entorno de CD&E se debe implementar en un laboratorio de pruebas con sistemas y equipos que reproduzcan el comportamiento de la NC de la manera más fidedigna posible. Este despliegue hay que acompañarlo de los medios y herramientas para poder reproducir escenarios tácticos reales. El objetivo es construir un entorno de validación y pruebas a partir de la solución de NC madurada en la fase de desarrollo de concepto.

---

17 Esto nos viene a marcar la necesidad de involucrar a personal de las FAS con experiencia en análisis operacional en la especificación y desarrollos de los servicios.

18 Industria y FAS deben colaborar estrechamente en estos procesos.

19 España. (2021). Número 103 resolución de mayo de 2021 de la Estructura de Gobierno de la Estrategia de Explotación de la Nube. *Boletín Oficial del Estado*.

20 Ministerio de Defensa (2021). *Estructura de Gobierno de la Estrategia de Explotación de la Nube*. Capítulo 24. Madrid, Ministerio de Defensa.

La NC está en permanente desarrollo, aparecerán continuamente nuevas necesidades que habrá que cubrir a través de la implementación de nuevos servicios. Un entorno de validación y pruebas agilizará el desarrollo y la implementación de estos servicios, proporcionando:

- Un entorno confiable y seguro donde validar y medir la efectividad de los desarrollos.
- Una NC consolidada donde se puedan hacer pruebas de integración con otros sistemas y plataformas para garantizar que cumplen los estándares de interoperabilidad con la NC.

Con este espacio de pruebas y validación, y con un equipo formado por la industria y expertos de las FAS, se dan las circunstancias para aplicar la metodología DevSecOps[21] que busca combinar desarrollo de servicios, seguridad y enfoque operacional. En la *Estrategia de explotación de la nube en el Ministerio de Defensa* se refleja esta misma necesidad, confirmando que, «se adquirirá una plataforma para permitir el desarrollo y prueba (DevTest - DevSecOps) de *software* en la nube.»[22] Esta filosofía permite que los desarrollos sean más efectivos al tener expertos de las tres ramas en el mismo equipo. Si además se disponen de entornos de desarrollo, validación y pruebas que replican escenarios reales, se dibuja el contexto perfecto para pasar de la necesidad a la solución en un reducido espacio de tiempo.

Se obtendrá un resultado más consistente y de manera más eficiente si se centralizan todos los medios y equipos relativos al despliegue de estas capacidades de análisis operacional, CD&E y validación y pruebas. Se generará así un equipo y espacio únicos donde se aborden los desarrollos de todas las iniciativas de NC para los diferentes ámbitos y sistemas de armas.

3.3. Implementación de la Nube de Combate

Una vez la tecnología de la nube y los servicios que la conforman se han desarrollado y validado en un entorno controlado, se está en disposición de implementar la solución en las plataformas que una vez desplegadas conformarán la NC.

3.3.1. Constituyendo la NC: conectando los nodos

La NC es una red de nodos colaborativos que se comporta como una infraestructura de supercomputación. Técnicamente, un nodo de una NC

[21] Del inglés *Developement, Security and Operations.*

[22] Ministerio de Defensa (2021). Modelo de desarrollo de la Nube. *Estructura de Gobierno de la Estrategia de Explotación de la Nube*. Capítulo 19. Madrid, Ministerio de Defensa.

es un servidor con capacidad para ejecutar procesos por sí solo y diseñado para trabajar en colaboración con otros nodos a través de una red de comunicaciones. Cuando el nodo se integra en una plataforma, este puede explotar las funcionalidades, recursos e información que la plataforma federa hacia la nube a través de los servicios estandarizados que se hayan decidido implementar.

La manera de constituir NC es conectando nodos; estos tendrán diferentes características en función el tipo de plataforma en el que estén integrados. La ambición es generar NC con el mayor número de nodos, a mayor número de nodos más capacidades se disponen en la NC.

Para las nuevas plataformas y sistemas de armas que se adquieran, se tendrán que considerar los estándares de compatibilidad con la NC desde el principio, pero para tener realmente una NC operativa en el medio plazo es necesario adaptar una parte importante de las plataformas actuales que componen las FAS, con el objetivo de que sean compatibles con los estándares de interoperabilidad de la NC.

En función de las capacidades que deba ir desplegando la NC durante su ciclo de desarrollo, se irán priorizando las plataformas que se deben modernizar primero y los servicios de C2 que se necesitan para explotarlas.

3.3.2. Adaptación de las plataformas actuales hacia la compatibilidad con la NC

Para que una plataforma se pueda conectar a la NC, debe disponer de: un sistema de comunicación compatible con la NC, un espacio de computación para procesar los servicios de la NC y el acceso a los datos e información compartidos desde la plataforma.

Estas modificaciones se adaptarán a las condiciones de SWaP de cada plataforma y serán más o menos complejas en función de las restricciones que estas impongan. La adaptación de las plataformas a la NC no debe afectar ni a su funcionamiento ni a sus capacidades originales.

Una manera de facilitar el proceso de implementación es identificando los cambios necesarios para adaptar las plataformas antes de que se termine de dar forma a las soluciones de la NC, de esta manera se podrán considerar durante la fase de desarrollo y facilitar así su integración posterior en la plataforma. Esto permite incluso plantear el diseño de equipos que integren la solución completa: las comunicaciones, el *hardware* de proceso y los interfaces con la plataforma, simplificando la integración a prácticamente un *Plug and Play*.

3.3.3. Conectando NC bajo los mismos estándares: la NC Federada

El concepto de NC se utiliza con dos acepciones, para referirse a una NC formada por los nodos de un sistema de armas o de un dominio concreto, y para referirse de manera genérica a la NC resultante de sumar todas las NC compatibles en una única NC, una nube de nubes. El término más preciso para este último caso es el de NC Federada, que es el nombre técnico que se utiliza cuando diversas nubes bajo los mismos estándares se conectan para formar una única NC que se gestiona y gobierna de manera única.

La NC se circunscribe únicamente al ámbito de las operaciones, pero se debe considerar la conexión con otras nubes de la infraestructura nacional para buscar sinergias entre ellas. En un entorno donde todo está digitalizado, todos los datos quedarán accesibles a aquellos que tengan acceso a la red. Integrar la NC dentro de estas infraestructuras de nubes multiplicaría el intercambio de información y la prestación de capacidades.

En la *Estrategia de explotación de la nube en el Ministerio de Defensa* se proyecta la conexión de la NC con la Infraestructura Integral de la Información para la Defensa (I3D)[23]. Esta conexión se describe a través de un Nodo de Interconexión (NI) de Clase-I,[24] permitiendo el acceso a usuarios de una red y otra. Eso es equivalente a conectar el frente de batalla a todos los recursos de datos e información guardados en las redes de Defensa y viceversa, y, por otro lado, llevar los datos del campo de batalla a los sistemas de información de la infraestructura de Defensa. Las capacidades potenciales de esta conectividad son prometedoras.

[23] «Infraestructura Integral de Información para la Defensa (I3D): Infraestructura tecnológica, bajo una autoridad operativa única, que mediante la convergencia de los sistemas de información y telecomunicaciones y los servicios que estos proporcionan, optimice el uso de los mismos y facilite a los organismos y usuarios el acceso eficaz a los recursos de información de la Defensa, desde cualquiera que sea su situación geográfica o dinámica (fija, estacionaria o en movimiento), y en todo momento, de forma segura. De esta I3D forman parte los CIS permanentes y en ella se integran los CIS desplegables, para asegurar su continuidad en los entornos estratégico, operacional y táctico.» Definición incluida en el documento de Política de los Sistemas y Tecnologías de la Información y las Comunicaciones ya referenciado en el capítulo 3.1.3.

[24] «Proporcionarán la conexión e integración de los medios CIS/TIC desplegables con los medios CIS/TIC permanentes. Permitirán el acceso de usuarios y redes desplegables a los Servicios CIS/TIC proporcionados por la I3D, mediante diversidad de medios de telecomunicaciones que se integrarán a través de puntos de interconexión de redes, conforme a la normativa técnica de interoperabilidad, conexión y seguridad de la información».

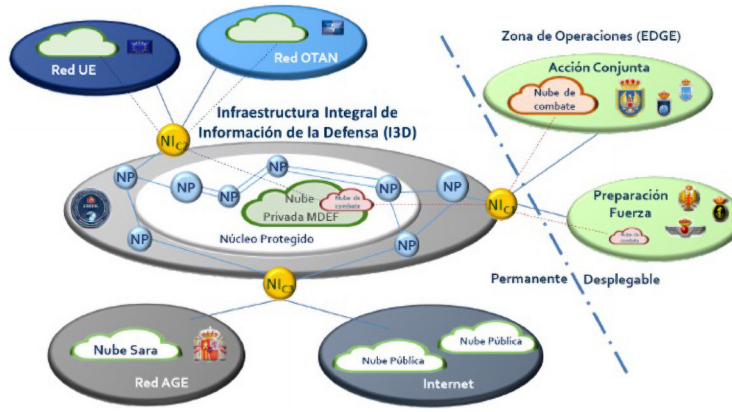


Figura 1.- Ideograma de la evolución de la I3D al concepto de NC25. Fuente: Estrategia de explotación de la nube en el Ministerio de Defensa

En la arquitectura de nubes de la ilustración superior (véase figura 1), la NC no solo tiene presencia en la zona de operaciones, también dispondrá de recursos orientados al combate o a su preparación en servidores instalados en instalaciones de Defensa dentro de la I3D.

Es importante destacar que la NC no solo se despliega en plataformas móviles de combate, también dispondrá de nodos fijos, algunos desplegados y otros en instalaciones permanentes. El rol de estos podrá ser de apoyo a la ejecución de la misión, pero también de preparación de la misión o de análisis posterior a la misión. La NC no solo opera en la fase de ejecución del enfrentamiento. Para disponer de un sistema de información refinado y que dé soporte a la preparación de la misión o a la toma de decisiones durante la ejecución de manera adecuada, se requiere de un constante entrenamiento, simulación y análisis de los escenarios de operaciones pasados y de los que se pueden presentar en el futuro[26].

La conectividad de la NC debe ir más allá de la infraestructura de red nacional, debe extenderse a NC aliadas para potenciar más la explotación de capacidades en torno al intercambio de información entre NC. En el caso de la OTAN, se están creando NC bajo la iniciativa de las Redes de Misión Federadas (FNM[27]). Estas NC siguen estándares adoptados por la OTAN que sería interesante contemplar para la NC nacional.

25 La figura plasma la «Estructura de Gobierno de la Estrategia de Explotación de la Nube».

26 Que las capacidades que ofrezca la nube durante el enfrentamiento sean las precisas en cada momento dependerá de lo bien preparada que previamente haya estado la nube. Este entrenamiento, que en esencia consiste en sacar el mayor partido en cada momento a los datos disponibles, requiere de horas de simulación, supervisión e interacción con la nube de operadores expertos y analistas operacionales.

27 Del inglés *Federated Mission Network*.

3.3.4. Conectividad fuera del estándar de la NC

No todas las nubes a las que se debe conectar la NC tendrán los mismos estándares. En estos casos los nodos de ambas nubes no podrán interoperar libremente y se necesitará hacer uso de pasarelas de datos para conectar una nube con otra. Estas pasarelas traducen los mensajes de un protocolo a otro, permitiendo el intercambio de información. Se definirán puntos de acceso entre NC por donde todos los nodos de una NC accederán a la información proporcionada por otra NC, en la práctica esto creará cuellos de botella que deberán ser considerados a la hora de definir el tipo de información y servicios que se intercambian entre las nubes.

La NC también deberá conectarse a enlaces de datos tácticos con protocolos ajenos a la NC para poder integrarse en la infraestructura de C2. Esto requerirá de la conversión de los protocolos tácticos fuertemente estructurados como el Link-16 a un esquema de información más abierto basado en el protocolo IP[28] que permita tener un contexto donde puedan intercambiarse datos e información.

Es importante determinar las nubes y protocolos tácticos de C2 en los que la NC se tendrá que integrar para ir identificando los requisitos de conectividad necesarios.

3.4. Cambio de paradigma en la concepción de la Fuerza

La NC tendrá un impacto en muchos ámbitos de las FAS: se requerirán cambios en los procesos, los recursos humanos, la organización y el sostenimiento.

Las MDO irán ganando más protagonismo y el mando conjunto a través de la NC irá cogiendo más importancia en el planeamiento y ejecución de las misiones.

La doctrina deberá considerar las ventajas que trae la NC y diseñar las reglas y procedimientos que las utilicen. La distribución de la información en todo el frente de batalla va a abrir nuevas posibilidades de delegación de autoridad que hay que resolver junto con los aspectos legales y éticos debidos al uso de la IA y los sistemas autónomos.

Este capítulo se centra solamente en el cambio referente a la concepción de la fuerza, de cómo se debe desplazar el foco de la adquisición de material de las capacidades de una plataforma a las capacidades colaborativas del global de la Fuerza.

[28] Protocolo de Internet es el lenguaje que se está adoptando dentro de la OTAN para los desarrollos de las nubes.

3.4.1. La Voluntad es la clave del cambio de planteamiento

Para alcanzar las capacidades multidominio que se articulan a través de la NC, es necesario que los sistemas y plataformas de las FAS potencien sus recursos de interoperabilidad para impulsar el combate colaborativo.

El paradigma actual de la Fuerza está lejos de ese objetivo. Las plataformas que forman las FAS están principalmente orientadas a desplegar sus capacidades de manera individual en los entornos tácticos. La información colectiva pasa a un segundo plano, cada plataforma trabaja principalmente con la información que tiene a su alcance. Dos plataformas diferentes pueden estar en un mismo enfrentamiento y cada una utilizando su propia información táctica con un formato compatible solo con su funcionalidad interna. La capacidad de interoperabilidad es limitada, dificultando así la cooperación táctica durante el enfrentamiento.

Es necesaria la implicación y determinación de las FAS para redirigir este planteamiento hacia un nuevo paradigma de conectividad y estandarización de la información que marque el camino de hacia dónde tienen que evolucionar los sistemas actuales y que garantice que las nuevas adquisiciones sean compatibles con este concepto de colaboración.

3.4.2. Adquisición de material orientado a la interoperabilidad

La manera de garantizar la compatibilidad de los nuevos sistemas con la NC es a través de requisitos. Los sistemas o plataformas que se adquieren se deben concebir para integrarse en ella y hacerlo a través del cumplimiento de requisitos específicos que garanticen la interoperabilidad entre todos los sistemas conectados. Todo ello sin limitar en ningún momento las capacidades individuales de cada plataforma o sistema para el que va a ser adquirido. Cada plataforma debe de poder cumplir su rol específico, aunque no esté conectada a la NC.

Estos requisitos se enfocarán en fijar una serie de estándares, interfaces y protocolos para permitir el intercambio de información y la ejecución de funciones colaborativas del sistema de sistemas sobre las plataformas. La colaboración pasa así a ser un requisito en lugar de una oportunidad.

Un enfoque más colaborativo a la hora de concebir las plataformas permite un cambio en su especificación, esta normalmente concibe sus sistemas centrados en la propia plataforma, en la explotación de la información que se generan de manera interna. En un modelo donde se potencien las actividades colaborativas, es posible delegar funcionalidades a otras plataformas para que no se tenga que disponer de toda la funcionalidad de manera interna dentro de la misma plataforma.

Como resultado tendremos sistemas más especializados, potenciando sus capacidades principales y más sencillas al reducir la necesidad de

implementar e integrar funciones que pasan a estar delegadas a la NC. Esto impacta positivamente en los plazos de ejecución de los contratos de adquisición e implica una reducción de costes al no generar excesivas duplicidades funcionales entre sistemas.

Además, este enfoque proporciona cierta soberanía a la hora de definir las capacidades de la Fuerza, estas estarán por encima de lo que cada plataforma puede ofrecer. Las plataformas pasan a convertirse en instrumentos que permiten explotar nuevos servicios colaborativos para generar capacidades exclusivas a medida de las necesidades de las FAS españolas. Tampoco será posible por parte del adversario tener la certeza de cuáles son esas capacidades, aun conociendo las unidades implicadas en cada enfrentamiento.

3.5. ¿Qué Nube de Combate se necesita? Plan estratégico y hoja de ruta

Es el último capítulo, pero debe ser lo primero a resolver. Antes de empezar a invertir en los medios se debe tener claro para qué se necesitan.

3.5.1. La Nube de Combate es un medio

La NC no es un fin, es un medio que habilitará a las FAS para potenciar sus capacidades colaborativas. No se trata, por tanto, de disponer de una NC, se trata de disponer de la NC que se necesita.

Actualmente la tecnología de vanguardia va por delante de la que está disponible para el empleo operativo en las FAS, la tendencia es incorporarla de manera rápida para tratar de sacar alguna ventaja operacional sobre el adversario lo antes posible. Puede ser contraproducente dar este paso sin tener claro para qué y cómo usarla y si se está en disposición de asimilarla adecuadamente. Son las necesidades operacionales las que deben dirigir la aplicación de la tecnología y no al revés.

3.5.2. Plan estratégico nacional para acometer MDO

Esto requiere de la elaboración de un plan estratégico que sea el punto de partida que gobierne y guíe los cambios necesarios para afrontar el reto que suponen las MDO.

Se deben analizar las necesidades nacionales a medio plazo, considerando las amenazas que se puedan proyectar en este periodo. El enfoque del análisis debe ser multidominio y realizado de manera conjunta por los Ejércitos y la Armada. En él se considerará especialmente el uso colaborativo de la Fuerza Conjunta para el combate.

El resultado debe ser la identificación de las capacidades estratégicas necesarias[29] y una voluntad clara de desarrollarlas de manera conjunta. A partir de este punto se podrán identificar las necesidades no cubiertas asociadas a estas capacidades, qué cambios se requieren y cómo afectarán al conjunto de factores MIRADO[30].

3.5.3. Generar la hoja de ruta

Una vez que se dispone del plan estratégico con la definición de las capacidades multidominio a desplegar a medio plazo, se puede comenzar el análisis de cómo se van a conseguir[31] y de las actuaciones que se pueden acometer en este plazo.

Este análisis describirá el uso de las Fuerza Conjunta en el enfrentamiento y cómo será el combate colaborativo para neutralizar las amenazas futuras. Esto permitirá concretar el concepto operacional[32] que se requiere en los escenarios multidominio.

Una vez se dispone de la estrategia y de cómo se va a ejecutar, se puede definir una hoja de ruta con objetivos intermedios que vayan estableciendo en el tiempo las capacidades que se van a necesitar. Este plan ayudará a priorizar las actividades desde todos los ámbitos de las FAS.

Para la elaboración completa de este análisis será necesario un equipo multidisciplinar que pueda analizar las alternativas desde diferentes prismas: operacional, tecnológico, organizativo, doctrinal, etc. La industria tendrá que acompañar a las FAS durante todo el proceso en un trabajo colaborativo ofreciendo herramientas, dando alternativas y aportando soluciones.

Particularizado para el caso de la NC, este plan estratégico con su hoja de ruta permitirá:

- Fijar el objetivo final, identificar cuáles son las capacidades colaborativas de la NC que se tendrán que desplegar.
- Disponer cómo se usará la fuerza en el combate multidominio, y cómo será el combate colaborativo.
- Conocer la composición del sistema de sistemas, qué plataformas y sistemas actuales deberán modernizarse para formar parte de la NC y qué

29 Alineadas por todas las partes: Ejércitos y Armada.
30 Material, Infraestructura asociada, Recursos Humanos necesarios, Adiestramiento necesario, Elaboración de la Doctrina de uso y Organización.
31 Teniendo en cuenta lo que se dispone en las FAS en el momento del análisis.
32 Se elaborará haciendo uso de la fuerza que se proyecta tener en los tiempos donde se requieren las capacidades.

sistemas se deberán adquirir. Saber cuándo se necesitan y con qué funcionalidad operativa.

- Disponer de un calendario con capacidades-objetivo trazadas a los sistemas y plataformas que se utilizarán para desplegarlas.

Este análisis irá evolucionando con el tiempo, pero con esta información se pueden iniciar las actividades relacionadas con la NC. Se dispondrá de una referencia para:

- Definir el concepto de uso de la NC.
- Definir el diseño más adecuado para las necesidades planteadas.
- Definir los Servicios de C2 que se necesitarán y cuándo.
- Identificar las acciones de modernización que se requieran para hacer compatibles los sistemas actuales con la NC.
- Priorizar actividades en función de las necesidades marcadas por la hoja de ruta.
- Desarrollar la doctrina que se adapte al combate multidominio colaborativo.
- Preparar y organizar a las FAS para que puedan operar con éxito con la NC.

Disponer de una estrategia y una hoja de ruta es clave para lograr los objetivos y hacer un uso eficiente de los recursos.

Los cambios se van a tener que producir, va a ser necesario adaptarse a los nuevos enfrentamientos multidominio. No disponer de un plan estratégico detallado obligará a avanzar de manera improvisada y esto normalmente conlleva un coste muy elevado.

La tarea de generar un plan tan detallado de lo que se va a necesitar y lo que hay que hacer por el camino es enorme, y requiere de la implicación de personal con experiencia, que normalmente está más centrado en solucionar los problemas del corto plazo.

Los programas de adquisición y planes de modernización y transformación de la Defensa disponen de presupuestos muy elevados; merece la pena invertir en potenciar los equipos que se centran en planificar cuál debe ser el futuro de las FAS.

4. Conclusiones

Es una realidad que los enfrentamientos se hacen utilizando los medios disponibles desde cada ámbito y que no es posible tener éxito en la batalla si

solo se opera desde uno de ellos. Los avances tecnológicos[33] están potenciando esta tendencia, provocando que cada vez la interacción entre ámbitos sea más estrecha y ágil.

La complejidad de estos escenarios dificulta la toma de decisiones. La superioridad de la información se presenta como el factor clave para sacar ventaja sobre el adversario, como consecuencia el resultado de los enfrentamientos estará cada vez más determinado por el bando que mejor preparado esté para generar y distribuir la información.

La NC ofrece una solución que posibilita potenciar la colaboración y el intercambio de información. Permite conectar los sensores de cualquier ámbito de operación con los efectores de diferentes ámbitos a través de propuestas para la toma de decisiones.[34]

Se han identificado algunas consideraciones necesarias para poder implementar la NC:

- Para poder explotar las capacidades de la NC se necesita una infraestructura digital de Defensa accesible que esté construida alrededor de los datos y la información.
- Se necesitan estándares para el desarrollo de la NC y definir las necesidades de conectividad con otras nubes y estructuras de C2.
- Las FAS[35] necesitarán dotarse de capacidades de análisis operacional y CD&E para aterrizar el concepto de la NC a la solución que mejor se adapte a las necesidades de las FAS.
- Se deben adaptar las plataformas y sistemas de la Fuerza para que cumplan los estándares y requisitos para operar dentro de la NC.

