

La guerra sin declaración

Cómo la tecnología redefine el poder antes del primer disparo.

DOI: 10.29236/sistemas.n180a8

Resumen

La geopolítica del siglo XXI ya no se decide únicamente en tratados o en despliegues visibles de tropas, sino en el control silencioso de semiconductores, satélites, algoritmos y percepciones. Este artículo sostiene que la “nueva guerra” no lo es en su naturaleza —dominar la voluntad del adversario sigue siendo el objetivo de siempre—, sino en su arquitectura: hoy opera de forma multidominio, simultánea y frecuentemente indetectable hasta el momento mismo de su ejecución. Se examina la carrera tecnológica entre bloques —semiconductores e inteligencia artificial— como el verdadero campo de batalla previo al conflicto armado declarado, y se conecta cada uno de los seis dominios reconocidos de la guerra —terrestre, marítimo, aéreo, espacial, cibernético y cognitivo— con el motor tecnológico específico que hoy lo transforma. Se ilustra con la Operación Resolución Absoluta, ejecutada en Venezuela en enero de 2026, como caso empírico de sincronización simultánea de los seis dominios en una sola acción de pocas horas. Se concluye que la hegemonía ya no se conquista: se administra tecnológicamente, y que las naciones sin postura estratégica propia corren el riesgo de convertirse en terreno de disputa ajena, y no en actores de su propia seguridad.

Palabras clave

Geopolítica tecnológica; guerra multidominio; hegemonía digital; dominio cognitivo; ciberdefensa.

Introducción

Durante siglos, la geopolítica se explicó a partir de variables tangibles: territorio, población, recursos naturales y capacidad de movilización militar. En el siglo XXI esa ecuación ha cambiado de naturaleza sin cambiar de propósito. El poder sigue buscando lo mismo de siempre —imponer voluntad, proteger intereses, sostener hegemonía—, pero el terreno donde se disputa ya no es exclusivamente físico: es el control de semiconductores, redes satelitales, algoritmos de inteligencia artificial y, en última instancia, de la percepción humana.

Este artículo parte de una pregunta incómoda para la doctrina clásica de la guerra: ¿sigue siendo útil distinguir tajantemente entre “guerra” y “paz” cuando el control sobre un adversario —o sobre un aliado— puede ejercerse de forma permanente, silenciosa y tecnológica, sin que medie jamás una declaración formal de hostilidades? La carrera tecnológica entre bloques —Estados Unidos, China, la Unión Europea— no es un telón de fondo económico de las tensiones internacionales actuales: es, en sí misma, la disputa central por la hegemonía del siglo XXI.

La tesis central de este artículo es que la guerra contemporánea ha dejado de tener un inicio y un final claramente delimitados, para con-

vertirse en un continuo de competencia tecnológica que se activa —de forma cinética y visible— solo cuando el desequilibrio de capacidades lo permite. Se desarrollan cuatro niveles de análisis, de lo macro a lo específico: primero, la carrera estructural por el control de la infraestructura tecnológica crítica entre bloques; segundo, el motor tecnológico que hoy transforma cada uno de los seis dominios reconocidos de la guerra —terrestre, marítimo, aéreo, espacial, cibernético y cognitivo—; tercero, la traducción operativa de ese marco en un caso real y reciente, la Operación Resolución Absoluta en Venezuela; y cuarto, una profundización del dominio cognitivo, que no es nuevo en su esencia pero sí en su escala y velocidad de ejecución. Se cierra con una reflexión sobre el lugar de naciones intermedias como Colombia en este nuevo tablero.

1. La nueva materia prima del poder: semiconductores, inteligencia artificial y bloques

En 2026 la soberanía de una nación ya no se mide solamente por sus reservas de crudo o por su capacidad de movilización militar convencional, sino también por su acceso a semiconductores avanzados (Yılmaz, 2026). Estos componentes son de naturaleza dual: sostienen tanto la economía digital como la precisión de los sistemas

de armas modernos y la eficacia de la guerra electrónica. La industria de los chips, que durante décadas fue percibida como un triunfo silencioso de la globalización, se ha revelado hoy como su vulnerabilidad más evidente: la fabricación de los nodos más avanzados se concentra en un puñado de instalaciones, en su mayoría en Taiwán, bajo presión geopolítica creciente.

Peters documenta cómo la Ley CHIPS and Science de Estados Unidos representa una ruptura deliberada respecto al libre mercado neoliberal, en favor de una estrategia de ciencia y tecnología dirigida y sostenida desde el nivel federal, con el objetivo explícito de reducir la dependencia de una cadena de suministro internacional fácilmente disruptible (2023). China, por su parte, no ha permanecido pasiva, impulsa arquitecturas abiertas como RISC-V¹ para reducir su dependencia de la propiedad intelectual estadounidense (ARM, x86), y compete no por frontera tecnológica absoluta, sino por velocidad y costo de despliegue. En el plano regional, Ruck muestra cómo la Unión Europea reorganiza sus propias cadenas de valor en semiconductores mediante lo que denomina un “geo-economic fix”, evidenciando

que la disputa ya no es bilateral, sino de bloques que compiten por autonomía tecnológica (2026).

