*Casus Belli* VI (2025), 135-159
Recibido: 12/08/2025 - Aceptado: 07/10/2025

# CONVERGENCIAS DISRUPTIVAS EN LA ARQUITECTURA DEL ORDEN GLOBAL

**Sergio Daniel Skobalski**
Universidad de la Defensa Nacional (UNDEF)

**Resumen:** Esta investigación se sitúa en un contexto de transformación profunda del orden estratégico internacional, caracterizado por alteraciones sustanciales en las formas de gobernanza, las dinámicas del conflicto y el ejercicio de la soberanía. Esta mutación se manifiesta en la convergencia de dos procesos estructurales que erosionan los pilares tradicionales de la política global: por un lado, el debilitamiento progresivo de la capacidad de las democracias liberales para sostener una participación política efectiva, pluralista y deliberativa; por otro, la emergencia de modalidades de conflictividad que desbordan el paradigma bélico convencional, articulándose mediante dispositivos híbridos, tecnológicos y cognitivos. El presente trabajo buscará evaluar la eficacia de los dispositivos institucionales de respuesta y extraer lecciones estratégicas para el fortalecimiento de la resiliencia democrática en un entorno internacional marcado por la disputa permanente por el control de los marcos interpretativos globales.

**Palabras clave:** guerra híbrida; guerra cognitiva; gobernabilidad híbrida; posdemocracia; soberanía cognitiva; seguridad democrática; tecnopolítica y algoritmos; zonas grises.

**Abstract:** This research is situated in a context of profound transformation of the international strategic order, characterized by substantial alterations in the forms of governance, conflict dynamics, and the exercise of sovereignty. This mutation is manifested in the convergence of two structural processes that erode the traditional pillars of global politics: on the one hand, the progressive weakening of the capacity of liberal democracies to sustain effective, pluralistic, and deliberative political participation; on the other, the emergence of forms of conflict that go beyond the conventional war paradigm, articulated through hybrid, technological, and cognitive mechanisms. This paper seeks to evaluate the effectiveness of institutional response mechanisms and draw strategic lessons for strengthening democratic resilience in an international environment marked by the permanent dispute over control of global interpretative frameworks.

**Key words:** hybrid warfare; cognitive warfare; hybrid governance; post-democracy; cognitive sovereignty; democratic security; technopolitics and algorithms; gray zones.

## Introducción

Las nuevas formas de confrontación no se limitan al plano militar: buscan moldear subjetividades, alterar los marcos de interpretación colectiva y actuar sobre el entorno informacional mediante estrategias simbólicas, narrativas, emocionales y algorítmicas. La noción de "posdemocracia", desarrollada por Colin Crouch (2004), adquiere particular relevancia en este contexto. Describe una configuración política en la que los procedimientos electorales permanecen operativos en su forma, pero los contenidos sustantivos del contrato democrático —como la soberanía popular, la deliberación pública y el control ciudadano— son progresivamente neutralizados por una captura decisional ejercida por élites tecnocráticas, financieras y corporativas. Esta anulación del contenido deliberativo se acompaña de una creciente administración tecnopolítica de lo social, donde las decisiones estratégicas son desplazadas desde los espacios públicos hacia circuitos opacos de gobernanza empresarial, automatizada o externalizada. En este contexto, la democracia liberal ya no funciona como una arquitectura de representación efectiva, sino que se transforma en una arquitectura ritualizada. Esta pérdida de sustancia la vuelve vulnerable a dinámicas de captura institucional, manipulación perceptual y dominación simbólica, especialmente en escenarios de guerra cognitiva e hibridación política. En paralelo, se consolida una nueva forma de conflictividad transnacional, caracterizada por la hibridez de

sus medios y métodos. Esta combina de manera estratégica operaciones militares convencionales con ciberataques, sabotajes económicos, guerra jurídica (*lawfare*), campañas de desinformación, manipulación algorítmica y operaciones psicológicas (Hoffman, 2009; Palmertz, 2022), tal como lo advierte el *European Centre of Excellence for Countering Hybrid Threats* respecto de las amenazas emergentes en el dominio cognitivo. La guerra híbrida contemporánea redefine los límites entre lo civil y lo militar, y entre lo interno y lo externo. Al desdibujar las fronteras estatales, actúa de forma simultánea en múltiples dominios, con lógica difusa, persistente y adaptativa. Su finalidad ya no se orienta a obtener victorias militares en el sentido clásico, sino a erosionar la arquitectura institucional, inducir fracturas emocionales sostenidas en el cuerpo social y colonizar los marcos interpretativos desde los cuales la sociedad construye su sentido político. Este fenómeno ha sido también conceptualizado como una *guerra cognitiva*, entendida como una forma de confrontación que actúa sobre el campo neuropsicosocial, con el objetivo de intervenir en las percepciones, los marcos de sentido y los patrones de conducta colectiva. Sus herramientas principales incluyen la inteligencia artificial, la minería de datos, la ingeniería social y la persuasión algorítmica (Claverie & du Cluzel, 2023; NATO Innovation Hub, 2021). La guerra cognitiva busca alterar el juicio crítico, instalar interpretaciones favorables al agresor y debilitar la capacidad de respuesta democrática, mediante tácticas como la saturación informativa, el shock emocional y la disonancia epistémica. En este marco, el dominio cognitivo es reconocido como el sexto dominio de la guerra —junto a los dominios terrestre, marítimo, aéreo, espacial y cibernético— conforme a la doctrina de la OTAN (2021). En este escenario, el presente trabajo parte de la premisa de que la convergencia entre *posdemocracia*, *guerra híbrida* y *guerra cognitiva* da lugar a un nuevo régimen global de poder, cuya lógica no es directa ni visible, sino que se despliega mediante mecanismos de invisibilización, simulación y captura simbólica del entorno. Su objetivo no se limita a imponer agendas por la fuerza, sino a construir hegemonía mediante dispositivos afectivos, narrativas polarizantes y tecnologías de control social que erosionan las condiciones mismas de posibilidad de una deliberación democrática auténtica. Desde una perspectiva metodológica, este trabajo se inscribe en un enfoque cualitativo, de carácter exploratorio y analítico, orientado a problematizar las transformaciones estructurales del orden global en el siglo XXI. La estrategia de investigación combina el análisis documental de fuentes primarias —como doctrinas estratégicas, discursos oficiales, documentos de defensa y estrategias nacionales de seguridad— con el estudio comparado de literatura académica, informes de *think tanks* y debates conceptuales provenientes de

los estudios estratégicos, enfoques críticos de la teoría política contemporánea y la epistemología del poder. Se adopta una perspectiva epistémica situada, en línea con las contribuciones de Donna Haraway (1988) y Sandra Harding (1986), que reconoce la imposibilidad de una neutralidad valorativa y reivindica la responsabilidad política del conocimiento. El objetivo general de esta investigación es analizar la reconfiguración estratégica del poder en el sistema internacional contemporáneo mediante la articulación teórica entre *posdemocracia*, *guerra híbrida* y *guerra cognitiva*. Se busca así producir un diagnóstico crítico y propositivo que permita comprender las nuevas formas de confrontación no convencional y sus implicancias para la soberanía democrática, la deliberación pública y la autonomía epistémica de las sociedades. Esta apuesta teórico-metodológica pretende contribuir al desarrollo de estrategias de resiliencia cognitiva, soberanía informacional y defensa institucional en contextos marcados por la manipulación perceptual y la fragmentación del vínculo político.

