



35/2026

27/03/2026

*Juan Carlos Andrés Herrero **

La guerra pulsante: combate a la velocidad de las máquinas

La guerra pulsante: combate a la velocidad de las máquinas

Resumen:

El siglo XXI redefine el arte de la guerra mediante el empleo masivo de tecnologías disruptivas como la inteligencia artificial (IA) y la robótica, que impactan especialmente en los dominios virtual y cognitivo. Este cambio sugiere el advenimiento de una revolución militar que desembocará en una nueva generación de la guerra. Las actividades cognitivas priorizan la manipulación de percepciones y narrativas, mientras que las virtuales aceleran el combate más allá de la capacidad humana. Esta revolución conduce a un combate hiperacelerado que denominamos guerra pulsante. Un concepto que utiliza sistemas autónomos (AWS) e IA para saturar al enemigo, atacando simultáneamente en todos los dominios y enfocándose en destruir su voluntad de lucha. El ser humano pasa de operar a entrenar estos sistemas, enfrentando desafíos éticos y legales de la autonomía de las máquinas en la guerra.

Palabras clave:

Pulsante, hiperacelerado, tempo, ritmo, inteligencia artificial, cognitivo, saturación.

***NOTA:** Las ideas contenidas en los **Documentos de Opinión** son responsabilidad de sus autores, sin que reflejen necesariamente el pensamiento del IEEE o del Ministerio de Defensa.

The Pulsating Warfare: combat at the speed of machines

Abstract:

The 21st century is redefining the art of war through the massive use of disruptive technologies such as Artificial Intelligence (AI) and robotics, which have a particular impact on the virtual and cognitive domains. This change suggests the advent of a military revolution that will lead to a new Generation of Warfare. Cognitive activities prioritize the manipulation of perceptions and narratives, while virtual activities accelerate combat beyond human capacity. This revolution leads to hyper-accelerated combat that we call Pulsating Warfare. This concept uses autonomous systems (AWS) and AI to overwhelm the enemy, attacking simultaneously in all domains and focusing on destroying their will to fight. Humans go from operating to training these systems, facing ethical and legal challenges of machine autonomy in warfare.

Keywords:

Pulse, hyperaccelerated, tempo, rhythm, artificial intelligence, cognitive, saturation.

Cómo citar este documento:

ANDRÉS HERRERO, Juan Carlos. *La guerra pulsante: combate a la velocidad de las máquinas*. Documento de Opinión IEEE 35/2026. [enlace web IEEE](#) y/o [enlace bie³](#) (consultado día/mes/año)

El empleo extensivo de tecnologías disruptivas en operaciones militares está cambiando los cimientos sobre los que se estructuraba el arte de hacer la guerra. El siglo XXI está siendo testigo de un desarrollo exponencial y del empleo masivo de tecnologías catalizadoras de nuevas capacidades. Se nos presenta un escenario repleto de nuevos medios para hacer la guerra que, sin duda, modificarán los modos de combatir. Si la tradición nos presentó la *guerra de atrición* y la modernidad la *guerra de maniobra*, esta nueva era nos sorprenderá con un nuevo tipo de guerra.

Los actuales impulsores tecnológicos disruptivos son, entre otros, la inteligencia artificial (IA), la robótica, el internet de las cosas (IoT), las comunicaciones 5G, la fabricación aditiva, la biotecnología, la nanotecnología y la tecnología cuántica. Entre ellos, destacamos la IA y la robótica por su aplicación directa en los dominios físicos (tierra, mar, aire y espacio), que a su vez, generan efectos de mayor impacto en los dominios del ciberespacio (virtual) y del cognitivo (información).

El JEMAD¹ destaca la importancia que tendrán los dominios virtuales y cognitivo en las guerras que están por llegar. El dominio cognitivo se define como el espacio no físico de las operaciones que afecta directamente a las percepciones y a la toma de decisiones, siendo el factor humano el elemento más relevante de la guerra: una lucha de voluntades contrapuestas. Este dominio ha cobrado una importancia renovada debido a la hiperconectividad global facilitada por el ciberespacio, lo que permite influir fácilmente en las poblaciones y en los líderes.

Catalizadores del cambio: aproximación tecnológica y social

Las revoluciones en el arte de la guerra se asocian con los momentos de la historia en los que una serie de cambios tecnológicos y sociales de gran escala alteran la manera de entenderla, modificando la doctrina, la organización y los modos de combatir. Se producen cuando surgen nuevas tecnologías (Revolución Industrial) o nuevas formas de entender el mundo (Revolución francesa) que desencadenan un cambio profundo en los sistemas económicos, las estructuras sociales y las fuerzas militares (Schwab², 2016).

¹ Lección inaugural del curso académico 2024-2025. Almirante general D. Teodoro López Calderón, jefe del Estado Mayor de la Defensa, el 21 de octubre de 2024 en la Academia de las Ciencias y las Artes Militares.

² SCHWAB, Dr. Klaus. *La cuarta revolución industrial*, 2016.

Con ello identificamos una relación en la tríada tecnología-guerra-sociedad. Las conocidas como revoluciones militares (RM) derivan de cambios sociopolíticos que modifican los recursos y la organización del Estado para la guerra. Por su parte, las revoluciones en los asuntos militares (RMA) son cambios en la doctrina y la organización de las fuerzas militares provocados por la tecnología emergente que buscan adaptarse al contexto contemporáneo. Si bien la naturaleza de la guerra sigue siendo la misma, los modos y medios empleados cambian (Tapia³, 2024).

La humanidad está inmersa en un período de evolución tecnológica acelerado que está cambiando de manera profunda las sociedades. La democratización de la tecnología y su carácter de doble uso han intensificado la relación tecnología-guerra-sociedad. Si bien hasta ahora el control y el empleo militar de la tecnología eran estatales, en la actualidad, el control está en manos privadas, lo que abre la puerta a la disrupción por parte de actores no estatales. Todo ello en una sociedad global interconectada en la que la información y la percepción son aspectos de relevancia estratégica.

