



ACADEMIA DE LAS CIENCIAS
Y LAS ARTES MILITARES

Comunicaciones académicas

Del dato al efecto: estrategia y organización en la guerra de redes

Guillem Colom Piella

Academia de las Ciencias y las Artes Militares
Sección de Pensamiento, Legislación y Moral Militar

16 de octubre de 2025

Introducción

A lo largo de la Historia, la guerra ha experimentado profundas transformaciones por la confluencia de factores estratégicos, doctrinales, organizativos y tecnológicos, además de políticos y sociales. Aunque el principal motor del cambio suele ser la doctrina –porque orienta el empleo de las capacidades militares– la tecnología actúa, a menudo, como catalizador visible de estas transformaciones. Desde la pólvora hasta la Inteligencia Artificial (IA), la tecnología ha incrementado la letalidad, la velocidad, la precisión, el alcance o la eficiencia de los sistemas de armas. Pero sin ajustes doctrinales, organizativos e industriales que conviertan los avances técnicos en ventajas en la toma de decisiones y efecto operativo, la tecnología no garantiza por sí sola la innovación militar.

La Cuarta Revolución Industrial acelera hoy esta dinámica al combinar digitalización, interconectividad, manufactura avanzada, revolución en los materiales y sensorización masiva del campo de batalla. El resultado es un entorno en el que la información en tiempo real, la automatización y la integración de dominios ocupan el centro del planeamiento y la conducción de operaciones. Sin

embargo, cuanto más digital es la fuerza, más vulnerable resulta a la disputa por la supremacía en el ciberespacio y el espectro electromagnético. En ese contexto, se perfilan cinco vectores de cambio con implicaciones estratégicas claras, que a continuación se detallan:

1. Inteligencia artificial y ventaja en la toma de decisiones.

La IA se consolida como herramienta transversal en logística, mantenimiento predictivo, guiado y automatización, detección de amenazas y – sobre todo – apoyo a la toma de decisiones. Al integrarse en sistemas de mando y control, permite gestionar grandes volúmenes de datos rápidamente y transformar información heterogénea en conocimiento accionable, reduciendo la latencia del ciclo de Observación, Orientación, Decisión y Actuación, y acortando la secuencia completa de acciones de ataque que conecta sensores, decisores y vectores para «detectar, identificar, decidir, atacar y evaluar» el objetivo. Esta aceleración no consiste solo en «ver antes», sino en decidir mejor bajo presión e incertidumbre y sincronizar fuegos y maniobra con mayor precisión.

Ahora bien, la IA no es únicamente un conjunto de algoritmos: descansa sobre datos de calidad, gobernanza e interoperabilidad. Sin estándares e interfaces abiertas, sin trazabilidad y sin verificación rigurosa del dato, su promesa se diluye. La clave estratégica no es «tener IA», sino poder integrarla con seguridad jurídica y operacional en redes conjuntas y combinadas, con procedimientos que aseguren *control humano significativo* y despliegue confiable.

2. Transparencia del campo de batalla y disputa del espectro.

La proliferación de sensores –desde satélites y radares a pequeños drones, móviles y redes sociales– y su integración en mallas de datos hacen más visible el espacio de batalla. La fusión de información permite localizar, clasificar y priorizar objetivos con rapidez inédita y alimentar cadenas de efectos a múltiples escalas. A ello se suma el abaratamiento y la difusión de munición guiada, que extiende la precisión más allá de plataformas exquisitas.

Pero la transparencia no es absoluta. La dependencia de enlaces, navegación y firmas electromagnéticas expone a interferencias, engaños y negación. En la práctica, la guerra de redes alterna periodos de visibilidad y ceguera en función de quién domina el espectro y protege mejor sus dependencias digitales. De ahí la necesidad de diseñar operaciones resilientes (capacidad de aguantar la presión o el ataque sin desmoronarse y de recuperar la situación original):

navegación alternativa a los sistemas de posicionamiento global, modos de baja probabilidad de interceptación/detección, computación en el borde/límite para mantener funciones críticas con conectividad degradada y procedimientos que aseguren degradación graciosa de las capacidades sin colapso del conjunto.

3. Burbujas Anti-Acceso/Denegación de Área (A2/AD) por capas.

La integración de sensores avanzados, misiles antibuque y superficie-aire de largo alcance, misiles balísticos, guerra electrónica, capacidades cibernéticas y opciones antisatélite –combinadas con medios tradicionales como minas, submarinos, artillería guiada o aviación de caza– genera redes de defensa multicapa, auténticas «matrioshkas» que expanden perímetros, elevan costes de acceso y complican la maniobra adversaria. Su existencia no es un muro infranqueable, pero sí disuade, proyecta control efectivo sobre áreas de interés y aporta ventajas en la gestión de la escalada, especialmente en la «zona gris», espacio vulnerable entre la paz/estabilidad y la guerra/conflicto abierto sin llegar al conflicto bélico.

La respuesta estratégica a estas burbujas defensivas pasa por tres líneas: 1) inteligencia persistente para identificar nodos críticos de la red; 2) saturación selectiva para forzar la dilución de interceptores; y 3) combinación de efectos cibernéticos, electromagnéticos y cinéticos que abran ventanas temporales de vulnerabilidad. La competición se decide tanto por la fuerza disponible como por la cadencia con la que se reconstituye la red tras cada golpe.

