papeles faes
FUNDACIÓN

Nº 296
6/4/2026

INTERNACIONAL

MINISTERIO DE ASUNTOS EXTERIORES, UNIÓN EUROPEA Y COOPERACIÓN
SECRETARÍA DE ESTADO DE ASUNTOS EXTERIORES Y GLOBALES

Actividad subvencionada por la Secretaría de Estado de Asuntos Exteriores y Globales

El poder militar en la era de la revolución digital

Guillem Colom-Piella
Doctor en Seguridad Internacional, Academia de las Ciencias y las Artes Militares

*Este **Papel** explora cómo la **digitalización** y la **Cuarta Revolución Industrial** están transformando los **escenarios de la guerra** y el **poder militar**. Así, analiza nuevas **potencialidades** como la **inteligencia artificial**, la creciente **transparencia en el campo de batalla**, el uso de **armas masivas** y eficaces como los drones **FPV**, o la **relevancia** del **ciberespacio** y los **entornos electromagnéticos**. El artículo aborda además las estrategias en **zonas de alta disputa**, las **arquitecturas de defensa**, los **entornos degradados** y la **guerra en mosaico**. Y destaca la necesidad de adaptarse rápidamente a un **escenario de guerra** en **constante cambio tecnológico** y cada vez más **digital, disperso y contestado**, capaz de difuminar la distancia entre **ventajas y vulnerabilidades**.*

Introducción

La guerra evoluciona constantemente, pero lo hace alternando ajustes incrementales con cambios disruptivos en la forma de combatir. A lo largo de la Historia, las transformaciones decisivas han surgido de la confluencia entre estrategia, doctrina, organización y tecnología[1]. Existe la tentación de atribuir el cambio a la última innovación tecnológica visible: el arco, ayer; los drones, hoy. Aunque la tecnología puede actuar como catalizador del cambio porque acelera lo posible, abarata lo eficaz y amplifica lo letal[2], la historia muestra que el motor suele ser la doctrina porque orienta el empleo de las capacidades disponibles y define una "teoría de la victoria". Desde la invención de la pólvora hasta la inteligencia artificial (IA), la tecnología ha incrementado la letalidad, velocidad, precisión, alcance, eficacia y eficiencia de los ejércitos; pero sin ajustes doctrinales y organizativos que optimicen su empleo, rara vez estos cambios generan una ventaja estratégica[3].

Este matiz importa porque el debate sobre las guerras futuras oscila entre el determinismo tecnológico y el inmovilismo burocrático. La cuestión no es si habrá cambio, sino qué parte será incremental y qué parte alterará estándares operativos. En este contexto, los cambios impulsados por la Cuarta Revolución Industrial –IA, datos y automatización– no constituyen por sí mismos una Revolución en los Asuntos Militares (RMA)[4], pero sí proporcionan el sustrato tecnológico que puede acelerar su maduración[5]. Lo decisivo, sin embargo, no es el catálogo de tecnologías, sino su efecto conjunto sobre el proceso de toma de decisiones y el modo de operar bajo degradación física, lógica y psicológica. La paradoja es evidente: la digitalización promete reducir la "niebla de la guerra", pero la competición militar empuja precisamente a lo contrario, a combatir en entornos informativa, electrónica y cibernéticamente contestados[6]. Dicho de otro modo: la ventaja no será "ver más" en abstracto, sino convertir la información en acción más rápido y con más resiliencia que el adversario.

---

1 **Barry Posen**, *The Sources of Military Doctrine* (Ithaca: Cornell University Press, 1984); Stephen Rosen, *Winning the Next War* (Ithaca: Cornell University Press, 1994); Dmitry Adamsky, *The Culture of Military Innovation* (Stanford: Stanford University Press, 2010).

2 **Christian Brose**, *The Kill Chain* (Nueva York: Hachette, 2020).

3 **Stephen Biddle**, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton: Princeton University Press, 2004).

4 Una RMA puede definirse como una innovación militar disruptiva: la combinación de nuevas tecnologías, conceptos operativos, organización y adiestramiento que reordena el modo de combatir, impone un nuevo estándar operativo y vuelve obsoletas – al menos parcialmente – prácticas previas. **Barry Watts**, *The Maturing Revolution in Military Affairs* (Washington DC: CSBA, 2011); **Guillem Colom-Piella**, *Entre Ares y Atenea* (Madrid: IUGM, 2008).