La empresa privada tiene mayor libertad de acción, con una menor gobernanza y regulación. Parece ganar un papel protagonista, en algunos casos equiparable al de los Estados. Por ello, la colaboración y el equilibrio consensuado entre el sector público y el privado marcarán la hoja de ruta en este siglo. La tendencia actual al rearme con sistemas más tecnológicos requiere un respaldo financiero que en muchas ocasiones es limitado, por lo que se requiere adoptar políticas tecnológicas sostenibles.

La aplicación de este modelo debe aprovechar las *tecnologías de doble uso*, aquellas que pueden ser empleadas tanto en el ámbito civil como en el militar, aplicando los cambios inherentes a cada ámbito. Las empresas que operan en el mercado comercial y de defensa son los actores clave. Emplear la aproximación Commercial-Off-the-Shelf (COTS) permite dar el paso al Military off-the-shelf (MOTS). Las sinergias COTS-MOTS son la clave de la adopción e integración militar de las tecnologías de doble uso.

³ SÁNCHEZ TAPIA, Salvador, G. B. (res.) prof. de Relaciones Internacionales en la Universidad de Navarra. «La tecnología como catalizador del cambio en la guerra».



Imagen 1. Catalizadores del cambio militar. Fuente: elaboración propia con Gemini

Las generaciones de la guerra: aproximación polemológica

La guerra es un camaleón⁴, se adapta al entorno. Por ello, ante la aplicación de tecnologías disruptivas en el combate, ¿estamos necesariamente ante una revolución militar o tan solo en la aplicación de la innovación militar? La realidad es que el cambio tecnológico no es el único para tener en cuenta, existen otras dimensiones como la doctrina o la organizativa que también deben cambiar para considerarse revolución. Javier Jordán⁵ condiciona la definición de revolución militar a la coincidencia en el tiempo y espacio de un número elevado de innovaciones tecnológicas. Es un proceso acumulativo, resultado del empleo simultáneo y sincronizado de elementos novedosos y disruptivos en los conflictos bélicos.

Esta discusión es antigua y los teóricos han constatado que las revoluciones militares son una forma de categorización intelectual de la guerra más acertada que las clasificaciones tradicionales como «convencional» o «guerrilla». Lo que es indudable es que las dinámicas empleadas en los campos de batalla han ido evolucionando al compás de la tecnología y de la sociedad. Cualquier cambio, innovación, adaptación o revolución

⁴ Clausewitz.

⁵ Javier Jordán es catedrático del Departamento de Ciencia Política y de la Administración de la Universidad de Granada.

tendrá un nivel diferente de impacto en los elementos de las capacidades militares (MIRADO-I): material, infraestructura, recursos, adiestramiento, doctrina, organización e interoperabilidad. Si establecemos la doctrina como el motor del cambio, los cambios coyunturales en técnicas, tácticas y procedimientos (TTP) aplicados a una zona de operaciones específica no tienen por qué producir un cambio doctrinal profundo.

Es habitual emplear clasificaciones básicas, muchas veces obsoletas, de la guerra en función de la tipología. Entre ellas destacamos:

- Convencional/no-convencional.
- Irregular/asimétrica/híbrida.
- De baja/media/alta intensidad.
- De bloques, de maniobra, de aproximación indirecta⁶, de desgaste (atrición).
- Guerra fría, blanda, económica y nuclear.

William S. Lind, uno de los pensadores militares más reconocidos de los últimos tiempos, protagonista de algunos de los cambios doctrinales más relevantes en el seno del Pentágono, ordena por generaciones⁷ las guerras de la era moderna desde el siglo XVII.

1GW - Primera generación (1648-1860): guerra de líneas y columnas, derivada de la Primera Revolución Industrial (1780), con las fábricas y la máquina de vapor, y de la Revolución francesa (1789), con la movilización en masa y la ideología. Los ejércitos se convierten en estatales y profesionales, con empleo extensivo de *armas de fuego*: mosquetes y cañones. Esta era de guerra premoderna se caracteriza por el empleo de grandes formaciones militares centralizadas, con enfrentamientos de carácter estático en un campo de batalla único.

2GW - Segunda generación (1860-1918): guerra de atrición, tras la Segunda Revolución Industrial 2IR (1870), con la electricidad y la producción en masa, y la Revolución militar prusiana (1860), que desembocó en el modelo de doctrina y organización eficiente. Las fuerzas militares centran el combate en la potencia de fuego, la artillería y el empleo de trincheras. La Revolución Industrial permitió la *producción en masa y sofisticación* de armamento y municiones, como la ametralladora o la artillería de

⁶ HART, Liddell. *The Strategy of Indirect Approach*, 1941.

⁷ LIND, William S. «Comprendiendo la guerra de cuarta generación», 1989.

alta cadencia. De hecho, este período también es conocido como el de la guerra industrializada.

3GW - Tercera generación (1918-1990): guerra de maniobra, catalizada por la Tercera Revolución Industrial 3IR (1950), que además trajo las telecomunicaciones y la producción automatizada. También influyeron la Declaración de los Derechos Humanos (1948) y las diferentes revoluciones por los derechos civiles, con las que la vida y la muerte de los soldados comienza a impactar en la opinión pública. Se caracteriza por la velocidad que otorga el empleo extensivo de medios mecanizados y la integración de la aviación, con la Blitzkrieg como máxima expresión. Esto permite romper los frentes atacando las vulnerabilidades del adversario, empleando el concepto de armas combinadas y de fuegos indirectos precisos. La finalidad es acabar con la voluntad de combatir del enemigo en vez de lograr la destrucción total del adversario. Destaca por el empleo extensivo de la radio, los vehículos de combate y la aviación militar.