La NC representa un pequeño cambio dentro del proceso de transformación que necesitan las FAS para poder llevar a cabo, con ventaja sobre el adversario, las MDO. Algunas de las claves para poder llevar a cabo este proceso son:

- Voluntad: orientar la Defensa a las MDO implica un cambio en la manera tradicional de operar de las FAS. Se necesita una voluntad extraordinaria para vencer la inercia en la manera de pensar y concebir las operaciones.
- Elaborar un Plan Estratégico: de importancia capital, todas las actuaciones que se pongan en marcha deben ir trazadas a la hoja de ruta del plan

33 Los avances en torno a la IA van a tener un impacto considerable.
34 Estas propuestas se generan en el momento adecuado y en el lugar preciso para la toma de decisión.
35 En fuerte colaboración con la industria.

estratégico. Un plan estratégico fruto de un análisis exhaustivo de dónde se quiere estar y de dónde se parte.

- Plan conjunto: la estrategia, la concepción de la Fuerza, la identificación de capacidades, los desarrollos; todo debe de hacerse de manera conjunta y proyectada para operar de manera colaborativa. Las actuaciones que se ejecuten desde cualquier ámbito deben estar alineadas con el resto.
- Colaboración con la industria: la industria debe apoyar a las FAS durante todo el proceso de cambio, dando soluciones técnicas y proporcionando herramientas.

Estamos ante un momento de cambio donde se tiene la oportunidad de definir dónde se quiere llegar y trazar el mejor camino para conseguirlo. Se debe acometer el proceso de transición con determinación, y evitar caer en la inacción derivada de la inercia del día a día que puede llevar a que sean otros los que definan nuestro futuro.

Capítulo 4

Seguridad y transformación digital para el multidominio

Rubén Vega Bustelo

Resumen

Las operaciones multidominio constituyen un modelo operativo habilitado por tecnologías digitales que permiten desarrollar nuevos paradigmas de combate centrados en datos. La transformación implica dejar de ver las fuerzas conjuntas como estructuras de mandos componentes coordinados, para pasar a verlas como nubes de combate. Es decir, como redes o nubes de elementos de combate digitalizados e interconectados, que se apoyan mutuamente con independencia de su encuadramiento orgánico o del ámbito en que operen.

En consecuencia, las redes y sistemas digitales que habilitan estas operaciones constituyen el centro de gravedad del multidominio y deben llevar la seguridad en su ADN.

Para conseguirlo se deben integrar múltiples tecnologías y múltiples modelos de seguridad, pero bajo una arquitectura coherente y flexible, que permita configurar el espacio de batalla cibernético a medida de las necesidades operativas conjuntas y garantizar la libertad de acción en el ámbito ciberespacial.

Palabras clave

Nube de combate, Ciberseguridad, *Edge Computing, Zero Trust*, SEGINFOSIT, Operaciones electromagnéticas, 5G, TDL.

Security and digital transformation for multi-domain

Abstract

Multi-domain operations are an operating model enabled by digital technologies that allow the development of new data-centric combat paradigms. The transformation means moving from thinking of forces as coordinated component command structures, to see them as combat clouds. That is, as networks or clouds of interconnected and digitalised combat elements that support each other regardless of their organic framework or the domain in which they operate.

Consequently, the digital networks and systems that enable such operations are the centre of gravity of the multi-domain paradigm and must have security in their DNA.

Achieving this goal will require the integration of multiple technologies and security models, but within a coherent and flexible architecture that allows the cyber battlespace to be configured according to common operational needs and assures freedom of action in cyberspace.

Keywords

Combat Cloud, Cybersecurity, Edge Computing, Zero Trust, DCS, Electromagnetic operations, Tactical Data Link, 5G.

1. Introducción

Según fuentes abiertas, minutos antes de la media noche del día 5 de septiembre de 2007, una formación de cazabombarderos iniciaba su misión (Makowsky, 2012). En poco menos de una hora y tras atravesar el sistema de defensa antiaérea sirio sin ser detectados, destruían primero la estación radar de Tall al-Abuad y a continuación su verdadero objetivo, el de relevancia estratégica: las instalaciones de Al-Kibar, presuntamente vinculadas a un programa de desarrollo nuclear sirio (Abrams, 2013). Son varias las hipótesis sobre el mecanismo empleado para burlar el sistema de defensa antiaéreo, entre ellas la simple perturbación electrónica aire-tierra, una combinación de la anterior con ciberataques a la red de mando y control (Fulghum y Wall, 2007), o la inyección de un código ejecutable a través las antenas receptoras de los radares[1]. La última opción, que hace posible ejecutar ciberataques mediados por técnicas de guerra electrónica (EW), parece contar con más adeptos. En 2007 pocos atisbaban que el ciberespacio se declararía algún día ámbito de operación de las FAS en términos similares a los clásicos tierra, mar y aire.

Casi cinco años más tarde, el 4 de diciembre de 2011, fuerzas militares iraníes localizaron en vuelo un dron furtivo RQ 170 Sentinel de los EE. UU., tomaron su control y lo hicieron aterrizar, apropiándose de él, mediante técnicas informáticas (Castro, 2019) y de intercepción de GPS (Clayton, 2011). Otro objetivo de repercusión estratégica alcanzado por la brecha ciber-electromagnética. Proporcionaba a Irán el acceso a tecnología que desconocía, con el consiguiente salto tecnológico (Soriano, 2016), le permitía el acceso a información de inteligencia recopilada por el dron en varias operaciones (Shane y Sanger, 2011) y le daba argumentos para una campaña internacional de información pública[2]. Pero el ciberespacio seguía sin declararse ámbito de operación. Aunque en España acababa de crearse el Mando Conjunto de Ciberdefensa (MCCD), aun habrían de pasar ocho años para su transformación en Mando Conjunto del Ciberespacio, (MCCE) persiguiendo una visión integradora de todas las capacidades de un ámbito de operación que se había incorporado a la doctrina conjunta nacional un año antes, en 2018.

Ambas misiones tienen en común el aprovechamiento táctico de vulnerabilidades de seguridad, fundamentalmente técnicas, para alcanzar

[1] Airforce Technology (2008). The Israeli 'E-tack' on Syria. Part II. [en línea]. *Airforce Technology*. [Consulta: 15 de septiembre de 2023]. Disponible en: https://www.airforce-technology.com/features/feature1669/?cf-view&cf-closed

[2] BBC (2011). Iran reject US request to return captured drone [en línea]. *BBC News*. [Consulta: 15 de septiembre de 2023]. Disponible en: https://www.bbc.com/news/world-middle-east-16154743

directamente objetivos estratégicos con impacto en la Seguridad Nacional mediante el encadenamiento de acciones y efectos a través de varios ámbitos de operación. Ambas tienen una esencia multidominio y, por tanto, ciberespacial, a pesar de ser previas al reconocimiento doctrinal de estos términos. Porque el ciberespacial y, en algunos casos, también el cognitivo son los ámbitos de operación transversales mediadores imprescindibles para la ejecución de Operaciones Multidominio (MDO). Su seguridad es vital para asegurar las MDO propias y para defendernos de las adversarias. Pero para lograrlo es imprescindible conocer la naturaleza real de unos ámbitos a los que la doctrina se refiere como no físicos.

Centrándonos en el ámbito ciberespacial, la asunción irrestricta de su carácter no físico, prescindiendo de su comprensión hermenéutica, conduciría a serios problemas de seguridad. La declaración del ciberespacio como ámbito de las operaciones buscaba inicialmente dar respuesta a un problema estratégico de Seguridad Nacional, derivado de su valor como cauce permanente para el espionaje y para la proyección de poder (Lyngaas, 2023). Un poder que se proyectaba en forma de información codificada sobre un soporte físico (eléctrico, electroóptico o electromagnético), primero para explotar o generar efectos sobre el ámbito cognitivo del adversario y más tarde, cuando el desarrollo tecnológico lo permitió, también sobre los tradicionales ámbitos físicos. Es decir, sobre aquellos en cuyo interior el hombre podía permanecer físicamente.

La importancia del ámbito terrestre para el ser humano siempre ha sido de carácter existencial. Sobre él se asienta la población y los elementos constitutivos del Estado, de él se extraen la mayor parte de materias primas, sobre él despliegan y operan las fuerzas terrestres y sobre él se sitúan las bases permanentes de otras fuerzas[3]. Es un ámbito de las operaciones desde la invención de la guerra (Ortega y Gasset, 1937). El resto de los ámbitos tradicionales se fueron desarrollando a medida que el avance tecnológico permitió al hombre estar en ellos, primero el marítimo, después el aeroespacial. Pero en los tres casos la consolidación de los ámbitos se hizo en sentido ascendente, de lo físico a lo conceptual, de lo táctico a lo estratégico.

El ámbito cognitivo siempre ha estado ahí y se ha explotado también desde la invención de la guerra. No obstante, el desarrollo del ámbito ciberespacial multiplicó la capacidad de penetración en la esfera cognitiva de adversarios y competidores, generando así entre ambos ámbitos un problema de seguridad estratégica.

[3] EMAD. (2023). *PDC-3.2 Operaciones en el Ámbito Terrestre*. Ministerio de Defensa.

El ámbito ciberespacial que, salvo su segmento electromagnético[4], es una construcción humana, se explota desde que la tecnología lo permite. Sin embargo, al no poder desplegar y maniobrar la fuerza militar sobre ellos, en su interior, los ahora llamados ámbitos no físicos inicialmente se conceptualizaron de forma diferente, poniendo el foco en su contribución al éxito de las operaciones desarrolladas sobre los tres ámbitos clásicos, únicos que entonces merecían tal categoría. Eran apoyos. En ambos casos, la transformación intelectual que llevó a declararlos ámbitos de operación se impulsó en sentido descendente, de lo conceptual a lo material, de lo estratégico a lo táctico.

Desde esta perspectiva estratégica, los dos ámbitos constituían canales explotables en todo el espectro del conflicto y no se planteaba la posibilidad de su destrucción física. En el caso cognitivo, por ser un ámbito inherente a la naturaleza humana. En el caso ciberespacial, porque el progreso es imparable y el problema estratégico de seguridad se planteaba en todo el espectro del conflicto, mientras la destrucción física (incluso parcial) se reserva para los estadios finales de la escalada. Pero desde la perspectiva militar, operacional y táctica, las prioridades cambian. Se hace imprescindible tener en cuenta que el ámbito ciberespacial consta de una capa física que puede ser objetivo de acciones cinéticas, que ocupa un espacio geográfico y radioeléctrico que se solapa con los ámbitos clásicos y que, además de ser un importante habilitador para las MDO, constituye un ámbito de operación más. Desde él se pueden desencadenar acciones multidominio con efectos físicos, virtuales o cognitivos[5] sobre otros ámbitos y viceversa.

La declaración del ciberespacio como *domain of operations* en la Cumbre de Varsovia de la OTAN[6] y las sucesivas declaraciones nacionales, deberían haber supuesto un impulso transformador para un ámbito y unas capacidades que hasta entonces habían evolucionado según líneas conceptuales y de capacidad bastante independientes, generando compartimentos estancos entre los que se abrían peligrosas brechas de seguridad. Como las explotadas en los episodios con que se abría esta introducción.

---

4 De acuerdo con la doctrina conjunta nacional el espectro electromagnético forma parte del ámbito ciberespacial. EMAD. (2018). *PDC-01(A) Operaciones en el Ámbito Terrestre*. Ministerio de Defensa. párr. 309.

5 *Ibid*. Párr. 308 y 312. La PDC-01(A) clasifica los efectos como físicos, virtuales o psicológicos, y establece que el ámbito cognitivo alcanza a la inteligencia artificial. En consecuencia, en el estado de madurez actual parece más coherente hablar de efectos cognitivos porque, a diferencia de los psicológicos, sí se pueden materializar sobre el ámbito ciberespacial, que contiene ciber-personas, pero no puede contener personas físicas.

6 OTAN. (2016). Warsaw Summit Communiqué [en línea]. *NATO Official Texts*. [Consulta: 16 de septiembre de 2023]. Disponible en: https://www.nato.int/cps/en/natohq/official_texts_133169.htm

Pero la transformación doctrinal y operativa no sería, ni es, fácil.. Por un lado, se trataba de un ámbito que en algunas líneas de capacidad arrastraba décadas de experiencia y ramas orgánicas y doctrinales fuertemente consolidas y difíciles de cambiar. Por otro, las visiones de lo que debe ser el ámbito siguen condicionadas por la perspectiva del observador: ascendente o descendente; técnico-empresarial y orientada a servicios o militar y orientada a la misión, etc.

En este contexto, a lo largo de las próximas páginas se abordarán algunos de los aspectos que, desde la perspectiva de la seguridad, se consideran más importantes en la transformación digital (TD) de la Fuerza Conjunta para el multidominio, poniendo el foco en la razón de ser de la propia fuerza: el cumplimiento de la misión.

El análisis se dirigirá principalmente desde los niveles operacional y táctico, ascendiendo al estratégico en lo requerido por el contexto operativo y por el aseguramiento de las capacidades militares, y descendiendo al técnico para facilitar la comprensión y para apoyar las ideas sobre realidades tangibles. Porque muchos problemas de seguridad no se pueden comprender si se abordan permanente desde la abstracción conceptual.

2. ¿Evolución o transformación de la seguridad?

Seguridad es un término con múltiples acepciones que dependen, entre otros aspectos, de los calificativos que lo acompañen, del sector o ámbito de empleo, del alcance y nivel de las medidas a aplicar, y de los riesgos que se pretenden eliminar o, al menos, mitigar. Aun así, todas las acepciones de seguridad que se deben considerar al abordar la TD de las FAS para el combate multidominio mantienen un elemento común y definitorio de su finalidad: precaverse contra el riesgo.

En consecuencia, la valoración continua del riesgo constituye un proceso fundamental para alcanzar la finalidad de la seguridad en cualquiera de sus categorías o dimensiones. De forma que, cuanto más robusta sea la metodología que rige este proceso de valoración, mayores serán los estándares de seguridad alcanzados. Aspectos como el respeto a los principios del método científico, el rigor en la delimitación del problema, en la estructuración y en la clasificación de factores, o la sistematización de subprocesos son imprescindibles para alcanzar metodologías suficientemente robustas.

Precisamente para delimitar el problema y sistematizar el análisis, resulta necesario establecer un marco conceptual que oriente la identificación y clasificación de los riesgos contra los que deben precaverse las FAS en su proceso de TD para el combate multidominio. La primera impresión resultante de una revisión normativa y doctrinal que persiga tal fin puede resultar

abrumadora. La dificultad clasificatoria radica principalmente en el gran número de casos de polisemia y sinonimia, derivados de matices terminológicos que se han ido conformando a medida que fueron evolucionando; por un lado, las tecnologías que hoy constituyen el ámbito ciberespacial y, por otro, las disciplinas vinculadas a la seguridad con sus distintos enfoques. Conceptos y definiciones a los que casi nadie parece dispuesto a renunciar para avanzar.

En términos generales, desde la perspectiva de la seguridad se pueden considerar tres líneas evolutivas principales: una de índole estratégica orientada a la Seguridad Nacional; otra de carácter más instrumental y orientada fundamentalmente a la definición de políticas y normas de seguridad de la información (SEGINFO); y, en el contexto del empleo de las FAS, otra orientada a la seguridad de las operaciones, a las operaciones en el ciberespacio, al multidominio, en fin, al cumplimiento de la misión. El desarrollo de cada una de ellas se produjo con un grado de independencia relativamente alto, salvo episodios de coordinación más o menos esporádicos.

Pero el desarrollo tecnológico que desembocó en la construcción del ciberespacio ha venido a trastocarlo todo. Con su carácter transversal, global y omnipresente, ahora el ciberespacio interconecta con fuerza creciente compartimentos que antes eran estancos. El entorno operativo ha cambiado radicalmente, las FAS y el Ministerio de Defensa deben adaptarse, pero ¿cómo?

En la primera edición del documento *Entorno Operativo 2035*, se señalaba que hay una sensible diferencia entre transformarse y adaptarse, que es casi la misma que hay entre revolución y evolución; y se preguntaba por qué se sigue hablando de transformación si el objetivo final de la adaptación no es el cambio en sí, sino la supervivencia. Así, aunque se reconocía que en algunos casos la transformación es imprescindible, se apostaba por un continuado proceso de adaptación de las FAS para aprovechar las oportunidades y afrontar todos los desafíos del EO 2035[7]. La primera revisión del documento avanza hacia la transformación, al reconocer explícitamente que los cambios tecnológicos y operativos serán más rápidos y de mayor profundidad, pudiendo no ser suficiente la adaptación constante en algunas áreas, demandando una auténtica transformación de las mismas. Sin que implique necesariamente una ruptura con la experiencia acumulada, ni una alteración esencial de las misiones y naturaleza de las FAS[8] ¿Será la que nos ocupa una de estas áreas?

Antes de responder conviene profundizar en el análisis.

7 EMAD. (2019) *Entorno Operativo 2035*. Ministerio de Defensa. Párr. 162, 164 y 165. Enero.

8 EMAD (2022). *Entorno Operativo 2035. Primera revisión*. Ministerio de Defensa. Párr. 220 a 223. Septiembre.

3. Aseguramiento de la misión en las operaciones multidominio

Las MDO son un subtipo de las operaciones conjuntas impulsadas y posibilitadas por la digitalización. Ampliando la definición doctrinal con algunas características conceptuales[9], se podría decir que las multidominio son: operaciones en red conducidas por datos en las que, bajo mecanismos de dirección centralizada, control y ejecución descentralizados y distribuidos, se pueden desarrollar acciones tácticas que encadenen tareas ejecutadas desde distintos ámbitos de operación, por fuerzas que pueden depender de distintos mandos componentes y distintos contingentes nacionales, para generar efectos sobre cualquier otro ámbito y con repercusión en cualquier nivel de conducción.

Desde la perspectiva de la seguridad, son varias las vulnerabilidades críticas que se derivan directamente de esta definición ampliada y que afectan a: la supervivencia de la red y de la Fuerza, la seguridad de los datos, el secreto de las operaciones y la libertad de acción.

Otros aspectos de la seguridad también relevantes como la seguridad cognitiva, el impacto del multidominio en la protección de la Fuerza y en la reducción del fratricidio (Presa y Perkins, 2017) o la interoperabilidad no se abordarán en esta ocasión.

3.1. La Nube de Combate y la supervivencia de la red

Una afirmación generalizada respecto a los paradigmas operacionales impulsados por la TD[10] es la necesidad de una infraestructura digital que los sustente. Si el combate multidominio llega a convertirse en una realidad plenamente implementada, esa infraestructura muy probablemente será el centro de gravedad (CoG) de cualquier fuerza operativa. En diversos entornos esa infraestructura ha dado en llamarse por el muy comercial nombre de «Nube de Combate (NC)» o *Combat Cloud*, que rápida e intuitivamente nos conduce a pensar en los servicios en la nube, en estrategias «cloud», quizás en alguien externo a la Fuerza que le aprovisiona los servicios digitales.

[9] EMAD (2023). *Evolución de la Fuerza Conjunta hacia las Operaciones Multidominio. Concepto exploratorio*. Ministerio de Defensa. Marzo.
EMAD (2021). *PDC-3 Doctrina de Operaciones*. Ministerio de Defensa. Párr. 44 y 45.

[10] Véase también el JADC2 de los Estados Unidos. U.S.DoD (2022). *Summary of The Joint All-Domain Command & Control (JADC2) Strategy*. [En línea]. US DoD. [Consulta: 16 de septiembre de 2023]. Disponible en: https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF

Dice un aforismo muy repetido en el mundillo de la informática: «*La nube no existe. Si tus datos están en la nube, están en el servidor de otro*». A lo que muchos verificadores de Internet responden que no es un simple servidor, que son potentes plataformas de prestación de servicios que incluyen servidores principales, espejo y de respaldo, balanceo de carga, virtualización, respuesta dinámica a la demanda de ancho de banda, etc. Desde la perspectiva militar y de seguridad, las preguntas deberían ser: ¿Quién controlará nuestro centro de gravedad? ¿Cuántos centros de procesamiento de datos nos tendrán que destruir? ¿Cuántas acciones de fuego? Las respuestas quizás no ofrezcan demasiadas esperanzas si de la Nube de Combate va a depender nuestra vida y hasta la supervivencia de la nación en venideros conflictos.

Si el CoG de una fuerza vencedora debe ser indestructible (Sun Tzu, s.f.: 41-42), la seguridad debe estar en su ADN. Debe ser seguro desde su concepción.

¿No será, acaso, que la Nube de Combate es otra cosa? ¿No será que, conceptualmente, poco tienen que ver la *Combat Cloud* con los «servicios en la nube» o con el *Cloud Computing*?

En el entorno operativo que se vislumbra, diferencias de segundos o milisegundos decidirán el éxito de las acciones tácticas. Alcanzar y mantener la superioridad multidominio en ese entorno exigirá que los ciclos OODA, vinculados a las acciones constituyentes de cada combate sean más rápidos y de mayor calidad que los del adversario. También exigirá que centros de mando, personas y sistemas puedan apoyar o participar en varios ciclos simultáneos, paralelos o concurrentes, cambiando de ciclo mientras cada uno de ellos sigue su curso. Para lograrlo, cada una de esas personas o sistemas deberá disponer de un punto de conectividad y proceso de datos, de forma que el despliegue de la Fuerza se podrá ver como una nube de puntos digitalizados (Hubert, 2021: 111-118): la Nube de Combate.

Se trata de una nube de puntos enlazados en red que, integrándose en sentido ascendente, van construyendo una red cada vez mayor, una *kill web* (Laird, 2016), que integra con fluidez múltiples redes y sistemas, para constituir un sistema de combate federado que carece de un jefe único y no presenta al adversario puntos de fallo críticos para toda la red.

La finalidad de esta nube es llevar, traer e intercambiar información oportuna y capacidad de procesamiento hasta, desde y en la primera línea de batalla; enlazar las pequeñas unidades y los sistemas de armas para que conformen un sistema de combate capaz de desarrollar operaciones sincronizadas, desagregadas y distribuidas por toda el área de operaciones. La clave es impulsar información de calidad en sentido descendente hasta el nodo efector. Además, debe superar las vulnerabilidades de los puestos de mando clásicos, grandes, centralizados, relativamente estáticos

(Deptula, 2022), y tan similares a los centros de proceso de datos que sustentan los modelos de provisión y explotación de servicios en nube, para pasar a un modelo descentralizado, distribuido, mallado, autoconfigurable, auto-reconfigurable, resistente a la degradación, altamente móvil y difícil de detectar. En fin, un modelo resiliente y con alta capacidad de supervivencia frente a cualquier tipo de amenaza.

Es decir, la Nube de Combate no es una tecnología. Es un paradigma operativo que, sustentándose en múltiples tecnologías complementarias, invierte la forma de empleo de las capacidades conjuntas, al dejar de articularse en torno a ámbitos de operación para pasar a articularse en torno a los datos. Datos cuya ubicuidad e interrelación ya no permitirán trazar fronteras arbitrarias entre ámbitos de operación (Hess *et al.*, 2016). De forma que la articulación en nube es transversal a todos y es multimisión o agnóstica a la misión (Deptula, 2016). Es decir, cualquier nodo de la NC y cualquier enlace pueden contribuir a varias misiones simultáneamente, incluso cuando no estén directamente asignadas a su unidad de encuadramiento operativo. Cuando el adversario bloquee las actividades de un nodo, la red lanzará un aviso a los nodos de cualquier ámbito que estén en condiciones de contribuir al desbloqueo (Goldfein, 2017). Cuando, con la información aportada por nodos de cualquier ámbito, la red detecte que un nodo está en peligro lanzará un aviso para alertarle a él y a los que estén en condiciones de defenderle. Así, se compensan las vulnerabilidades individuales, se multiplican sinérgicamente las fortalezas y se dota de resiliencia a la red de nodos y a la nube de combatientes.