5 **Robert Work** y **Shawn Brimley**, *20YY: Preparing for War in the Robotic Age* (Washington, DC: CNAS, 2014).

6 **Bryan Clark** et al., *Winning the Invisible War: Gaining an Enduring U.S. Advantage in the Electromagnetic Spectrum* (Washington DC: CSBA, 2019).

La IA se está consolidando como una herramienta clave en las fuerzas armadas. Su capacidad para gestionar grandes volúmenes de datos en tiempo real, identificar patrones y automatizar tareas está mejorando la logística, el mantenimiento predictivo, la detección de amenazas y el mando y control

A partir de aquí, el análisis puede ordenarse en cinco tendencias que, más que sumarse, se encadenan: cada una refuerza a la siguiente y, al mismo tiempo, abre nuevas superficies de vulnerabilidad que un adversario competente intentará explotar. No se trata, por tanto, de un inventario de novedades, sino de una lógica de competición: acelerar el propio ciclo de decisión y degradar el ajeno, ver sin ser visto, y golpear con precisión sin quedar expuesto.

La IA: aceleradora del mando y control… y tensionadora del control humano

La IA se está consolidando como una herramienta clave en las fuerzas armadas. Su capacidad para gestionar grandes volúmenes de datos en tiempo real, identificar patrones y automatizar tareas está mejorando la logística, el mantenimiento predictivo, la detección de amenazas y, sobre todo, el mando y control (C^2)[7]. Bien empleada, la IA permite reducir la latencia del ciclo de Observación-Orientación-Decisión-Actuación (OODA *loop*) y acortar la cadena de muerte (*kill chain*), entendida como el proceso que comprende desde la detección de un blanco hasta su neutralización. Esta ambición está en la base de las arquitecturas contemporáneas de C^2 conjunto, que buscan integrar sensores y efectores en paquetes flexibles para operar en entornos altamente dinámicos[8]. Conviene precisar, además, que esa cadena tiende a concebirse cada vez menos como un proceso lineal y más como una red letal (*kill web*)[9]: un entramado distribuido de sensores, decisores y efectores que puede recombinarse para cerrar el ciclo de selección y asignación de objetivos (*targeting*) por rutas alternativas cuando el adversario degrada enlaces, sensores o C^2.

Pero este mismo vector tecnológico que acelera los procesos de decisión abre un dilema político-operativo: la automatización permite reducir –e incluso elimi-

7 **Paul Scharre**, *Army of None: Autonomous Weapons and the Future of War* (Nueva York: WW Norton, 2018).

8 Department of Defense, *Summary of the Joint All-Domain Command and Control (JADC2) Strategy* (Washington, DC, DoD, 2022).

9 Por *kill chain* suele entenderse la secuencia de detectar–identificar–asignar–batir–evaluar (F2T2EA), mientras que una *kill web* subraya que, en arquitecturas distribuidas, esa secuencia se recompone dinámicamente con múltiples rutas sensor-decisor-efector (**Nicholas O'Donoughue** et al., *Distributed Kill Chains: Drawing Insights for Mosaic Warfare from the Immune System and from the Navy* (Santa Monica: RAND Corporation, 2021).

La automatización permite reducir –e incluso eliminar– la intervención humana en labores de observación, navegación, selección de objetivos o lanzamiento de armas, posibilitando sistemas semiautónomos o autónomos que operan de forma aislada, en colaboración con humanos u otros sistemas, o en enjambres

nar– la intervención humana en labores de observación, navegación, selección de objetivos o lanzamiento de armas, posibilitando sistemas semiautónomos o autónomos que operan de forma aislada, en colaboración con humanos u otros sistemas, o en enjambres[10]. La literatura lleva tiempo advirtiendo que una parte del combate tiende a salir del "espacio humano" (con ritmos y complejidades gobernables por la cognición humana) y a desplazarse hacia procesos donde el humano queda como mero supervisor, un papel en el que, por razones psicológicas y organizativas, solemos rendir peor de lo que creemos[11]. La cuestión, por tanto, no es si habrá automatización, sino cómo se gestionará su empleo para mantener la responsabilidad, el control y la estabilidad en crisis[12].