4GW - Cuarta generación (1990-¿actualidad?): guerra híbrida. La Cuarta Revolución Industrial 4IR (2000) o Revolución digital potencia las capacidades de conectividad global, procesamiento y almacenamiento de información a gran escala, con una alta tasa de adopción tecnológica (mayor velocidad de desarrollo e integración en los procesos). También se produce la denominada revolución de identidad y justicia social, en el que se establece la doctrina de «bajas cero». Guerras descentralizadas, asimétricas e híbridas, de actores no estatales contra Estados, principalmente a través de la insurgencia. Las acciones cinéticas en los dominios físicos ceden protagonismo a las no cinéticas en el dominio cognitivo (información) y virtual (ciber), orientadas a la influencia social. La estrategia pasa por los factores políticos, económicos, sociales y religiosos, con el foco en la dimensión psicológica y cognitiva del conflicto. La guerra es librada por actores no estatales contra la legitimidad del Estado, utilizando una mezcla de medios cinéticos y no cinéticos. Mezcla de medios cinéticos (violencia) y no cinéticos (propaganda). Uso de la tecnología de la información (medios).

Sin embargo, muchos autores contemporáneos consideran esta clasificación como incompleta, al no contemplar las generaciones de la guerra anteriores a la Paz de Westfalia (1648), y obsoleta, al haber pasado más de treinta años de su análisis prospectivo de guerra híbrida, en el que el Estado pierde el monopolio de la violencia.

Por ejemplo, Fernando del Castillo Durán⁸ viene a completar el período histórico previo a las generaciones desarrolladas por Lind y lo expande hasta con ocho generaciones de la guerra. De ahí la duda de si aún continuamos en la 4GW.

Las innovaciones tecnológicas puntuales no deberían desencadenar una RMA, sino más bien una revisión de los aspectos afectados. Este es el caso de la RMA declarada por el Pentágono a finales del siglo XX, derivada de las tecnologías de la información, que prometía acabar con la «niebla de la guerra». Se planteó la posibilidad de cambiar por completo la organización de las fuerzas armadas hacia un modelo reducido y tecnológicamente avanzado que aprovechara la ventaja hegemónica tecnológica. Sin embargo, las guerras de contrainsurgencia en Afganistán e Irak acabaron poniendo de manifiesto lo precipitado de la idea. Este es un ejemplo de entendimiento prematuro del momento y modo de cambio, en el que no se analizó la sobredependencia de la tecnología sin una integración con el factor humano ni se anticipó la resistencia natural de las instituciones militares a los cambios (Knox y Murray, 2001⁹).

Si bien la clasificación de Durán nos parece más completa, nos apoyaremos en la clásica de Lind, al ser la referencia general más empleada, a la que interrelacionamos cronológicamente con revoluciones tecnológicas y sociales.

⁸ CASTILLO DURÁN, Fernando del. «Sobre las generaciones de la guerra», *Revista Ejército*. 2021.

⁹ KNOX, MacGregor y MURRAY, Williamson. *The Dynamics of Military Revolution, 1300–2050*. 2001.

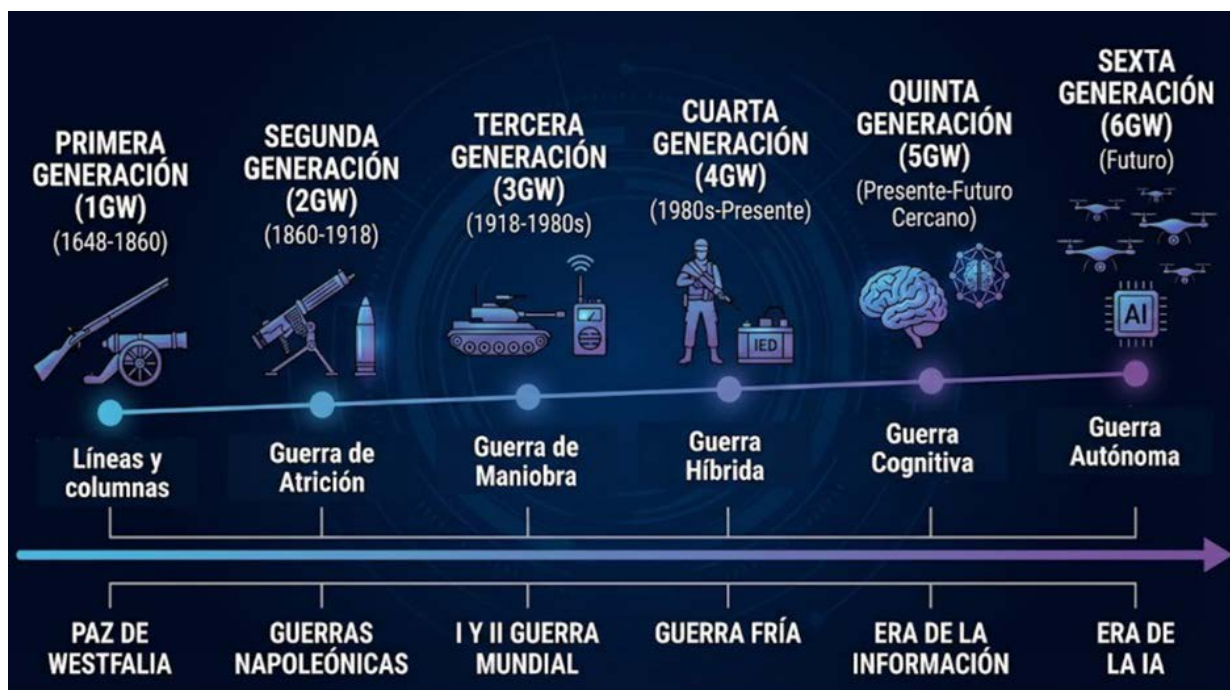


Imagen 2. Las generaciones de la guerra. Fuente: elaboración propia con Gemini

Aunque la opinión mayoritaria es que seguimos en la 4IR, algunos estudiosos, principalmente europeos y japoneses, creen que la IA, especialmente la generativa, va a iniciar una nueva revolución industrial basada en la colaboración humano-máquina (en vez de la automatización), el *Deep Learning*, la autonomía productiva y la sostenibilidad (en vez de eficiencia). De esta manera, si bien no se ha producido aún, es posible que estemos en los albores de la Quinta Revolución Industrial (5IR).