Llegados a este punto, conviene recordar los párrafos previos sobre la naturaleza del ámbito ciberespacial, sobre las peligrosas avenidas de aproximación que su conectividad ofrece a la amenaza y sobre las peligrosas brechas ocultas bajo las líneas y parcelas arbitrarias que se han ido trazando sobre los distintos ámbitos operativos y dominios de la seguridad. Así, será fácil percibir que no basta resolver por separado cada uno de los problemas de seguridad que deberá enfrentar la NC, porque no se garantiza la seguridad de conjunto. En consecuencia, tampoco se garantiza la de sus componentes. Alcanzar una solución eficaz para el conjunto exige una visión integradora y global, una visión que asegure la libertad de acción en el ámbito ciberespacial. Una libertad de acción que solo se podrá lograr ejecutando operaciones en el ámbito ciberespacial.

3.2. Asegurando la capacidad de combate hasta el último nodo

Aceptando como premisa que la clave del combate multidominio es impulsar información de calidad obtenida desde múltiples nodos, en sentido descendente hasta el nodo efector, es habitual concluir que para combatir

se requiere conectividad ubicua. Conclusión que intuitivamente conduce a pensar en modelos centralizadores orientados a la provisión de conectividad con puntos de acceso por zonas de cobertura del área de operaciones. Aceptar sin matices tal conclusión conduciría indudablemente a las vulnerabilidades ya expuestas respecto a los modelos generalizados de explotación en nube. El matiz esencial es que realmente no se necesita conectividad en todas partes, sino en todas las capacidades de combate: unidades, sistemas, plataformas, sensores, etc.

Para conseguir que los puntos de acceso centralizadores no constituyan una vulnerabilidad, se podrían suprimir, distribuyéndolos y llevándolos al extremo, haciendo que cada nodo pueda funcionar como punto de conectividad o como nodo terminal. Se trata de establecer un modelo de computación distribuida, una red mallada hasta el último nodo. Así, cada nodo, incluso aislado, mantendría la capacidad mínima necesaria para seguir combatiendo. Es decir, se podría adoptar una solución técnica de *Edge Computing* de, computación en los extremos de la red (Dalan *et al.,* 2019) en primera línea de combate. Una solución que creciese en conectividad y potencia de computación hacia el interior de la red según un modelo de *Fog Computing* (en la niebla, en el interior de la nube de nodos), sin renunciar a los modelos basados en cobertura zonal para situaciones y cometidos concretos[11].

Casi se podrían encontrar tantas definiciones de *Edge Computing,* y tantos criterios para delimitarla con *Fog Computing*, como contextos de desarrollo y aplicación de la tecnología. Pero desde la perspectiva del aseguramiento de la misión, una de las que mejor se adapta al contexto de las MDO quizás sea la dada conjuntamente por el *Edge Computing Consortium* y la *Alliance of Industrial Internet de China*[12], que se puede trasladar en los siguientes términos:

Es una plataforma abierta, federada y distribuida en el borde de la red y sobre todo el área de operaciones conjunta que alcanza efectores, decisores, sensores y otras fuentes de datos, dotándolos de conectividad, capacidad de almacenamiento y aplicaciones. Al habilitar capacidades permanentes de computación e IA en primera línea, se permite alcanzar los requisitos clave de la digitalización del campo de batalla para garantizar

[11] Por ejemplo: *Infodefensa* (2023). El Ejército encarga a Telefónica una nube de combate 5G con un enjambre de drones para ampliar la conexión. [Consulta: 22 de septiembre de 2023]. Disponible en: https://www.infodefensa.com/texto-diario/mostrar/4247276/ejercito-encarga-telefonica-nube-combate-5g-enjambre-drones-ampliar-conexion

[12] ECC y AII. (2017). *Edge Computing Reference Architecture 2.0* [en línea] Jointly issued by the Edge Computing Consortium (ECC) and Alliance of Industrial Internet (AII). p. 11. Noviembre. [Consulta: 22 de septiembre de 2023]. Disponible en: http://en.ecconsortium.net/Uploads/file/20180328/1522232376480704.pdf

disponibilidad y agilidad en la conectividad, servicios en tiempo real, optimización de datos, inteligencia de aplicaciones, seguridad y protección de la información. Al servir como puente entre los ámbitos clásicos, el ciberespacial y el cognitivo, la computación en el borde habilita efectores inteligentes, enlaces inteligentes, sistemas y servicios inteligentes.

Es decir, el *Edge* es un combatiente, una plataforma, un sistema de armas, un sistema ISR, un puesto de mando, una capacidad de combate guiada por datos, etc. *Edge* asegura mayor supervivencia, mayor disponibilidad y una capacidad de procesamiento de datos más rica, más rápida, más segura y en tiempo real, incluso en entornos degradados y con pérdidas de conectividad. Es una capacidad de combate tecnológicamente reforzada, incluso en situaciones de aislamiento en el seno de un campo de batalla no lineal.

Para ello, cada nodo debe conocer el origen, el camino de actualización y el tiempo de vida de cada dato. Por autenticidad y por trazabilidad, pero también para saber qué datos van perdiendo vigencia y poder representarlos consecuentemente sobre los interfaces de usuario. Los algoritmos y los modelos de inteligencia de cada nodo también se deben actualizar, aunque con menos frecuencia que los datos. En contrapartida, para optimizarlos se necesitarán los datos del mayor número posible de nodos. Por eso, la optimización no se calculará en el borde, sino en capas superiores: *Fog* o incluso *Cloud*. Para este fin, se emplearán técnicas de *big data* y el análisis en profundidad de los datos preprocesados (y, por tanto, resumidos, además de comprimidos, en el borde), que se recibirán de miles de nodos, cuando las condiciones de combate lo permitan, para generar y actualizar modelos de inteligencia lo más exactos posibles. Estos modelos y algoritmos, a medida de cada tipo de nodo, se enviarán al borde para actualizarlo, pero cuando la situación lo permita. Porque *Edge* no se empleará de forma aislada, sino con otras tecnologías (Cao *et al.,* 2020) para reducir vulnerabilidades y multiplicar capacidades, también en el dominio de la seguridad (Wan *et al.,* 2019).

Sin embargo, llevar la capacidad de computación a la zona de contacto con el enemigo plantea nuevos retos de seguridad, derivados de que la potencia computacional disponible en el borde es menor que en los nodos interiores, los enlaces tienen menor capacidad y los equipos están en mayor riesgo de alcance físico o captura por el enemigo.

Las limitaciones en potencia computacional y calidad de enlace podrían suplirse en algunos casos mediante mecanismos de externalización propios de la explotación en nube, pero erosionarían la concepción segura de la red, por lo que conviene buscar soluciones más resilientes.

La limitación de prestaciones afecta igualmente a los mecanismos criptográficos y se intenta paliar mediante el desarrollo de mecanismos y

estándares de criptografía ligera (Biryukov y Perrin, 2017). También afecta a las herramientas específicas de seguridad, que deberán ser más ligeras y correr en sistemas operativos menos capaces. Aquí la diversidad quizás mejore la defensa en profundidad, pero al precio de gestionar información más heterogénea. A pesar de las limitaciones expuestas, en una red concebida segura, el compromiso de un terminal suele ser de bajo impacto, por la dificultad para progresar en la red.

La proximidad física del adversario plantea retos de seguridad también relevantes. En este aspecto, hay una conciencia generalizada de la vulnerabilidad que ofrecen los puertos de comunicación inalámbrica, pero quizás no haya tanta concienciación en relación con los sensores y en especial con la explotación de puertos abiertos a sensores electromagnéticos. Tampoco se debe olvidar que muchos de estos sensores emiten señales electromagnéticas, lo que recomienda emplear tecnologías de baja probabilidad de detección o reemplazarlos por sensores pasivos[13].

En caso de captura de terminales, no es suficiente la fortaleza matemática de los métodos de cifrado. Además, los sistemas que los implementan deben ser resistentes a ataques por inducción de fallos (Boneh *et al.,* 1997) y por canal lateral (Standaert, 2005). Por ejemplo, los que explotan información del comportamiento de los chips durante el procesado (temperatura, tiempo de respuesta, ruido, emisiones electromagnéticas, etc.) para apoyar la ruptura del criptosistema.

El modelo propuesto evita las vulnerabilidades críticas, implícitas en la existencia de nodos centralizadores y enlaces troncales, y reduce los problemas relacionados con el tráfico y gestión de acceso a los datos, principalmente en las dimensiones de disponibilidad, conservación y confidencialidad[14], al tiempo que facilita el despliegue de varias líneas de defensa añadiendo nuevas capas de seguridad. En contrapartida, al acercar la capacidad de computación al extremo, al adversario, y al aumentar el número de interconexiones y la extensión, alinealidad, discontinuidad y difuminado del perímetro de seguridad, trae consigo nuevos problemas de seguridad, aunque más leves.

3.3. Una arquitectura de red segura desde su concepción *¿Zero Trust?*

Aun hoy, es frecuente encontrar modelos de seguridad en red basados en defender el perímetro. A pesar de que hace ya décadas se propugnaban modelos de seguridad basados en establecer redes verdaderamente

[13] Indra (2013). Indra desarrolla el primer sistema radar pasivo de alta resolución [en línea] [Consulta: 23 de septiembre de 2023]. Disponible en: https://www.indracompany.com/es/noticia/indra-desarrolla-sistrema-radar-pasivo-alta-resolucion

[14] España (2022). Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Art. 1. y Anexo IV.

defendibles. Es decir, redes que se pudiesen inventariar, auditar y monitorizar internamente y en tiempo real; redes que limitasen la capacidad de maniobra interna de posibles intrusos; redes que permitiesen solo los servicios necesarios e inventariados; redes actualizadas y fácilmente actualizables (Bejtlich, 2005: 20-24). Si entonces defender el perímetro era insuficiente para enfrentar la amenaza, hoy lo es más. La amenaza ha evolucionado y los perímetros de red se han difuminado. Quizás por eso, hoy, el modelo de moda es *Zero Trust*[15], propuesto hace más de una década (Kindervag, 2016)[16].

Este modelo se fundamenta en que la confianza (*trust*) solo se puede otorgar a las personas y, una identidad, un usuario[17] (incluso acreditado), no es una persona. Tampoco los son los equipos, ni los paquetes de datos. Por tanto, la confianza no puede ser la base de la estrategia de seguridad y no cabe hablar de lado interno o externo de la red en términos de confianza. La clave del modelo *Zero Trust* es la simplicidad y, cuando se aplica una política de desconfianza por defecto, proteger la red es más simple y fácil[18].

A priori, un modelo de seguridad basado en la desconfianza parece contradecirse con un modelo operativo que se basa en la necesidad de compartir, que busca la coordinación multiagente a través de un medio compartido, que persigue la autosincronización (Alberts *et al.*, 2010: 60-71), que antepone el acceso de los colaboradores frente al rechazo a los hostiles (Hess *et al.*, 2016). Pero la consciencia de que se aplica un filtrado estricto es, precisamente, un elemento de refuerzo de la confianza necesaria para evolucionar desde procesos de decisión centralizadores a otros compartidos, flexibles y robustos. La clave está en que el filtro de confianza sea transparente para los usuarios, sencillo para los responsables de la seguridad y responda a los usuarios en términos de agilidad y seguridad. Esta es una de las novedades y ventajas de la filosofía *Zero Trust*, que tiene en cuenta la necesidad de compartir información con rapidez[19].

---

15 Palo Alto Networks. (2021). *La ciberseguridad* más allá de las palabras de moda: qué deben saber los directivos sobre el modelo Zero Trust. Resumen. [En línea] Palo Alto Networks. [Consulta: 27 de septiembre de 2023]. Disponible en: https://www.paloaltonetworks.es/content/dam/pan/es_ES/assets/pdf/cxo/articles/beyond-the-buzzword-zero-trust-es.pdf

16 El analista de Forrester John Kindervag propuso en modelo Zero Trust en el informe Forrester de 2010: *No More Chewy Centers: Introducing the Zero Trust Model of Information Security* y lo actualizó en 2016.

17 EMAD. (2021). *PDC-3.20 Operaciones en el Ámbito Ciberespacial*. Ministerio de Defensa.

18 Delloite.(2021).JohnKindervag:'TheHallmarkofZeroTrustIsSimplicity'.[Enlínea]*TheWall Street Journal*.[Consulta:13deseptiembrede2023].Disponibleen:https://deloitte.wsj.com/riskandcompliance/john-kindervag-the-hallmark-of-zero-trust-is-simplicity-01618513330

19 Forrester (2013). *Developing a Framework to Improve Critical Infrastructure Cybersecurity*. [En línea] NIST, pp.4. [Consulta: 28 de septiembre de 2023]. Disponible en: https://www.nist.gov/system/files/documents/2017/06/05/040813_forrester_research.pdf

Desde la propuesta original, se han desarrollado muchas variantes, ampliando los principios y arquitecturas[20]. Los tres principios originales (Kindervag, 2016), mantienen plena vigencia e interés para la Nube de Combate:

1) Verificar y asegurar todos los recursos con independencia de su localización. No hay subredes ni dispositivos de confianza y el tráfico no es confiable hasta verificar que está autorizado y es seguro. Tampoco hay usuarios de confianza, por lo que los datos en alojamientos internos se deben proteger igual que en el exterior.

2) Se debe adoptar el criterio de mínimo privilegio y estricto control de acceso, que se debe aplicar a dispositivos, procesos, datos y usuarios, especialmente a los usuarios con más permisos.

3) Inspeccionar y registrar todo el tráfico. El tráfico se debe inspeccionar en tiempo real, empleando herramientas de monitorización y análisis que aporten simplicidad mediante la automatización, integración y gestión centralizada de múltiples tareas, herramientas y sistemas[21].

El modelo arquitectónico de *Zero Trust* se basa en concebir redes seguras por diseño, y en construirlas desde el interior, es decir, desde las funciones clave hacia las conexiones exteriores. Traducido a la NC, desde los nodos más próximos al adversario, porque allí residen los datos y procesos clave para ejecutar con éxito las operaciones. Así, la propuesta arquitectónica es renunciar a las redes jerárquicas, inherentemente inseguras, para adoptar arquitecturas caracterizadas por la segmentación, la descentralización mediante múltiples núcleos de conmutación en paralelo, y la administración dinámicamente centralizada de recursos distribuidos (Kindervag, 2010). Propuestas perfectamente alineadas con las necesidades de supervivencia física de la red en combate, matizando que la centralización de la administración no lo será en términos absolutos y debe responder dinámicamente a la necesidad de auto-reconfiguración de la red y de integración ascendente. En este aspecto, la solución debe venir de la mano de los modelos de federación que se adopten.

En cuanto a las propuestas de implementación técnica del modelo, la más relevante para la Nube de Combate multidominio es la de construir las redes en torno a puertas de enlace de segmentación o *segmentation gateways* (SG). Estos dispositivos deben integrar, por fabricación, las

[20] Por ejemplo: NIST (2020). *Zero Trust Architecture*. [En línea] NIST Special Publication 800-207 [Consulta: 28 de septiembre de 2023]. Disponible en: https://doi.org/10.6028/NIST.SP.800-207 o CISA (2023). *Zero Trust Maturity Model V 2.0.* [En línea] Cybersecurity and Infrastructure Security Agency [Consulta: 28 de septiembre de 2023]. Disponible en: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

[21] Delloite. (2021). *Op. cit.,* nota 43.

funciones de seguridad y conmutación de paquetes, convirtiéndose en el núcleo de cada segmento de red, *microcore and perimeter* (MCAP), para llevar al extremo los criterios de segmentación, eliminación de cuellos de botella (paralelización) y simplicidad de la administración y de la monitorización de seguridad[22]. En un modelo de NC intrínsecamente seguro, los MCAP se deberían construir a nivel de cada pequeña unidad, sistema de armas, plataforma, clúster (Presa y Perkins, 2017: 23-29), puesto de mando, etc.

Pero la implementación del modelo requiere además un amplio rango de tecnologías, y soluciones adicionales para hacerlas eficaces cuando se aplican a modelos de computación distribuida y en el borde. Entre estas destacan las de autenticación de identidad, para garantizar la «confiabilidad» de usuarios, aplicaciones y equipos y, entre ellas, las de autenticación interdominios con firma única *Single Sign-On* (SSO) (Cao *et al.*, 2020), incluida la transferencia de autenticación entre dominios en situaciones de movilidad (Tsitaitse *et al.*, 2018: 2.221-2.243).

La identidad autenticada determinará los accesos que se autorizan. Pero como las tecnologías criptográficas tradicionales se adaptan mal a entornos de computación distribuida y paralela, será necesario recurrir a otras tecnologías para control de accesos, como las basadas en atributos (*Attribute-Based Encryption, ABE, Identitiy-Based Encryption, IBE*) (Sahai y Waters, 2004), complementando a las basadas en roles (Kuhn *et al.,* 2010: 79-81).

Al seguir un modelo centrado en datos donde el cifrado es fundamental, se plantea una contradicción con el principio de monitorización continua, para el que también se debe avanzar en las soluciones. Por ejemplo, los aceleradores de cifrado y descifrado en los puntos de monitorización (Bejtlich, 2005: 20).

3.4. Aseguramiento de los enlaces

Para tejer la red de nodos que constituye la Nube de Combate, son imprescindibles los enlaces, que en su mayor parte deberán ser altamente móviles, es decir, inalámbricos. Entre los requisitos de seguridad exigibles a dichos enlaces, cabe destacar un perfil de emisiones compatible con la seguridad de las operaciones (OPSEC)[23], y unas medidas de seguridad de las comunicaciones que, en términos generales, la previsible evolución de la amenaza en el nivel táctico recomendaría priorizar por disponibilidad, autenticidad, integridad, trazabilidad y confidencialidad.

22 *Ibidem,* pp. 9-22.
23 EMAD. (2021). *PDC-00 Glosario de Terminología de uso Conjunto*. Ministerio de Defensa, p. 47.

Las familias tecnológicas a considerar para estos enlaces se podrían clasificar en dos grandes grupos: las que establecen topologías malladas y las que establecen áreas de cobertura conformando una topología de estrella.

En el primer grupo, se encuentran los estándares TDL, que llevan décadas ofreciendo soluciones de enlace de datos interoperables (Sabatini *et al.,* 2008) que mejoran la consciencia situacional y contribuyen a la autosincronización de los elementos de combate, incrementando significativamente la eficacia del conjunto (Gonzales *et al.*, 2005).

Las versiones TDL más actuales[24] emplean la radiodifusión uno a varios, accediendo al medio electromagnético por división de tiempo (TDMA) e incorporando tecnologías de espectro ensanchado, con las consiguientes ventajas de seguridad y eficiencia espectral (por ejemplo, con *multinetting*). Las sucesivas actualizaciones y estándares han ido añadiendo características de baja probabilidad de intercepción; baja probabilidad de detección, muy importante para plataformas furtivas (*stealth*); capacidad de autoformado y reconfigurado automático de la red mallada que permiten formar, donde todos los terminales pueden actuar como retransmisores de paquetes (porque está diseñada para no tener nodos críticos); ampliación de las bandas de radiofrecuencia empleadas; y, excepto para funciones críticas, posibilidad de externalización de tráfico a redes satélite o IP, aunque como norma general emplean formatos de trama específicos para cometidos tipo (series J, K, etc.), que aumentan la eficiencia y contribuyen a la seguridad.

En cuanto a las técnicas de espectro ensanchado, cabe destacar la contribución del salto de frecuencia a la baja probabilidad de intercepción, que se refuerza con el mezclado de ruido aleatorio. También la combinación de salto de frecuencia con técnicas de doble pulso (emisión), aumentando la resistencia a la perturbación y a las interferencias. Respecto al secreto de las comunicaciones, incorpora dos capas de seguridad criptográfica: una sobre los propios mensajes y otra sobre la transmisión, que incluye el añadido de ruido aleatorio y se combina con el patrón de salto de frecuencia. Los estándares más recientes incorporan una capa criptográfica adicional que permite el cifrado a alto nivel sin perjuicio de la transmisión. Asimismo, incorporan mecanismos para detectar intentos de ataque a la red.

En cuanto a gestión de red, los pocos aspectos que requieren centralización se basan en funciones de gestión distribuidas. Aun así, para algunas se deben designar nodos específicos, que siempre tendrán un suplente en espera, reasignándose automáticamente las suplencias para garantizar

[24] Northrop Grumman (2014). *Understanding Voice and Data Link Networking. Northrop Grumman's Guide to Secure Tactical Data Links.* [en línea]. [Consulta: 3 de octubre de 2023]. Disponible en: *https://dl.icdst.org/pdfs/files/e90d37a-9b93e2e607206320ea07d7ad2.pdf*

que no hay puntos únicos de fallo. Además, disponen de sistemas de monitorización centralizada del estado de la red. Desde la perspectiva de la disponibilidad destacan las funciones de enrutamiento en tiempo real y la gestión de la congestión por reconfiguración de red o por control del flujo de retransmisiones.

Por último, cabe destacar las características TDL de más reciente desarrollo y orientadas a plataformas furtivas, como las formas de onda definidas por *software* y la direccionalidad de los enlaces (Keller, 2020). Aspectos que también marcan la evolución en el paradigma de la comunicación celular.

En el grupo de tecnologías orientadas a la cobertura de zona, la prospectiva tecnológica apunta con fuerza a las tecnologías celulares, 5G, 6G, etc. y a los satélites, cobrando especial importancia en el nivel táctico los de baja y muy baja órbita. En comparación con los sistemas de acceso mallado, cabe destacar tres debilidades de la topología zonal: el perfil de emisiones, la disponibilidad y los puntos únicos de fallo.

Hasta 4G LTE, las estaciones base (BS) radiaban la información necesaria para el acceso de los terminales móviles permanente sobre todo su área de cobertura. Además, la imprecisión en el control de potencia impedía reutilizar canales en celdas contiguas para evitar interferencias. Es decir, eran muy fácilmente localizables desde más allá de la zona de cobertura deseada y cada BS constituía un punto de fallo único para una zona relativamente amplia. Las tecnologías 5G traen avances muy significativos de cara a la seguridad en el contexto operativo. Por un lado, debido a la alta tasa de datos y densidad de conexiones que pretende soportar 5G, el área de cobertura de las BS debe ser mucho más pequeña que en 4G, aumentando el número de estaciones (Wang *et al.*, 2020) y, por tanto, difuminando su perfil en una nube de puntos más densa y homogénea, que dificulta el levantamiento de nodos críticos. Este efecto difuminado y las mejoras en seguridad respecto a otras tecnologías de zona convierten a 5G en candidata para aplicaciones de *clustering, platooning*[25] y enlace interno de sistemas de armas distribuidos o robotizados.