En este punto se inserta el debate sobre las armas autónomas y el "control humano significativo". Las discusiones en el marco de la Convención sobre Ciertas Armas Convencionales de las Naciones Unidas sugieren que el reto al que nos enfrentamos es definir umbrales operativos (qué tareas pueden automatizarse, con qué límites, sobre qué objetivos y en qué condiciones de supervisión). La presión competitiva empuja a automatizar los sistemas para no quedarse fuera de ciclo, pero la prudencia estratégica exige evitar dinámicas de escalada accidental y errores irreversibles en entornos saturados de interferencias y engaño.

De ahí que la promesa de la IA no sea sólo una guerra "sin humanos", sino una guerra por la decisión: quien logre comprimir el ciclo OODA y, a la vez, mantener su integridad bajo interferencias, engaños y ataques a la red, impondrá el ritmo de la campaña. El reto es político-operativo: acelerar sin descontrolar, automatizar sin eludir la responsabilidad y diseñar fuerzas capaces de operar cuando la conectividad falle. Porque en un campo de batalla saturado de señales falsas, la victoria no la da la máquina que decide antes, sino la organización que sigue decidiendo cuando todo se degrada.

---

10 **Jack Watling**, *The Arms of the Future: Technology and Close Combat in the Twenty-First Century* (Londres: Bloomsbury, 2023).

11 **Thomas Adams**, "Future Warfare and the Decline of Human Decisionmaking", *Parameters* 41, nº 4 (2001), pp. 51-71.

12 **Scharre**, *Army of None*.

Esta nueva transparencia redefine la economía del riesgo y la forma de generar masa en el combate. Cuando la detección es persistente y la localización puede convertirse en destrucción en minutos o segundos, la concentración de medios y la acumulación de logística pasan de ser una ventaja a ser una vulnerabilidad

La transparencia del campo de batalla: se ve más, pero la niebla se desplaza

El segundo cambio es la creciente transparencia del campo de batalla. Su sensorización empezó a consolidarse con las ideas del "sistema de sistemas" y la "guerra en red" derivados de la RMA de los noventa. Sin embargo, la diferencia actual es su escala y la convergencia civil-militar: satélites, radares y drones conviven con teléfonos móviles, redes sociales y una firma electrónica ubicua, de modo que movimientos y emisiones pueden ser detectados casi en tiempo real[13]. Además, la integración en red de sensores, sistemas de C^2 y combatientes puede acercar el ideal del "sistema de sistemas" prometido hace décadas: un ecosistema federado capaz de fusionar información de múltiples fuentes y asignar blancos al vector más eficiente.

Ahora bien, transparencia táctica no equivale a omnisciencia. Precisamente porque "se ve más", también hay más incentivos para degradar la visión del enemigo. La niebla de la guerra clausewitziana no desaparece, sino que se desplaza a la lucha por la firma, el engaño, las interferencias (*jamming*) o la suplantación de señales (*spoofing*). En términos prácticos, esto empuja a fuerzas más dispersas, con mejor disciplina de emisiones, más señuelos y una protección más integrada frente a drones y sensores. El campo de batalla se vuelve más observable, sí; pero también más disputado y "ruidoso".

Esta nueva transparencia también redefine la economía del riesgo y la forma de generar masa en el combate. Cuando la detección es persistente y la localización puede convertirse en destrucción en minutos o segundos, la concentración de medios y la acumulación de logística pasan de ser una ventaja a ser una vulnerabilidad. De ahí la expansión de prácticas que antes eran secundarias: camuflaje y ocultación como disciplina básica, dispersión y movilidad por microsaltos, fortificación y protección en profundidad, y una gestión deliberada de la huella térmica,

[13] **Carlos Frías**, "Rusia, Ucrania y el campo de batalla 'transparente'", *Documento de Opinión del IEEE*, 16 de febrero de 2024, disponible en: https://www.defensa.gob.es/documents/2073105/2077230/Rusia%2C+Ucrania+y+el+campo+de+batalla+transparente.pdf