Las siguientes generaciones de la guerra

Sea como fuere, parece que la tendencia del gráfico cronológico es a que las revoluciones industriales y las sociales anticipan la aparición de una nueva generación de la guerra. En este caso, la 4IR y la revolución de la sostenibilidad y la justicia social podrían ser los disparadores de una quinta generación de la guerra (5GW), y quien sabe, si la 5IR propiciará una sexta generación de la guerra (6GW). Lo que es obvio, es que los tiempos entre revoluciones y generaciones se van acortando en un crecimiento exponencial. Podría parecer que estamos en pleno proceso de cambio y a la vez, sentando las bases del siguiente.

Estas teorías se apoyan en dos movimientos derivados del uso extensivo de la IA (desde la dimensión virtual): la *revolución cognitiva (REVCOG)* en el dominio cognitivo y la *revolución autónoma (REVAUT)* en los dominios físicos. La *REVCOG* traslada el campo de batalla a las mentes de los combatientes (militares) y de los ciudadanos (ámbito social) mediante la IA para realizar análisis predictivo, ingeniería social y campañas de desinformación masiva creando un escenario deliberadamente ambiguo y no atribuible. El objetivo es manipular la percepción y la voluntad del adversario para alcanzar la parálisis social, política y militar del enemigo, sin recurrir necesariamente a acciones cinéticas.

La *REVAUT* genera un campo de batalla sin límites temporales y espaciales mediante el empleo masivo y simultáneo de sistemas de armas autónomos (AWS) en todos los dominios físicos impulsados por IA, que acelerarán los ciclos de toma de decisiones (OODA-Loop) más allá de la capacidad humana.

En este sentido, expertos como Antonio Herrera¹⁰ han empezado a definir una 5GW en la que lo virtual y lo cognitivo desplazan a lo cinético. Y otros como Armin Krishnan¹¹ hablan ya de la 6GW que tiene como modo de combate principal el colapso de la sociedad mediante acciones no cinéticas sobre objetivos estratégicos.

5GW - Quinta generación de la guerra. Guerra cognitiva entre actores estatales y no estatales tecnológicos. Establece la primacía de los dominios cognitivos y virtual, con una IA perceptiva y generativa con control humano *on the loop*. Es un conflicto no cinético, invisible, cuyo objetivo final es conquistar el dominio humano y social del adversario a través de las percepciones y de las narrativas. Empleando actores proxy para mantener la ambigüedad, esta estrategia utiliza la inteligencia artificial (IA) y las plataformas sociales para llevar a cabo operaciones de información con armas de confusión masiva, creando un vórtice de desinformación, caos y conflicto psicológico. Se priorizan las acciones no cinéticas, como la ingeniería social, los ciberataques y las operaciones psicológicas (PSYOPS), sobre la violencia abierta. El objetivo no es destruir al enemigo, sino paralizar su voluntad de luchar e inducir el comportamiento deseado, logrando la rendición o la parálisis atacando continua y simultáneamente en múltiples

¹⁰ Antonio Herrera. Lisa Institute, 2023.

¹¹ KRISHNAN, Armin. *Fifth Generation Warfare: Dominating the Human Domain*, 2024,

dominios cognitivos y cibernéticos. En esta generación, los dominios físicos pierden importancia frente al ciberespacio y, fundamentalmente, el dominio cognitivo.

6GW - Sexta generación. Guerra autónoma entre superpotencias tecnológicas. La toma de decisiones en el campo de batalla se cede, parcial o totalmente, a la inteligencia artificial (IA) y a los sistemas de armas autónomos (AWS), incluidos los letales (LAWS). Los avances tecnológicos disruptivos impulsan este salto, permitiendo operaciones sin intervención humana directa (HOOTL). El campo de batalla se deshumaniza y se emplean enjambres de drones pequeños y coordinados. El factor definitorio es la hiperaceleración del ciclo de toma de decisiones (OODA-Loop), dejando obsoleta la capacidad de respuesta humana. Lleva la guerra a un nivel de velocidad y sofisticación sin precedentes, planteando serios desafíos legales, morales y éticos en torno a la sustitución y la relegación del juicio humano.

Pero como veíamos, la sola aplicación de una tecnología novedosa no conlleva necesariamente una revolución generacional de la guerra. En la actualidad estamos siendo testigos de la aplicación de un alto nivel de robótica en los campos de batalla, con cierto nivel de IA, pero sin llegar a generar cambios permanentes en las doctrinas. Sin embargo, la combinación y coincidencia en los campos de batalla con otras tecnologías disruptivas emergentes anteriormente citadas como las armas hipersónicas, energía dirigida, tecnología cuántica o nanotecnología podrían llegar a provocar cambios profundos en la manera de entender la guerra, una revolución.

El programador humano del sistema define los parámetros de la misión para el AWS, incluyendo objetivos. A diferencia de los sistemas no tripulados (UxS) convencionales operados remotamente, los AWS son capaces de modificar sus itinerarios y tomar decisiones sobre sus actividades gracias a la integración de inteligencia artificial (IA). Los sistemas autónomos adquieren conciencia situacional de los datos que recopila del entorno operativo con sus propios sensores y de los que se comparten en la red colaborativa autónoma a través de la nube de combate.

La guerra pulsante: combatir a la velocidad de las máquinas

Como ya hemos visto, la tecnología está acelerando todos los procesos humanos, tanto físicos como cognitivos, incluyendo los relativos al combate. De todas las tecnologías, destacan por su carácter catalizador en combate la inteligencia artificial (IA) o/y la

robótica aplicada a los sistemas no tripulados (UxS). La combinación de ambas herramientas genera los conocidos como sistemas de armas autónomos (AWS). La OTAN define los AWS como sistemas que deciden y actúan para alcanzar los objetivos deseados, dentro de unos parámetros definidos, basándose en los conocimientos adquiridos y en la evolución de la conciencia de la situación, siguiendo una línea de acción óptima pero potencialmente impredecible.