A esta carrera se suma la disputa por la inteligencia artificial, que Yilmaz (2026) caracteriza como una nueva dimensión del poder geopolítico que trasciende lo económico. La IA influye directamente en cómo los Estados proyectan autoridad, regulan la innovación y negocian normas globales. El estudio identifica tres paradigmas de gobernanza en competencia —el modelo liberal orientado a la innovación (Estados Unidos), el modelo autoritario de control estatal (China) y el modelo regulatorio orientado a la ética (Unión Europea)— y advierte que la IA intensifica asimetrías de poder, generando “jerarquías algorítmicas” que refuerzan la dependencia digital, particularmente en el Sur Global (Yilmaz, 2026).

Conviene precisar, sin embargo, que esta tercera posición europea es de naturaleza distinta a las otras dos: mientras Estados Unidos y China compiten de forma directa por volumen de inversión y capacidad de cómputo —los cientos de miles de millones de dólares referidos más arriba—, la Unión Europea no dispone de un competidor propio a esa escala de capital, y ejerce su influencia geopolítica en la IA no como tercer polo de inversión, sino como poder regulatorio: sus normas, como la Ley de IA europea, tienden a convertirse en estándar

¹ *Reduced Instruction Set Computer* (“Computador de Conjunto de Instrucciones Reducido”). Es una filosofía de diseño de procesadores que usa instrucciones simples y pocas, en lugar de instrucciones complejas y numerosas (el enfoque contrario se llama CISC, usado por ejemplo en x86 de Intel). La ventaja de RISC es que los chips resultan más simples, rápidos, eficientes en consumo de energía y más fáciles de personalizar.

de facto global por el llamado “efecto Bruselas”, dado que muchas empresas prefieren cumplir la norma más exigente una sola vez para todo el mercado mundial.

Akram et al. (2025) refuerzan el punto estructural al mostrar cómo los clústeres de innovación en inteligencia artificial —Silicon Valley, Shenzhen, Tel Aviv— funcionan hoy como nuevos centros de influencia geopolítica, y cómo la soberanía de datos se ha convertido en una dimensión crítica de la seguridad nacional y de la palanca diplomática de los Estados. El resultado estructural es la formación de bloques tecnológicos de facto, alianzas de suministro, de infraestructura y de gobernanza que se parecen cada vez más a los bloques geopolíticos tradicionales, pero cuya moneda de cambio ya no es únicamente territorio o tratados militares, sino acceso garantizado a chips, datos y capacidad computacional.

2. Los seis dominios de la guerra y su motor tecnológico

La doctrina militar contemporánea reconoce seis dominios de la guerra: terrestre, marítimo, aéreo, espacial, cibernético y cognitivo. Lo que este artículo sostiene es que, si bien los seis han existido conceptualmente por décadas —los tres primeros desde siempre, el espacial desde la Guerra Fría, el cibernético desde finales del siglo XX y el cognitivo desde que existe la guerra misma—, hoy cada uno está siendo transformado por un motor

tecnológico específico, y es precisamente esa transformación simultánea la que redefine el carácter de la guerra contemporánea.

En el dominio terrestre, el motor son los vehículos no tripulados de combate y reconocimiento, los exoesqueletos que amplían la capacidad física del combatiente, y los sistemas C4ISR de campo que integran mando, control, comunicaciones e inteligencia en tiempo real hasta el nivel de escuadra, junto con munición de precisión guiada que reduce drásticamente el margen de error operativo. En el dominio marítimo, la transformación llega de la mano de drones navales y submarinos autónomos, sensores de fondo marino para vigilancia persistente, y una nueva forma de vulnerabilidad estratégica: la guerra de cables submarinos, por donde transita más del noventa por ciento del tráfico de datos intercontinental y que hoy constituye un objetivo de sabotaje de alto valor, tan crítico como cualquier estrecho marítimo tradicional.

El dominio aéreo se transforma con la aviación de quinta y sexta generación, los enjambres de drones capaces de saturar defensas antiaéreas mediante numerosidad más que mediante sofisticación individual, y la guerra electrónica aérea que ciega sensores y radares antes de que el adversario perciba la amenaza. El dominio espacial depende hoy de constelaciones de satélites de observación e inteligencia, de la

capacidad de mando integrada como la que ejerce el Comando Espacial estadounidense (SPACECOM), y de una competencia creciente por capacidades anti-satélite que podrían inutilizar en minutos la infraestructura orbital de un adversario, incluyendo constelaciones comerciales de conectividad masiva que ya se emplean con fines militares.