La abundancia de vectores guiados –desde sofisticados misiles de largo alcance hasta drones de visión en primera persona (FPV)– permite batir objetivos con precisión, reducir daños colaterales, maximizar el impacto táctico y simplificar las cadenas logísticas

electromagnética o visual que convierte cada emisión en una posible delación. En este entorno, no solo importa batir los objetivos (acortar la *kill chain*), sino también sobrevivir (romper la cadena enemiga): detectar cuándo nos han detectado, reducir la firma, emplear señuelos y forzar al adversario a gastar munición sobre objetivos secundarios[14]. La consecuencia es un combate más "competitivo" en el sentido literal: una carrera de adaptación entre medidas y contramedidas –drones contra defensas antidrón, sensores contra engaños, precisión contra guerra electrónica– en la que la ventaja tiende a ser temporal y local. Por eso, el campo de batalla se vuelve no sólo más transparente, sino también más dinámico: quien aprende y ajusta más rápido convierte la información en efectos; quien no lo hace, convierte la información en vulnerabilidad. En ese contexto, la precisión tiende a democratizarse y el volumen vuelve a importar.

Precisión masiva: del misil exquisito al dron fungible

La tercera tendencia es la proliferación y abaratamiento del armamento de precisión[15]. La abundancia de vectores guiados –desde sofisticados misiles de largo alcance hasta drones de visión en primera persona (FPV) *letalizados*– permite batir objetivos con precisión, reducir daños colaterales, maximizar el impacto táctico y simplificar las cadenas logísticas[16]. El efecto resultante es un campo de batalla donde activos valiosos pueden ser batidos por medios baratos y abundantes, y donde la saturación se convierte en una táctica estructural.

Sin embargo, Ucrania también ha mostrado el talón de Aquiles de parte de esta precisión: el guiado (y la conectividad) es vulnerable a interferencias electromagnéticas. Cuando los sistemas de posicionamiento y los enlaces de datos se degradan, el rendimiento de estas municiones se reduce notablemente[17]. De ahí que el problema ya no sea solo tener precisión, sino poder sostenerla cuando el ad-

14 **Guillem Colom-Piella**, "From battlefield transparency to the contact layer. Organisational throughput and conditional manoeuvre in Ukraine", *RUSI Journal* [en prensa]

15 **Barry Watts**, *The Evolution of Precision Strike* (Washington, DC: CSBA, 2013).

16 **Jack Watling** y **Nick Reynolds**, *Tactical Developments During the Third Year of the Russo-Ukrainian War* (Londres: RUSI, 2025).

17 **Guillem Colom-Piella** y **Cristina Marzal**, "Has Russian Electronic Warfare Underperformed in the Ukrainian Conflict?", *Journal of Strategic Security*, 18, nº 4 (2025), pp. 78-95.

Esta democratización de la precisión abarata el ataque y encarece la defensa. Un dron FPV o una munición merodeadora obliga, a día de hoy, a emplear interceptores mucho más caros; y, si se lanza en masa, puede saturar el mejor sistema de defensa

versario impone degradación electrónica y cibernética. Y de ahí también el retorno de un debate que Occidente había olvidado: la masa. La guerra de alta intensidad consume munición, repuestos y plataformas a ritmos que penalizan arsenales mínimos y ciclos industriales lentos[18]. La precisión masiva no elimina la guerra industrial; la reconfigura.

Esta democratización de la precisión altera, además, un equilibrio clásico: abarata el ataque y encarece la defensa. Un dron FPV o una munición merodeadora obliga, a día de hoy, a emplear interceptores mucho más caros; y, si se lanza en masa, puede saturar el mejor sistema de defensa. Se impone así una lógica de competición de salvas: no vence necesariamente quien tiene el arma más sofisticada, sino quien puede sostener el intercambio durante más tiempo –con *stocks*, reposición y capacidad de adaptación– y quien logra que el adversario gaste munición cara sobre blancos baratos mediante señuelos y saturación. Al mismo tiempo, esta dinámica empuja a rediseñar la fuerza: más defensa por capas, más integración entre sensores y fuegos, más dispersión logística y más tolerancia a la pérdida de sistemas fungibles. En este entorno, la precisión deja de ser un atributo de plataformas selectas y se convierte en un rasgo sistémico del combate: la supervivencia depende tanto de la protección como de la capacidad de desorganizar el ciclo de decisión adversario. Y eso explica por qué, inmediatamente, el debate desemboca en el siguiente punto: la guerra por la conectividad en el espectro electromagnético y el ciberespacio.