## Transformaciones sistémicas

El sistema internacional experimenta una reconfiguración estratégica de gran escala que trasciende las categorías analíticas heredadas de la posguerra fría. La hegemonía unipolar de Estados Unidos, consolidada tras la caída del Muro de Berlín, ha dado paso a una multipolaridad inestable, en la que interactúan potencias emergentes, actores no estatales, corporaciones transnacionales y plataformas digitales capaces de incidir de forma decisiva en la arquitectura del orden global (Ikenberry, 2018; Bremmer, 2022). Esta transición no constituye un simple retorno al equilibrio clásico de poder, sino una mutación sistémica caracterizada por el debilitamiento institucional, la fractura de consensos normativos y la expansión de zonas grises geopolíticas (Kaplan, 2025; Nye, 2022). El análisis prospectivo de Stratfor (2025) identifica el período 2025–2035 como una "década crítica", marcada por la competencia entre bloques geoeconómicos, alianzas fluidas y arquitecturas híbridas de poder. En este contexto, el sistema se comporta como un complejo adaptativo, donde múltiples variables interactúan sin linealidad ni previsibilidad (Global Trends, 2017). La aceleración de los cambios erosiona la capacidad de las instituciones creadas en el siglo XX para gestionar amenazas emergentes, mientras el declive de los patrones tradicionales de interdependencia impulsa estrategias de desacoplamiento y disuasión por negación. La soberanía estatal se redefine bajo el impacto combinado de tecnologías disruptivas, flujos de datos no regulados, inteligencia artificial y financiarización de las decisiones estratégicas, debilitando la eficacia de organismos como la ONU, la OMC o la OTAN. Estos

enfrentan una tensión estructural entre la obsolescencia de sus marcos normativos y la irrupción de poderes paralelos —estatales y no estatales— que operan fuera de reglas estables (Kupchan, 2020; Acharya, 2021). Kaplan (2025) describe este escenario como una "tierra baldía" geoestratégica, donde la incertidumbre reemplaza la previsibilidad jurídica y la lógica de la fuerza recupera centralidad. Esta dinámica convive con actores no convencionales —milicias, grupos híbridos y redes cibernéticas— que compiten por recursos, legitimidad y control de espacios físicos y simbólicos. La difusión de capacidades tecnológicas, desde armas hipersónicas hasta operaciones de desinformación, reduce las ventajas de las potencias tradicionales y abre nuevas brechas de vulnerabilidad (Global Trends, 2017). Los conflictos en zonas grises, según Tellis (2022), representan la expresión operativa de este cambio: enfrentamientos híbridos y cognitivos que evaden las formas convencionales de guerra (Mazarr, 2015; CIDOB, 2024). En el plano interno, Crouch (2004) vincula esta transformación externa con el fenómeno de la posdemocracia, en el que las formas institucionales subsisten, pero el contenido sustantivo —deliberación pública y soberanía ciudadana— se ve desplazado por intereses corporativos, lógicas tecnocráticas y agendas securitarias (Fraser, 2003; Mouffe, 2000). La convergencia entre erosión externa e interna deriva en lo que Held y Young (2022) denominan gobernanza fallida: instituciones formalmente existentes, pero operativamente desconectadas de las dinámicas reales de poder. El Global Risks Report 2025 del Foro Económico Mundial advierte una incapacidad creciente para gestionar riesgos sistémicos interconectados —desde amenazas híbridas hasta crisis climáticas—, lo que evidencia un deterioro funcional de la gobernabilidad global. Esta erosión se manifiesta en la parálisis de foros multilaterales por vetos cruzados, capturas institucionales y aplicación selectiva de normas, debilitando la articulación entre fines políticos y medios disponibles y habilitando reordenamientos autoritarios en la década 2025–2035. El EUISS (2024) subraya que la competencia híbrida y la dimensión cognitiva están redefiniendo las hegemonías regionales, fenómeno observable en el caso de Ucrania (2014–2025), donde confluyen acciones coordinadas en dominios político, militar e informacional. Frente a estas transformaciones, se impone una visión estratégica integradora que aborde tanto las amenazas emergentes como las oportunidades de cooperación entre actores diversos. Ello exige reformular el pensamiento estratégico hacia enfoques multidimensionales, intersectoriales y resilientes. En este nuevo escenario global, la dispersión normativa y las amenazas difusas favorecen conflictos regionales que, aunque anclados en dinámicas locales, responden a patrones estructurales de competencia por la influencia. Predominan acciones híbridas, asimétricas y de atribución ambigua orientadas a erosionar

capacidades institucionales, dividir alianzas y debilitar la gobernabilidad. La lógica resultante es la de una confrontación sistémica de bajo umbral, donde actores estatales y no estatales combinan instrumentos económicos, jurídicos, digitales e informacionales para disputar zonas de influencia sin activar los mecanismos clásicos de disuasión. Esta competencia simultánea, que abarca desde presiones económicas hasta manipulación electoral y saturación narrativa, requiere marcos interpretativos flexibles y fundamentados. En definitiva, lo que emerge es un régimen global de poder definido no por equilibrios militares formales, sino por la capacidad de manipular el entorno cognitivo, erosionar legitimidades institucionales y disputar hegemonías simbólicas en tiempo real.

## Zonas grises, guerra híbrida y disrupción estratégica del conflicto contemporáneo

El desdibujamiento progresivo de las fronteras entre guerra y paz constituye uno de los rasgos más disruptivos del escenario estratégico contemporáneo. Más que la mera incorporación de innovaciones tecnológicas a la violencia organizada implica una mutación estructural de los marcos normativos, políticos y estratégicos que sostenían una comprensión binaria del conflicto internacional (guerra/paz; interno/externo; legal/ilegal) (Rid, 2020). Este proceso cuestiona la arquitectura institucional heredada de la posguerra y demanda una revisión profunda de los instrumentos analíticos y operativos disponibles para enfrentar confrontaciones no convencionales. En esta línea, Arrosio y Skobalski (2024) proponen interpretar esta dinámica como expresión de una *guerra segmentada global*: un patrón estratégico donde múltiples conflictos regionales, interrelacionados, pero aparentemente desconectados, constituyen manifestaciones fragmentadas de una tensión estructural persistente entre grandes potencias. Este modelo sustituye la confrontación interestatal directa por una sucesión de escenarios híbridos —deslocalizados, superpuestos y convergentes— en los que la ambigüedad táctica, la negación plausible y la manipulación cognitiva se consolidan como dispositivos centrales en la disputa por la hegemonía global.

En esta nueva arquitectura de confrontación, actores estatales y no estatales articulan operaciones en dominios cinéticos y no cinéticos —militar, informacional, económico, jurídico y cognitivo— mediante una sinergia táctica que busca maximizar el impacto estratégico y preservar la ambigüedad atribucional. Esta lógica se manifiesta paradigmáticamente en las denominadas *zonas grises*: espacios intermedios de ambigüedad jurídica y estratégica, donde los marcos tradicionales del