Disponer de sistema autónomos, que tomen sus propias decisiones tácticas mediante IA, permitirá incrementar exponencialmente el *ritmo* de las operaciones y el *tempo* de las decisiones. El *ritmo* frenético que imponen las máquinas por su velocidad física y el mayor *tempo* en la toma de decisiones de la IA terminará dejando al humano fuera de muchas actividades y acciones. Esta autonomización requerirá una menor implicación humana en las acciones, y como consecuencia directa, un menor grado de conocimiento situacional. Nos encontraremos en un campo de batalla con dos cogniciones: una natural (humana) y otra artificial (IA).

La doctrina necesita evolucionar hacia una concepción que enmarque ambas cogniciones y formas híbridas de resolver problemas militares. Derivado de ello, la capacidad de engaño y decepción sobre estas cogniciones cambiará. Si bien hasta ahora el humano engañaba al humano, en adelante podrán aplicarse maniobras de decepción máquina-humano, máquina-máquina y humano-máquina. Las fuerzas autónomas crean un nuevo paradigma en la dimensión del planeamiento, la toma de decisiones y la decepción al adversario. Como hemos visto anteriormente, la 5GW se caracteriza por la preeminencia de las acciones en el dominio cognitivo, con ambigüedad y manipulación de las percepciones. Va a ser más difícil discernir qué es real y qué no, o si estamos cayendo en un engaño del adversario.

Por otro lado, podríamos considerar que la tendencia de los tiempos necesarios para la toma de decisiones (*tempo*) y la ejecución de acciones (*ritmo*) tiende a cero. A su vez, la franja temporal entre *tempo* y *ritmo* también se acorta y tiende a cero, mientras que sus espacios de cognición y actuación tienden a infinito. La IA lo entiende todo y los enjambres robóticos lo cubren todo. Por consiguiente, con valores equivalentes, *tempo* (lo cognitivo) y *ritmo* (lo físico) se equiparan para crear un nuevo concepto de guerra más allá de las guerras de atrición, maniobra e híbrida, o quizás todas a la vez.

Imaginemos acciones en las que la IA es capaz de identificar en tiempo real vulnerabilidades del sistema adversario y aplicar una cantidad ingente de masa en base a enjambres de AWS durante el tiempo estrictamente necesario para alcanzar los efectos deseados y evitar la pérdida de capacidad de combate, y repetir esto una y otra vez de manera constante, sin permitir margen de reacción o recuperación al enemigo.

Estas acciones pulsantes serían el concepto de empleo idóneo para un sistema de combate autónomo. Una guerra pulsante, de naturaleza multidominio, en base a una gran red federada de combatientes autónomos que no requieren de una cadena jerárquica para tomar la mejor decisión, aplicando simultáneamente los principios de la guerra, una repetición constante de estímulo-decisión-acción que satura al adversario (ritmo) y rompe su ciclo de toma de decisiones (tempo).

Acciones pulsantes autónomas que no solo se ejecutarán en los dominios físicos, sino que emplearán otros canales de actuación en el dominio virtual a través de IA generativa. Las acciones ciber buscarán un doble propósito. Por un lado, atacar sistemas vitales para el normal funcionamiento y sostenimiento del enemigo (efectos físicos), creando caos y desconcierto; y por otro lado, generando campañas de desinformación masiva a través del empleo de *bots* que manipulen las narrativas y las percepciones de los combatientes y sociedad adversaria (efectos cognitivos).

De esta manera, la IA se convierte en la coordinadora única y omnipresente en los dominios físicos y virtuales, creando efectos combinados entre ambos entornos, que alcanzan sinergias multiplicadoras en el dominio cognitivo. El resultado es la aniquilación de la voluntad de combatir de la sociedad adversaria, y con ello, la retirada de recursos y fuerzas del combate. Es el resultado de una combinación repetitiva de acciones cinéticas y no cinéticas sobre un enemigo abrumado y sobrepasado en los frentes físicos, virtuales y cognitivos.