Ciberespacio y entorno electromagnético: la degradación como requisito

El cuarto cambio –en buena medida consecuencia de los anteriores– es la centralidad del ciberespacio y del entorno electromagnético como condición de posibilidad del combate contemporáneo. Si la guerra del siglo pasado se definió por la potencia de fuego y la movilidad, la del siglo XXI se caracteriza por la dependencia de la conectividad: satélites, drones, radios, enlaces de datos, redes tácticas, teléfonos, sistemas de posicionamiento, sensores y sistemas de C^2 forman

[18] **Guillem Colom-Piella**, "The Bear in the Labyrinth. First Impressions of Russia's Performance in Ukraine", *RUSI Journal*, 167, nº 6-7 (2023), pp. 72-81.

La supervivencia depende tanto de la protección como de la capacidad de desorganizar el ciclo de decisión adversario. Inmediatamente, el debate desemboca en el siguiente punto: la guerra por la conectividad en el espectro electromagnético y el ciberespacio

un "sistema nervioso" que permite ver, coordinar y atacar[19]. El problema es que ese sistema nervioso no es un facilitador neutro; es un campo de batalla. Y, por tanto, un objetivo.

Esta dependencia introduce una paradoja: cuanto más "digital" y "en red" es una fuerza, más vulnerable se vuelve a la disrupción, interferencia o suplantación[20]. En términos simples, el enemigo no necesita destruir tus plataformas más selectas para reducir tu eficacia: a veces le basta con cegar, confundir o descoordinar algunos nodos. La precisión se resiente si el guiado falla; la maniobra se ralentiza si el C^2 pierde coherencia; y la logística se vuelve frágil si los flujos de datos sufren interrupciones. El combate deja de ser "plataformas contra plataformas" y pasa a ser, en buena medida, de "redes contra redes".

De ahí se derivan tres consecuencias operativas que conviene explicitar:

- **Primera:** la capacidad de "combatir degradado" deja de ser una contingencia para ser un estándar. El planeamiento, el adiestramiento y los procedimientos deben asumir pérdidas de conectividad, navegación y enlaces. Esto implica, por ejemplo, operar con sistemas de posicionamiento degradados, comunicaciones intermitentes, tiempos de reacción más largos y mayor autonomía táctica. No es un detalle técnico: condiciona el mando tipo misión (*mission command*), el reparto de responsabilidades y la tolerancia a la incertidumbre en los escalones bajos.

- **Segunda:** el espectro electromagnético se consolida como un componente transversal de la fuerza: quien domina este espectro determina quién puede detectar, clasificar, comunicarse y coordinar fuegos. Esto altera la economía del combate: obliga a gestionar firmas, reducir emisiones, emplear señuelos, desplegar nodos redundantes, y aceptar que la superioridad no se decide solo por quién tiene mejores sensores, sino por quién consigue que los sensores del enemigo no sirvan o sirvan mal.

---

19 **Andrew Krepinevich**, *The Origins of Victory: How Disruptive Military Innovation Determines the Fates of Great Powers* (New Haven: Yale University Press, 2023).

20 **Jennifer McCardle**, *Victory Over and Across Domains: Training for Tomorrow's Battlefield*s (Washington DC: CSBA, 2019).

La guerra del siglo XXI se caracteriza por la dependencia de la conectividad: satélites, drones, radios, enlaces de datos, redes tácticas, teléfonos, sistemas de posicionamiento, sensores y sistemas de mando y control forman un "sistema nervioso" que permite ver, coordinar y atacar

- **Tercera:** el ciberespacio añade profundidad, ambigüedad y riesgo de escalada. A diferencia de un ataque cinético, muchas acciones cibernéticas son difíciles de atribuir con rapidez y pueden producir efectos no lineales sobre infraestructuras críticas, sistemas civiles o redes duales. Esto complica la escalada y la disuasión: una interferencia puede interpretarse como preludio de ataques mayores; un fallo puede atribuirse a sabotaje; y una operación diseñada para "molestar" puede generar consecuencias sistémicas inesperadas.

En suma, si el futuro de la guerra está marcado por la información, entonces la guerra por la información será una dimensión decisiva de la ventaja operativa. La cuestión ya no es si se perderá conectividad, sino cuánto, durante cuánto tiempo y quién estará mejor preparado para seguir combatiendo cuando eso ocurra.