4. Operaciones multidominio como disciplina de integración.

La incorporación plena de los ámbitos cibernético, espacial e informativo en el marco operacional ha desdibujado la frontera entre frente y retaguardia. Las operaciones multidominio no son un eslogan, sino una disciplina de integración: sincronizar acciones terrestres, navales, aeroespaciales y ciber-electromagnéticas –junto a instrumentos no-militares– para explotar asimetrías y generar dilemas operativos al adversario. La prioridad ya no es solo mover plataformas de combate, sino mover datos con seguridad, compartirlos donde importa y a la velocidad adecuada. En la práctica, esto se materializa en una red de muerte: un entramado de múltiples cadenas sensor-tirador que comparten información y asignan efectos de forma dinámica, añadiendo redundancia, si una vía cae, otra sigue y acelerando la decisión a escala.

En este marco, el centro de gravedad no está únicamente en la plataforma de combate que porta el efecto, sino en la arquitectura que la conecta: estándares, interfaces, gobierno del dato y procedimientos comunes. Sin esa base, la promesa de «conectar todo con todo» se torna fricción; con ella, la cooperación conjunta y combinada gana profundidad y ritmo. La red de muerte es, en última instancia, la consecuencia operativa de esa arquitectura: una red que reconfigura rutas sensor-efector en segundos y sostiene la iniciativa incluso bajo degradación del espectro.

5. Guerra mosaico y distribución funcional.

La creciente transparencia, el coste y los largos ciclos de desarrollo de grandes plataformas, junto con su vulnerabilidad a saturaciones de vectores baratos y abundantes, impulsan una lógica de distribución funcional. La denominada «guerra mosaico» propone «desagregar funciones críticas en múltiples nodos pequeños, asequibles y fungibles que operan de forma colaborativa, tripulados y no-tripulados». Se gana así resiliencia frente a pérdidas, se incrementa la flexibilidad táctica y se reduce el riesgo estratégico de depender de pocos activos de alto valor.

El mosaico exige dos compromisos: estándares abiertos (para reemplazar y evolucionar módulos rápidamente) y contratos orientados a la iteración (para introducir mejoras por software y por bloque en ciclos más cortos). Sin ellos, la fragmentación tecnológica, los bloqueos de proveedor y la rigidez presupuestaria neutralizan los beneficios de la distribución.

De lo anterior se desprende que la competición militar es por el proceso de decisión, lo que supone varias implicaciones: En primer lugar, la superioridad ya no reside únicamente en ver más, sino en decidir antes y mejor bajo estrés, negación y ambigüedad. Por ello, la IA, los datos y el mando y control deben evaluarse según su impacto verificable en el tiempo de ciclo y en la sincronización de efectos a nivel conjunto y combinado, no por el brillo tecnológico de cada pieza.

La segunda implicación es la resiliencia de redes. La ventaja informativa sólo se sostiene si la fuerza puede operar en espectros degradados, asumiendo periodos de ceguera parcial y cortes intermitentes. La preparación debe interiorizar esa realidad y diseñar procedimientos, redundancias y modos de empleo que permitan seguir actuando con «fallas controladas», preservando la iniciativa pese a la fricción.

En tercer lugar, la economía de fuego condiciona la sostenibilidad estratégica. La defensa por capas y la proliferación de vectores obligan a equilibrar coste por efecto

con cadencia logística y reposición de inventarios. Una disuasión creíble exige capacidad industrial, cadenas de suministro robustas y planificación que resista campañas prolongadas, donde el ritmo de producción y mantenimiento pesa tanto como el rendimiento táctico.

La cuarta es la interoperabilidad soportada por arquitecturas abiertas. La cooperación aliada –y, en última instancia, la eficacia del multidominio– descansa sobre estándares, interfaces y gobernanza del dato comunes. Sin una columna vertebral digital que garantice intercambio seguro y latencias adecuadas, «conectar todo con todo» se convierte en una promesa vacía; con ella, la integración gana profundidad y ritmo.

Además, y de forma relevante, el talento individual y la cultura organizativa son el verdadero multiplicador. La adopción de la IA, la distribución funcional y la operación en redes requieren alfabetización tecnológica en todos los niveles, mandos capaces de dirigir por intención y equipos habituados a aprender rápido mediante experimentación, ejercicios realistas y ciclos efectivos de lecciones aprendidas.

Por último, la adquisición adaptativa marca la diferencia entre innovar y transformar. La innovación útil es la que entra en servicio y se mejora en operación. Para ello, conviene acortar la transición laboratorio/teatro, generalizar *bancos de pruebas* operativos y aceptar despliegues incrementales que permitan iterar con rapidez, manteniendo el control de riesgos y la trazabilidad de los cambios.

Conclusión

La tecnología es una condición necesaria, pero no suficiente para la innovación militar. El desafío consiste en transformarla en ventaja sostenible a través de doctrina, organización, talento, industria y contratos adecuados. La IA y la automatización aceleran la decisión; la sensorización y la precisión extienden el alcance; las redes disputadas exigen resiliencia; las burbujas A2/AD revalorizan la negación por capas; y la guerra mosaico distribuye funciones para sobrevivir y golpear. Quien pase de la promesa a la integración responsable –arquitecturas abiertas, gobierno del dato, procedimientos compartidos– verá antes, decidirá más rápido y golpeará en los puntos más débiles o centrales del adversario. En un entorno competitivo y fluido como el actual, hay que moverse muy rápido, más rápido que los acontecimientos; si no, van siempre por delante, pero lo decisivo no es moverse rápido, sino saber hacia dónde y dotarse de las estructuras que permitan llegar. ■

Nota: Las ideas y opiniones contenidas en este documento son de responsabilidad del autor, sin que reflejen, necesariamente, el pensamiento de la Academia de las Ciencias y las Artes Militares.

© Academia de las Ciencias y las Artes Militares - 2025