Por otro lado, *5G New Radio* supera la radiodifusión de direccionalidad reducida para adoptar modelos de propagación de alta precisión, incluyendo técnicas de apuntado mediante la conformación de haces de emisión estrechos[26]. Los terminales se localizan mediante barrido, emitiendo

[25] Huawei (2017). *5G unlocks a world of opportunities. Top Ten 5G Use Cases* [en línea] [Consulta: 1 de octubre de 2023]. Disponible en: https://www-file.huawei.com/-/media/corporate/pdf/mbb/5g-unlocks-a-world-of-opportunities-v5.pdf

[26] Huawei (2018). *Huawei 5G Wireless Network Planning Solution White Paper* [en línea] [Consulta: 1 de octubre de 2023]. Disponible en: https://www-file.huawei.com/-/media/corporate/pdf/white%20paper/2018/5g_wireless_network_planing_solution_en_v2.pdf

sucesivos haces en frecuencias y direcciones concretas, lo que permite ubicarlos con precisión y apuntar la señal con un aumento muy significativo de la ganancia. Además, controlando la dirección y sección de los haces se evita que rebasen el borde de la zona de cobertura deseada. Inicialmente las BS emiten con un patrón por defecto, pero, al emplear antenas activas, pueden adaptar los haces siguiendo distintos estándares de realimentación y optimizando mediante IA. Para la comunicación también se emplea apuntamiento, además de técnicas de seguimiento y transferencia de haz durante el movimiento del terminal (Gómez Liberal, 2021). Las ventajas en cuanto a perfil de emisiones, resistencia a la perturbación y resiliencia en entornos electromagnéticamente degradados son evidentes, pero cada BS sigue siendo un punto crítico.

El empleo de satélites tampoco está exento de problemas de seguridad, como la indiscreción de las emisiones que permiten ubicar las antenas terrestres (Wattles, 2022) o, en el caso de la externalización de tráfico, la pérdida de confidencialidad o de control sobre el flujo de comunicaciones, según el criterio del propietario de la red (Jordan, 2023) o en beneficio de terceros (Frąckiewiczen, 2023)[27]. Asimismo, las etapas inalámbricas y la radiodifusión descendente permiten explotar simultáneamente vulnerabilidades de gran número de estaciones terrenas, incluso a gran escala (Steinbrecher, 2022).

3.5. Asegurando la libertad de acción para combatir en nube

Siendo comúnmente aceptado que la superioridad aérea es condición necesaria para el éxito de las operaciones acorazadas y mecanizadas, también debería serlo que, para el éxito de las MDO es imprescindible la libertad de acción en el ámbito ciberespacial. Debería serlo porque, además de aportar al paquete conjunto las capacidades específicas del ciberespacio, el ámbito ciberespacial constituye el nexo integrador del multidominio, que da soporte físico (electrónico y electromagnético) al conocimiento transversal e inmediato que posibilita las MDO.

La libertad de acción en el ámbito ciberespacial podría definirse como la posibilidad de decidir, preparar y emplear las capacidades propias del

[27] *Noticias Seguridad Informática* [En línea] (2022). Internet en territorio ucraniano es desviado a Rusia para distribuir desinformación. [Consulta: 1 de octubre de 2023]. Disponible en: https://noticiasseguridad.com/hacking-incidentes/internet-en-territorio-ucraniano-es-desviado-a-rusia-para-distribuir-desinformacion/
Frąckiewiczen, M. (2023). *¿Cómo se compara* Starlink con otros proveedores de Internet satelital que actualmente operan en Ucrania*?* [en línea] *TS2* [Consulta: 1 de octubre de 2023]. Disponible en: https://ts2.space/es/como-se-compara-starlink-con-otros-proveedores-de-internet-satelital-que-actualmente-operan-en-ucrania/

ámbito a pesar de la voluntad del adversario. Por tanto, debe conservarse a todo trance y, si se pierde, debe tratar de recuperarse utilizando todos los medios disponibles[28] y, en consecuencia, todos los tipos de operaciones. Esta definición obliga a reflexionar sobre las condiciones de necesidad y suficiencia de las medidas técnicas de ciberseguridad, orientadas a la protección y seguridad de los sistemas, en relación con las MDO.

La reflexión sobre la necesidad de la ofensiva, la suficiencia de la defensiva y la mayor fortaleza de una u otra no son nuevas. De hecho, resurgen con cada cambio tecnológico, generando una intensa dialéctica cuyo desenlace es fundamental (Buzan, 1987: 49, 155). Porque la correcta determinación de la calidad ofensiva o defensiva de los sistemas condicionará su correcta forma de empleo en todos los niveles de conducción. Al respecto, las numerosas vulnerabilidades del ámbito ciberespacial inclinan a pensar en su mayor calidad ofensiva.

Por otro lado, siguiendo una línea de pensamiento ligeramente diferente, Clausewitz reflexionó en términos absolutos, concluyendo que la defensa es la forma más fuerte de conducir la guerra, pero al perseguir un fin negativo, preservar, es insuficiente y debe abandonarse, pasando a la ofensiva, en cuanto se disponga de la fuerza para aspirar a un fin positivo: conquistar (Clausewitz, s. f: 252-253). Reflexionado sobre este particular, Fuller niega la fortaleza o debilidad intrínseca del ataque o la defensa, para afirmar su complementariedad basada en el sentido común. Además, citando a Napoleón: «Todo el arte de la guerra reside en una defensiva bien razonada y circunspecta, seguida de un ataque rápido y audaz», Fuller nos facilita retornar al ámbito ciberespacial (Fuller, 1961: 51, 70-71), el único ámbito de las operaciones construido por el hombre.

La transcendencia de esta característica es inmensa, porque al permitir a los contendientes construir el espacio de batalla a medida de sus necesidades, la defensiva deja de estar condicionada por la orografía, para estarlo por la capacidad tecnológica de cada parte. De forma que el contendiente que no esté en condiciones de adaptar con rapidez, al menos, el ciberespacio propio a las demandas operativas estará condenado al fracaso (López Calderón, 2021).

Así, resulta lógico que la doctrina de operaciones en el ciberespacio añada las Operaciones de Infraestructura CIS (CISIO) a los tres tipos de operaciones que son comunes al resto de ámbitos (ofensivas, defensivas e ISR[29]). Porque solo en el ciberespacio tenemos alguna posibilidad de construir el espacio de batalla ideal. En los ámbitos aeroespacial y marítimo es

[28] Adaptada de la definición dada por la PDC-01(A). *Op. cit.,* nota 13, párr. 264.
[29] Operaciones de Inteligencia, Vigilancia y Reconocimiento / Intelligence, Surveillance and Reconnaissance.

imposible. En el terrestre solo cabe organizarlo para la defensa, con las restricciones de la orografía, y es impensable asignar la autoridad sobre la organización del terreno a alguien ajeno a la cadena de mando de la operación.

Pero, incluso en el ámbito ciberespacial sería en cierto modo utópico pensar en construir un nuevo ciberespacio para cada operación. Gran parte de él está ya construido de antemano, otra parte se puede construir; y otra, que se solapa a las anteriores, se puede reconfigurar.

Luego, hay tres condicionantes para establecer esa *defensiva bien razonada y circunspecta* que permita proteger el CoG multidominio y mantener la libertad de acción para pasar a la ofensiva: el ciberespacio ya construido, el que podemos construir o modificar con los recursos disponibles y la autoridad conferida para hacerlo. La doctrina no desarrolla estos aspectos fundamentales y los difiere al contexto específico de cada operación.

Iniciemos su análisis caminando a hombros de la antigua Doctrina de la Fuerza Terrestre[30], que organizaba la defensa en una zona de seguridad y una zona principal de defensa, ambas bajo la autoridad del responsable de la defensa. La traslación al ámbito ciberespacial aumenta la complejidad, pues debe proyectarse sobre tres capas: física, lógica y ciberpersonal[31]; pero no por ello pierde validez conceptual.

En consecuencia, en el ámbito ciberespacial deben conferirse a la autoridad operativa las atribuciones necesarias para organizar el ciberterreno[32] a medida de las necesidades operativas. Es decir, las configuraciones de *hardware* y *software*, el despliegue geográfico de los equipos y la gestión del espacio electromagnético asignado para la operación.

La zona de seguridad, orientada fundamentalmente al principio operativo de seguridad, tenía como objetivo precaverse contra la acción del enemigo, evitando la sorpresa. Con tal fin, en ella se establecía un despliegue destinado a obtener información del enemigo, proporcionar seguridad, ganar tiempo, desgastar y canalizar al adversario. En el ámbito ciberespacial, con los mismos fines, esta zona estaría constituida al menos por todos los nodos terminales, operando en zonas de proximidad o contacto físico o lógico; por los nodos de interconexión con otras redes, propias, aliadas o

[30] Estado Mayor del Ejército. (1996). *Doctrina de Empleo de la Fuerza Terrestre* (DO1-001). Cap. 13. (DL, Derogada).

[31] PDC-3.20. *Op. cit.,* nota 41, p. 3.

[32] Véase consideraciones sobre la traslación al ámbito ciberespacial de conceptos tácticos relativos al terrero en: DoA (2021) *FM 3-12 Cyberspace Operations and Electromagnetic warfared* [en línea]. Department of the Army of the United States of America, pp. 4-10 y 4-11. [Consulta: 30 de septiembre de 2023]. Disponible en: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN33127-FM_3-12-000-WEB-1.pdf

de terceros; por los enlaces de dichos nodos; y por el entorno electromagnético (EEM) contiguo.

La zona principal de defensa es la destinada a la batalla defensiva decisiva y se organiza en torno a zonas y posiciones fundamentales, que en el ciberespacio pueden obedecer a dos fines: constituir los pivotes sobre los que apoyar el mecanismo de destrucción del enemigo o asegurar el CoG multidominio. Si dichas posiciones caen, la derrota está asegurada, por eso, la clave es que el CoG no dependa significativamente de ninguna de ellas. Esta zona estaría constituida principalmente por nodos de puesto de mando y de clúster, por sus enlaces y por el EEM.

Precisamente, en torno al EEM se abre actualmente una brecha doctrinal para la seguridad de las operaciones propias que, como en los ejemplos introductorios, puede ser explotada por el adversario para anular nuestra libertad de acción en el ámbito ciberespacial. Se trata de un caso paradigmático de viejas estructuras que se resisten a dejar paso a las nuevas, imprescindibles para la transformación.

La doctrina conjunta nacional fue pionera entre las de nuestro entorno al incluir el EEM en el ámbito ciberespacial[33]. La transformación del Mando Conjunto de Ciberdefensa en Mando Conjunto del Ciberespacio fue el primer paso para aplicarla. Pero el camino no es fácil. El corsé impuesto por el ramificado histórico del árbol doctrinal, la necesidad de mantener la interoperabilidad doctrinal con nuestros aliados, y las diversas figuras creadas o mantenidas en sus marcos doctrinales para conservar el espectro electromagnético como una suerte de ámbito o dimensión independiente siembran el camino de obstáculos.

Sirvan como ejemplos, las incoherencias sobre el particular del AJP-3.20[34], o las contradicciones implícitas en el reciente cambio terminológico que incorpora las «operaciones electromagnéticas» y redenomina la guerra electrónica como «electromagnética». Mientras etimológicamente los términos estrechan el concepto de guerra electrónica, al centrarse en las ondas y olvidarse de los imprescindibles equipos electrónicos (Smith y Tourangeau, 2021: 179-186), en la práctica, parecen querer independizarse del ámbito ciberespacial o, contradictoriamente, incluso absorberlo (Willis y Stathopoulos, 2020: 72-77), añadiendo una serie de disciplinas relacionadas. Disciplinas, todas ellas inviables, o innecesarias, sin las capas lógica y física del ámbito ciberespacial, electrónica y EEM incluidos. Así, no sorprende que, incluso entre los que reconocen que la fragmentación es incompatible con la eficacia operativa, haya quienes se resistan a abandonar los viejos términos o incluso pretendan invertirlos (Willis y Sathopoulos,

33 PDC-01(A). *Op. cit.,* nota 13, párr. 309.
34 OTAN. (2020) *AJP-3.20 Allied Joint Doctrine for Cyberspace Operations*, pp. 2 a 4.

2020: 74-76), a pesar de que «misunderstanding words can kill» (Smith y Tourangeau, 2021: 179, 184).

4. De la SEGINFOSIT a la seguridad centrada en datos

Catorce años antes de que la OTAN declarase el ciberespacio como ámbito de las operaciones militares, el Ministerio de Defensa unificó bajo la misma Orden Ministerial la experiencia que hasta entonces se había acumulado en el campo de la seguridad de las Tecnologías de la Información propiamente dichas, y en el de la seguridad de la información cuando es almacenada, procesada, transmitida o manejada por un sistema. Así, bajo el término INFOSEC pasó a regular la «protección de la información almacenada, procesada o transmitida, por Sistemas de Información y Telecomunicaciones (Sistemas), mediante la aplicación de las medidas necesarias que aseguren o garanticen la confidencialidad, integridad y disponibilidad de la información y la integridad y disponibilidad de los propios Sistemas»[35].

Tan solo cuatro años más tarde, la evolución de la sociedad y de las tecnologías de la información motivaron la actualización normativa, que se materializó en la política de Seguridad de la Información del Ministerio de Defensa, actualmente vigente. Esta política divide la seguridad de la información en áreas, atendiendo al elemento tangible que hace uso de ella, ya sea elaborándola, presentándola, almacenándola, procesándola, transportándola o destruyéndola: personas, documentos, sistemas de información y telecomunicaciones, instalaciones y empresas. La INFOSEC es así desplazada por la SEGINFOSIT (*Seguridad de la Información en los Sistemas de Información y Telecomunicaciones*) que «entiende de las medidas de protección aplicables en los sistemas de información y telecomunicaciones con el objeto de garantizar razonablemente la confidencialidad, integridad y disponibilidad de la información que manejan»[36].

Si se comparan ambas definiciones, salta a la vista una diferencia de matiz de gran calado. Sorprendentemente, la más actual olvida las medidas aplicables directamente a la propia información, o a su representación digital, *virtual*, para centrarse en las medidas de protección aplicables a los sistemas que la manejan. Desde la perspectiva actual, habiéndose sumado ya el ciberespacial a los ámbitos de operación, y habiéndose clasificado doctrinalmente los tipos de

[35] España. (2006). Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la política de seguridad de la información del Ministerio de Defensa. Preámbulo y art. séptimo de la Política.

[36] España (2002). Orden Ministerial 76/2002, de 18 de abril, por la que se establece la política de seguridad para la protección de la información del Ministerio de Defensa almacenada, procesada o transmitida por sistemas de información y telecomunicaciones. (Derogada). Art,s 1, 2 y Preámbulo.

operaciones en el ciberespacio, incluyendo la protección de los sistemas[37], quizás fuese más lógico recuperar lo olvidado y olvidar lo mantenido. Es decir, centrar la SEGINFOSIT en la información propiamente dicha. Precisamente este es el enfoque de la seguridad centrada en los datos.

La seguridad centrada datos o *Data Centric Security* (DCS) cambia el enfoque de la SEGINFOSIT, al enfatizar la seguridad de los propios datos por encima de la de los dispositivos, aplicaciones, servidores o redes que los manejan. Con este enfoque se pretende identificar, clasificar, proteger, monitorizar y controlar el acceso a los datos propiamente dichos durante todo el ciclo de vida, incluso fuera de las redes y equipos de la propia organización (Fritsh y Wonham, 2019).

Los sistemas tradicionales orientados a la seguridad de los sistemas solo dan solución parcial a los objetivos de la DCS. Por ejemplo, los sistemas DLP (*Data Leak Prevention*), o su versión CASB (*Cloud Access Security Brokers*) para aplicaciones en la nube, son difíciles de ajustar para filtrar automáticamente los ficheros que pueden salir de la organización, porque además del tipo de información deberán considerar el destinatario y la situación. El cifrado también es insuficiente, pues, una vez fuera de la organización y descifrada, se pierde el control sobre la información[38].

Entre los elementos clave que necesariamente debe incluir un sistema DCS cabe destacar los necesarios para: identificar, descubrir y clasificar la información a proteger; establecer los mecanismos y controles de seguridad sobre los propios datos, que son los bloques constituyentes de esa información; aplicar mecanismos de auditoría continua para evaluar posibles desvíos sobre los patrones esperados de uso y acceso a los datos; y administrar y gestionar dinámicamente las políticas de seguridad y los permisos de acceso, incluso sobre los datos que ya han salido de las redes y sistemas de la organización[39].

En la actualidad ya se dispone de herramientas eficaces para implementar DCS sobre ficheros de aplicaciones de usuario que corren sobre sistemas operativos de uso común[40]. Sin embargo, la aplicación a paquetes de datos

37 PDC-3.20. *Op. cit.*, nota 41, pp.17-A.

38 CCN-CERT (2021). *Ventajas de un enfoque de seguridad centrado en los datos* [en línea] CCN-CERT. pp. 1, 2 [Consulta: 29 de septiembre de 2023]. Disponible en: https://www.ccn-cert.cni.es/informes/abstracts/5705-ventajas-de-un-enfoque-de-seguridad-centrado-en-los-datos/file.html

39 CCN-CERT (2022). *Trazabilidad del dato en el contexto del Esquema Nacional de Seguridad (ENS)* [en línea] CCN-CERT. pp. 1-4 [Consulta: 29 de septiembre de 2023]. Disponible en: https://www.ccn-cert.cni.es/informes/abstracts/6816-abstract-trazabilidad-del-dato-en-el-contexto-del-ens/file.html

40 Por ejemplo, la herramienta CARLA. CCN-CERT (s.f). *Carla* [en línea] CCN-CERT. [Consulta: 29 de septiembre de 2023]. Disponible en: https://www.ccn-cert.cni.es/soluciones-seguridad/carla.html

de bajo nivel, procesados en los sistemas específicos y más limitados de los terminales de la NC, y con exigencias de interoperabilidad, plantea la necesidad de soluciones a medida y retos tecnológicos aún en desarrollo que requieren estrategias a largo plazo[41]. Por otro lado, la relevancia de las dimensiones de la seguridad y de los tiempos también varía. Mientras a nivel operacional y estratégico es clave garantizar la confidencialidad en plazos largos de tiempo, en el nivel táctico los tiempos se reducen y la preocupación recae principalmente en la disponibilidad, autenticidad e integridad.

Las soluciones técnicas para la plena implementación de DCS en la NC requieren el desarrollo, estandarización e implementación de metadatos estándar para cada tipo de dato, estándares de vinculación o incrustado de metadatos y datos, estándares criptográficos practicables y mecanismos de aplicación de las políticas de filtrado y acceso[42]. Mecanismos que nos llevan de nuevo a las *segmentation gateways,* de la arquitectura *Zero Trust*, que se encargarán de aplicarlas en cada nodo, clúster o subred, añadiendo una capa de seguridad centrada en los datos a otras más orientadas a los sistemas.

Aquí las tecnologías criptográficas también son fundamentales para garantizar el almacenamiento, procesado e intercambio de datos confidencial, íntegro y trazable. Entre ellas es obligatorio destacar las técnicas de cifrado con capacidad de búsqueda, que permiten buscar en bases de datos sin descifrar los datos almacenados ni los términos buscados. También los cifrados homomórficos, que permiten operar sin necesidad de descifrar los datos (Rivest y Adleman y Dertouzos, 1978)[43].

5. Ciberseguridad Nacional y aseguramiento de la capacidad de ejecución

La transversalidad de los nuevos ámbitos de operación, así como la evolución de la amenaza hacia estrategias híbridas que, mediante acciones coordinadas y multidimensionales, tratan de explotar las vulnerabilidades de los Estados y sus instituciones demandan una capacidad de disuasión creíble

CCN- CERT (2021). *CARLA. Protección y trazabilidad del dato* [en línea] CCN-CERT. [Consulta: 29 de septiembre de 2023]. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/5720-datasheet-carla/file.html

41 Por ejemplo, en el nivel técnico la estrategia desarrollada en el marco de FMN y en el estratégico la «Data Centric Security Vision and Strategy Proposal for the Alliance Federation, Including the NATO Enterprise».

42 Por ejemplo, el NATO STANAG 4774, Confidentiality Metadata Label Syntax - ADatP-4774 Edition A, o el NATO STANAG 4778, Metadata Binding Mechanism - ADatP-4778 Edition A.

43 AEPD (2020) *Cifrado y Privacidad III: Cifrado Homomórfico* [en línea] Agencia Española de Protección de datos [Consulta: 10 de octubre de 2023]. Disponible en: https://www.aepd.es/prensa-y-comunicacion/blog/cifrado-privacidad-iii-cifrado-homomorfico

y efectiva y una capacidad de defensa autónoma, frente a toda forma de agresión: desde las estrategias híbridas (de baja intensidad o zona gris) hasta el conflicto convencional[44]. Es decir, es necesario contemplar la sincronización de acciones y efectos entre las capacidades militares y las del resto de poderes del Estado, desde las operaciones permanentes de las FAS en tiempo de paz[45], hasta el combate de alta intensidad. En consecuencia, las MDO deben incluir esta forma de acción integrada, alineándola con el principio de unidad de acción que orienta el funcionamiento del Sistema de Seguridad Nacional[46]. Este principio será de capital importancia en el ámbito ciberespacial para asegurar desde tiempo de paz, y en todos los ámbitos, la capacidad de combate de la Fuerza Conjunta, su sostenimiento y las infraestructuras y medios necesarios para su proyección.

La Estrategia Nacional de Ciberseguridad[47], clasifica las amenazas y desafíos en el ciberespacio en dos categorías: las que atacan activos en el ciberespacio y las que usan el ciberespacio para realizar actividades maliciosas de todo tipo. A ambos tipos pertenecen las que, aprovechando las avenidas de aproximación que ofrece el ciberespacio, pueden erosionar lenta y sigilosamente las capacidades de la Defensa Nacional, incluyendo las ya mencionadas de la Fuerza Conjunta.

La complejidad y amplitud del problema exige mecanismos de solución de amplio espectro. Es decir, orientados por los principios de la Seguridad Nacional y en el contexto de la Ciberseguridad, entendida como ámbito de especial interés para la Seguridad Nacional[48]. Ámbito que encuentra en la Ciberdefensa el área central de su espacio de intersección con la Defensa Nacional y con las capacidades de las FAS, pero que en sus bordes difusos alcanza otras infraestructuras, actores y capacidades. Esta es la Ciberseguridad con enfoque descendente; la que se define desde la perspectiva operativa en la Doctrina de Operaciones en el Ámbito Ciberespacial[49]; y la que más interesa desde la perspectiva conjunta y multidominio del problema que nos ocupa. Sin prescindir, claro está, del

44 Presidencia del Gobierno de España. (2021). *Estrategia de Seguridad Nacional 2021.* [En línea] Departamento de Seguridad Nacional, pp. 23, 53, 56 [Consulta: 23 de septiembre de 2023]. Disponible en: https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021

45 España. (2020). Real Decreto 521/2020, de 19 de mayo, por el que se establece la organización básica de las Fuerzas Armadas. Arts. 7 y 9.