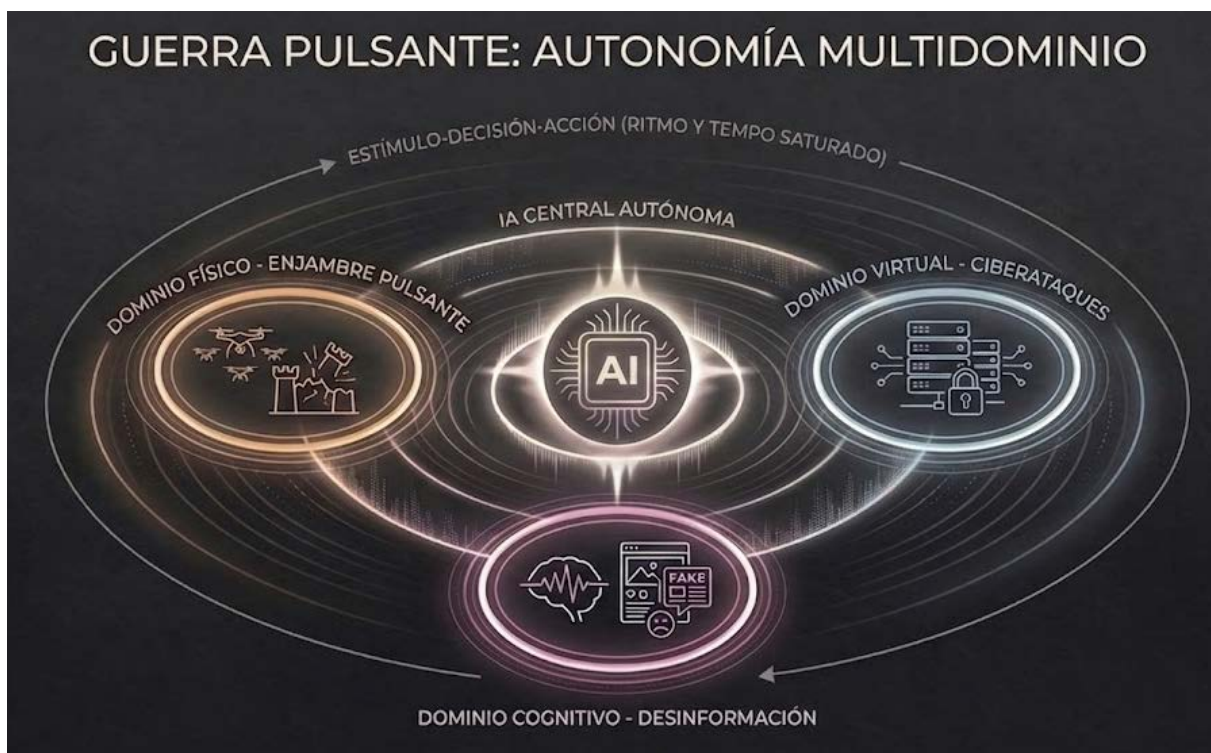


Imagen 3. Imagen conceptual de la guerra pulsante. Fuente: elaboración propia con Gemini

Dimensión física

Las tecnologías disruptivas que hemos mencionado están elevando los conceptos de velocidad y precisión a niveles sin precedentes, a la vez que desligan la operatividad de los sistemas de los operadores humanos. Más allá del debate de si se trata de innovación o de una auténtica revolución militar, lo que es cierto es que se están creando los mimbres para un cambio de paradigma. Con ello, las fuerzas militares que anticipen estos cambios y se adapten se garantizarán la ventaja en el enfrentamiento.

El sostenimiento deberá reorientarse a apoyar plataformas autónomas en las que la presencia humana será residual. El apoyo sanitario perdería peso específico en beneficio del mantenimiento, de manera que el antiguo esfuerzo de evacuación y tratamiento de bajas se orientará a la recuperación y reparación de máquinas. Además, la sensorización de los sistemas creará gemelos digitales que permitirán llevar a cabo acciones de mantenimiento predictivo.

Las clases de aprovisionamiento centradas en el sostenimiento humano (I, II, VI y VIII) ceden peso ante las orientadas a las máquinas (clases III y IX). La fabricación aditiva está permitiendo a unidades militares crear de manera autosuficiente repuestos

esenciales y sistemas de combate completos. Esto supone un cambio radical en la concepción de la logística, apareciendo una nueva función: la producción. Con ello, la adquisición de sistemas no recaería totalmente en la industria civil, sino que se llevaría hasta el propio campo de batalla, acelerando la velocidad de reposición.

El volumen y peso que se dedicaba al componente humano de los sistemas será reducido o empleado en otras capacidades. Con ello las plataformas autónomas podrán hacer lo mismo, o más, con un menor tamaño y coste. La tendencia en el diseño de sistemas autónomos es a disminuir los factores SWaP¹² para ganar en discreción y abaratar costes. Con un ratio SWaP inferior, el campo de batalla será inundado por un ecosistema de pequeños sensores y vehículos autónomos.

La doctrina podrá integrar los nuevos modos de empleo basados en sistemas tripulados, remotamente controlados, semiautónomos o autónomos. Destacan dos conceptos: como concepto interesante en esta materia encontramos las plataformas opcionalmente tripuladas OMP (Optionally Manned Platform), que dependiendo de la misión contarán con personal a bordo, estarán controladas remotamente o serán plenamente autónomas; por otro lado, aparece el combate colaborativo con los protocolos MUM-T (Manned-Unmanned Teaming) que permite operar en conjunción a unidades tripuladas y sistemas autónomos de acompañamiento.

Y como ya hemos anticipado, algunas funciones del combate, y en un futuro puede que todas, podrán convertirse en autónomas; si bien, por el momento, otras permanecerán humanas o en un punto intermedio. La IA permitirá al humano ampliar el rango de datos a su alcance y realizar procesos simultáneos. Paradójicamente esto provocará que la organización exija aún más al operador humano. Por ello, el adiestramiento del componente humano deberá adaptarse a estos nuevos requerimientos.

Dimensión virtual

Salvaguardar la cognición de la IA será fundamental para la supervivencia de una fuerza militar autónoma. El objeto de la protección pasaría de lo físico a lo virtual. La ciberseguridad se convertirá por tanto en el esfuerzo principal para la protección de las vulnerabilidades propias y explotación de las del enemigo. Todo ello en un entorno

¹² Space, Weight and Power.

operativo con un espectro electromagnético congestionado y en competición, en el que se producirán acciones ciberpulsantes, que generarán efectos físicos y cognitivos.

Profundizando en esta idea, la concepción de las fuerzas militares autónomas se alejarán de la visión tradicional física (*hardware*) basada en plataformas, orientándose hacia una arquitectura virtual (*software*). Más allá de datos, ancho de banda, sensores o equipos de enlace, la gestión eficiente de la información y el conocimiento (IKM) generado por estos elementos será la base de funcionamiento de fuerzas autónomas (objetivo cognitivo). La ventaja táctica, por tanto, se alcanzará con la capacidad de implementar algoritmos de misión superiores a los del adversario. En definitiva, alcanzar un alto grado de integración basado en un *software* único, robusto y soberano.

El componente humano estará capacitado para la interacción humano-máquina que garantice el empleo eficiente de fuerzas híbridas. Una porción de este personal será, además, responsable de la programación y supervisión del entrenamiento de la IA encargada de gobernar los sistemas autónomos de toda la fuerza. El *Machine Learning* evoluciona hacia el *Deep Learning* que permite a los sistemas no solo aprender y replicar la capacidad cognitiva humana.

La protección de la integridad de la IA, sus algoritmos y el entrenamiento son objetivos de alto valor para el adversario. Nos encontramos ante una vulnerabilidad del sistema, una puerta trasera que puede ser activada en un momento crítico del combate. Podría provocar que los AWS dejen de funcionar, limiten su operatividad, o en el peor de los casos deserten. La IA necesitará un entrenamiento robusto (que cubra todo el espectro del combate) y seguro (garantice la cognición que la fuerza usuaria desea).