A2/AD, zona gris, multidominio y mosaico

Estas dinámicas también están contribuyendo a la normalización de las burbujas Anti-Acceso y Denegación de Área (A2/AD), entendidas menos como una "capacidad" aislada que como un resultado sistémico de la integración entre sensores persistentes, vectores de precisión, C^2 en red y contestación del espectro electromagnético[21]. Conviene subrayar el punto de partida: estas arquitecturas emergen como respuesta al estilo de combate asociado al régimen de precisión en red, que convirtió la proyección de poder en un problema de información, coordinación y fuegos de precisión en profundidad[22]. Si el estilo de guerra occidental derivado de la pasada RMA aspiraba a ver primero, decidir antes y batir con precisión, la lógica A2/AD busca exactamente lo contrario: impedir el acceso, degradar la red, fragmentar el mando y encarecer la operación hasta hacerla políticamente menos asumible.

---

21 **Sam Tangredi**, *Anti-Access Warfare: Countering A2/AD Strategies* (Annapolis: Naval Institute Press, 2013); **Guillem Colom-Piella**, "A2/AD: ¿concepto controvertido o problema operativo?", *Revista de aeronáutica y astronáutica*, nº 911 (2022), pp. 256-260.

22 En puridad, sus antecedentes directos surgieron en la URSS en la década de 1980. Se trata de los complejos de reconocimiento y ataque (*Razvedyvatel no-Udarnyy Kompleks* o RUK). Compuestos por tres elementos – municiones de precisión, sensores avanzados y un sistema automatizado de mando y control– los RUK serían capaces de identificar las fuerzas adversarias y batirlas con precisión desde grandes distancias. Un RUK estaría situado dentro de una burbuja, principalmente antiaérea, para evitar que el adversario batiera sus elementos más preciados, como la aviación o los misiles de largo alcance.

La capacidad de "combatir degradado" deja de ser una contingencia para ser un estándar. El planeamiento, el adiestramiento y los procedimientos deben asumir pérdidas de conectividad, navegación y enlaces

Aunque la intención de restringir la libertad de maniobra del adversario no es nueva, su densidad actual sí lo es. La combinación de sistemas de inteligencia, observación y reconocimiento avanzados, misiles antibuque, defensas aéreas de largo alcance, capacidades balísticas, medios electromagnéticos y cibernéticos, minas o armas antisatélite permite articular arquitecturas multicapa que expanden perímetros defensivos, generan "soberanía" *de facto* en zonas disputadas y encarecen de forma sustantiva la proyección de poder.

Conviene, no obstante, evitar simplificaciones analíticas. Ni una arquitectura A2/AD es inexpugnable, ni su supresión es un trámite. Los enfoques centrados en "barrer" estas defensas mediante campañas sostenidas de ataque profundo pueden resultar prohibitivos en coste y arriesgados por riesgos de escalada, especialmente cuando implican batir objetivos en el territorio continental de una potencia nuclear[23]. De ahí un criterio analítico útil: evaluar tanto las arquitecturas A2/AD como sus "contraconceptos" por su contribución a objetivos políticos concretos –negar un hecho consumado, sostener un aliado, impedir coerción, etc.– y no por la mera posibilidad de "operar" fuerzas en abstracto. En otras palabras: el problema no es solo operativo (el acceso), sino estratégico (qué fines justifican qué riesgos y qué costes).

Precisamente, esta cobertura ampliada facilita otra dinámica característica del mundo actual: la proyección de zonas grises bajo el paraguas que proporcionan las estrategias A2/AD. Cuando un actor percibe que puede dominar la escalada en su periferia gana margen para diseñar estrategias de presión sostenida: sabotaje, intimidación, coerción económica, operaciones de influencia y hechos consumados graduados[24]. En los próximos años cabe esperar un aumento y un solapamiento de estas burbujas a medida que los Estados se doten de vectores terrestres, navales y aéreos de largo alcance para influir más allá de sus fronteras.

La implicación para los contendientes es doble: por arriba, eleva los costes de la proyección de poder; por abajo, facilita coerción graduada bajo el umbral del conflicto. Por ello, cualquier innovación para resolver este problema estratégico

---

23 **Stephen Biddle** e **Ivan Oelrich**, "Future Warfare in the Western Pacific: Chinese Antiaccess/Area Denial, U.S. Air Sea Battle, and Command of the Commons in East Asia", *International Security* 41, nº 1 (2016), pp. 7-48.