El dominio cibernético, sostenido por comandos especializados como el Comando Cibernético de Estados Unidos (CYBERCOM), ha probado su capacidad de sabotear infraestructura crítica —energía, comunicaciones, sistemas financieros— sin disparar un solo proyectil, y hoy incorpora inteligencia artificial ofensiva capaz de identificar y explotar vulnerabilidades a una velocidad que ningún equipo humano de ciberdefensa puede igualar. Finalmente, el dominio cognitivo, que se desarrolla con mayor profundidad en la sección tercera de este artículo, encuentra en la inteligencia artificial generativa, los deepfakes y el targeting psicográfico su motor de transformación: la capacidad de moldear percepciones de forma masiva, personalizada y en tiempo real.

La implicación central de este marco es que ningún conflicto contemporáneo de relevancia estratégica se libra hoy en un solo dominio. La ventaja decisiva pertenece a quien logra sincronizar los seis de forma simultánea, no a quien es superior

en uno de ellos de manera aislada. El caso que se desarrolla a continuación —la Operación Resolución Absoluta en Venezuela— constituye, hasta la fecha, el ejemplo más completo y mejor documentado de esta sincronización multidominio ejecutada en pocas horas.

3. Guerra multidominio en tiempo real: el caso de la Operación Resolución Absoluta en Venezuela

Si el nivel anterior describe la estructura, este segundo nivel ofrece evidencia empírica de su traducción operativa. La madrugada del 3 de enero de 2026, fuerzas estadounidenses ejecutaron en Caracas la Operación Resolución Absoluta, con el objetivo de capturar con vida a Nicolás Maduro y Cilia Flores. El análisis de esta operación, permite sostener un argumento disruptivo: no se trató de una operación militar convencional “apoyada” por tecnología, sino de una operación en la que la tecnología fue la operación misma, y donde la acción cinética final —el asalto físico— fue apenas el último eslabón de una cadena multidominio ya consumada.

La secuencia técnica es reveladora. Durante meses, la inteligencia estadounidense combinó inteligencia de señales (SIGINT), inteligencia de imágenes (IMINT) e inteligencia humana (HUMINT) para mapear en detalle la red de seguridad, rutinas y entorno inmediato del objetivo. En el momento de ejecución, el SPACECOM y el CYBER-

COM superpusieron efectos coordinados para abrir un corredor seguro de aproximación; los sistemas de defensa antiaérea de origen ruso y los radares de origen chino fueron neutralizados mediante guerra electrónica antes de que las aeronaves entraran en su alcance; y un corte cibernético selectivo de energía facilitó el desplazamiento terrestre de las fuerzas de extracción. Una flota de drones —inteligencia, vigilancia y reconocimiento (ISR), armados (Reaper) y furtivos— sostuvo monitoreo casi permanente sobre el objetivo durante semanas, mientras la guía satelital dirigía en tiempo real a las tropas en tierra durante el asalto final.

Este caso ilustra con precisión la tesis del artículo: los dominios espacial, cibernético, los elementos de inteligencia y cinéticos no actuaron de forma secuencial, sino simultánea e integrada, en una ventana operativa de apenas unas horas. La superioridad no residió en el número de tropas desplegadas, sino en el control absoluto de la información y de la infraestructura crítica del adversario antes de que este pudiera siquiera reaccionar. Es, en ese sentido, el ejemplo más nítido disponible hasta la fecha de cómo la carrera tecnológica descrita en la sección anterior se convierte en capacidad de intervención real.

4. El dominio cognitivo: lo antiguo con motor nuevo

El tercer nivel de análisis corresponde al dominio cognitivo, que

conviene precisar no es una novedad conceptual: la guerra psicológica y la disputa por la percepción del adversario y de la propia población han existido desde la misma génesis de la guerra. Lo verdaderamente nuevo es la escala, la velocidad y la precisión de segmentación que la tecnología actual permite. Deppe y Schaal (2024) documentan cómo la OTAN, a través de su concepto exploratorio de guerra cognitiva (NATO ACT), define este dominio como el uso de tácticas, técnicas y herramientas habilitadas por tecnología para influir en la toma de decisiones humanas a nivel individual y social, alineando el comportamiento del adversario con los objetivos políticos, sociales, económicos o militares propios.