A diferencia de las fuerzas militares actuales, cuyo centro de gravedad radica en grandes plataformas y sistemas, las fuerzas autónomas se basarán en el empleo simultáneo y colaborativo de sistemas operativos compatibles, lo que supone un cambio profundo en la concepción de fuerza, variando del *hardware* del dominio físico tradicional al *software* del dominio virtual en fuerzas autónomas.

Llevar a cabo operaciones militares empleando un amplio ecosistema de ASW requerirá un nivel de sincronización sin precedentes. Todos los sistemas operativos empleados deberán ser iguales o, al menos, compatibles. De esta manera se garantiza el flujo de información en la red federada que gobierna la fuerza. Los AWS podrán compartir los datos obtenidos de manera conjunta por los sensores de todo el ecosistema, creando un

campo de batalla transparente. Igualmente, las armas y componentes robóticos podrán alcanzar sinergias al combinarse eficazmente.

Los sistemas definidos por *software* se presentan como la mejor opción. Por ello, para que las IA de todos estos sistemas puedan intercomunicarse y entenderse en el campo de batalla, los programas de adquisición deberán ir determinados por el *software* y el sistema operativo dominante. El *software* se convierte así en la piedra angular de la fuerza autónoma.

Esta simbiosis en base a una red distribuida federada con una profunda coordinación multiagente, requiere un *software* común compatible con máquinas, sensores y humanos. La relación multiagente colaborativa genera una estructura aplanada monitorizada en un Combat Management System (CMS) que canaliza la función de control de la fuerza simbiótica gobernada por máquina y humano.

Dimensión cognitiva

El componente humano está siendo sustituido paulatinamente por máquinas y sistemas en aquellos procesos físicos que así lo permitan (ritmo), y como asistentes en ciertos procesos cognitivos relacionados con la toma de decisiones (tempo). Todo ello sincronizado por sistemas de comunicaciones, mando y control que crean el entorno virtual en el que se integra el humano y la máquina, y en el que el humano gobierna a la máquina, por el momento. Retomamos aquí la idea de que, en el campo de batalla definido por la guerra pulsante, encontramos dos cogniciones: una natural (humana) y otra artificial (IA), ambas con procesos de toma de decisiones diferenciados.

Con todo lo anterior, la atención humana podría llegar a centrarse más en cómo operan los sistemas autónomos, en vez de cuál es la situación táctica en el campo de batalla, un cambio de la *niebla de la guerra* a la *niebla de los sistemas*. Hay pensadores que van más lejos y anticipan una singularidad en el campo de batalla, según la cual la capacidad cognitiva humana no podrá seguir estos ritmo y tempo impuestos por las máquinas. Es decir, los humanos no harían contribuciones significativas, convirtiéndose en irrelevantes para las tomas de decisiones. Esto deriva en una cuestión de trascendencia: mantener o sacar al humano del bucle de control de las máquinas.

Tenemos, por lo tanto, una nueva forma de entender el papel del ser humano en la guerra. El humano abandonará las tareas relativas a «operar» y se reinventará para «entrenar» máquinas. Una fuerza militar autónoma, o parcialmente autónoma, operará con tres modos de control y supervisión humana:

- Human-in-the-loop (HITL): supervisión e instrucciones. Es necesaria la orden humana de actuación, aplicando la tradicional *Kill Chain*. Ejemplo: AEGIS.
- Human-on-the-loop (HOTL): solo supervisión; relacionado con el nuevo concepto de *Kill Web*. Ejemplo: CIWS Phalanx.
- Human-out-of-the-loop (HOOTL): ni supervisión ni instrucciones, totalmente autónomas, *Killer Robots*. Las máquinas son capaces de aprender y operan sin ningún tipo de intervención para alcanzar el objetivo fijado.

En situaciones de presión y con poco margen temporal, cuando una máquina presenta una recomendación, el ser humano recurre al razonamiento automático en vez de al deliberativo. La psicología social identifica aquí un *sesgo de automatización* por el que el humano comienza a ser marginado de la toma de decisiones al depositar una excesiva confianza en las máquinas. Ningún operador humano es capaz de actuar con la suficiente velocidad y precisión como para interceptar una amenaza a las altas velocidades que han empezado a conquistar el campo de batalla.

En estos escenarios en los que el ataque y la defensa se producen a velocidades sobrehumanas, se empiezan a diferenciar las acciones que pueden llevar a cabo humanos de las que deben ser autónomas. No se plantean restricciones al empleo de AWS-HOOTL para operaciones de apoyo como logística o producción a retaguardia, alejados de las zonas de conflictos. Por otro lado, los AWS-HOTL se están convirtiendo en fundamentales para acciones defensivas o reactivas. Pero parece que las acciones ofensivas deliberadas seguirán requiriendo al humano para «apretar el botón» que desencadene una acción cinética con potenciales bajas humanas, con AWS-HITL.

La teoría de las tres manzanas aplicada a los niveles de control humano en sistemas autónomos, con los tres modos de control ocurriendo simultáneamente en el mismo campo de batalla. Sin duda, el marco legal y ético debería ser el primer proceso a cerrar para dejar claros los límites en la programación y empleo de estos sistemas.

La gran diferencia entre la 5GW y la 6GW será la elevada capacidad de percepción, análisis y decisión de la IA. El *Deep Learning*¹³ define las cuatro categorías de la IA:

- Perceptiva (sensorial). Reconocimiento e interpretación del mundo exterior a través de sensores visión, audio, temperatura, etc.
- Computacional (análisis). Procesamiento de datos, optimización, cálculos complejos y repetitivos a gran escala, con capacidad predictiva.
- Cognitiva (razonamiento). Planificación, y toma de decisión, imitando el pensamiento, la toma de decisiones y el aprendizaje estratégico humano.
- Generativa (creación). Generación de contenido, síntesis, producción de resultados nuevos y originales (texto, imagen, audio).