derecho internacional, las normas de guerra y los mecanismos diplomáticos resultan insuficientes o inoperantes (ODNI, 2025; NATO, 2021). En estos entornos, el objetivo no es la derrota militar directa del adversario, sino la inducción de una parálisis sistémica a través de la fragmentación del tejido social, el descrédito institucional y la manipulación de las percepciones colectivas. Como ya advertía Hoffman (2018), estas nuevas formas de agresión indirecta no responden a los esquemas convencionales de guerra o paz, sino que se insertan en un terreno intermedio donde coexisten coerción encubierta, manipulación estratégica y tácticas no atribuibles. Este enfoque híbrido explota deliberadamente las ambigüedades legales y políticas del entorno internacional para alcanzar objetivos estratégicos sin desencadenar respuestas proporcionales, consolidando así un paradigma de conflicto no lineal y persistente. El desplazamiento del conflicto hacia el plano cognitivo e informacional se afirma como un nuevo eje del pensamiento estratégico contemporáneo. La literatura especializada —particularmente en el ámbito de los estudios sobre *Cognitive Warfare*— señala que los actores ya no se limitan a modificar correlaciones materiales de fuerza, sino que buscan condicionar la arquitectura cognitiva, manipular emociones colectivas y erosionar la coherencia narrativa de las sociedades blanco (Berzina & Shattuck, 2020). En este escenario, la superioridad cognitiva emerge como un objetivo prioritario, redefiniendo el poder como la capacidad de influir sobre percepciones, intenciones y marcos interpretativos de la realidad (NATO, 2021). En los regímenes híbridos, se consolidan arquitecturas de poder opacas que integran dispositivos de simulación institucional, coerción legal selectiva (*lawfare*), monopolización del discurso legítimo, algoritmos de segmentación social y tecnologías de inducción emocional selectiva (Ficek, 2023). Esta matriz permite tanto corroer las democracias desde dentro como proyectar estrategias ofensivas hacia el exterior, especialmente sobre periferias geopolíticas o zonas de soberanía debilitada. Como advierte el informe *NATO Battle Space of the Mind* (2021), los escenarios contemporáneos ya no se estructuran por fronteras físicas, sino por límites mentales, donde lo que está en disputa es la interpretación legítima de la realidad y el control de la memoria colectiva. La literatura reciente sobre conflictos en zonas grises refuerza esta perspectiva. Autores como Mazarr (2015) y Rid (2020) subrayan que estos conflictos se desarrollan en espacios de ambigüedad operativa, donde actores estatales y no estatales explotan las brechas del sistema internacional mediante tácticas no convencionales: guerra cibernética, operaciones de influencia, propaganda, sabotaje institucional y coerción económica. Los tres vectores dominantes de esta modalidad conflictiva son la manipulación informacional, la explotación del ciberespacio y la intervención deliberada en el campo cognitivo como nuevo teatro de operaciones

estratégicas. El *Global Risks Report* del Foro Económico Mundial (2025) identifica como una de las principales amenazas globales la proliferación transnacional de campañas de desinformación, ciberataques, sabotajes institucionales y presión económica selectiva. Estas tácticas no solo dificultan la atribución formal de responsabilidades, sino que socavan los marcos legales multilaterales y debilitan la operatividad de la diplomacia tradicional como herramienta de resolución de conflictos. En esta línea, Córdova (2024) sostiene que las guerras híbridas constituyen una mutación estratégica del injerencismo clásico, que opera bajo la apariencia de disputas políticas internas mientras responde a objetivos exógenos de desestabilización. Estas formas de agresión diluyen las fronteras de la soberanía, erosionan el entramado estatal y obstaculizan la formulación de respuestas legítimas desde el derecho internacional vigente. Esta guerra subumbral o sin umbral (*non-threshold warfare*) configura un régimen de conflictividad permanente, difusa e incremental, caracterizado por su invisibilidad táctica, su ambigüedad operacional y su capacidad para generar dislocaciones estratégicas sin activar mecanismos convencionales de respuesta. En este tipo de confrontación, el tiempo, la percepción y la ambivalencia se convierten en recursos ofensivos clave, desplazando el foco desde la confrontación militar directa hacia la saturación institucional y la manipulación del entorno cognitivo. Comprender cómo se organizan las fases de una confrontación híbrida —desde las acciones encubiertas hasta las operaciones abiertas— resulta fundamental para identificar sus lógicas de escalamiento, evasión y persistencia. Esta dinámica ha sido ejemplificada en modelos operativos que integran planos estratégicos, tácticos y temporales, como el adaptado por Kilcullen (2020) a partir de una relectura de la Doctrina Gerasimov (véase Figura 2). En este esquema, se articulan fases no atribuidas, encubiertas y abiertas, orientadas a evitar respuestas proporcionales, desestructurar marcos normativos y mantener la iniciativa ofensiva sin cruzar umbrales bélicos formales.

## Tecnologías disruptivas como vectores estratégicos

En el marco de la transformación sistémica del orden internacional, las tecnologías disruptivas han dejado de ser simples herramientas subordinadas a la voluntad humana para convertirse en vectores estructurantes del poder global contemporáneo. Dispositivos como la inteligencia artificial (IA), el aprendizaje automático, el análisis masivo de datos (big data), los sistemas autónomos letales (LAWS), los enjambres de drones, los deepfakes y las plataformas algorítmicas de vigilancia y control están redefiniendo no solo las doctrinas militares, sino también los fundamentos simbólicos

de la gobernanza, la seguridad y la soberanía estatal. Su capacidad para operar simultáneamente en dominios físico, cognitivo e informacional permite redirigir el conflicto hacia la percepción, el juicio y la acción colectiva (ODNI, 2025; NATO ACT, 2023). Estas capacidades actúan de forma sinérgica en múltiples esferas —militar, informacional, jurídico, cognitivo y simbólico—, amparadas en la proyección remota, el anonimato operativo y la ambigüedad atribucional. Ello posibilita el desarrollo de conflictos progresivos por debajo del umbral de la guerra convencional, con impactos estratégicos acumulativos que no activan mecanismos interestatales tradicionales de respuesta (Hybrid Threat Centre of Excellence, 2024). En este escenario, la IA se posiciona como un instrumento clave de superioridad decisional, al procesar datos masivos en tiempo real, anticipar escenarios tácticos y ejecutar operaciones automatizadas de manipulación cognitiva, desinformación estratégica y sabotaje institucional sin mediación humana directa. La inteligencia artificial generativa representa un punto de inflexión en las operaciones cognitivas al permitir la producción masiva de contenidos persuasivos visual y lingüísticamente indistinguibles de los creados por humanos. Esta capacidad es utilizada en campañas de desinformación, manipulación perceptual e intervención emocional planificada, con incidencia en la estructura decisional tanto civil como militar. En el plano operativo, posibilita distorsionar en tiempo real el ciclo OODA (observar, orientar, decidir, actuar), erosionando la capacidad de respuesta del adversario mediante saturación informativa y alteración deliberada de marcos interpretativos (Saavedra, 2024). El denominado "capitalismo de la vigilancia" se configura como una arquitectura de poder donde la información es convertida en un activo estratégico para el control conductual. Mediante la extracción masiva de datos y su procesamiento algorítmico opaco, este régimen actúa sobre la emoción, la intención y la toma de decisiones individuales, con capacidad de predecir y modificar comportamientos a escala poblacional. En el plano geopolítico, las plataformas digitales se constituyen como actores con poder estructurante, al regular la distribución de la atención, el acceso a la información y la percepción colectiva del riesgo (Zuboff, 2019). En consecuencia, el conflicto contemporáneo se desplaza desde el enfrentamiento físico hacia una disputa por la arquitectura de la subjetividad. La saturación informativa, la construcción de realidades alternativas y la manipulación emocional de audiencias masivas se convierten en herramientas de intervención que diluyen los límites entre verdad y percepción. En este contexto, el campo de batalla se expande al ecosistema digital, donde redes sociales, metadatos y emociones colectivas se convierten en objetivos estratégicos de operaciones sistemáticas de ingeniería narrativa. Esta lógica fue anticipada por