Miller (2023) profundiza en la dimensión ética del fenómeno, advirtiendo que la manipulación cognitiva mediada por tecnología plantea desafíos normativos distintos a los de la propaganda tradicional, precisamente por su capacidad de operar de forma personalizada y a gran escala mediante inteligencia artificial generativa y algoritmos de recomendación. En el caso venezolano, este dominio se activó en dos capas diferenciadas: una capa operativa, orientada a generar parálisis psicológica en las fuerzas de custodia antes y durante el asalto; y una capa narrativa posterior, en la que el aparato comunicacional oficialista caracterizó lo ocurrido como una “guerra cognitiva imperial” contra el pueblo venezolano, mientras la Ca-

sa Blanca amplificó testimonios virales de la propia operación como demostración de poder disuasivo hacia la región. Ambas narrativas, cabe subrayarlo, son actores interesados en la disputa, no fuentes neutrales, lo cual confirma que el dominio cognitivo permanece activo mucho después de que cesa la acción cinética.

5. Colombia y la periferia tecnológica

El cierre analítico exige una pregunta incómoda para naciones intermedias como Colombia: en este nuevo tablero, ¿somos actores o somos terreno? La evidencia sugiere que, sin una postura estratégica propia, países como el nuestro corren el riesgo de convertirse en espacio de disputa ajena antes que en sujetos activos de su propia seguridad. Esto exige incorporar explícitamente los espacios comunes de la seguridad —el marítimo, el espacial y el ciberespacio— como ámbitos de especial interés dentro de la arquitectura de seguridad nacional, con estrategias transversales que hoy, en buena medida, siguen pendientes de institucionalización plena.

La lección de la Operación Resolución Absoluta para una nación como Colombia no es únicamente táctica, sino conceptual: la superioridad ya no se mide en número de tropas o en plataformas convencionales, sino en la capacidad de un Estado para comprender, defender y eventualmente disputar el control

de sus propios dominios espacial y cibernético. Ningún Sistema de Seguridad Nacional del siglo XXI puede considerarse completo si no integra lo ciber y lo espacial como ámbitos operativos propios, y no simplemente como anexos tecnológicos de los dominios tradicionales.

Conclusiones

La guerra contemporánea ya no se declara; ocurre porque todo el desequilibrio tecnológico entre las partes permite que suceda tan rápidamente que comienza mucho antes de que el mundo sepa que está en problemas. La hegemonía global ya no se trata simplemente de ocupación territorial, sino que se gestiona constantemente mediante el control de infraestructuras críticas (semiconductores, satélites, redes) y la capacidad de operar en dominios espaciales, cibernéticos y cognitivos simultáneamente, integrando en cada uno de ellos inteligencia de múltiples fuentes (SIGINT, IMINT, HUMINT) que hace posible la sincronización.

El caso de la Operación Resolución Absoluta confirma empíricamente esta tesis. La tecnología no acompañó la operación militar, la constituyó. Y el dominio cognitivo, lejos de ser una novedad, demuestra que la naturaleza de la guerra —disputar la voluntad del adversario— permanece intacta; lo que cambia es la velocidad, el alcance y la precisión con que hoy puede ejercerse.

Para países intermedios como Colombia, la conclusión es tanto una advertencia como una hoja de ruta.

La elección no es entre la paz y la guerra; se requiere que desarrollemos nuestra propia postura tecnológica y doctrinal, o que aceptemos que nuestro país está a punto de convertirse en un campo de batalla para disputas entre terceros. La geopolítica de las tecnologías de la información no es un asunto exclusivo de las grandes potencias, sino que es una condición de existencia para cualquier estado que quiera determinar su propio destino estratégico.

Referencias

- Akram, S., Shahid, M., & Tunio, H. (2025). The Geopolitics of AI: Analyzing the Impact of Artificial Intelligence on Global Power Dynamics and International Relations. *Review Journal of Social Psychology & Social Works*, 282-300.
- Deppe, C., & Schaal, G. (2024). Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept. *Frontiers in Big Data*.
- Miller, S. (2023). Cognitive warfare: an ethical analysis. *Ethics and Information Technology*, 1-10.
- Ruck, J. (2026). A Geoeconomic Fix? European Industrial Policy on Semiconductors Amidst Global Competition. *JCMS: Journal of Common Market Studies*, 742-761.
- Yilmaz, C. (2026). The Geopolitics of Artificial Intelligence Power, Regulation, and Global Governance. *Journal of Academic Social Studies*, 39-70.
- Peters, M. (2023). Semiconductors, geopolitics and technological rivalry: The US CHIPS & Science Act, 2022. *Educational Philosophy and Theory*, 1642-1646. 

Fabricio Cabrera Ortiz es general de la reserva del Ejército Nacional de Colombia, doctor en Seguridad Internacional, consultor en seguridad y defensa, Presidente de la Junta Directiva del Consejo de Generales de la Reserva del Ejército Nacional (CGREN) y Asesor Estratégico del Centro de Pensamiento y Obsevación Estratégica (CEPOE).