24 **Michael Mazarr**, *Mastering the Gray Zone* (Carlisle: U.S. Army War College, 2015).

Si el futuro de la guerra está marcado por la información, entonces la guerra por la información será una dimensión decisiva de la ventaja operativa. La cuestión ya no es si se perderá conectividad, sino cuánto, durante cuánto tiempo y quién estará mejor preparado para seguir combatiendo cuando eso ocurra

no puede limitarse a "más plataformas" o "más alcance", sino a conceptos operativos y diseños de fuerza capaces de competir en un espacio de batalla degradado y altamente disputado. En ese marco se inscriben dos movimientos complementarios[25].

Por un lado, las operaciones multidominio. Si las arquitecturas A2/AD pretenden degradar la capacidad de una fuerza conjunta para operar en entornos contestados, estas buscan resolver el problema integrando y orquestando las actividades en distintos dominios, combinando tierra, mar, aire, espacio, ciber y electromagnético (junto con instrumentos no-militares) para generar dilemas simultáneos al adversario, degradar nodos críticos y abrir "ventanas" temporales de superioridad local[26]. La lógica no es "ganar un dominio" de forma permanente, sino sincronizar efectos para desorganizar el proceso de decisión del rival, reducir su capacidad de concentración y explotar sus vulnerabilidades sistémicas (sensores, C^2, logística, defensas por capas, etc.).

Por otro lado –y como tendencia más estructural– emerge el impulso hacia diseños de fuerza distribuidos y fungibles, que está cristalizando en la guerra mosaico. En un campo de batalla densamente sensorizado, donde la precisión se democratiza y la saturación se convierte en una táctica estructural, las grandes plataformas son objetivos de alto valor: pueden ser identificadas, sus defensas saturadas y su sustitución es lenta y costosa[27]. La lógica de la guerra mosaico propone lo contrario: distribuir funciones críticas entre múltiples sistemas más pequeños, asequibles, fungibles y reemplazables, conectados mediante arquitecturas abiertas, de modo que el conjunto pueda recomponerse tras pérdidas y operar bajo degradación. La metáfora de las "teselas" que se recombinan para formar paquetes de fuerza adaptativos resume bien esta aspiración[28]. El objetivo no es

[25] **Guillermo Pulido**, *Guerra multidominio y mosaico: El nuevo pensamiento militar estadounidense* (Madrid: Catarata, 2021).

[26] **Amos Fox** y **Franz-Stefan Gady** (eds.), *Multidomain Operations: The Pursuit of Battlefield Dominance in the 21st Century* (Havant: Howgate Publishing, 2026).

[27] **Bryan Clark** et al., *Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations* (Washington DC: CSBA, 2020).

[28] **O'Donoughue** et al., *Distributed Kill Chains*.

La lógica de la guerra mosaico propone distribuir funciones críticas entre múltiples sistemas más pequeños, asequibles, fungibles y reemplazables, conectados mediante arquitecturas abiertas, de modo que el conjunto pueda recomponerse tras pérdidas y operar bajo degradación

únicamente incorporar la tecnología, sino aumentar la resiliencia, reduciendo puntos únicos de fallo, complicando la selección de blancos enemigos y sosteniendo el combate cuando la red sea contestada.

Vistas en conjunto, las tendencias dibujan un hilo coherente: a la maduración del régimen de precisión en red le responde la difusión de A2/AD, y a esta, la adaptación mediante enfoques multidominio y diseños distribuidos. El punto decisivo no es la tecnología aislada, sino la capacidad de sostener la ventaja bajo contestación.

Implicaciones prácticas

El diagnóstico anterior es útil solo si se traduce en implicaciones prácticas. De lo contrario, se convierte en un ejercicio de literatura futurista. Las consecuencias más relevantes pueden formularse en cinco proposiciones:

- **Primera:** la ventaja militar no se fundamenta sólo en tener más potencia de fuego, sino en la capacidad de decidir antes y sostener la decisión en campos de batalla degradados. El núcleo del cambio es una competición por acortar el ciclo OODA propio y alargar o disrumpir el ajeno.