Pomerantsev (2019), quien subraya que el nuevo conflicto se libra sobre los significados más que sobre los territorios. En el plano institucional, las transformaciones tecnopolíticas han favorecido la consolidación de regímenes híbridos que mantienen la arquitectura formal de la democracia, pero neutralizan sus funciones sustantivas. Levitsky y Way (2010) señalan que esta modalidad de control no precisa recurrir a la represión directa: se sustenta en mecanismos preventivos de exclusión simbólica, como la segmentación algorítmica, la vigilancia de trazas digitales y la configuración anticipada de burbujas informativas. En este esquema, la oposición no es acallada por la fuerza, sino debilitada en su capacidad de incidencia a través de dinámicas de aislamiento perceptual cuidadosamente diseñadas. Tal como advierten Morozov (2012) y Gillespie (2020), algunos regímenes han perfeccionado el uso instrumental de las tecnologías digitales para conservar las apariencias externas de la democracia, a la vez que neutralizan su contenido deliberativo. Mediante algoritmos de vigilancia, control selectivo de flujos informativos y el uso de plataformas cerradas, proyectan una fachada institucional que oculta la erosión de los mecanismos efectivos de rendición de cuentas. Esta dinámica facilita que decisiones de alta sensibilidad estratégica —incluidas las referidas a defensa y seguridad— sean delegadas a sistemas automatizados opacos, sin el debido escrutinio público ni control parlamentario efectivo. La consolidación de un autoritarismo algorítmico ha sido señalada por Zuboff (2019), O'Neil (2016) y Greene (2022), quienes coinciden en que el poder digital contemporáneo puede ejercer control social sin recurrir a formas clásicas de represión. A través de sistemas automatizados de predicción, segmentación conductual y vigilancia masiva, es posible modelar comportamientos y modular emociones sin intervención directa del aparato estatal. Este régimen tecnológico erosiona de forma sostenida el espacio público deliberativo, reconfigurando la interacción entre ciudadanía, plataformas y estructuras de gobernanza, y restringiendo de manera creciente la autonomía decisional efectiva de los individuos. En el plano estratégico-operacional, múltiples potencias desarrollan capacidades de guerra autónoma orientadas a alcanzar superioridad táctica en entornos de alta volatilidad. De acuerdo con el ODNI (2025), sistemas como enjambres de drones, algoritmos de reconocimiento facial militar y plataformas de decisión automatizada están reconfigurando el ciclo operativo, incrementando la precisión, reduciendo los tiempos de reacción y minimizando la exposición humana en escenarios hostiles. No obstante, como advierten Walsh (2022) y Cummings (2023), estos avances implican riesgos estratégicos sustantivos, tales como escalamiento automatizado no intencional, errores en la atribución de ataques, sesgos en decisiones letales y potenciales vulneraciones al

Derecho Internacional Humanitario. Por ello, la integración de inteligencia artificial en operaciones militares demanda marcos éticos y normativos robustos que aseguren su utilización conforme a criterios de transparencia, rendición de cuentas y sujeción a la legalidad internacional. Las tecnologías disruptivas se han consolidado como vectores estructurales del poder internacional, actuando simultáneamente en dominios militares, cognitivos, jurídicos e informacionales. Han dejado de ser herramientas subordinadas para convertirse en arquitecturas de proyección de influencia. Su integración en sistemas de seguridad y estrategias geopolíticas redefine la competencia interestatal, desplazando el énfasis del control territorial hacia la capacidad de influir en la percepción, el juicio y la acción colectiva. Capacidades como la inteligencia artificial, la vigilancia predictiva y el análisis masivo de datos (big data) posibilitan disputar narrativas dominantes, modelar entornos perceptuales y reconfigurar dinámicas de gobernabilidad sin requerir presencia física directa ni ocupación del espacio geográfico. Informes recientes de la OTAN (2023) y del Center for a New American Security (CNAS, 2023) advierten que las capacidades tecnológicas disruptivas habilitan la ejecución de operaciones en tiempo real, caracterizadas por baja trazabilidad, alta precisión y elevada eficacia psicológica. Estas capacidades no requieren recurrir a la violencia física para modificar las condiciones de gobernabilidad: generan impactos estratégicos acumulativos sobre la percepción pública, la cohesión social y la legitimidad institucional, alterando de manera sostenida el equilibrio político interno de los Estados objetivo. En este contexto, la competencia interestatal se reconfigura como una disputa por el dominio del entorno simbólico, la modulación emocional colectiva y la arquitectura narrativa que sostiene los marcos de legitimidad y gobernanza de las democracias contemporáneas. Este desplazamiento estratégico impone la necesidad de reformular los enfoques clásicos de seguridad y replantear la propia lógica de la disuasión estratégica. En lugar de focalizarse exclusivamente en el volumen y despliegue de capacidades militares convencionales, las nuevas modalidades de confrontación se consolidan en entornos híbridos donde el dominio informacional y narrativo se convierte en el eje central de la competencia. En este marco, las tecnologías emergentes actúan como multiplicadores de poder no cinético, posibilitando la configuración de zonas de influencia simbólica que interactúan —y en ocasiones entran en fricción— con los marcos normativos e institucionales del sistema internacional, alterando sus equilibrios sin necesidad de una confrontación armada directa. La expansión de la tecnopolítica global carece de mecanismos de contención efectivos dentro de los marcos del derecho internacional vigente, cuya arquitectura normativa se muestra insuficiente frente a la velocidad y complejidad de estas

transformaciones. En el plano tecnopolítico, esta lógica se traduce en una anarquía funcional digital, caracterizada por la incapacidad de las instituciones para regular eficazmente a actores tecnológicos no estatales y sistemas automatizados de alcance transnacional. Decisiones críticas en materia de seguridad, privacidad y gobernanza del conocimiento son delegadas a plataformas y algoritmos opacos, ajenos a la deliberación democrática y al control ciudadano. Este panorama refuerza la necesidad de una doctrina estratégica integral que articule soberanía tecnológica, defensa cognitiva y regulación algorítmica, integrando capacidades técnicas, principios éticos y resiliencia institucional como ejes inseparables para la preservación de la seguridad democrática. La proliferación de dispositivos algorítmicos orientados al control social y a la gestión de riesgos plantea dilemas estratégicos y normativos de creciente complejidad, especialmente en los regímenes democráticos, donde la legitimidad institucional se fundamenta en la transparencia y en la deliberación ciudadana. La expansión de tecnologías de vigilancia y modulación emocional introduce tensiones estructurales entre seguridad y libertad, reconfigurando los límites de lo aceptable en el ejercicio del poder. En este marco, surgen interrogantes esenciales: ¿hasta qué punto es legítima la recolección masiva de datos personales o la alteración deliberada del estado emocional colectivo en nombre de la estabilidad? ¿Qué implicancias estratégicas y jurídicas conlleva la delegación de decisiones críticas a sistemas opacos, ajenos al control público y a la rendición de cuentas efectiva? Estas cuestiones adquieren centralidad en un entorno tecnopolítico que, si bien promete eficiencia operativa, puede erosionar el vínculo de confianza entre ciudadanía y autoridad, debilitando progresivamente los fundamentos normativos y la legitimidad sustantiva del pacto democrático contemporáneo. Esta deriva plantea dilemas éticos y estratégicos cada vez más relevantes en torno a la legitimidad del control algorítmico en sistemas democráticos. Preguntas como ¿quién define los parámetros de funcionamiento de los algoritmos?, ¿qué criterios se utilizan para su validación? o ¿cómo se garantiza la rendición de cuentas? adquieren centralidad, especialmente cuando se reconoce que, como advierte O'Neil (2016), los sistemas mal diseñados no solo perpetúan desigualdades preexistentes, sino que las institucionalizan bajo una apariencia de objetividad técnica. En este escenario, la gobernanza transparente del diseño algorítmico y la deliberación pública sobre sus implicancias emergen como condiciones imprescindibles para asegurar una seguridad democrática compatible con el estado de derecho. En el plano tecnopolítico, se afianza una anarquía funcional digital en la que plataformas y algoritmos opacos asumen decisiones críticas sobre seguridad, privacidad y circulación del conocimiento, al margen del control democrático y de la