Es precisamente en la letalidad de estos sistemas donde radica el centro de la discusión ética. El factor legal de las consecuencias de las decisiones y acciones llevadas a cabo por sistemas autónomos es una asignatura pendiente. La responsabilidad del comandante-operador-programador, el instinto de supervivencia de los AWS, o los daños colaterales son algunos de los puntos a desarrollar. El empleo de sistemas autónomos debe observar la legalidad intencional basada en la Ley Humanitaria Internacional y la de Conflictos Armados, con aspectos clave como la distinción entre combatiente y civil, la proporcionalidad y la necesidad del uso de la fuerza. La ONU está trabajando en un tratado internacional para 2026 que prohíba los sistemas autónomos letales (LAWS) sin control ni supervisión humana.

¹³ GOODFELLOW, Ian, BENGIO, Yoshua y COURVILLE, Aaron. *Deep Learning*, 2016.

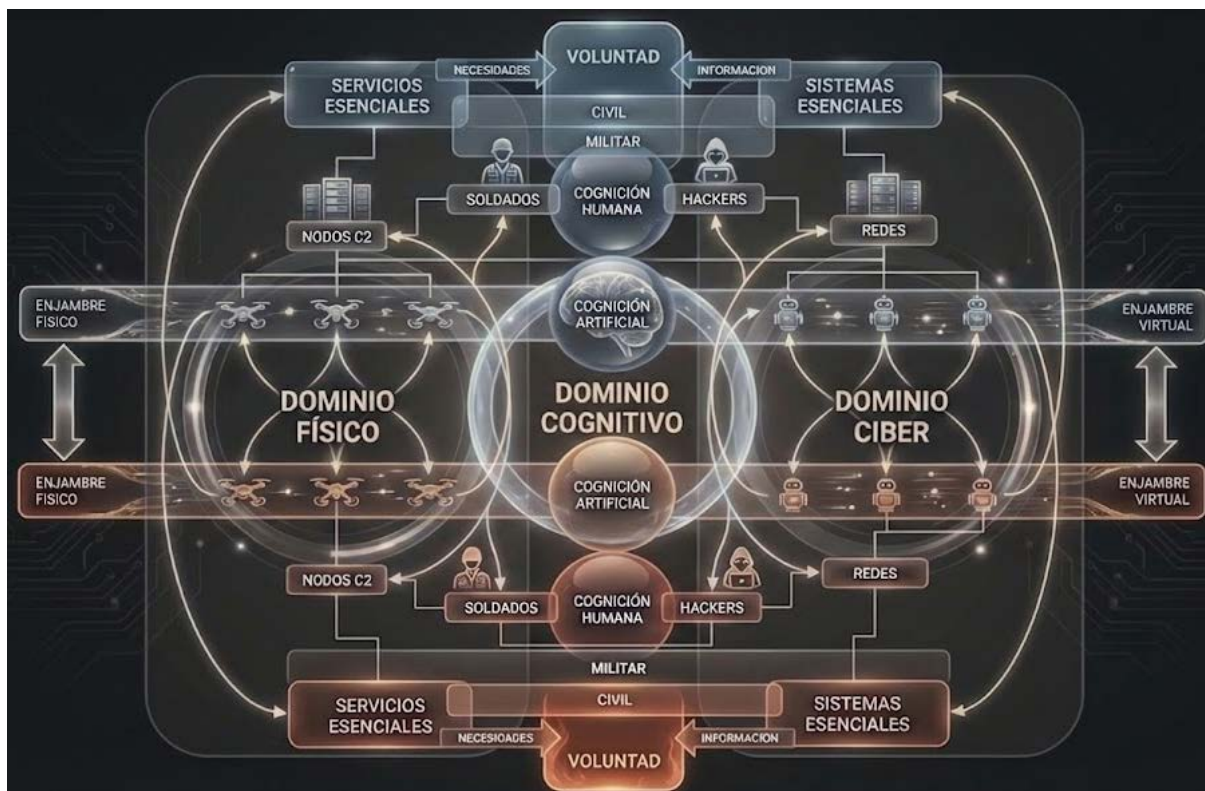


Imagen 4. Orden de batalla de la guerra pulsante. Fuente: elaboración propia con Gemini

Conclusiones

Dentro de las generaciones de la guerra, los expertos indican que es probable que hayamos superado la era de la guerra híbrida (cuarta generación - 4GW) y nos encontremos en los anales de la guerra cognitiva (quinta generación - 5GW), en la que el combate se centra en la mente, las voluntades y las percepciones. El objetivo no es destruir físicamente, sino quebrantar la voluntad de lucha del adversario, desde sus combatientes hasta la sociedad a la que protegen.

La inteligencia artificial y los sistemas no tripulados han hiperacelerado los procesos de toma de decisiones y las acciones tácticas. Nace la guerra pulsante, un modo de combatir en el que se busca la saturación de los sistemas de defensa adversarios en las dimensiones física y virtual con acciones constantes, masivas y precisas empleando sistemas dirigidos por inteligencia artificial.

El ser humano se convierte en el eslabón débil del ciclo de la toma de decisiones. La velocidad del combate actual supera la capacidad biológica de reacción. El humano deja de ser quien aprieta el botón para convertirse en un entrenador y supervisor de

algoritmos, quedando inevitablemente fuera de la toma de decisiones tácticas inmediatas.

Dotar de autonomía total a los sistemas de combate sigue siendo un dilema ético y moral sin resolver. Sin embargo, los expertos ya dan como una posibilidad real el inicio de la guerra autónoma (sexta generación - 6GW), una era en la que las máquinas operarán con total autonomía en unos campos de batalla deshumanizados. La evolución es exponencial y los períodos entre generaciones cada vez más cortos.

El *software* se convierte así en el centro de gravedad de estas nuevas generaciones de la guerra. La ventaja estratégica consiste en tener sistemas operativos compatibles y una ciberseguridad robusta para evitar que la inteligencia artificial y el sistema de mando y control que emplea sea hackeada. La soberanía tecnológica será la clave en un ámbito en el que la dependencia de la empresa privada es cada vez mayor, con actores no estatales capaces de acceder a sistemas de alto potencial militar.

*Juan Carlos Andrés Herrero**
Comandante de Infantería de Marina