46 PDC-01(A). *Op. cit*., nota 13, pp. 30, 94-96.

47 Presidencia del Gobierno de España. (2019). *Estrategia Nacional de Ciberseguridad* [en línea]. Departamento de Seguridad Nacional. pp. 10, 23-27 [Consulta: 23 de septiembre de 2023]. Disponible en: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

48 España. (2015). Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. Art,s. 4, 9 y 10.

49 PDC-3.20. *Op. cit*., nota 41, p. 4-B.

enfoque técnico de la ciberseguridad, el equivalente a seguridad CIS/TIC[50], ni de cualquier otro plano sobre el que pueda proyectarse el término ciberseguridad que, por su amplio alcance, no es un concepto o materia reconducible a un único título competencial[51].

El centro neural de esta forma de acción integrada se puede ubicar en el Consejo de Seguridad Nacional, órgano de dirección y gestión que constituye la piedra angular del Sistema de Seguridad Nacional y Gestión de Crisis[52], donde las FAS están representadas por el JEMAD. Descendiendo al ámbito de la Ciberseguridad, la acción integradora se coordina y desarrolla desde el Consejo Nacional de Ciberseguridad, donde las FAS están representadas por el comandante del Mando Conjunto del Ciberespacio que, a su vez, actúa en representación del JEMAD. En el nivel operacional de coordinación interministerial, el Mando Conjunto del Ciberespacio se integra en la Comisión Permanente de Ciberseguridad, que se Compone de los órganos y organismos representados en el Consejo Nacional de Ciberseguridad que tienen responsabilidades operativas[53].

El Mando Conjunto del Ciberespacio atiende a estas responsabilidades operativas en dos vertientes. Una es la de las operaciones militares propiamente dichas[54]. La otra, de mayor amplitud estratégica, es la de los operadores con incidencia en la Defensa Nacional, que debe contribuir a asegurar la capacidad de ejecución de las FAS, tanto desde la perspectiva del aseguramiento de las capacidades militares propiamente dichas, como desde la perspectiva del mantenimiento de un entorno operativo apropiado.

Para atender a esta segunda vertiente de responsabilidad, y en línea con su competencia estratégica para garantizar la libertad de acción en el ciberespacio, previniendo y actuando ante amenazas o agresiones que puedan afectar a la Defensa Nacional[55], el JEMAD cuenta con el ESPDEF-CERT del MCCE. Este CERT, es uno de los tres CSIRT[56] de referencia a escala

50 España. (2016). Instrucción 58/2016, de 28 de octubre, del Secretario de Estado de Defensa, por la que se aprueba la Arquitectura Global de Sistemas y Tecnologías de Información y Comunicaciones del Ministerio de Defensa. Apéndice II, Definiciones.

51 Tribunal Constitucional. (2023). Sentencia 10/2023, de 23 de febrero de 2023. Recurso de inconstitucionalidad 718-2020 [en línea]. *Boletín Oficial del Estado* [Consulta: 23 de septiembre de 2023] Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2023-8217

52 Estrategia de Seguridad Nacional 2021. *Op. cit*., nota 96, pp. 104-105.

53 Estrategia Nacional de Ciberseguridad. *Op. cit*., nota 99, pp. 61-65.

54 Real Decreto 521/2020. Art. 13. *Op. cit*., nota 98.

55 *Ibidem*. Art. 4.

56 *Computer Security Incident Response Team*, término empleado frecuentemente en Europa, equivalente a CERT (*Computer Emergency Response Team*), término registrado en EE. UU.

nacional y constituye la capacidad de respuesta e incidentes de seguridad para el ámbito de la Defensa Nacional[57]. En consecuencia, asume diversos cometidos entre los que, para la finalidad aquí analizada, destacan la supervisión y respuesta a incidentes a escala nacional, el análisis dinámico de riesgos e incidentes, el conocimiento de la situación y la alerta temprana[58], contribuyendo también al sistema de indicadores de seguridad nacional[59]. Cometidos que habitualmente ejecutará en relación con el Ministerio de Defensa y los operadores esenciales con Incidencia en la Defensa Nacional que reglamentariamente se determinen[60], en coordinación con los otros dos CSIRT de referencia nacional: el CCN-CERT y el INCIBE-CERT.

Por último, es imprescindible señalar la gran importancia de garantizar la seguridad de la cadena de suministro en un ámbito que, como el tecnológico, tanto depende de proveedores externos. Con tal fin, cobran especial valor las iniciativas para potenciar la Base Industrial y Tecnológica de la Defensa en el ámbito nacional; así como las iniciativas legislativas orientadas a impulsar la seguridad integral de nuestro ecosistema digital y a evitar la presencia de suministradores de riesgo. Como ejemplo de las primeras, se puede señalar el Foro Nacional de Ciberseguridad que, en el marco del Sistema de Seguridad Nacional, actúa en la potenciación y creación de sinergias público-privadas relativas a oportunidades, desafíos y amenazas a la seguridad en el ciberespacio[61]. Como ejemplo de las segundas, se puede señalar el Real Decreto-Ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación.

6. Conclusiones

La declaración del ciberespacio como ámbito de las operaciones militares debería haber supuesto un impulso transformador para un ámbito donde se intersecan líneas de evolución conceptual, doctrinal y de capacidad que seguían trayectorias bastante independientes, generando compartimentos estancos, entre los que se abrían peligrosas brechas de seguridad.

El éxito aparentemente limitado de dicho impulso, la subsistencia de brechas de seguridad difíciles de cerrar sin modificar sustancialmente un modelo excesivamente compartimentado, y la imposibilidad de establecer

57 España. (2022). Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Art. 33.
58 España. (2018). Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Arts 11 y 12.
59 Estrategia Nacional de Ciberseguridad. *Op. cit*., nota 99, pp. 13, 80, 107-108.
60 España. (2021). Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Arts. 4 y 15.
61 Estrategia Nacional de Ciberseguridad. *Op. cit*., nota 99, pp. 51, 64.

un modelo conceptual suficientemente robusto sobre las estructuras previas, parecen sugerir la necesidad de transformar la seguridad para garantizar el éxito de la TD para las MDO.

Dicha transformación debe simplificar las líneas normativas y doctrinales: asimilando la existencia e integridad del ámbito ciberespacial, con todas sus implicaciones operativas; centrando la SEGINFOSIT en la información propiamente dicha; integrando coherentemente todas las capacidades para operar en el ámbito ciberespacial, incluidas las disciplinas tradicionalmente orientadas al entorno electromagnético; estableciendo un marco conceptual coherente que permita abordar el problema de la seguridad desde un análisis de riesgo continuo, sistematizado y metodológico; y todo ello sin perder la perspectiva finalista de asegurar el cumplimiento de las misiones que se asignen a las FAS.

Las MDO solo son posibles si se dispone de una red de sistemas digitales que las sustenten. Por tanto, dicha red constituye su centro de gravedad y debe llevar la seguridad en su ADN.

En consecuencia, la Nube de Combate debe ser una capacidad genuinamente militar y responder a un modelo descentralizado, distribuido, mallado, autoconfigurable y autoreconfigurable, capaz de operar en entornos degradados, altamente móvil, y difícil de detectar. Debe ser un sistema de combate federado, agregable y segregable, en consecuencia, carente de un jefe único, y que no presente al adversario puntos de fallo críticos para toda la red.

La Nube de Combate no es una tecnología, es un paradigma de combate centrado en datos que se sustenta en múltiples tecnologías y permite entender la Fuerza como una red o nube de nodos digitalizados: sensores, decisores, efectores, etc.

Por consiguiente, la seguridad de la Nube de Combate también debe integrar múltiples modelos de seguridad y múltiples tecnologías, pero bajo una arquitectura coherente y flexible, que permita reconfigurar el espacio de batalla ciberespacial a medida de las necesidades operativas. Tecnologías de seguridad, tecnologías elegidas por su seguridad y tecnologías rechazadas por su inseguridad.

La seguridad CIS es necesaria, pero no suficiente. El éxito de las operaciones exige libertad de acción en el ámbito ciberespacial, y esta solo se puede alcanzar ejecutando también operaciones ISR, defensivas y ofensivas en el ciberespacio. Las operaciones de seguridad CIS son necesarias para el resto e inseparables de ellas, en tanto que permiten organizar el ciberterreno del espacio de batalla.

Por último, es fundamental integrar las MDO y la Ciberseguridad Nacional desde el nivel estratégico. En este sentido, el ESPDEF-CERT es clave para

el aseguramiento de las capacidades militares propiamente dichas y para el mantenimiento de un entorno operativo apropiado. Tampoco se debe olvidar la importancia de garantizar la seguridad de la cadena de suministro y de potenciar la base tecnológica nacional en un campo tan crítico.

Capítulo 5

El Mando y Control en el Entorno Operativo 2035: la transformación esencial en el camino hacia a una Fuerza Conjunta de 6.ª generación

Juan Ramón González Espadas

Resumen

El futuro entorno operativo exige dotarse de una Fuerza Conjunta, capacitada para el planeamiento y ejecución de operaciones militares en un entorno multidominio.

Un factor de éxito en dicha capacitación es la transformación del modelo actual de C2, solo posible determinando qué nos empuja a la misma, qué hay que cambiar, con qué fin y cómo llevarla a cabo, con el objetivo último de poner al servicio de quien tenga la responsabilidad de gestionar la batalla, un C2 único para todos los mandos componentes, con la agilidad necesaria para adaptarse a las necesidades que la dinámica del combate requiera y que garantice la superioridad en la información, en la toma de decisión y en la ejecución de la misión.

Palabras clave

Mando y Control descentralizado, Atribución de derechos de decisión, Patrón de interacciones, Distribución de la información, Cadena letal, Agilidad, Superioridad en la toma de decisión, Experto en Mando y Control de operaciones multidominio.

Comand and Control in the Operating Environment 2035. The essential transformation on the way of joint force of 6th generation

Abstract

The future operational environment requires a joint force capable of planning and executing military operations in a multi-domain environment.

A success factor in achieving this is the transformation of the current command and control model, which is only possible by identifying what drives us to it, what needs to be changed, for what purpose and how to be implemented, with the ultimate aim of putting at the service of those responsible for managing the battle, a single command and control for all component commands, with the necessary agility to adapt to the needs required by the dynamics of combat, and ensuring superiority in information, in decision making and in the execution of the mission.

Keywords

Decentralised Command and Control, Attribution of decision rights, Pattern of interactions, Distribution of information, Kill chain, Agility, Decision superiority, Multi-domain operations Command and Control expert.

US Air Force Commander, General David Goldfein:

"Whoever discovers how to quickly integrate information from different fields and with equal promptness order military actions, will achieve a decisive advantage in combat".

1. Introducción

La transformación digital de las FAS para el combate multidominio no es una opción, sino, por el contrario, es una transformación obligada por las características del entorno operativo futuro.

Los ámbitos de operación[1] físicos (terrestre, marítimo, aeroespacial) y no físicos (ciberespacial y cognitivo) siempre han estado ahí, y ha sido el desarrollo tecnológico lo que ha ido permitiendo su conquista y explotación por nuestras FAS, pero no olvidemos, también por los potenciales enemigos que ponen en riesgo nuestros intereses vitales y estratégicos.

Aun a pesar de la significativa evolución de mentalidad hacia la conveniencia y necesidad de operar conjuntamente, el esquema tradicional «mando componente/ámbito de actuación/ámbito de efectos» sigue estando muy presente en el planeamiento, control y ejecución de las operaciones militares.

Sin embargo, las nuevas tecnologías, es especial las denominadas EDT, nos permiten, hoy y en el futuro inmediato, plantear la ruptura de dicho esquema y abordar la problemática de la Fuerza Conjunta para hacer frente a las MDO, y que podría resumirse en: cómo aprovechar las ventajas que la hiperconectividad ofrece para mejorar el conocimiento global del escenario de combate y agilizar la decisión de qué acciones a realizar. Es seguro que la solución que se encuentre al problema planteado afectará a la doctrina, a la organización, a la infraestructura, a la preparación, al material, a la interoperabilidad e, indudablemente, al liderazgo de las personas.

Los capítulos previos de este trabajo de investigación han descrito los cambios transformacionales necesarios tanto en individuos como en organizaciones y las dificultades que hay que encarar; la necesaria conexión entre todos los elementos que intervienen de forma directa o indirecta en el campo de batalla; el elemento que tecnológicamente facilitará la globalización del dato; y, por último, el reto que implica, en el entorno multidominio, lograr la seguridad del mismo y de la información derivada.

Todo ello dirigido a un objetivo final: la toma de decisión, facultad intrínseca a la función de *Mando y Control (C2).*

A través de los Planes de Adquisición de la Defensa disponemos de unos medios de ISR más sofisticados y precisos y nos dotamos de sistemas de combate más letales. Sin cuestionar su necesidad, lo cierto es que de poco valdrían esas extraordinarias capacidades para lograr el éxito de las operaciones militares sin una estructura, organización y procedimientos de C2 adaptables en cada momento a las exigencias del entorno de combate

[1] Terrestre, marítimo, aeroespacial, ciberespacial y cognitivo, según la (PDC-01 (A).

futuro, un C2 más ágil que el del enemigo que, mediante la superioridad en la toma de decisión, permita lograr alcanzar la superioridad en la ejecución.

Como potencial respuesta a esta necesidad surge el concepto *Joint All-Domain Command and Control* (JADC2), definido en el documento *USAF role in Joint All-Domain Operations* (March 2020) como «[...] el arte y la ciencia de la toma de decisiones para traducir rápidamente las decisiones en acciones, aprovechando las capacidades en todos los dominios para lograr una ventaja operativa y de información tanto en competición como en conflicto».

Este capítulo, sustentado en las principales ideas vertidas en diferentes estudios, pretende fomentar el pensamiento crítico sobre porqué, qué, para qué y cómo transformar el C2 de nuestra Fuerza Conjunta para afrontar los ámbitos de actuación en los que muy probablemente operará en 2035.

2. El marco de referencia: conceptos clave

Antes de proceder al desarrollo del contenido del capítulo es necesario fijar una serie de conceptos que permitan a autor y lector partir de un entendimiento común.

En línea con la opinión de diferentes Grupos de Investigación de la OTAN (SAS - *System Analysis and Studies Panel*) encuadrados dentro del NATO *Science and Technology Organization*, se entiende el *C2* como una función que asigna derechos de decisión, la configuración de los procesos de toma de decisiones y los procesos que adquieren, gestionan, comparten y explotan la información en apoyo de la toma de decisiones individuales y colectivas para el cumplimiento de una empresa.

La realización de las funciones asociadas con el C2 sirve para utilizar, de manera oportuna, eficaz y eficiente, toda la información y los activos disponibles necesarios para tener éxito en el cumplimiento de las operaciones militares.

En España, el *término multidominio* nace para entender el entorno operativo al que se enfrentan las FAS, y se define como «[...] un entorno de actuación muy complejo, que engloba a todos los ámbitos de operación, con una gran interdependencia e interacción entre todos ellos (bien sean físicos o no físicos)»[2].

La doctrina nacional define las *Multi-Domain Operations (MDO)* como:

> «[...] aquellas operaciones realizadas por la Fuerza Conjunta que, por su agilidad y complejidad, necesitan de una adecuada

[2] PDC-00 Glosario de Terminología de Uso Conjunto. Julio 2021.

> interoperabilidad y conectividad que posibiliten un control distribuido de los medios para permitir la mejor concentración e integración de todas sus capacidades con criterio de oportunidad y así poder producir efectos en y desde cualquiera de los ámbitos de operación»[3].

Control distribuido[4] debe entenderse como una estructura de control en la que ciertas responsabilidades y competencias son delegadas desde los niveles superiores, limitadas en tiempo y lugar, y de acuerdo con criterios preestablecidos.

De los *contextos operativos* identificados en «Entorno Operativo 2035 Primera revisión», el capítulo pone el foco de atención en el Contexto Operativo (CO) 1: de Defensa Militar (disuasión, vigilancia, prevención y respuesta) por las siguientes razones:

1) Porque es el principal contexto operativo de actuación y en el que las Fuerzas Armadas desarrollan su misión primordial.
2) Porque en este contexto la capacidad de defensa autónoma, incluido el C2, es imprescindible.
3) Porque las operaciones y misiones que en él se lleven a cabo van a realizarse tanto en los ámbitos de operación terrestre, marítimo y aeroespacial, como además transversalmente en el ciberespacial y el cognitivo, adoptando generalmente una naturaleza multidominio.
4) Por su ámbito geográfico de aplicación, que es el comprendido por el territorio nacional, así como las áreas marítimas y aeroespaciales de interés prioritario para la seguridad nacional y que al contar con dos archipiélagos separados de la península y plazas de soberanía en el norte de África hacen esencial mantener una situación militar favorable.

En el hipotético caso de que se produjera una agresión contra la soberanía nacional, no sería descartable un escenario de alta intensidad, el establecimiento de una condición A2/AD[5] y el hostigamiento de las comunicaciones marítimas y aéreas. La amenaza a nuestra estructura de C2 considerada más probable en esta hipótesis es que los esfuerzos del enemigo se centren en degradar o interrumpir el flujo de información desde los nodos de información y los sistemas de combate, distorsionar las redes de comunicación establecidas y alterar la calidad de la información para ralentizar la toma de decisión o provocar que esta sea equivocada. En otras palabras,

[3] *Ibid.*
[4] A lo largo del capítulo se utilizan indistintamente los términos distribuido y descentralizado como contrapartida al término centralizado.
[5] Del inglés *Anti-Access Area Denial.*

gran parte de su actuación tendría lugar desde el ámbito ciberespacial y, no tanto, desde los ámbitos físicos de operación desde donde generar un efecto cinético en las instalaciones.

Es dentro del marco descrito en los párrafos anteriores en el que se aborda la transformación del modelo de C2.

3. El Mando y Control en el Sistema de Combate Futuro

El sistema de combate del futuro ha de ser la combinación e integración de la capacidad de recolectar datos, de explotar los mismos para generar la información pertinente, de elaborar las alternativas para la toma de decisión y de disponer de los efectores más adecuados para conseguir las condiciones finales deseadas, con el objetivo de obtener en el momento preciso la superioridad de información, decisión y ejecución sobre el enemigo en el entorno multidominio.

Una representación gráfica de lo anterior y que relaciona ambiciones, impacto en las actividades, capacidades operacionales requeridas y tecnología necesaria es la siguiente (véase imagen 1).

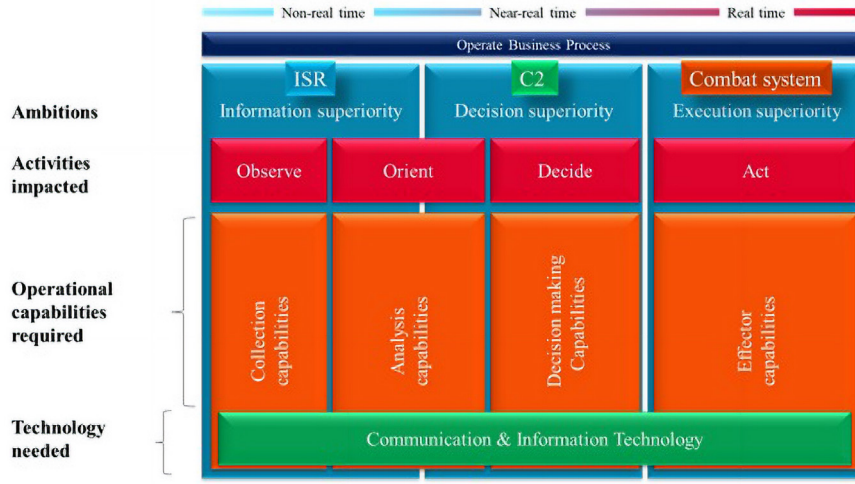


Imagen 1. Fuente: elaboración propia

La superioridad de la información se consigue ganando la batalla del dato, o lo que es lo mismo, capturar el que se necesita en tiempo, forma y lugar, y negárselo al enemigo. La superioridad en la decisión se logra por la óptima explotación de dichos datos a través de unos algoritmos que ofrezcan, al que tiene la responsabilidad de decidir y más rápido de lo que pueda hacerlo el enemigo, un elenco de opciones fiables para ganar la batalla. La superioridad en la ejecución se obtiene al combinar óptimamente las

capacidades de combate de los efectores, sea cual sea su ámbito de operación, para lograr infligir en el enemigo el efecto deseado, sea este físico, virtual o cognitivo.

La piedra angular del sistema de combate futuro es el C2, ya que es esta función, con independencia del nivel considerado (los clásicos estratégico, operacional y táctico), donde se decide qué información se necesita, cómo obtenerla, quién la necesita y en qué momento, con qué fin y, por último, qué acciones han de llevarse a cabo para alcanzar este.

Si relacionamos la función de C2 con el ciclo de decisión (*OODA*), aquella engloba tres de los cuatro elementos de dicho ciclo: observar, orientar y decidir. El último elemento, actuar, no es parte del C2, sino el resultado del mismo.

Mandar y Controlar es gestionar óptimamente la batalla y la misión asignada y constituye el factor decisivo para lograr la victoria. Nada nuevo, pero que hoy y en el futuro requiere una capacidad esencial, la *agilidad***,** entendida como la capacidad de efectuar, afrontar o explotar con éxito cambios en las circunstancias en el campo de batalla[6].

El C2 de la Fuerza Conjunta en el entorno multidominio requiere satisfacer dos ambiciones operacionales imperativas:

1) Tener una visibilidad global del escenario del conflicto (superioridad en la información y observar).
2) Aumentar la agilidad en la identificación de las posibles acciones a realizar (superioridad en la toma de decisión, orientar y decidir).

4. ¿Por qué transformar el Mando y Control?

Destacan tres factores que obligan a transformar el actual modelo de C2.

El *primer factor* es que *las características del escenario de combate* en los que ejercer el C2 para la gestión de la batalla (*battle management)* han mutado significativamente si comparamos los tiempos de la Guerra Fría con los del siglo en curso.

Publicado en el año 2006, David S. Alberts y Richard E. Hayes en el documento titulado *Understanding Command & Control* describen esta situación mediante la siguiente figura (véase figura 1).

Capítulo 5 Figura 1

Figura 1. Tipos de C2. *Fuente:* Alberts, D. y Hayes, R. (2006). *Understanding Command & Control.*

[6] OTAN. (2014). *SAS-085 Final report on C2 Agility (Studies, Analysis and Simulation Panel Group).*

Según estos autores, tres dimensiones y su consiguiente variabilidad determinan las características del escenario de combate en el que el comandante, desde el nivel estratégico al nivel táctico, ha de tomar su decisión.

Indican que, comparando los escenarios operacionales de la Guerra Fría con los del siglo XXI, estos últimos se caracterizan por la alta velocidad con que cambian las circunstancias que los enmarcan: militares, políticas, sociales y económicas (*rate of change*); por la incertidumbre y falta de anticipación sobre qué información se necesita acorde a la dinámica de la situación y sobre quién la necesita (*familiarity*); y por la inseguridad de que la información pertinente llegue a la entidad relevante en el desarrollo de las operaciones militares (*strength of information position*).