deliberación pública. La ausencia de marcos regulatorios sólidos para sistemas automatizados de alto impacto genera zonas grises de responsabilidad, favoreciendo la vigilancia persistente, la segmentación emocional dirigida y formas de gobernanza algorítmica sin transparencia ni rendición de cuentas. Este escenario demanda una doctrina estratégica integral que combine soberanía tecnológica, defensa cognitiva y regulación algorítmica, sustentada en principios de transparencia, auditabilidad y resiliencia institucional, con el fin de salvaguardar la seguridad democrática frente a los riesgos estructurales que plantean las tecnologías disruptivas. En síntesis, las tecnologías disruptivas ya no operan únicamente como instrumentos subordinados a las dinámicas interestatales, sino que se han constituido en dominios estratégicos autónomos, con capacidad para redefinir el equilibrio global de poder y reconfigurar los patrones clásicos de confrontación. Al desdibujar las fronteras entre guerra y política, tensionan la agencia estatal, la legitimidad normativa y la gobernanza democrática. Como advierte el informe de la Comisión Europea sobre amenazas híbridas (2025), la supremacía futura dependerá menos del control territorial o del poder de fuego y más de la capacidad para disputar el espacio cognitivo, influir en los marcos interpretativos colectivos y modelar el comportamiento de las sociedades abiertas desde dentro. Este desplazamiento sitúa a la soberanía cognitiva como un pilar esencial de la seguridad nacional. Su preservación requiere estrategias que integren la defensa del espacio simbólico, el fortalecimiento de la deliberación pública y el desarrollo de una resiliencia perceptual capaz de resistir la manipulación externa. En la década crítica 2025–2035, la capacidad de proteger este dominio será determinante para la estabilidad de las democracias y para la configuración del orden internacional emergente.

## Crisis de gobernabilidad y degradación democrática

La limitada capacidad de los Estados para anticipar, contener y responder de manera integral a amenazas complejas ha dado lugar a un escenario de inseguridad estructural que trasciende episodios aislados de violencia o disrupción. Esta condición, persistente y transversal a contextos geográficos, institucionales y sociales diversos, constituye un rasgo inherente al nuevo orden global, caracterizado por la fragmentación, la interdependencia y la acumulación progresiva de tensiones híbridas (CEIUC, 2025; Global Solidarity Report, 2024). En este marco, la inseguridad deja de ser un fallo ocasional para convertirse en un régimen de gobierno que justifica la vigilancia extendida, la restricción de derechos y la concentración de poder bajo el

argumento de una estabilidad siempre amenazada. Este proceso erosiona los pilares tradicionales de la legitimidad democrática y favorece la emergencia de liderazgos autoritarios y lógicas gubernamentales sustentadas en la gestión emocional del miedo, la securitización de lo político y la instrumentalización de la incertidumbre como mecanismo de control (Kaplan, 2025; Levitsky & Ziblatt, 2018). La degradación de la calidad democrática no se manifiesta únicamente en rupturas institucionales abiertas, sino en un vaciamiento progresivo de sus dimensiones deliberativas, participativas y epistémicas. Tanto en democracias consolidadas —como Estados Unidos— como en sistemas frágiles de regiones geopolíticamente tensionadas, se observa la coexistencia de procedimientos electorales formales con prácticas de deslegitimación institucional, polarización afectiva y captura de narrativas públicas. Informes como el *Strategic Risk Outlook* (Atlantic Council, 2024) y el *Global State of Democracy* (International IDEA, 2023) advierten sobre la consolidación de democracias procedimentales carentes de sustancia, en las que el pluralismo se erosiona mediante disuasión simbólica, desinformación estructurada y represión selectiva del disenso. La normalización de regímenes de excepción —leyes de emergencia, marcos antiterroristas, control digital masivo o militarización de la seguridad pública— institucionaliza el recorte de derechos fundamentales y desactiva el principio de proporcionalidad. En este contexto, la excepcionalidad deja de ser una respuesta extraordinaria para convertirse en un dispositivo permanente de gobernanza por decreto, debilitando los contrapesos institucionales y legitimando una anarquía funcional en la que las formas jurídicas se mantienen, pero vaciadas de contenido normativo y empleadas estratégicamente para neutralizar la soberanía popular. Kaplan (2025) subraya que el colapso interno de los contratos sociales se vincula estrechamente con la erosión externa del orden internacional. La pérdida de previsibilidad normativa y de mecanismos eficaces de resolución de conflictos genera un entorno de vulnerabilidad transversal en el que el miedo estructural —sin necesidad de un enemigo claramente definido— se convierte en un recurso político central, facilitando la concentración vertical del poder y la supresión gradual de la deliberación democrática. En términos performativos, Ficek (2023) sostiene que los regímenes híbridos no requieren de una represión abierta para desactivar la movilización social: la saturación informativa, la fragmentación del espacio público digital y la simulación de pluralismo resultan herramientas más eficaces. Esta gobernanza emocional coloniza los afectos colectivos, generando subjetividades apáticas o conformistas, e inhibe la emergencia de liderazgos democráticos alternativos. En este escenario, la noción de posdemocracia formulada por Crouch (2004) adquiere una dimensión operativa. Las instituciones representativas se convierten en un decorado

que encubre la transferencia de las decisiones sustantivas a foros tecnocráticos, plataformas corporativas o algoritmos predictivos. La política institucional pierde así su capacidad transformadora y se limita a legitimar consensos preconfigurados por élites transnacionales. La relevancia estratégica de esta degradación democrática se amplifica en el marco de las amenazas híbridas. El *Global Risks Report* del Foro Económico Mundial (2025) identifica la erosión de la cohesión social, la desconfianza institucional y la percepción de injusticia como factores críticos que alimentan ciclos prolongados de conflictividad. Combinadas con la saturación cognitiva y la inseguridad jurídica, estas dinámicas debilitan la resiliencia estratégica de los Estados y facilitan la acción de actores no estatales con agendas disruptivas o desestabilizadoras. Lejos de ser anomalías periféricas, estas tendencias constituyen manifestaciones de una mutación estructural del sistema internacional (CIDOB, 2024). En un entorno interconectado pero descoordinado, donde las reglas dejan de ser compartidas y aplicadas de forma homogénea, la sostenibilidad democrática se convierte en un problema de seguridad estratégica. El reto ya no reside únicamente en preservar las formas democráticas, sino en redefinir sus fundamentos materiales, culturales y simbólicos para enfrentar la volatilidad permanente. La gobernanza estratégica del siglo XXI exige, por tanto, una visión integral de la seguridad democrática que articule defensa institucional, justicia social, soberanía digital y resiliencia cognitiva. Solo la integración de legitimidad y eficacia, pluralismo y gobernabilidad, protección y participación podrá impedir que la inseguridad estructural consolide regímenes autoritarios de baja intensidad que, aunque compatibles con la arquitectura formal del sistema internacional, resultan irreconciliables con sus principios fundacionales.

## Guerra cognitiva y disputa por la soberanía mental en el nuevo orden global

La guerra cognitiva (GC) se ha consolidado como uno de los núcleos estratégicos más sofisticados del conflicto contemporáneo, desplazando el centro de gravedad desde la ocupación territorial hacia la intervención directa en la mente humana. A diferencia de los modelos bélicos convencionales, centrados en el dominio físico, la GC redefine el campo de batalla como una contienda ontológica y simbólica por el control de percepciones, emociones y marcos interpretativos, constituyéndose en una forma radical de proyección de poder, invisible pero decisiva (du Cluzel, 2020; NATO Innovation Hub, 2021). Este vector se articula con las dinámicas de degradación democrática y gobernabilidad híbrida descritas en el apartado anterior, funcionando

