EXPEDIENTE ABIERTO



ALGORITMOS DE PODER

LA ESTRATEGIA DE INTELIGENCIA ARTIFICIAL DE LA REPÚBLICA POPULAR CHINA Y SU PROYECCIÓN EN CENTROAMÉRICA.

OCTUBRE 2026

EXPEDIENTE ABIERTO

La misión de Expediente Abierto es producir y difundir contenido investigativo y periodístico de alta calidad que fortalezca el análisis crítico, la participación ciudadana y la defensa de la democracia en América Central.

Autor: Juan Manuel Aguilar Antonio.
Edición: Sergio Cabrales y Javier R. Meléndez.
Diseño: Expediente Abierto

RESUMEN EJECUTIVO

La inteligencia artificial (IA) se ha convertido en uno de los principales escenarios de la competencia geopolítica contemporánea. Sus aplicaciones trascienden la innovación productiva y la modernización de los servicios públicos, al incorporar capacidades para transformar las operaciones de influencia política, vigilancia digital y confrontación híbrida. En este contexto, la República Popular China ha desarrollado una estrategia tecnológica que articula objetivos económicos, militares y políticos bajo la conducción del Partido Comunista Chino (PCCh). El presente informe examina la evolución de esta estrategia, sus mecanismos de proyección internacional y las implicaciones que representa para Centroamérica, una región cuyas necesidades de modernización tecnológica contrastan con sus limitadas capacidades institucionales para gobernar las tecnologías que incorpora.

El ascenso chino en materia de IA no constituye un fenómeno reciente ni exclusivamente atribuible al dinamismo de sus empresas tecnológicas. Por el contrario, responde a cuatro décadas de planificación estatal, desde el Programa 863 de 1986 hasta el Plan de Desarrollo de la Nueva Generación de Inteligencia Artificial de 2017, que estableció el objetivo de convertir a China en líder mundial del sector para 2030. Bajo el liderazgo de Xi Jinping, esta trayectoria adquirió una dimensión estratégica más pronunciada mediante la vinculación de la innovación científica con la seguridad nacional, la autosuficiencia tecnológica y la modernización militar. La denominada fusión civil-militar constituye uno de sus principales instrumentos, al integrar las capacidades de universidades, centros de investigación y empresas privadas con las necesidades del Ejército Popular de Liberación.

En esta arquitectura, los llamados campeones nacionales, entre ellos Huawei, Baidu, Alibaba, Tencent y SenseTime, desempeñan funciones que exceden la competencia comercial. Su participación en el desarrollo de infraestructura digital, sistemas de reconocimiento facial, servicios en la nube y procesamiento de datos contribuye a materializar las prioridades del Partido-Estado. La convergencia entre intereses empresariales y objetivos estratégicos dificulta establecer fronteras precisas entre las

aplicaciones civiles, gubernamentales y militares de estas tecnologías. Paralelamente, Beijing busca trasladar su influencia al ámbito de la gobernanza internacional de la IA, promoviendo mecanismos multilaterales, estándares tecnológicos y programas de cooperación dirigidos especialmente a los países del Sur Global.

Una de las principales conclusiones del informe es que la IA no constituye, por sí misma, una estrategia de conflicto híbrido, sino un multiplicador de capacidades previamente existentes. Su incorporación permite producir contenidos sintéticos, automatizar campañas de propaganda, analizar audiencias y personalizar mensajes a una escala anteriormente difícil de alcanzar. Los casos documentados en Taiwán, Filipinas, Hong Kong y otros escenarios internacionales muestran aplicaciones que comprenden desde la fabricación de noticias mediante presentadores virtuales y videos manipulados hasta el monitoreo de voces críticas y el hostigamiento transnacional. No obstante, la sofisticación tecnológica no equivale necesariamente a efectividad política, por lo que resulta indispensable distinguir entre las capacidades operativas identificadas y sus impactos efectivamente comprobados.