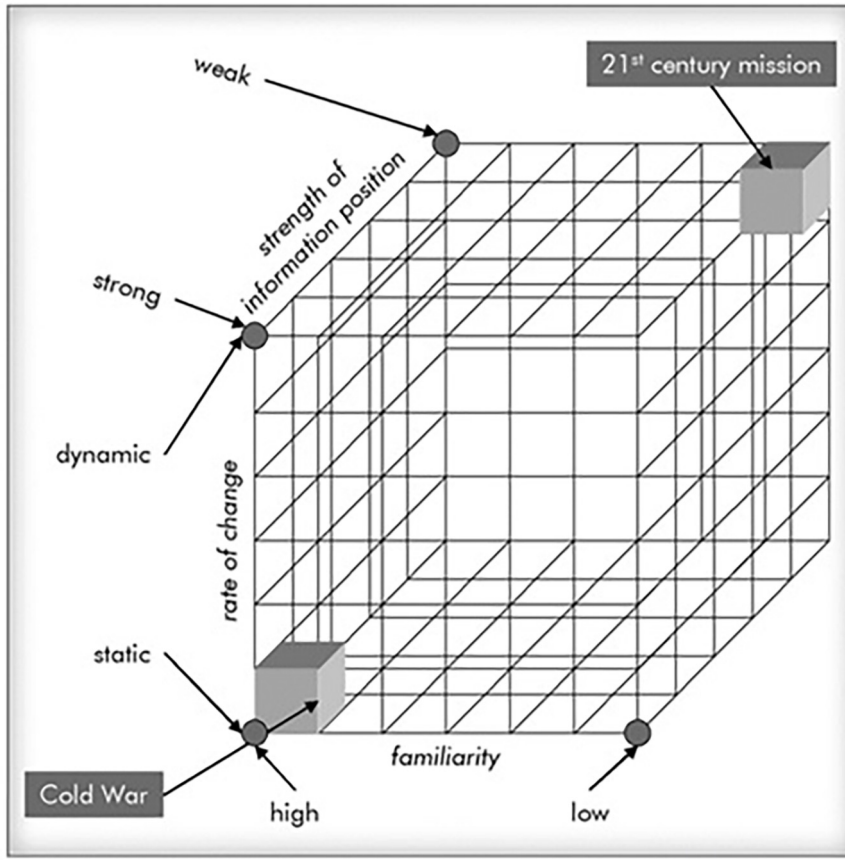


Figura 1. Tipos de C2. Fuente: Alberts, D. y Hayes, R. (2006). Understanding Command & Control.
Según estos autores, tres dimensiones y su consiguiente variabilidad determinan las características del escenario de combate en el que el comandante, desde el nivel estratégico al nivel táctico, ha de tomar su decisión

Pasados casi 20 años desde la fecha de su publicación ¿Se dan estas circunstancias en los ámbitos de actuación en los que nuestras FAS muy probablemente operarán en 2035 para proteger y garantizar los intereses nacionales?

La respuesta es sí. Las principales características del entorno operativo presente y futuro en el que ejercer el C2 de la Fuerza Conjunta quedan recogidas en el modelo «VUCA incrementado (VUCAH)»[7] y en él fácilmente puede reconocerse la variabilidad de las dimensiones descritas por David S. Alberts y Richard E. Hayes.

La actual arquitectura de C2, su infraestructura, sus procedimientos, sus procesos, su tecnología y su recurso humano han logrado hasta ahora adaptarse al cambio a través de diversos programas de actualización, pero la evolución del entorno futuro requiere un cambió más radical para poder dar respuesta a las nuevas demandas del combate.

El *segundo factor* para transformar el C2 es que, aun cuando nuestras FAS tienen unos *medios de combate* con mejores capacidades que en el pasado, *su número se ha reducido significativamente*, lo que obliga a desarrollar los mecanismos necesarios para hacer un uso flexible de la «masa de combate» disponible con independencia de su dominio de actuación.

Tener menos sensores y efectores obliga a utilizarlos más eficientemente, determinar qué utilizar, cuándo, cómo y para qué, lo que lleva a la necesidad de tener una consciencia situacional en tiempo real no solo de la amenaza, sino de las fuerzas propias.

El *tercer factor* es que el relativamente fácil acceso de los potenciales adversarios a *capacidades de combate en el ámbito ciberespacial* les permite desarrollar contramedidas que obstaculicen o incluso lleguen a colapsar la función de C2. Las operaciones desde este ámbito representan quizás la máxima expresión de ambigüedad e incertidumbre. Por otro lado, la razón coste-efecto de las operaciones efectuadas desde el ciberespacio puede ser muy baja y las consecuencias en la gestión de la batalla pueden ser decisivas en el resultado final.

Llevado al extremo, no será necesario al enemigo ejecutar operaciones desde los entornos físicos con el fin de infligir un efecto cinemático (*hard kill*) en nuestras infraestructuras de C2, ni causar un índice de atrición elevado en la fuerza de combate, sino que le bastará dificultar el acceso al dato o alterar el mismo para impedir que obtengamos la correcta visión global del escenario del conflicto, comprometer así la agilidad del ciclo de

[7] VUCAH: *Volatility, Uncertainty, Complexity, Ambiguity and Hyperconnectivity*.

decisión y, finalmente, negar la superioridad en la ejecución aun cuando dispongamos de sistemas de combate más capaces.

Hay motivos para revisar el modelo de C2 de hoy con la vista puesta en el futuro, ante la siempre posible y probable existencia de un conflicto convencional y la necesidad cada vez mayor de hacer creíbles los mecanismos de disuasión, ya sea para enfrentarse a la amenaza colectiva a través de los compromisos adquiridos por la pertenencia a Organizaciones Internacionales de Seguridad y Defensa (Contexto Operativo 2: De proyección de estabilidad en el exterior); o bien para oponerse autónomamente a adversarios regionales - estatales o no - en espacios no estructurados (Contexto Operativo 1: De Defensa Militar y Contexto Operativo 3: De seguridad y bienestar de los ciudadanos).

5. ¿Qué transformar en el Mando y Control?

Encontradas las razones por las que es necesario transformar el C2, es el turno de explorar dónde incidir para delinear qué modelo es el más conveniente para afrontar el entorno operativo 2035.

Tres variables (Alberts and Hayes, 2006) definen su morfología:

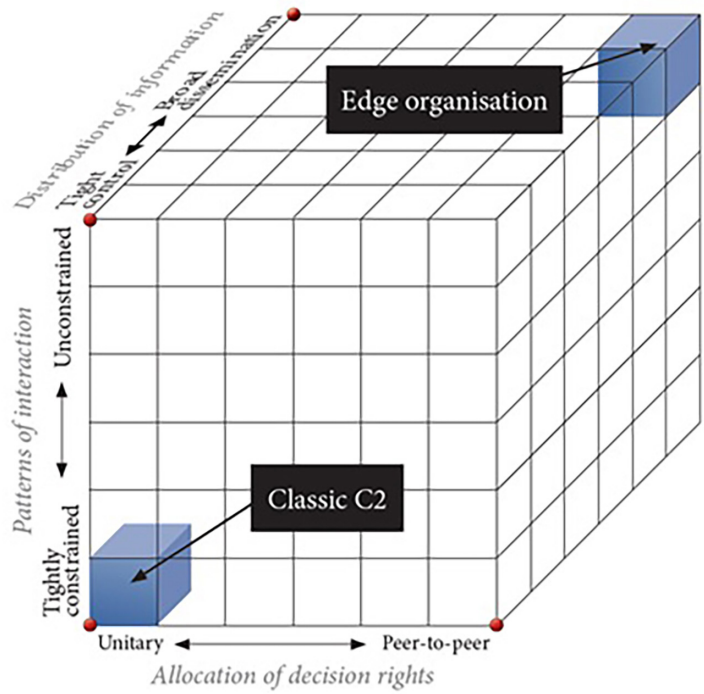


Figura 2. Modelos de C2. Fuente: Alberts, D. y Hayes, R. (2006). Understanding Command & Control

La primera de ellas y con mayor influencia es la «atribución de derechos de decisión» *(Allocation of decision rights)* y se refiere a la autoridad de un individuo u organización para elegir una opción entre las alternativas disponibles sobre un asunto particular en determinadas circunstancias y condiciones. Es condición *sine qua non* para asumir la responsabilidad del *battle management*, en último extremo por el combatiente en primera línea en el campo de batalla, que el individuo u organización sea competente para ello. Propósito, entre otros, del Plan de Acción para la Transformación Digital del Ministerio de Defensa, al incorporar acciones encaminadas al cambio de mentalidad y desarrollo de habilidades en el ámbito de las personas y de la organización, ya que en caso contrario la delegación es fallida.

La segunda es el «patrón de interacciones» *(Pattern of interactions)*, referida al número y variedad de participantes en la estructura de C2, a la calidad de la información que comparten y al grado de interacción entre ellos desarrollado, asunto este último, condicionado por el tipo de estructura de red que se considere[8]. Está íntimamente relacionada con la necesidad de nuevos modelos de organización y el concepto de redarquía, ambos tratados en el capítulo 1[9].

La última variable es la «distribución de la información» *(Distribution of information*) y se refiere al proceso del C2, por el cual se hace llegar la información relevante y segura, en el momento oportuno y a la entidad pertinente. Está impactada tanto por la atribución de derechos de decisión como por el patrón de interacciones; pero también por la voluntad de compartir la información, por la voluntad de querer adquirirla, por las herramientas y habilidades de las entidades para acceder a ella y por la habilidad de colaborar. Tiene, por tanto, un componente técnico, pero también una significativa influencia del factor humano y las formas de trabajo que se establezcan entre los individuos de las organizaciones a las que pertenecen.

---

8 Alberts D S. y Hayes R E. identifican en *Understanding Command & Control* cuatro tipos posibles de red en la Era de la Información: *fully connected networks, random networks, scale-free networks y small world networks*. En su opinión, la estructura de red más eficaz, efectiva y resiliente en un entorno multidimensional es una combinación de todas ellas: a nivel global *fully connected networks*, a nivel intermedio *scale-free networks* y a nivel local *small world networks*.

9 Redarquía es un cambio de paradigma organizacional. Apuesta por un modelo organizativo colaborativo que emerge en la era de la agilidad aumentando la capacidad de adaptación y colaboración de toda la estructura, con la finalidad de coordinar los esfuerzos de los miembros de la organización para alcanzar los objetivos marcados. La redarquía se basa en una estructura en red, en la conectividad, dejando paso a la iniciativa y colaboración de las personas que forman parte de la organización. Se centra en el futuro y en las nuevas oportunidades que este presenta. Se basa en la confianza y en el valor añadido, y entiende a los empleados como agentes movilizadores del cambio.

Las características de la «solución clásica» de C2, que ha permitido hacer frente con éxito a unos contextos operativos estáticos, propios de la Guerra Fría, son la centralización de la toma de decisión, una rígida relación entre los actores que participan en la ejecución de las operaciones militares y una férrea gestión y distribución de la información. Es decir, se trata de un concepto tradicional de mando centralizado que depende de un canal de información estable entre los sistemas de combate y el nodo central de C2.

Quizás podamos ver reflejado en esta solución clásica nuestro modelo. El talón de Aquiles de esta solución es que la rigidez para dar respuesta a las nuevas circunstancias del entorno operativo (VUCAH), al insuficiente número de sistemas de combate y la amenaza ciberespacial, podría invalidarla para cumplimentar el conjunto de funciones que lleve a generar en el enemigo el efecto deseado.

Es necesario, por tanto, explorar qué medidas ayudarán a adaptar y adoptar la óptima combinación de atribución de derechos de decisión, de patrón de interacciones y de distribución de información que mejor responda a las circunstancias y necesidades operativas que el futuro entorno de combate requiere.

El reto que se plantea es dotarse de la capacidad para migrar desde un modelo único de C2 válido para todas las situaciones (*one-size fits all*) pero individualizado para cada mando componente, condición presente, a un conjunto de opciones de C2 común a todas las FAS que permitan, dinámicamente, seleccionar de entre todas ellas el modelo más conveniente en función de la coyuntura de las operaciones militares.

6. ¿Para qué transformar el Mando y Control?

El C2 no es un fin en sí mismo, sino uno de los medios esenciales para cumplir una misión o tarea.

Es necesario transformar el C2 para dotarlo de la capacidad de efectuar, afrontar o explotar con éxito cambios en las circunstancias en el campo de batalla, en definitiva, *de agilidad para adaptar y ejecutar una cadena letal más eficaz y resistente*.

Las Fuerzas Aéreas han utilizado el método de *find, fix, track, target, engage, assess* (F2T2EA) para describir la cadena letal desde finales de los 90 y sigue siendo un modelo útil para explicar los distintos pasos a ejecutar y cómo estos se referencian a los sensores físicos, plataformas u otras capacidades necesarias para lograr efectos en el espacio de batalla.

Para dar respuesta a los retos planteados, la cadena letal en el entorno operativo 2035 debe reunir cuatro atributos:

- *Escalabilidad:* referida como la capacidad para incrementar el número de cadenas letales que simultáneamente pueden ser ejecutadas mediante la adecuada combinación de los medios de combate en servicio, a los que habrá que dotar de la necesaria conectividad e interoperabilidad.
- *Alcance:* entendido como la distancia, el área y la duración a la que la cadena letal puede ser realizada, lo que conlleva una concepción expedicionaria de la Fuerza debido a nuestro escenario geoestratégico.
- *Velocidad:* concebida como la habilidad para materializar la cadena letal antes de que las acciones del enemigo tengan efectos sobre la misma, velocidad no solo aplicable a efectores, sino al tratamiento, gestión y transmisión de datos e información.
- *Supervivencia:* en alusión a la capacidad para mantener la integridad y efectividad de la cadena letal, incluso cuando está siendo atacada y que conduce al concepto de cadena letal web (*kill web*).

Existe el riesgo de que, en el futuro inmediato, la hasta ahora exitosa ejecución de funciones concatenadas y que llevaba a producir en el enemigo el efecto deseado, o bien no puede completarse o, de hacerlo, no con la rapidez necesaria, lo que hace ineficiente el empleo de los medios disponibles, por muy modernas capacidades de combate que estos dispongan. Es por ello por lo que sensores, plataformas, armamento y sistema de C2 no pueden desacoplar su evolución y deben todos ellos encuadrarse en la más avanzada generación posible.

El objetivo de la transformación del C2 es proteger y explotar, eficaz y eficientemente, la componente física (sensores, *data links*, plataformas y armamento) y la componente informativa del proceso para ganar la competición por la cadena letal, garantizar que la cadena *sensor-to-shooter* se acelere, mantenga su integridad y cierre el ciclo antes de que el enemigo lo haga. Si no es así, no se alcanza la victoria.

Es necesario reflexionar sobre el hecho de que, de mantener el esquema tradicional «*mando componente-ámbito de actuación-ámbito de efectos*», unido a un inventario cada vez más reducido de medios de combate, puede conllevar que la pérdida de alguno impida la ejecución de algunos de los pasos de la cadena letal (F2T2EA), o bien que no se disponga de la masa crítica de combate que puntual y temporalmente sea necesaria. Todo ello debilita la robustez e integridad de la cadena letal.

Asimismo, al disponer de un menor número de medios, no explotar las sinergias de sus capacidades merma la escalabilidad de las acciones en curso con el fin de aumentar la presión sobre el enemigo.

Por lo tanto, es sustancial la concienciación a nivel estratégico, operacional y táctico de que los ámbitos de operación no son estancos y que los

sistemas de combate, que en cada uno de ellos opera, pueden generar el efecto deseado en cualquiera de los otros; y así, mitigar los riesgos a la integridad de la cadena letal y facilitar alcanzar la escalabilidad, alcance, velocidad y supervivencia que esta precisa.

La transformación del C2 es necesaria para dotarla de agilidad. Conlleva mutar de un C2 a nivel componente a un único C2 multidominio como objetivo último, donde, recordemos, al dictado de las circunstancias del combate se adaptan dinámicamente quién decide, con quién interactúa y qué información precisa. Este nuevo paradigma demanda significativos cambios en la organización, formación, material, liderazgo, personal, instalaciones e interoperabilidad.

Puede ser de ayuda para entender el para qué del cambio, el trabajo realizado por el SAS-065 NATO NEC C2 Maturity Model Approaches, en el cual se representan en cubos de colores diferentes modelos de C2 coherentes, en el sentido de que la distribución de la información y el patrón de interacciones apoyan la atribución de derechos de decisión deseada.

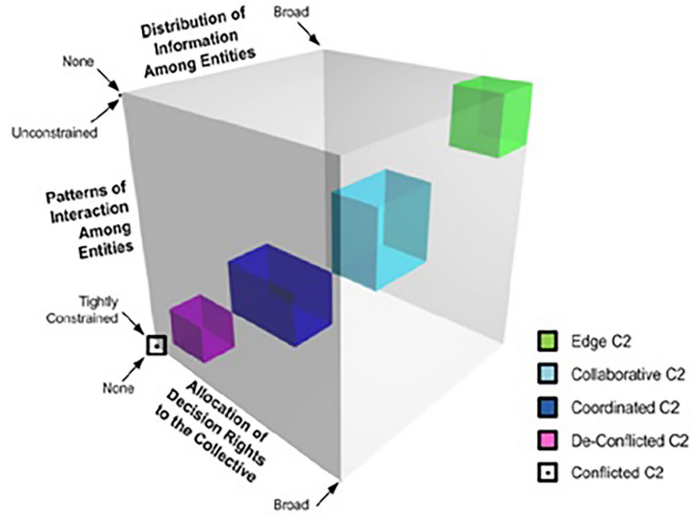


Figura 3. Coherencia de modelos de C2.
Fuente: SAS-065 NATO NEC C2 Maturity Model Approaches

Un C2 ágil significa que, en función de las necesidades operativas, se puede adoptar uno o más de los enfoques (agilidad de la solución), que se puede añadir enfoques adicionales o que se dispone de la habilidad para moverse adecuadamente entre varios de los enfoques.

Elementos facilitadores de la agilidad son la versatilidad, la flexibilidad, la adaptabilidad, la innovación, la resiliencia y la capacidad de respuesta, los cuales residen en las características y capacidades del sistema, de los

procesos, de la organización y, fundamentalmente, de los individuos que constituyen el C2 en su conjunto.

El estado final deseado es cambiar desde un modelo de C2 independiente por servicio y único para todas las coyunturas del entorno de combate (*one-size fits all*), a una condición en la que se dispone de una «caja de herramientas» donde escoger la aproximación de C2 multidominio, común para todos los servicios, más adaptada a la dinámica de la situación.

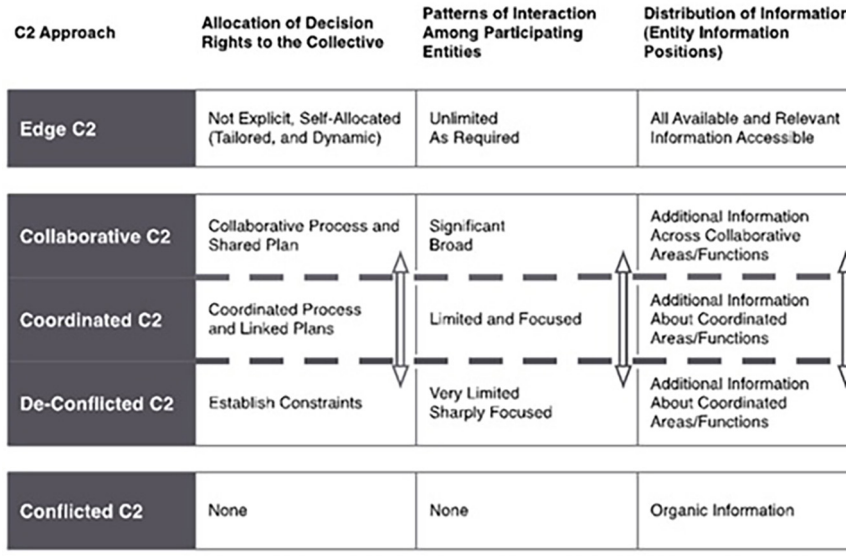


Figura 4. Factores y variables a considerar en los modelos de C2. Fuente: SAS-065 NATO NEC C2 Maturity Model Approaches

La siguiente tabla permite vislumbrar la dimensión de la transformación del C2 de la Fuerza Conjunta en función de la variabilidad de los factores considerados.

Cómo iniciar el camino de la transformación es lo que aborda el siguiente apartado.

7. ¿Cómo transformar el Mando y Control?

Con la realidad que impone el potencial militar, económico, industrial y tecnológico de nuestra nación, y teniendo presente el horizonte temporal 2035 para la gestión de lo que se ambicione, es necesario adoptar medidas en los cuatro ámbitos del C2: físico, de la información, cognitivo y social.

Incrementar el número de nodos de C2 es una de dichas medidas. Focalizada a la mitigación de la potencial vulnerabilidad de las infraestructuras frente a

la amenaza contemplada en el contexto operativo de referencia, incide en el ámbito físico y de la información.

Actualmente, cada servicio dispone de su propio sistema de C2 con capacidades redundantes para garantizar el cumplimiento de su función. Sin embargo, la entrada en escena de las operaciones militares desde el ciberespacio es un cambio de paradigma y lo que ha sido válido hasta ahora para asegurar la integridad de la cadena letal pudiera no ser suficiente en el futuro inmediato.

Las condiciones del escenario operativo 2035 obligan a dotarse de más nodos de C2, lo que conduce a reconsiderar uno de los principios clave de la doctrina OTAN para lograr la unidad de esfuerzo[10]: el control centralizado de las operaciones aéreas. Hoy se plantea abiertamente su descentralización o distribución.

La idea fuerza tras ello es poder ejercer la función de C2 allí donde sea necesario, desde las instalaciones «bunkerizadas» de un Cuartel General al combatiente en primera línea.

El grado de descentralización requerido del C2 de la Fuerza Conjunta dependerá de las circunstancias del campo de batalla. Cuanto mayor sea el nivel de conciencia situacional, mayor sea el volumen de operaciones y el grado de concurrencia, mayor sea la incertidumbre de la misión o el grado de interacción entre operadores tácticos, en especial de otros servicios, y mayor sea el grado de fragmentación del marco espacio-temporal impuesto o permitido por el contexto operativo y el tipo de misión bajo consideración, más necesaria es la distribución del C2. Por el contrario, cuantas más operaciones se basen en parámetros relativamente bien establecidos (entorno, amenazas, etc.) que puedan planificarse a tiempo, menos distribución parece necesaria.

Incrementar el número de nodos de C2 precisa cumplir *dos condiciones clave.* La primera es *la disponibilidad de nuevas tecnologías*. Estas juegan un papel fundamental en la migración hacia un control distribuido, al poner al servicio de la función de C2 los avances necesarios para *ganar la batalla del dato*, explotar de forma «inteligente» la ingente cantidad que de estos disponemos a través de los algoritmos más convenientes y facilitar la toma de la decisión correcta en el momento preciso.

Tecnologías como el IoT, la robótica, la realidad mixta (realidad virtual y realidad aumentada), la IA, el *big data* o el procesamiento o computación en

[10] El AJP-3.3 *Allied Joint Doctrine for Air and Space Operations* Edition B Version 1 April 2016 señala, entre los principios básicos necesarios para lograr una unidad de esfuerzo robusta, la unidad de mando, el control centralizado y la ejecución descentralizada.

la nube son, entre otros, factores multiplicadores que proporcionarán al combatiente superioridad en la información, en la toma de decisión y en la ejecución.