como catalizador de la erosión institucional y la captura narrativa. Impulsada por la convergencia de inteligencia artificial, plataformas algorítmicas, neurociencia aplicada y vigilancia digital, la GC opera como una confrontación sin umbral físico ni declaración formal, capaz de erosionar la agencia mental de individuos y comunidades. A través de la manipulación intensiva de creencias, emociones y narrativas colectivas, supera con creces la propaganda tradicional, integrando tecnologías NBIC, big data, sistemas de influencia masiva y desarrollos en neurociencia militarizada que permiten intervenir en tiempo real sobre la arquitectura mental de las poblaciones objetivo (Hybrid CoE, 2024; European Defence Agency, 2023). Su eficacia radica en la explotación sistemática de sesgos cognitivos y en la construcción de entornos informacionales altamente personalizados, que inducen polarización y fragmentan la cohesión social. Esta dimensión neurocognitiva incluye técnicas de estimulación cerebral no invasiva, manipulación de neurotransmisores e interferencia perceptual, con el objetivo de desorganizar la racionalidad colectiva, erosionar la memoria histórica compartida y debilitar la confianza en instituciones clave (Giordano, 2020; Burda, 2023). El resultado es la creación de *cogniscapes* bélicos (Boulianne et al., 2021), donde la verdad objetiva se diluye, la emoción desplaza a la razón y el diálogo deliberativo es sustituido por una saturación de ruido e incertidumbre estratégicamente inducida. Este cambio plantea dilemas normativos y éticos sustantivos: la línea entre influencia legítima y manipulación hostil se vuelve difusa, desafiando las salvaguardas democráticas. Autores como Floridi (2021) y Brunstetter y Braun (2020) advierten que la manipulación algorítmica no solo debilita la confianza institucional, sino que atenta contra valores fundantes como la dignidad humana y la autonomía política. Así, la GC puede ser tanto una herramienta externa de desestabilización como un instrumento interno de control por parte de regímenes híbridos. Documentos doctrinales como *Cognitive Warfare: A Battle for the Brain* (NATO, 2021) y *Cognitive Superiority: Information to Power* (NATO ACT, 2022) señalan que su objetivo último es condicionar el comportamiento social sin recurrir a la fuerza física, mediante la manipulación de estímulos sensoriales, patrones lingüísticos y narrativas emocionales. La degradación selectiva de nodos críticos —en particular del liderazgo político y militar— constituye una táctica prioritaria, dado que su juicio e intuición pueden ser alterados mediante sobrecarga informativa y estímulos emocionales disruptivos. Ante este escenario, la construcción de resiliencia cognitiva emerge como un recurso estratégico equivalente a la defensa territorial o cibernética, combinando pensamiento crítico, alfabetización digital avanzada, soberanía epistemológica y capacidades institucionales de detección temprana (Mareš & Mlejnková, 2021; NATO ACT, 2023). Modelos como los del Hybrid CoE proponen un

enfoque escalonado que va desde la formación ciudadana en habilidades metacognitivas hasta sistemas de alerta algorítmica en sectores estratégicos. Sin embargo, el desafío reside en que estas defensas no reproduzcan las lógicas intrusivas de los actores que se busca contrarrestar, preservando así la legitimidad democrática. En síntesis, la GC no es un complemento de la guerra convencional, sino una arquitectura de poder autónoma que convierte la soberanía cognitiva —la capacidad de interpretar la realidad y decidir con autonomía frente a estímulos manipulativos— en un objetivo geopolítico de primer orden. La próxima década verá la expansión de tecnologías neurodigitales e interfaces cerebro-máquina que ampliarán las posibilidades de intervención sensorial y afectiva a escala poblacional, en un contexto carente de regulación internacional efectiva. La cooperación multilateral en neuroética, gobernanza cognitiva y soberanía mental será indispensable para preservar la libertad de pensamiento, la deliberación informada y la cohesión narrativa como bienes estratégicos en el orden global del siglo XXI.

## Gobernabilidad híbrida y reconfiguración tecnopolítica del poder

En continuidad con la dinámica analizada en el apartado anterior sobre la guerra cognitiva y la disputa por la soberanía mental, se observa que este tipo de confrontación no opera de forma aislada, sino que se integra en un patrón más amplio de control político: la gobernabilidad híbrida. Este concepto describe una modalidad estructural de ejercicio del poder que combina procedimientos democráticos formales con dispositivos tecnológicos de vigilancia extendida, manipulación informacional y erosión deliberada de los espacios de deliberación pública. En el contexto estratégico del siglo XXI, la gobernabilidad híbrida no debe interpretarse como una anomalía institucional ni como un fenómeno restringido a determinadas regiones, sino como una tendencia global convergente. Se manifiesta en sistemas políticos formalmente diversos —desde regímenes autoritarios hasta democracias consolidadas— que comparten una creciente dependencia de la tecnopolítica como arquitectura central del poder. En este marco, el control se desplaza desde la coerción física hacia la captura de la atención, la emoción y la interpretación, consolidando una gobernanza simbólica que redefine las condiciones del consentimiento ciudadano. Los estudios recientes del Carnegie Endowment for International Peace (2024), el European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) y el Center for a New American Security (CNAS) advierten sobre la consolidación de lo que denominan "posdemocracias funcionales": estructuras que mantienen las formas externas de la democracia —como

las elecciones, la legalidad o la división de poderes— mientras vacían progresivamente sus contenidos sustantivos mediante estrategias de intensificación afectiva disruptiva, vigilancia algorítmica, manipulación perceptiva y cooptación institucional. En esta arquitectura, la guerra cognitiva no convencional —conceptualizada por el NATO Innovation Hub (2023) y el Atlantic Council— se integra orgánicamente, desplazando el énfasis desde la represión directa hacia la colonización sistemática de los marcos interpretativos. La erosión de la autonomía decisional se logra mediante entornos digitales diseñados para amplificar sesgos cognitivos, inducir polarización y saturar el ecosistema informativo con narrativas emocionales, ambiguas o contradictorias. Esta "disolución de la verdad" favorece una gobernanza sostenida en la opacidad emocional y la ambigüedad narrativa. Informes del Instituto Clingendael (2024), la Brookings Institution, el Fund for Peace y el Instituto Igarapé identifican un patrón común en distintas regiones: la articulación de control normativo selectivo (lawfare), manipulación mediática, vigilancia predictiva y desinformación sistémica. Estos mecanismos no solo gestionan el disenso, sino que lo anticipan, encapsulan y redirigen, transformando al ciudadano en un agente involuntario de su propia subordinación simbólica. La legalidad, lejos de garantizar derechos, se convierte en herramienta de disciplinamiento, como evidencia la proliferación de estados de excepción permanentes, leyes antiterroristas expansivas y plataformas de vigilancia masiva en países como China, India, Turquía, Rusia y Hungría. Este fenómeno ha sido conceptualizado como "nuevo constitucionalismo autoritario" (Tushnet, 2021), en el que la ley sirve para estabilizar la excepcionalidad antes que para proteger la libertad. El autoritarismo tecnopolítico, definido por Greene (2022), cristaliza este modelo: un régimen donde la infraestructura digital sustituye al aparato represivo clásico e institucionaliza un control descentralizado, ubicuo y emocionalmente adaptativo. No requiere censura explícita, sino una sobreabundancia de estímulos contradictorios que, amplificados por algoritmos, optimizan la confusión antes que la comprensión. Este patrón, documentado también en informes como AI and Society del MIT Media Lab (2023) o Litigating Algorithms del AI Now Institute (2022), revela un uso sistemático de tecnologías de microsegmentación política y extracción de datos conductuales para maximizar la adicción emocional, amplificar respuestas afectivas y optimizar la vigilancia predictiva. El carácter transnacional de las infraestructuras digitales plantea un desafío adicional: la extraterritorialidad algorítmica. Grandes corporaciones tecnológicas —como Meta, Google o X— operan más allá de las jurisdicciones nacionales, ejerciendo funciones cuasi regulatorias mediante la moderación de contenidos, la jerarquización de mensajes o la segmentación de audiencias en procesos