- **Segunda:** la transparencia del campo de batalla empuja hacia la dispersión, el engaño y la protección integrada. El principio de “Si te ven, te baten” funciona como regla general, pero la respuesta no es esconderse, sino gestionar la firma, desplegar señuelos, dispersar nodos y dotarse de defensas antidrón y de guerra electrónica distribuidas. La protección ya no es un apéndice; es parte del modo de combatir.

- **Tercera:** vuelve la masa, pero no como antes. La precisión barata y los drones fungibles cambian la economía del combate: no basta con plataformas exquisitas si faltan *stocks*, repuestos o capacidad de producción escalable. Las guerras largas premian la resiliencia industrial: reservas, líneas de fabricación adaptables y cadenas de suministro robustas.

Ni una arquitectura A2/AD es inexpugnable, ni su supresión es un trámite. Los enfoques centrados en "barrer" estas defensas mediante campañas sostenidas de ataque profundo pueden resultar prohibitivos en coste y arriesgados por riesgos de escalada

- **Cuarta:** la automatización y la autonomía tensionan el control humano y puede erosionar la estabilidad estratégica. Automatizar para no quedar fuera de los ciclos OODA empuja hacia sistemas más rápidos, con menor control contextual y mayor riesgo de error. El problema no es solo ético; es estratégico: la autonomía, la interferencia y la atribución imperfecta pueden generar incidentes escalatorios. De ahí la necesidad de definir y *operacionalizar* el control humano significativo con criterios verificables de prueba, empleo y supervisión.

- **Quinta:** el cuello de botella de la innovación es institucional. La adaptación al cambio no depende tanto de incorporar tecnologías nuevas como de ajustar las burocracias de defensa para convertir esa aceleración en capacidades reales. Esto choca con inercias conocidas: grandes programas lentos, procedimientos de compra rígidos, aversión al riesgo y culturas organizativas que premian la plataforma por encima del sistema[29]. En un entorno competitivo, la ventaja se convierte en una carrera de aprendizaje: quien experimenta, integra y adapta con mayor rapidez sostiene la iniciativa; quien no lo hace, la pierde. La tecnología acelera, pero son las instituciones las que deciden si esa aceleración se convierte en ventaja o en vulnerabilidad.

Conclusiones: correr para no quedarse atrás

El futuro de la guerra ya está en curso. Estamos abocados a una competición permanente por la decisión en un entorno más transparente, más letal y más disputado, donde la conectividad es simultáneamente ventaja y vulnerabilidad. La consecuencia estratégica de este cambio es clara: el valor no reside en una gran plataforma aislada, sino en la arquitectura que convierte información en efectos bajo degradación y que, a la vez, niega esa conversión al adversario.

La digitalización y la democratización de la precisión están reordenando la economía del combate, elevan el peso del espectro electromagnético, el ciberespacio y el espacio exterior como "terrenos" operativos, y favorecen arquitecturas A2/AD

[29] **Christian Villanueva**, "La guerra contra la inercia", *Ejércitos*, 7 de marzo de 2024, disponible en: https://www.revistaejercitos.com/opinion/la-guerra-contra-la-inercia

El futuro de la guerra ya está en curso. Estamos abocados a una competición permanente por la decisión en un entorno más transparente, más letal y más disputado, donde la conectividad es simultáneamente ventaja y vulnerabilidad

que encarecen la proyección de poder y amplían el espacio de coerción por debajo del umbral del conflicto. Frente a ello, las respuestas más prometedoras combinan lo multidominio con diseños orientados al mosaico de medios.

Pero el verdadero criterio de éxito no será quién adquiera antes una tecnología, sino quién la convierta antes en una capacidad real. Como advertía la Reina Roja a Alicia, "…para quedarte donde estás tienes que correr lo más rápido que puedas; si quieres ir a otro sitio, deberás correr, por lo menos, dos veces más rápido".

faes FUNDACIÓN

Suscripción a *Cuadernos de Pensamiento Político:*
https://fundacionfaes.org/analisis-de-faes/#htmegatab-11b63d74
www.fundacionfaes.org

C/ Ruiz de Alarcón, 13. 2ª planta
28014 Madrid
Tlf 915 766 857
info@fundacionfaes.org
fundacionfaes@fundacionfaes.org

DONACIONES

REDES SOCIALES