La claridad de concepto en lo que se refiere al porqué de la necesidad de las EDT, con qué fin emplearlas, por quién, cuándo, dónde y cómo, será la clave del éxito en la TD de la función de C2.

De entre las tecnologías emergentes, la 5G es el catalizador tecnológico en la TD del Ministerio de Defensa y en la transformación de la Fuerza Conjunta, al proporcionar soluciones óptimas para habilitar e integrar el empleo de las tecnologías mencionadas[11].

Figura 5. EDT en el Entorno Operativo 2035. Fuente: elaboración propia

Así se recoge en el siguiente gráfico (véase figura 6), publicado en la Resolución 307/08135/21, de 17 de mayo de 2021, de la Secretaría de Estado de Defensa, que establece la estrategia de comunicaciones móviles de quinta generación (Estrategia 5G) del Ministerio de Defensa.

[11] En el capítulo 4 se abordan extensamente aspectos relacionados con la seguridad y la ciberdefensa.

Las redes 5G se articulan como una infraestructura habilitadora y potencialmente necesaria para la consecución de las capacidades NEC (*Network Enabled Capabilities*) de la forma más eficiente posible proporcionando, además de los tradicionales servicios de voz, vídeo y datos; nuevos servicios como la integración masiva de dispositivos y sensores (*massive Machine Type Communications*, mMTC); servicios fiables y de baja latencia (*Ultra-Reliable and Low Latency Communications*, URLLC) para habilitar procesos de decisión más ágiles, dinámicos y descentralizados; e incrementar la interoperabilidad y agilidad en la información y el conocimiento compartido en tiempo real, a través de comunicaciones de gran ancho de banda (*enhanced Mobile BroadBand,* eMBB).

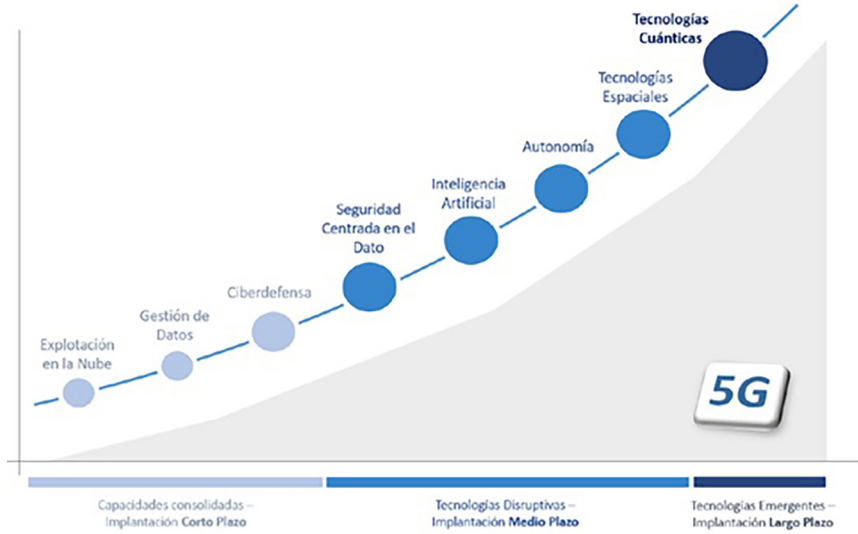


Figura 6. Estrategia de comunicaciones móviles de quinta generación. Fuente: resolución 307/08135/21, de 17 de mayo de 2021, de la Secretaría de Estado de Defensa

No cabe duda de que las EDT son esenciales en la definición de las potenciales morfologías del C2, por las posibilidades que abren en cuanto a cómo distribuir la información, a la habilitación de nuevas formas de interactuar y al aumento de las opciones de delegación de responsabilidad.

Sin que se entienda como exclusivo, el mapa de relevancia de las EDT en su potencial contribución al desarrollo de las capacidades asociadas para lograr la superioridad en la información, toma de decisión y ejecución podría ser el siguiente (véase figura 7).

La segunda condición para incrementar los nodos de C2 *es la integración de las nuevas tecnologías en los sistemas de combate en servicio y en los de nueva adquisición*. La visión de dispositivos inteligentes, ciudades

inteligentes o bases militares inteligentes requiere que los objetos y dispositivos incorporen sensores e inteligencia para detectar y tomar decisiones sin intervención humana sobre tareas complejas hasta el nivel que se decida, de ejecución inmediata, basadas en flujos de trabajo complejos. Las máquinas (dispositivos, objetos...) tendrán la capacidad de comunicarse en tiempo real con el resto de los objetos que conforman el ecosistema tecnológico en proximidad, generando un entorno colaborativo que permita alcanzar la superioridad en la ejecución.

Figura 7. Agility in Combat Operations. Fuente: elaboración propia

Las capacidades de los efectores (por ejemplo, *performances* de la plataforma, características de los sensores y equipos de comunicación, armamento) no son suficientes por sí solos para lograr el tan demandado combate colaborativo, sino que se precisa de elementos que faciliten este en busca de la superioridad en la ejecución, que dependiendo de las circunstancias comporta la descentralización del C2. Esta idea es lo que pretende representar el siguiente gráfico.

La implementación de nuevas capacidades operativas en los sistemas de combate actuales, a través de programas de actualización, y la definición de los requisitos en los futuros han de asegurar que concurren las condiciones necesarias para asumir la responsabilidad de la gestión de la batalla, la función del C2, allí donde esta se delegue. Sin pretender ser exhaustivo, se debe ser capaz de poder:

— Evaluar el riesgo de la misión en relación con la amenaza y el entorno, actividad esencial en el ciclo de toma de decisión.

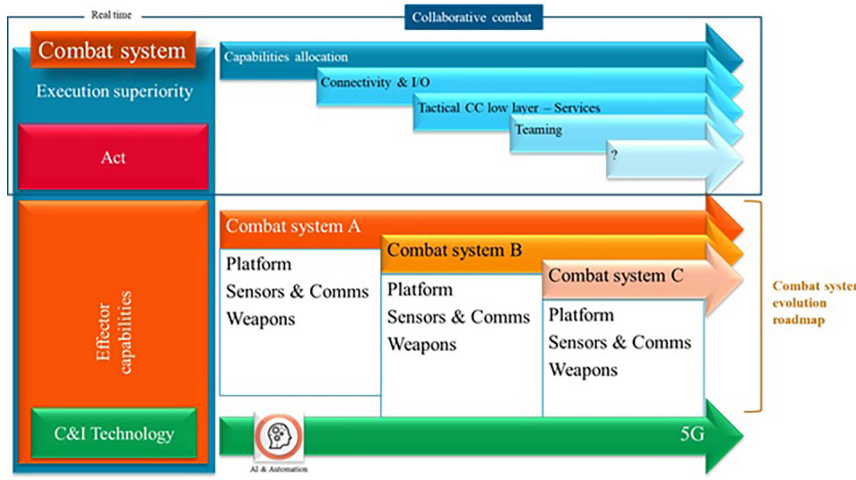


Figura 8. Elementos que alteran la capacidad de los efectores. Fuente: elaboración propia

— Definir y priorizar las misiones tácticas (objetivos y tareas) a realizar por los medios bajo control, en el marco de la autoridad otorgada dentro del espacio-tiempo establecido.

— Definir y priorizar los objetivos a asignar y los efectos tácticos directos a conseguir.

— Asignar las misiones a los medios bajo control.

— Determinar las tareas a realizar por medios bajo control.

— Impartir órdenes a los medios bajo control.

— Dirigir la ejecución de las misiones y tareas.

— Evaluar la ejecución de estas misiones y tareas.

Las mencionadas capacidades permiten la evolución del concepto tradicional de C2, haciendo cada vez más accesible la información de niveles superiores a nivel de combatiente, de modo que los directores de batalla, hoy actuando desde dominios separados, pero en el futuro actuando como directores de batalla multidominio, situados en la vanguardia de los enfrentamientos con las fuerzas enemigas serán el elemento clave para identificar, componer y gestionar cadenas letales desagregadas, capaces de responder a la velocidad y escala necesarias.

Un cambio importante es entender que, aunque la descentralización suele plantearse verticalmente en forma de delegación de autoridad a uno o varios nodos tácticos subordinados de un componente (en cualquier ámbito de operación), puede resultar igual de necesaria en sentido horizontal, en

el contexto de la integración aire-superficie, lo que nos lleva a la transferencia de autoridad entre componentes, en plena aplicación de los conceptos de MDO.

Es imperativo una estrecha coordinación y alineamiento entre las actuaciones encaminadas a la transformación del C2 y el proceso de definición de las capacidades futuras de los sistemas de armas de las FAS.

Un último apunte que justifica implantar la capacidad de control distribuido es la necesidad de aplicar el principio de subsidiariedad, es decir, conceder a cada nivel de mando la libertad de acción indispensable para la buena ejecución de las misiones recibidas, delegándole las responsabilidades de C2 apropiadas y las funciones más adecuadas, persiguiendo la eficacia óptima de su acción y el aprovechamiento máximo de sus capacidades de iniciativa.

La descentralización del C2 y la aplicación del principio de subsidiariedad necesitan de un nuevo estilo de liderazgo, tal y como se ha señalado en el capítulo 1 al hablar del mando orientado a la misión.

Resumiendo, contar con un mayor número de nodos de C2 y la posibilidad de distribuir entre ellos el control es un elemento decisivo en la transformación del C2. Pero esto implica la implantación de nuevas tecnologías para facilitar, cuando sea necesario, una nueva atribución de derechos de decisión entre las entidades implicadas en el escenario de combate, el establecimiento de nuevos patrones de interacción entre ellos y la implantación de una adecuada política de distribución de la información. Algo nada sencillo.

Otra medida básica para la transformación del C2 es *mejorar la interoperabilidad de los sistemas de combate* participantes, desde los diferentes ámbitos de operación, en la ejecución de las operaciones de combate.

Una interoperabilidad óptima comporta usar estándares comunes, establecer una gobernanza del dato única para todos los servicios de las FAS, elaborar una doctrina y léxico común para la explotación del dato, usar unas mismas reglas y algoritmos, y tener una infraestructura con alto grado de homogeneidad entre los servicios. Incide en el ámbito físico, informativo y cognitivo del C2.

El propósito no es mejorar la efectividad conectando todos los nodos (C2, sensores y efectores) entre ellos y compartiendo globalmente toda la información disponible. Por el contrario, la transformación perseguida debe lograr que aquel que tenga la autoridad de decidir sea capaz de conocer qué plataformas y/o sensores son relevantes para la misión en curso; y qué información debe ser compartida entre los nodos para alcanzar la escalabilidad, alcance, velocidad y supervivencia de la cadena letal que la situación demande, sin un exceso de redundancia ni esfuerzo malgastado.

Conocer la realidad del grado de interoperabilidad entre sensores, plataformas y armamento de los sistemas de combate por parte de la autoridad que ostenta la responsabilidad de C2, le permitirá maximizar el número de posibles cadenas letales en el futuro campo de batalla al integrar en ellas el efector o sensor más conveniente para el combate multidominio, determinar la complementariedad de las cadenas letales en curso y decidir cómo estas deben ser interconectadas. Asimismo, le permitirá distribuir el C2 según requieran las circunstancias de la batalla.

La interoperabilidad está íntimamente ligada al éxito de la TD del C2 y a la creación de una cadena letal web, donde se combinan y complementan los sistemas de armas para mantener la integridad en cada una de las funciones F2T2EA, al comportarse como una malla en la que cada una de las cadenas letales constituidas tiene la capacidad de hacer llegar sus datos a través de rutas de red alternativas para garantizar que los nodos de la cadena letal reciben los datos que necesitan para acercarse a los objetivos.

Gráficamente, puede expresarse mediante las figuras 9 y 10[12].

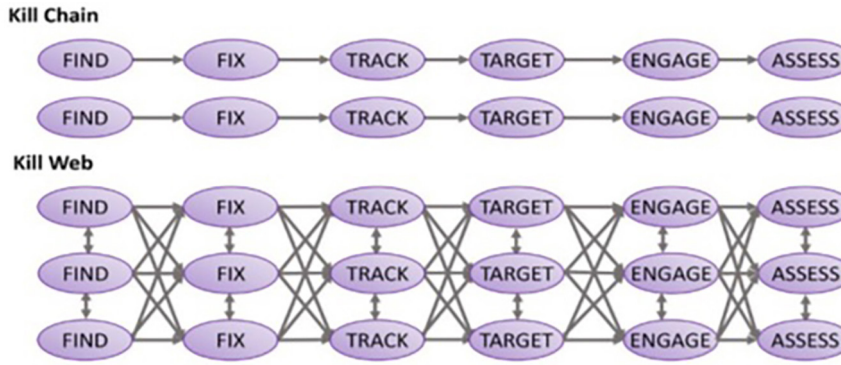


Figura 9. Relaciones F2T2EA.
Fuente: Mitchell Institute. (2023) Scale, Scope, Speed & Survivability: Winning the Kill Chain Competition. Policy Papers. Vol.40. Mayo

Para lograrlo, los nodos de «reemplazo» deben ser del tipo correcto (C2, sensor o efector), ser interoperables con múltiples sistemas diversos, posicionarse en las ubicaciones físicas óptimas y estar conectados a otros nodos y efectores de la cadena letal.

La mejora de la interoperabilidad entre los medios terrestres, navales y aeroespaciales de nuestras FAS permite establecer nuevos patrones de interacción entre ellos y favorece la distribución de información más conveniente a los fines perseguidos. Lo anterior, en combinación con una flexible

[12] Mitchell Institute. (2023) Scale, Scope, Speed & Survivability: Winning the Kill Chain Competition. *Policy Papers.* Vol. 40. Mayo.

atribución de derechos de decisión, mejora la tolerancia de la cadena letal a la atrición de los medios de combate involucrados en las diferentes fases.

Potenciar la interoperabilidad es un paso crucial para dar solución a la necesidad de disponer de una visibilidad global del escenario del conflicto, al posibilitar que cualquier sensor, plataforma, arma u otra capacidad, independientemente del dominio o del origen del servicio, contribuya a acelerar las relaciones entre los ciclos de inteligencia, ISR y operación, y a romper la tradicional aproximación «mando componente-ámbito de actuación-ámbito de efectos».

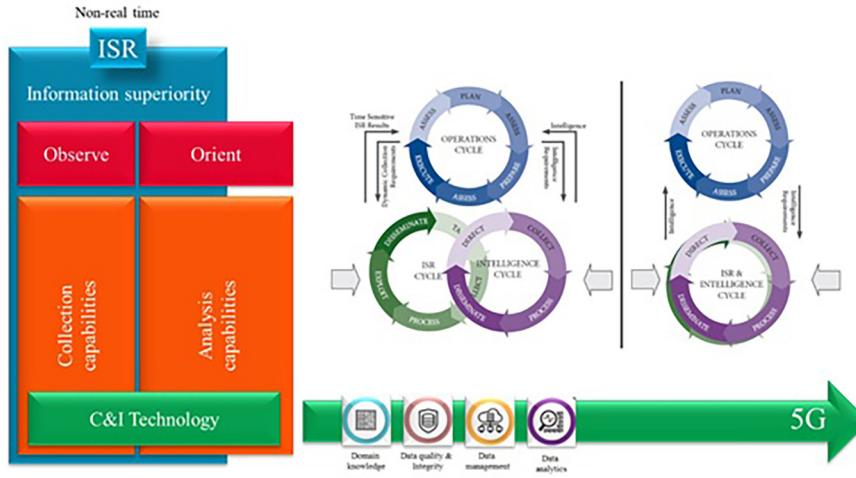


Figura 10. Relación de ciclos: Inteligencia, ISR y Operación. Fuente: elaboración propia

La interoperabilidad es una característica decisiva para alcanzar la superioridad en la información, componente básico de un C2 ágil.

Otro componente necesario en la transformación del C2 es el *empleo de los medios satelitales.* Las comunicaciones (de datos, imágenes, video, etc.) basadas en el espacio pueden aumentar enormemente la *velocidad* de las operaciones de la cadena letal, especialmente cuando los nodos de la misma (sensores y efectores) están situados más allá de la línea de visión de los demás, a la par de que también aumentan el alcance de dónde ejecutar la cadena letal y su *integridad y supervivencia*.

Disponer en el espacio de sensores (ópticos, radar, infrarrojos...) contribuye a lograr la superioridad en la información y en la toma de decisión.

Las operaciones desde el espacio en apoyo de la función de C2 abren las puertas a nuevos patrones de interacción y a nuevas posibilidades de distribución de información entre los sistemas de combate que es necesario analizar y evaluar.

La transformación del C2 requiere *acelerar la velocidad de procesamiento, emparejamiento y construcción de la cadena letal*. Afecta a los ámbitos de la información y cognitivo.

Es necesario desarrollar herramientas automatizadas basadas en las EDT que puedan proporcionar a los responsables de la gestión de la batalla aérea, allá donde se descentralice, de imágenes operativas comunes fusionadas, precisas y oportunas; un óptimo emparejamiento de plataformas de ataque, armas y objetivos; y una capacidad para construir en tiempo real redes de cadenas letales.

El beneficio obtenido es que disminuye el tiempo necesario para cumplimentar la cadena letal y aumenta su resistencia frente a los intentos del enemigo para denegarla, perturbarla o destruirla

Aumentar la capacidad de supervivencia nodal y de red es una medida irrenunciable en la transformación del C2 y que debe ser considerada desde su génesis, obligada especialmente por la amenaza procedente del ámbito ciberespacial y por la necesidad de hacer frente a la vulnerabilidad que supone el incremento de nodos de cualquier naturaleza.

El capítulo 4 ha profundizado en la seguridad de la red, en la seguridad de las relaciones establecidas entre los actores de la *kill web*, sin la cual no es posible plantear el viaje desde un modelo clásico de C2 a un modelo *Edge* como se representa en la siguiente figura:

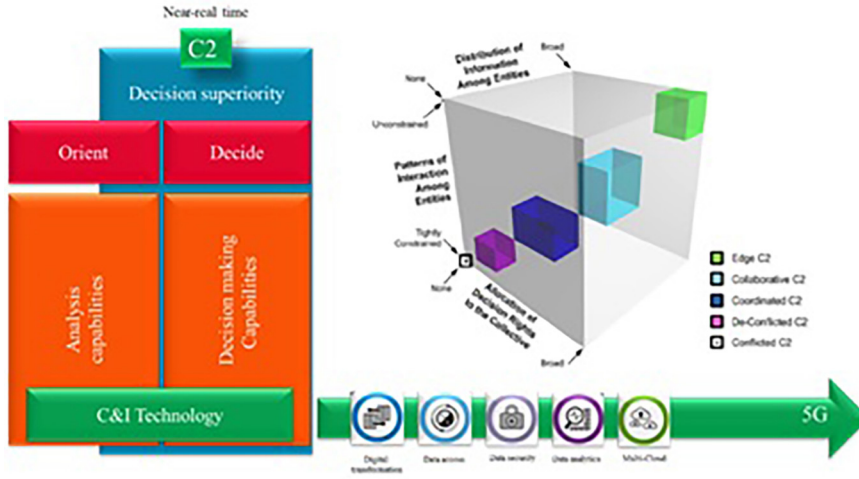


Figura 11. Relación entre modelos C2. Fuente: elaboración propia

La implantación de las nuevas tecnologías, la adaptación de las organizaciones, la adquisición de modernos sistemas de armas, el incremento de la interoperabilidad, la explotación del espacio para fines de seguridad y defensa, la mitigación de los riesgos a la integridad de instalaciones e información,

son condiciones necesarias, pero no suficientes, en el largo camino de la TD del C2 de la Fuerza Conjunta en su preparación al combate multidominio.

Piedra angular del éxito de dicha transformación son las personas, su *liderazgo, pensamiento y formación***,** abordado extensamente en el capítulo 1 del estudio.

Educar y promover el comportamiento individual y colectivo, orientado a romper las barreras existentes en el entorno de C2 entre los servicios, es crítico para su transformación, así como en la consecución de un pensamiento y proceder multidominio.

El militar experto en C2 de MDO será una pieza cardinal en esta metamorfosis y si bien podrá seguir vistiendo el uniforme propio de su servicio, su mentalidad no distinguirá entre ellos y empleará los medios de combate, con independencia de su ámbito de operación, como un conjunto único de capacidades para alcanzar el fin perseguido.

8. Conclusiones

El C2 del 2035 debe caracterizarse por ser un *C2 Multidominio* y debe ser un modelo de *C2 ágil*.

El esquema tradicional ya mencionado de «mando componente-ámbito de actuación-ámbito de efectos» responde ciertamente a un planeamiento conjunto, pero el C2 de las operaciones militares es independiente en cada uno de los servicios.

Es necesario progresar hacia un esquema de «mando conjunto-ámbito conjunto de actuación-ámbito conjunto de efectos», en el que las arquitecturas de C2 de las fuerzas componentes converjan en una única arquitectura de C2 que englobe todos los ámbitos de operación, físicos y no físicos, que conecte con éxito sensores, plataformas y armas de todos los servicios para tener la capacidad de constituir un sistema de sistemas de cadenas letales más flexibles y resistentes, con las ventajas de escala, alcance, velocidad y capacidad de supervivencia sobre el potencial enemigo.

La esencia del concepto es interconectar entre todos los ámbitos de operación el C2, las comunicaciones, la informática, la inteligencia, la vigilancia y el reconocimiento para coordinar rápidamente la potencia de fuego y ordenar las acciones que han de ejecutarse, bajo el gobierno del dato único.

Se ha de ser consciente de que la transformación del C2 en su preparación para el combate multidominio debe estar abierta a actores militares y no militares, a los que se atribuirán los derechos de decisión que sean más convenientes, entre los que será necesario establecer patrones de

interacción nuevos; y entre los que se distribuirá la información según la necesidad del momento.

Lograr alcanzar esta situación antes del 2035 no parece factible por el calado de la transformación, pero el simple planteamiento establece los cimientos sobre cómo alcanzarla.

Analizar la capacidad que tiene nuestra arquitectura de C2 para adaptar las variables consideradas y para poner en marcha las medidas propuestas a lo largo del capítulo, determinará cuál es el grado de transformación del C2 que podemos alcanzar.

Bibliografía

Abrams, E. (2013). Bombing the Syrian Reactor: The Untold Story [en línea]. *Commentary*. [Consulta: 15 DE septiembre DE 2023]. Disponible en: https://www.commentary.org/articles/elliott-abrams/bombing-the-syrian-reactor-the-untold-story/

Agrawal A., Gans A. y Goldfarb A. (2018). *Prediction Machines, the simple economy of artificial intelligence*, Harvard Business Review Press. ISBN 9781633695672.

Alberts D. S. y Hayes R. E. (2006) *Understanding Command & Control*. CCRP Publication Series.

Alberts, D. S. *et al.* (2010). NATO NEC C2 maturity model [en línea] *CCRP Publication Series*, pp. 60-71, 281-282. [Consulta: 28 DE septiembre DE 2023]. Disponible en: http://www.dodccrp.org/files/N2C2M2_web_optimized.pdf

Astorga, L. (2011). La esencia de la Guerra y el concepto NEC. *Cuadernos del CESEDEN*. 152, pp. 11-32.