electorales. Estas decisiones, ejecutadas a través de procesos algorítmicos opacos y sin mecanismos efectivos de rendición de cuentas, erosionan tanto la soberanía digital como los principios esenciales del constitucionalismo democrático (Council of Europe, 2021; Naciones Unidas, 2022). Aunque instrumentos como el Digital Services Act de la Unión Europea (Parlamento Europeo y Consejo de la Unión Europea, 2022) y el Artificial Intelligence Act (Parlamento Europeo y Consejo de la Unión Europea, 2024) representan avances al imponer obligaciones de transparencia, trazabilidad y responsabilidad a las plataformas, su alcance sigue siendo parcial. Persisten vacíos jurídicos —como la ausencia de un tratado internacional vinculante en materia de gobernanza algorítmica— y barreras estructurales derivadas de la asimetría tecnológica y la competencia geopolítica por el control de los flujos de datos (Organisation for Economic Cooperation and Development [OECD], 2023). Este panorama refuerza la urgencia de articular un marco regulatorio internacional robusto, inspirado en experiencias como el Convention on Cybercrime (Consejo de Europa, 2001) y la Declaración Universal sobre Inteligencia Artificial y Derechos Humanos (UNESCO, 2023), que permita preservar la soberanía cognitiva en ecosistemas democráticos interconectados. La gobernabilidad híbrida se consolida como una mutación estructural del poder político, donde las instituciones democráticas conservan su apariencia formal, pero ven vaciado su contenido deliberativo. El Global State of Democracy Report (International IDEA, 2024) documenta que más del 70% de la población mundial vive en regímenes donde se restringen las libertades políticas y civiles, incluso con elecciones periódicas. En este contexto, la gobernanza por saturación —informativa, emocional y normativa— convierte las crisis en instrumentos de control: el conflicto se administra como un recurso estabilizador, sustentado en represión selectiva, encapsulamiento narrativo y arquitecturas invisibles de datos. Ejemplos recientes incluyen el uso masivo de sistemas de vigilancia predictiva en contextos de protesta (Hong Kong, 2019–2020) y la manipulación de narrativas en entornos digitales para neutralizar disenso en procesos electorales (Brasil, 2022; Nigeria, 2023). En este marco, la soberanía cognitiva puede definirse operacionalmente como la capacidad colectiva de preservar la autonomía interpretativa frente a arquitecturas de influencia —estatales o privadas— diseñadas para intervenir en el juicio, la memoria y las emociones sociales. Este enfoque trasciende la defensa estatal tradicional y exige una corresponsabilidad que involucre a gobiernos, sector privado, sociedad civil y ciudadanía. Su protección requiere: i) alfabetización digital avanzada y crítica mediática; ii) regulación con transparencia algorítmica y auditorías independientes; iii) sistemas de monitoreo de narrativas hostiles; y iv) fortalecimiento

institucional para garantizar el derecho a la deliberación libre de interferencias encubiertas (UN Human Rights Council, 2022; Freedom House, 2024). En definitiva, la gobernabilidad híbrida no es una anomalía temporal, sino la cristalización de un régimen de control tecnopolítico en el que convergen seguridad, información y subjetividad. En este entorno, la soberanía cognitiva compartida debe concebirse como un vector estratégico de proyección internacional. La disputa por la hegemonía sobre los marcos interpretativos globales se ha vuelto tan decisiva como la competencia por recursos materiales, y la capacidad de una sociedad para generar, proteger y proyectar sus narrativas constituye un activo geopolítico central, clave para preservar legitimidad, influencia y poder blando en el sistema internacional. Comprender la gobernabilidad híbrida y su intersección con la reconfiguración tecnopolítica del poder ofrece el marco analítico para abordar las arquitecturas independientes de la soberanía híbrida. Estas estructuras —configuraciones normativas, tecnológicas y simbólicas que trascienden las fronteras estatales— actúan como nodos autónomos de influencia y control. Su estudio, mediante metodologías comparadas y casos empíricos, permitirá identificar cómo el poder híbrido se institucionaliza y se proyecta más allá de los límites tradicionales de la soberanía, configurando un orden global cada vez más interdependiente, fragmentado y disputado.

## Hacia una visión sistémica del conflicto híbrido

El conflicto del siglo XXI opera en zonas grises, disuelve umbrales entre normalidad y excepción y desplaza el centro de gravedad hacia la dimensión cognitiva. La seguridad deja de ser un problema exclusivamente material para incorporar la protección del entorno informacional y de la deliberación democrática. En este marco, la gobernabilidad híbrida —documentada por Hybrid CoE, NATO Innovation Hub, CSIS y EUISS— combina procedimientos democráticos formales con dispositivos tecnopolíticos de vigilancia y manipulación algorítmica, reconfigurando los incentivos estratégicos de Estados y actores no estatales. (conservar una sola aparición). Lejos de las confrontaciones armadas convencionales, la disputa estratégica se desplaza hacia zonas grises donde la manipulación informacional, la saturación institucional, la deslegitimación del adversario y la captura del sentido colectivo se erigen como mecanismos centrales de poder. La guerra híbrida, en sus formas no lineales, liminales y de baja visibilidad, redefine la noción misma de amenaza al priorizar la colonización simbólica, la erosión de la voluntad política y el condicionamiento del juicio colectivo por sobre la ocupación territorial. Esta mutación implica un cambio ontológico en

la concepción de la seguridad: los actores estatales y no estatales ya no se limitan a alterar correlaciones materiales de fuerza, sino que intervienen deliberadamente en la arquitectura cognitiva de las democracias, debilitando su capacidad deliberativa y su resiliencia narrativa frente a la saturación informativa, la manipulación emocional y la desinformación estratégica. Los análisis del *European Centre of Excellence for Countering Hybrid Threats* (Hybrid CoE, 2024), el *NATO Innovation Hub* (2023), el *Center for Strategic and International Studies* (CSIS, 2023) y el *European Union Institute for Security Studies* (EUISS, 2024) advierten sobre la consolidación de un régimen de gobernabilidad híbrida sustentado en la coexistencia de procedimientos democráticos formales con dispositivos tecnopolíticos de vigilancia, represión segmentada y manipulación algorítmica. En este modelo, la erosión institucional se despliega sin necesidad de violencia abierta ni suspensión formal de derechos, utilizando estrategias como el *lawfare*, los estados de excepción normalizados, el *targeting* emocional y la ingeniería informacional de percepciones para reconfigurar las condiciones cognitivas y simbólicas de la deliberación democrática. Esta lógica configura lo que Crouch (2004) define como *posdemocracia funcional*: una estructura que simula pluralismo y legalidad mientras vacía de contenido sustantivo la representación política. La fachada democrática se mantiene —procesos electorales, división de poderes, sistema legal—, pero su funcionamiento se ve intervenido mediante dinámicas de control perceptual y captura simbólica que moldean el comportamiento político y la experiencia ciudadana como parte de una estrategia sostenida de gobernabilidad híbrida. La dimensión tecnopolítica de esta mutación es decisiva. Tecnologías disruptivas como la inteligencia artificial, el *big data*, la neurociencia computacional y las plataformas algorítmicas actúan como vectores de intervención silenciosa sobre la subjetividad colectiva, generando entornos hiperpersonalizados y emocionalmente densos en los que la acción política se aleja de la deliberación racional y deriva hacia reacciones impulsivas y fragmentadas. En este escenario, la soberanía simbólica —capacidad de una sociedad para preservar sus marcos de sentido, narrativas compartidas y agencia epistemológica— se convierte en un activo geopolítico de primer orden. Informes como *Governing with AI* de la OCDE (2024) alertan sobre la convergencia creciente entre seguridad, gobernanza algorítmica y control emocional. Estos documentos subrayan riesgos estructurales que comprometen la resiliencia cognitiva de las sociedades, tales como la opacidad decisional, la reproducción de sesgos automatizados y la erosión de la autonomía ciudadana. Frente a ello, la seguridad contemporánea debe trascender la protección de fronteras físicas y priorizar la defensa de la autonomía interpretativa, la coherencia narrativa y la integridad cognitiva de las sociedades abiertas, articulando

de manera estratégica lo militar con lo simbólico, lo jurídico con lo emocional y lo institucional con lo digital.

Las premisas analizadas constituyen un andamiaje conceptual sólido para entender las nuevas dinámicas de poder y conflicto en la era digital. La interacción entre gobernabilidad híbrida, tecnopolítica y dominación cognitiva revela un desplazamiento estructural en las formas de control político y una erosión sostenida de las condiciones simbólicas de la deliberación democrática. Ante ello, se impone el desarrollo de estrategias de resiliencia estructural sustentadas en políticas públicas de soberanía tecnológica, alfabetización crítica, transparencia algorítmica, justicia epistémica y arquitecturas institucionales de alerta temprana, acompañadas de mecanismos de cooperación internacional.

En última instancia, esta reconceptualización exige comprender la democracia no solo como un régimen jurídico-formal, sino como un ecosistema de soberanía cognitiva compartida en el que ciudadanía, instituciones y tecnologías interactúan sobre la base de la equidad informacional, la autonomía interpretativa y la deliberación sustentable. Desde esta perspectiva, la legitimidad democrática se sostiene en su capacidad para adaptarse a escenarios híbridos, resistir la manipulación perceptiva y responder a amenazas no convencionales sin renunciar a sus principios fundacionales.

## Conclusiones

Podemos afirmar que la crisis de nuestras democracias es, antes que nada, una crisis de interpretación. Defender la libertad política implica proteger la infraestructura de la verdad compartida sin sacrificar la pluralidad. Las políticas públicas deben alinear neurociencia social, ética algorítmica y filosofía política con prácticas de educación cívica que fortalezcan autocontrol emocional, verificación distribuida y deliberación informada.

La cooperación internacional no es un suplemento, sino la condición de posibilidad de cualquier estrategia eficaz: ningún Estado puede, aisladamente, regular plataformas globales ni contener la exportación transfronteriza de narrativas tóxicas. La defensa epistémica demanda estándares interoperables de transparencia algorítmica, acceso auditado a datos de impacto social y marcos de responsabilidad compartida que coloquen el interés público por encima de las asimetrías de información.

El objetivo estratégico es simple y ambicioso: sostener un ecosistema donde la discrepancia no sea explotada como arma, la atención no sea capturada como botín y el disenso no sea patologizado como amenaza. Asegurar ese ecosistema es, desde hoy,

la forma más alta de seguridad democrática. Si el poder del siglo XXI se decide en la disputa por el sentido, nuestra tarea —académica, institucional y ciudadana— es que ese sentido siga siendo un bien común.

## Referencias Bibliográficas

Atlantic Council. (2022). Digital authoritarianism in Venezuela. DFRLab.

Center for a New American Security. (2023). AI and the Future of Geopolitical Competition. https://www.cnas.org/publications/reports

CEIUC. (2025). Informe de Riesgos Estratégicos para América Latina. Centro de Estudios Internacionales UC.

Claverie, B., & du Cluzel, F. (2023). The Cognitive Warfare Concept. NATO Innovation Hub.

Córdova Arellano, L. L. (2024). Las guerras híbridas: nuevas formas de agresión, injerencismo e intervencionismo. UNAM. https://archivos.juridicas.unam.mx/www/bjv/libros/15/7355/7.pdf

Crouch, C. (2004). Post-democracy. Cambridge: Polity Press.

Du Cluzel, F., & Claverie, F. (2022). Cognitive Warfare: Key Challenges and Future Trajectories. NATO Innovation Hub.

European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). Giordano, J. (2020). The brain is the battlefield of the 21st century. Strategic Studies Quarterly, 14(4), 18–36.

European Union Institute for Security Studies (EUISS). (2021). Strategic Compass: Towards a Strategic Compass for Security and Defence. EUISS. https://www.iss.europa.eu

Ficek, R. (2023). The Patria Platform and Venezuela's Digital Authoritarianism. Latin America Digital Studies, 5(1), 21–45.

Fraser, N. (2003). La justicia social en la era de la política de la identidad: Redistribución, reconocimiento y participación. Editorial Morata.

Greene, D. (2022). The Promise of Access: Technology, Inequality, and the Political Economy of Hope. MIT Press.

Haraway, D. (1988). Situated knowledge: The science question in feminism and the privilege of partial perspective. Feminist Studies, 14(3), 575–599.

Harding, S. (1986). The Science Question in Feminism. Cornell University Press.

Hoffman, F. (2018). Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges. PRISM, 7(4). https://www.jstor.org/stable/26542705

Hoffman, F. G. (2009). Hybrid threats: A new era of warfare. Potomac Institute.

Hoffman, F. G. (2009). Hybrid Warfare and Challenges. Joint Force Quarterly, 52(1), 34–39.

IDEA International. (2022). The Global State of Democracy Report 2022: Forging Social Contracts in a Time of Discontent. https://www.idea.int

Kaplan, M. (2025). Venezuela's Illicit Economies and Authoritarian Resilience. Strategic Studies Quarterly, 19(1), 44–66.

Kaplan, R. D. (2025). Tierra baldía: Un mundo en crisis permanente. Random House.

Kilcullen, D. (2009). The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One. Oxford University Press.

Levitsky, S., & Way, L. (2022). The New Competitive Authoritarianism. Cambridge University Press.

Levitsky, S., & Ziblatt, D. (2018). How Democracies Die. Crown Publishing

Mouffe, C. (2000). The Democratic Paradox. Verso.

NATO ACT. (2021). Cognitive Warfare and Strategic Foresight. Allied Command Transformation.

NATO StratCom COE. (2021). Hybrid Threats and Critical Infrastructure: Lessons from the Caucasus. NATO Strategic Communications Centre of Excellence.

NATO StratCom COE. (2021). Hybrid Threats in the South Caucasus. Retrieved from https://stratcomcoe.org

NATO StratCom COE. (2022). Russian hybrid warfare: Tools, narratives and countermeasures. NATO StratCom COE. https://stratcomcoe.org/publications

NATO Strategic Communications Centre of Excellence (NATO StratCom COE). (2021). Hybrid Threats and Cognitive Warfare: Implications for NATO. NATO StratCom COE. https://stratcomcoe.org

NATO Strategic Communications Centre of Excellence (StratCom COE). (2020).

Cognitive Warfare and the Future of Conflict. NATO.

NATO Strategic Communications Centre of Excellence. (2023). Information Warfare in Ukraine: Lessons Learned. Riga: NATO StratCom COE. https://stratcomcoe.org

NATO. (2020). NATO's Approach to Countering Hybrid Threats. NATO. https://www.nato.int/cps/en/natohq/topics_156338.htm

Mazarr, M. J. (2015). Mastering the Gray Zone: Understanding a Changing Era of Conflict. U.S. Army War College Press.

OECD. (2024). Governing Artificial Intelligence. OECD Publishing. https://doi.org/10.1787/1cd8a4e5-en

ODNI. (2025). Annual Threat Assessment of the U.S. Intelligence Community. Office of the Director of National Intelligence.

ODNI. (2025). Foreign Threats to the 2024 U.S. Elections. Office of the Director of National Intelligence.

O'Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown Publishing.

Pomerantsev, P. (2022). This is Not Propaganda: Adventures in the War Against Reality. Faber & Faber.

Rid, T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux.

Saavedra, B. (2024). La inteligencia artificial generativa: amenaza, reto y oportunidades para la seguridad y defensa. Centro de Estudios Estratégicos del Ejército del Perú (CEEEP). https://revistas.ceeep.mil.pe/index.php/seguridad-y-poder-terrestre/article/view/78

Skobalski, S., & Arrosio, M. (2024). Antagonismo Dominante: La Guerra Global Segmentada. Buenos Aires: UNDEF.

Stratfor. (2025). Decade Forecast 2025–2035. Stratfor Global Intelligence.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.