Astorga, L. (2021). Manipulación cognitiva en el siglo XXI. *Revista del Instituto español de estudios estratégicos* (16), pp 15-43. Disponible en: https://revista.ieee.es/article/view/2208

Bejtlich, R. (2005). *El Tao de la Monitorización de Seguridad en Redes*. Madrid, Pearson Educación, pp. 20-24. ISBN: 84-205-4600-3.

Biryukov, A. y Perrin, L (2017). *State of the Art in Lightweight Symmetric Cryptography* [en línea]. IACR Cryptology ePrint Archive, Report 2017/511, 2017. [Consulta: 23 DE septiembre DE 2023]. Disponible en: https://eprint.iacr.org/2017/511

Boneh, D., Demillo, R. A. y Lipton, R. J. (1997). On the Importance of Checking Cryptographic Protocols for Faults (Extended abstract) [en línea] Fumy, W. (eds.) Advances in Cryptology - EUROCRYPT

1997. *Lecture Notes in Computer Science*. Vol 1.233. Springer, Berlin, Heidelberg. [Consulta: 6 DE octubre DE 2023]. Disponible en: https://doi.org/10.1007/3-540-69053-0_4

Borque, E. *et al.* (2015). *Travesía al Liderazgo. Reflexiones para el siglo XXI*. Madrid, Ministerio de Defensa.

Buzan, B. (1991). *Introducción a los estudios estratégicos. Tecnología Militar y Relaciones Internacionales.* Perez, C. y Abajo, R. (trad.). [Trabajo fechado en 1987]. Ediciones Ejército, pp. 49 y 155. ISBN: 84-86806-27-5.

Clausewitz, K. (2006) *De la Guerra, Táctica y Estrategia*. Díez, A. (trad.). Idea Books, pp. 252-253. [Trabajo original sin fecha]. ISBN: 84-8326-128-7.

Cao, K. *et al.* (2020). An Overview on Edge Computing Research [en línea].

Institute of Electrical and Electronics Engineers. IEEE. Vol.8. [Consulta: 23 DE septiembre DE 2023]. Disponible en: https://ieeexplore.ieee.org/document/9083958

Castro, M. A. (2019). Cyber Electromagnetic Activities, La nueva versión de la Guerra Digital. *Revista de Aeronáutica y Astronáutica.* N.º 889, pp. 944-951. Diciembre.

Chabert, V. (2023). The outer-space dimension of the Ukraine conflict: toward a new paradigm for orbits as a war domain? *Journal of International Affairs*. Vol. 75, n.º 2, pp. 145-56. Disponible en: https://www.jstor.org/stable/27231743

Clayton, M. (2011). Did Iran hijack the 'beast'? US experts cautious about bold claims [en línea]. *Christian Science Monitor*. [Consulta: 15 DE septiembre DE 2023]. Disponible en: https://www.csmonitor.com/USA/Military/2011/1216/Did-Iran-hijack-the-beast-US-experts-cautious-about-bold-claims

Dalan, D. *et al.* (2019). An overview of Edge Computing. En NCACCT-2019 Conference Proceedings [en línea]. *Intenational Journal of Engineering Research & Tecnology (IJERT).* [Consulta: 22 DE Dseptiembre E 2023]. Disponible en https://www.ijert.org/research/an-overview-of-edge-computing-IJERTCONV7IS05016.pdf

Deptula, D. A. (2016). Evolving Technologies and Warfare in the 21st Century: Introducing the "Combat Cloud" [en línea]. *Mitchell Institute Policy Papers*, Vol. 4. Septiembre. [Consulta: 17 julio 2023]. Disponible en: https://mitchellaerospacepower.org/wp-content/uploads/2021/02/a2dd91_73faf7274e9c4e4ca605004dc6628a88.pdf

—. (2022). A New Battle Command Architecture for Joint All-Domain Operations [en línea]. *AETER: A Journal of Strategic Airpower &*

Spacepower. Vol.1, No.1, Spring 2022. [Consulta: 17 de septiembre de 2023]. Disponible en:

https://www.airuniversity.af.edu/Portals/10/AEtherJournal/Journals/Volume-1_Issue-1/08-Deptula.pdf

Di Francesco, R., y Karlsson, P. (2018). Machine-type communication in the 5G era: Massive and ultrareliable connectivity forces of evolution, revolution, and complementarity. En: M. I. Chlamtac, F. *et al.* (Eds.), *5G Networks: Fundamental Requirements, Enabling Technologies, and Operations Management* Wiley-IEEE Pres. Disponible en: https://ieeexplore.ieee.org/document/8501534

Frąckiewiczen, M. (2023). *¿Cómo se compara* Starlink con otros proveedores de Internet satelital que actualmente operan en Ucrania*?* [en línea] *TS2*. [Consulta: 1 de octubre de 2023]. Disponible en: https://ts2.space/es/como-se-compara-starlink-con-otros-proveedores-de-internet-satelital-que-actualmente-operan-en-ucrania/

Freedberg Jr, S. J. (2023). Dumb and cheap: when facing electronic warfare in Ukraine, small drones' quantity is quality. *Breaking Defense*, Disponible en: https://breakingdefense.com/2023/06/dumb-and-cheap-when-facing-electronic-warfare-in-ukraine-small-drones-quantity-is-quality/

Friedman, N. (2004). Making NEC worthwhile. *RUSI Journal*. 149(5), pp. 14-18. DOI: https://doi.org/10.1080/03071840408522986

Fritsh, J. y Wonham, N. (2019). *How to Successfully Design and Implement a Data-Centric Security Architecture* [en línea] Gartner research. [Consulta: 29 de septiembre de 2023]. Disponible en: https://www.gartner.com/en/documents/3953491

Fulghum, D. A. y Wall, R. (2007). U.S. Electronic Surveillance Monitored Israeli Attack on Syria [en línea]. *World Security Network*. [Consulta: 15 de septiembre de 2023]. Disponible en: https://www.worldsecuritynetwork.com/Israel-Palestine/David-A.Fulghum-and-Robert-Wall-/U.S.Electronic-Surveillance-Monitored-Israeli-Attack-On-Syria

Fuller, J.F.C. (1984). *La Dirección de la Guerra.* Ibarrola, C. (trad.). [Trabajo fechado en 1961]. Ediciones Ejército, pp. 51, 70-71. ISBN: 84-505-0082-6.

García Cantalapiedra, D. (2019) Hacia un nuevo concepto de seguridad en un espacio multidominio: complejidad, guerra y seguridad transdominio. *IEEE*. Disponible en:

https://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO85_2019DAVGAR_seguridad.pdf

—. (2020). Navegar en el temporal de la incertidumbre [en línea]. *Sintetia*. [Consulta: 1 de noviembre de 2023]. Disponible en: https://www.sintetia.com/navegar-en-el-temporal-de-la-incertidumbre/ [Consulta: 1 de noviembre de 2023]

Goldfein, D. (2017). Enhancing Multi-Domain Command and Control [en línea]. CSAF. Letter to Airmen. *CSAF Focus Area Paper*. N.º 3, 10 de marzo. [Consulta: 17 DE septiembre DE 2023]. Disponible en: https://www.af.mil/News/Article-Display/Article/1108931/csaf-letter-toairmen/

Gómez Liberal, C. (2021). *Redes Móviles 5G. Evolución New Radio* [en línea] UOC TFM. [Consulta: 1 DE octubre DE 2023]. Disponible en: https://openaccess.uoc.edu/bitstream/10609/126666/7/cgomezlibTFM0121memoria.pdf

Gonzales, D. *et al.* (2005). *Network-Centric Operations Case Study Air-to-Air Combat With and Without Link 16*. [en línea] RAND Corporation. [Consulta: 28 DE septiembre DE 2023]. Disponible en: https://www.rand.org/content/dam/rand/pubs/monographs/2005/RAND_MG268.pdf

Hennessey, M. G. (2007). La anticipación de las crisis, una aplicación del enfoque del caos. Eidos. *Revista de Filosofía de la Universidad Del Norte*. 7, pp.128-159.

Hess, J. *et al.* (2016). The Combat Cloud. Enabling Multidomain Command and Control across the Range of Military Operations [en línea]. Air Command and Staff College. *Wright Flyer Paper*. N.º 65. [Consulta: 28 DE julio DE 2023]. Disponible en: https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/wf_0065_hess_combat_cloud.pdf

Hubert, S. (2021). Multi-Domain Combat Cloud. En *Joint Air & Space Power Conference 2021* Read Ahead. Cap.XI, pp. 111-118. [En línea]. JAPCC. [Consulta: 2 DE octubre DE 2023]. Disponible en:

https://www.japcc.org/wp-content/uploads/Read_Ahead_2021_Screen.pdf

Jordan, D. (2023). Elon Musk dice que bloqueó el acceso de Ucrania a su sistema de satélites Starlink para evitar una escalada de la guerra y Kyiv lo acusa de maldad [en línea]. *BBC News Mundo*. [Consulta: 10 DE octubre DE 2023]. Disponible en: https://www.bbc.com/mundo/articles/cg38zxnp9l4o

Keller, J. (2020). Air Force wants directional RF communications for tactical airborne networking of high-performance aircraft [en línea]. *Military Aerospace Electronics*. [Consulta: 1 DE octubre DE 2023]. Disponible en: https://www.militaryaerospace.com/communications/article/14186998/airborne-networking-highperformance-aircraft-directional

Kindervag, J. (2010). *Build Security Into Your Network's DNA: The Zero Trust Network Architecture* [en línea] Forrester, pp. 6-9. [Consulta: 28 DE septiembre DE 2023]. Disponible en: https://www.actiac.org/system/files/Forrester_zero_trust_DNA.pdf

—. (2016). *No More Chewy Centers: The Zero Trust Model Of Information Security.* [en línea] Forrester. [Consulta: 27 DE septiembre DE 2023]. Disponible en: https://crystaltechnologies.com/wp-content/uploads/2017/12/forrester-zero-trust-model-information-security.pdf

Kuhn, D. R., Coyne, E. J. y Weil, T. R. (2010). Adding Attributes to Role-Based Access Control [en línea] *IEEE Computer.* Vol. 43, n.º 6, pp. 79-81. [Consulta: 6 octubre 2023]. Disponible en: *https://csrc.nist.gov/files/pubs/journal/2010/06/adding-attributes-to-rolebased-access-control/final/docs/kuhn-coyne-weil-10.pdf*

Laird, R. (2016). Rear Admiral Manazir in Australia: Allied Convergence on the Kill Web. [en línea]. *Second Line o Defence*. [Consulta: 6 DE septiembre DE 2023]. Disponible en:

https://sldinfo.com/2016/08/rear-admiral-manazir-in-australia-allied-convergence-on-the-kill-web/

Lyngaas, S. (2023). Pentagon vows to use cyberspace to project power and frustrate US adversaries [en línea]. *CNN Politics*. [Consulta: 15 DE septiembre DE 2023]. Disponible en: https://edition.cnn.com/2023/09/12/politics/department-of-defense-cyber-strategy-china/index.html

López Calderón, T. E. (2021). *El Ciberespacio Como Ámbito en las Operaciones Militares. Protección de los Intereses Nacionales*. Conferencia presentada en CUNEF. Noviembre.

Mishra, S., y Tyagi, A. K. (2022). The role of machine learning techniques in Internet of Things-based cloud applications. En: S. Pal, D. De, y R. Buyya (Eds.), *Artificial Intelligence-based Internet of Things Systems*. ISBN: 9783030870584.

Makowsky, D. (2012). The Silent Strike [en línea]. *The New Yorker*. [Consulta: 15 DE septiembre DE 2023]. Disponible en: https://www.newyorker.com/magazine/2012/09/17/the-silent-strike

McLeary, P. (2022). Ukraine in direct contact with Musk amid Starlink drama. *Político.* Disponible en: https://www.politico.com/news/2022/10/20/ukraine-elon-musk-starlink-00062841

Milevski, L. (2022). *Two Less Obvious Lessons for Baltic Defense from Russia's Invasion of Ukraine*. United States of America. Disponible en: https://policycommons.net/artifacts/2480833/

two-less-obvious-lessons-for-baltic-defense-from-russias-invasion-of-ukraine/3503002/

Monserrat, J. (2009). Carencias de la realidad: conciencia, universo y mecánica cuántica, *Revista Pensamiento*. Vol. 6.

Nielsen J. (1998). *Nielsen´s law of Internet bandwidth* [en línea]. Nielsen Norman Group. Disponible en: https://www.nngroup.com/articles/law-of-bandwidth/

O'Hanlon, M. E. (2019). *The Senkaku Paradox: Risking Great Power War Over Small Stakes*. Washington, DC. Brookings Institution Press.

Ortega y Gasset. (1996). *La Rebelión de las Masas. Epílogo para Ingleses*. Editorial Andrés Bello, p. 228. [Trabajo original publicado en 1937].

Payne K. y Warbot I. (2021). *The Dawn of Artificially Intelligent Conflict*. Londres, C. Hurst & Co Publishers Ltd.

Presa, C. y Perkins, W. A. (2017). Air Warfare Communication in a Networked Environment [en línea]. *JAPCC*. Cap. 10. [Consulta: 28 DE septiembre DE 2023]. Disponible en: https://www.japcc.org/white-papers/air-warfare-communication-in-a-networked-environment/

Rahaman Sarkar, A. (2023). Elon Musk 'stopped Ukraine military using Starlink for military operation'. *The Independent*. Disponible en: https://www.independent.co.uk/news/world/europe/elon-musk-starlink-ukraine-war-b2384702.html

Rivest, R. L. Adleman, L. y Dertouzos, M. L. (1978). *On data banks and privacy homomorphisms*. [En línea] Massachusetts Institute of Technology, Academic Press. [Consulta: 10 DE octubre DE 2023]. Disponible en:https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&-doi=c365f01d330b2211e74069120e88cff37eacbcf5

Roulette, J. (2023). SpaceX curbed Ukraine's use of Starlink internet for drones -company president. *Reuters.* Disponible en: https://www.reuters.com/business/aerospace-defense/spacex-curbed-ukraines-use-starlink-internet-drones-company-president-2023-02-09/

Sabatini, R. *et al.* (2008). *Multifunctional Information Distribution System (MIDS) Low Volume Terminal (LVT) Development and Integration Programs Towards LINK-16 Network Centric Allied/Coalition Operations* [en línea] NATO RTO RTO-MP-IST-083 [Consulta: 14 DE de septiembre DE 2023]. Disponible en: https://www.researchgate.net/publication/264742534

Sahai, A. y Waters, B. (2004). *Fuzzy Identity-Based Encryption* [en línea] Eurocrypt 2005 conference [Consulta: 28 DE septiembre DE 2023]. Disponible en: https://eprint.iacr.org/2004/086.pdf

Singh, A. (2023). *Lessons from the Ukraine-Russia conflict,* Observer Research Foundation. India. Disponible en: https://policycommons.net/artifacts/3456529/lessons-from-the-ukraine-russia-conflict/4256912/

Shane, S. y Sanger, D. E. (2011). Drone Crash in Iran Reveals Secret U.S. Surveillance Effort [en línea]. *The New York Times*. [Consulta: 15 DE septiembre DE 2023]. Disponible en: https://www.nytimes.com/2011/12/08/world/middleeast/drone-crash-in-iran-reveals-secret-us-surveillance-bid.html

Smith, D. A. D. y Tourangeau, S. (2021). Electronic Protective Measures. It's About Protecting Access, *Not Aircraft*. En: *Joint Air & Space Power Conference 2021 Read Ahead*. [en línea]. Joint Air Power Competence Centre. Cap. XVIII, pp 179-186. [Consulta: 17 DE septiembre DE 2023]. Disponible en https://www.japcc.org/wp-content/uploads/Read_Ahead_2021_Screen.pdf

Soriano, G. (2016). Irán presenta su nuevo dron diseñado a partir del 'Sentinel' que capturó a EE. UU [en línea]. *Infodefensa*. [Consulta: 15 DE septiembre DE 2023]. Disponible en: https://www.infodefensa.com/texto-diario/mostrar/3079940/iran-presenta-nuevo-dron-disenado-partir-sentinel-capturo-eeuu

Standaert, F. (2005). *Introduction to Side-Channel Attacks* [en línea] [Consulta: 6 DE octubre DE 2023]. Disponible en: https://crysp.uwaterloo.ca/courses/cs458/S17-material/sidechannel.pdf

Steinbrecher, D. (2022). *VIASAT KA-SAT Attack* [en línea]. CCDCOE. [Consulta: 1 DE octubre DE 2023]. Disponible en: Viasat KA-SAT attack (2022) International cyber law: interactive toolkit (ccdcoe.org)

Sun Tzu (1993). *El Arte de la Guerra*. (A. Colondrón, trad.). Versión de Thomas Cleary. Arca de la Sabiduría, pp. 41-42. [Trabajo original sin fecha]. ISBN.84-7640-653-3.

Tsitaitse, T. J., Cai, Y. y Suntu, S. L. (2018). Secure Roaming Authentication Mechanism for WI-FI Based Networks [en línea] *International Journal of Innovative Computing, Information and Control*. Volume 14, n.º 6, pp. 2.221-2.243. Diciembre. ISSN 1349-4198. [Consulta: 28 DE septiembre DE 2023]. Disponible en: http://www.ijicic.org/ijicic-140618.pdf

Wan, T. *et al.* (2019). A Secure IoT Service Architecture with an Efficient Balance Dynamics Based on Cloud and Edge Computing [en línea] *Institute of Electrical and Electronics Engineers. IEEE Internet of Things Journal*. Vol.6, no.3. June. [Consulta: 23 DE septiembre DE 2023]. Disponible en: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8464241

Wang, J. *et al.* (2020). 3D Beamforming Technologies and Field Trials in 5G Massive MIMO Systems [en línea] *IEEE Open Journal of Vehicular Technology*. Vol. 1. [Consulta: 1 DE octubre DE 2023]. Disponible en: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9226455

Wattles, J. (2022). SpaceX sent Starlink internet terminals to Ukraine. They could paint a 'giant target' on users' backs, experts say [en línea] *CNN Business*. [Consulta: 10 DE octubre DE 2023]. Disponible en: https://edition.cnn.com/2022/03/03/tech/spacex-starlink-ukraine-internet-security-risks-scn

Willis, M. y Stathopoulos, P. (2020). Cyber-Electromagnetic Domain. The Necessity of Integrating the Electromagnetic Spectrum's Disciplines Under a Single Domain of Operations. En: *The Journal of the Joint Air Power Competence Centre* [en línea]. Joint Air Power Competence Centre. 18th Edition 30, Spring / Summer 2020, pp. 72-77. [Consulta: 30 DE septiembre DE 2023]. Disponible en https://www.japcc.org/wp-content/uploads/JAPCC_J30_screen.pdf

Glosario

A2/AD	*Anti-Access / Area Denial*
ARGO	Plataforma para la Armonización de la Gestión de la Organización en el Ministerio de Defensa español
C2	*Command and Control*
C3	*Communications, Command and Control*
CD&E	*Concept Development and Experimentation*
CCN-CERT	Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional
CERT	*Computer Emergency Response Team*
CIS	Communications and Information Systems/Sistemas de Información y Comunicaciones
CMAD	Comisión Ministerial de Administración Digital del Ministerio de Defensa
CO	Contexto Operativo
CoG	Center of Gravity / Centro de Gravedad
COP	*Common Operational Picture*
COPD	*Comprehensive Operations Planning Directive*
CSA	*Cyber Situational Awareness*
CSIRT	*Computer Security Incident Response Team*
EDT	*Emerging and Disruptive Technologies*
EMAD	Estado Mayor de la Defensa

EMSS	*Electromagnetic Spectrum Strategy*
EO 2035	Entorno Operativo 2035
ESN	Estrategia de Seguridad Nacional
E S P D E F - CERT	Centro de Respuesta a Incidentes de Seguridad de la Información del Ministerio de Defensa español
FAS	Fuerzas Armadas
FCAS	*Future Combat Air System*
FMN	*Federated Mission Network*
I3D	Infraestructura Integral de Información para la Defensa
IA	Inteligencia Artificial
INCIBE-CERT	Centro de Respuesta a Incidentes de Seguridad de la Información del Instituto Nacional de Ciberseguridad
IOC	*Initial Operational Capability*
IoT	*Internet of Things*
ISR	*Intelligence, Surveillance and Reconnaissance*
JADC2	*Joint All-Domain Command and Control*
JEMAD	Jefe del Estado Mayor de la Defensa
JREAP	*Joint Range Extensión Application Protocol*
LAMP	Proceso de lecciones aprendidas y mejores prácticas
LEO	*Low Earth Orbit*
MBIT	Indicador de Myers-Briggs
MCCE	Mando Conjunto del Ciberespacio
MDO	*Multi-domain Operations*
ML	*Machine Learning*
MoM	Mando Orientado a la Misión
NC	Nube de Combate
NCIO	*NATO Communications and Information Organization*
NEC	*Network Enabled Capability*
NI	Nodo de Interconexión
NIAG	*NATO Industrial Advisory Group*
OODA	Observación, Orientación, Decisión y Acción
OTAN	Organización del Tratado del Atlántico Norte
PDC	Publicación Doctrinal Conjunta
QoS	*Quality of Service*
RAP	*Recognised Air Picture*
SAS	*System Analysis and Studies Panel (NATO)*

SC2N	Sistema de Mando y Control Nacional
SEGINFO	Seguridad de la Información
SHF	*Super High Frequency*
SoS	Sistema de Sistemas
STO	*Science and Technology Organization (NATO)*
TD	Transformación Digital
TDL	*Tactical Data Links*
TIC	Tecnologías de la Información y las Comunicaciones
UAS	*Unmanned Aerial Systems*
UE	Unión Europea
UHF	*Ultra High Frequency*
UME	Unidad Militar de Emergencias
USAF	*United States Air Force*
VHF	*Very High Frequency*
VUCAH	*Volatility, Uncertainty, Complexity, Ambiguity and Hyperconnectivity*.

Composición del grupo de trabajo

Presidente: **D. Fernando Carrillo Cremades**
General de Brigada, Ejército del Aire y del Espacio
Segundo jefe y jefe de Estado Mayor del Mando Aéreo de Canarias

Secretario: **D. Luis Olalla Simón**
Teniente coronel del Ejército del Aire y del Espacio
Segundo Representante Nacional Militar ante NATO SACT

Autores: **D. Fernando Luis Morón Ruiz**
General de división del Ejército de Tierra
Mando de Adiestramiento y Doctrina (DIDOM/MADOC)

D. Luis Francisco Astorga González
Capitán de navío (R) de la Armada
Organización de Comunicaciones e Información de la OTAN (NCIO)

D. Manuel Buesa Bueno
Ingeniero de Sistemas de Indra
Responsable Técnico del proyecto FCAS en París

D. Rubén Vega Bustelo
Teniente coronel del Ejército de Tierra
Mando Conjunto del Ciberespacio (MCCE)

D. Juan Ramón González Espadas
Comandante del Ejército del Aire y del Espacio (Excedencia)
Future Combat Air System Operational Advisor

PUBLICACIONES
Pd
DE DEFENSA

GOBIERNO
DE ESPAÑA

MINISTERIO
DE DEFENSA

SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

SUBDIRECCIÓN GENERAL
DE PUBLICACIONES
Y PATRIMONIO CULTURAL