En América Latina, estas prácticas adquieren expresiones particulares mediante operaciones como *Spamouflage*, *Paperwall* y *Glass Onion*, así como campañas de *astroturfing.* Aunque sus procedimientos difieren, comparten la intención de amplificar narrativas favorables a Beijing, simular consensos sociales y dificultar la identificación del origen de determinados contenidos. El monitoreo de 1,334 menciones digitales en Panamá, El Salvador y Costa Rica, realizado entre mayo y noviembre de 2024, identificó patrones de repetición y amplificación de mensajes relacionados con China, aunque estos indicios no demuestran, por sí mismos, coordinación encubierta. Por su parte, las operaciones Paperwall y Glass Onion ilustran mecanismos más complejos de influencia informativa mediante la simulación de medios periodísticos y la intermediación de plataformas digitales que confieren apariencia de legitimidad a contenidos propagandísticos.

Para Centroamérica, estas dinámicas convergen con vulnerabilidades estructurales relacionadas con la dependencia tecnológica, la insuficiencia de especialistas y la debilidad de los marcos regulatorios. La creciente participación de empresas chinas en

telecomunicaciones, infraestructura digital, capacitación y servicios gubernamentales ofrece oportunidades de modernización, pero también plantea riesgos cuando los Estados carecen de capacidades independientes para auditar sistemas, proteger información sensible o diversificar proveedores. Esta problemática resulta especialmente relevante en contextos de deterioro democrático, donde las tecnologías adquiridas para mejorar la administración pública o la seguridad ciudadana pueden ser utilizadas para ampliar mecanismos de vigilancia y control político.

De cara al periodo 2026–2036, el informe identifica cuatro escenarios posibles: soberanía digital cooperativa, dependencia tecnológica controlada, alineación geopolítica mediante protectorados digitales y apropiación autoritaria de tecnologías. Su materialización dependerá menos del origen nacional de los proveedores que de la capacidad institucional de los países centroamericanos para regular, supervisar y sustituir los sistemas tecnológicos que incorporan.

En consecuencia, se recomienda construir una arquitectura regional de resiliencia democrática y digital basada en la gobernanza anticipatoria de la IA, la protección de datos, la auditoría independiente, la diversificación tecnológica y el fortalecimiento de la alfabetización mediática. La cooperación entre gobiernos, universidades, empresas, medios de comunicación y sociedad civil resulta indispensable para evitar que la modernización profundice dependencias difíciles de revertir. En última instancia, el desafío para Centroamérica no consiste en renunciar a las oportunidades que ofrece la inteligencia artificial, sino en garantizar que su aprovechamiento contribuya al desarrollo sin comprometer la autonomía política, el pluralismo informativo y los derechos ciudadanos. La soberanía digital, desde esta perspectiva, debe entenderse como la capacidad efectiva de decidir sobre la tecnología, antes que como su simple adquisición.

CONTENIDOS

Resumen ejecutivo 3

Introducción 7

1. La IA como acelerador de los conflictos híbridos 9

Contaminación informativa 10

La maquinaria del autoritarismo digital y su exportación global 12

2. Análisis de la estrategia china de IA 13

3. Fusión civil-militar 19

4. Configuración del ecosistema digital de china y los "campeones nacionales" 21

5. Casos de estudio a nivel internacional 25

Categoría 1. Producción automatizada de propaganda 25

Categoría 2. Desinformación e interferencia política 27

Categoría 3. Vigilancia digital y monitoreo de voces críticas 30

Categoría 4. Reproducción de narrativas en modelos de lenguaje 30

Categoría 5. Hostigamiento transnacional personalizado 32

6. Casos identificados en América Latina 35

Caso 1. Astroturfing: fabricación del consenso social 36

Caso 2. Spamouflage: amplificación y propaganda coordinada 37

Caso 3. Operación Paperwall: medios locales sin redacción real 38

Caso 4. Operación Glass Onion: las capas del lavado informativo 40

7. Impacto y vulnerabilidades para Centroamérica 43

8. Escenarios prospectivos (2026–2036) para Centroamérica 47

9. Recomendaciones para la resiliencia democrática y digital en Centroamérica 51

Conclusiones 54

Referencias 56

Introducción

La inteligencia artificial (IA) se ha convertido en una tecnología de alcance estratégico que modifica las formas contemporáneas de la competencia geopolítica, el conflicto híbrido y la influencia política. Su capacidad para procesar grandes volúmenes de datos, automatizar tareas, producir contenidos sintéticos, personalizar mensajes y ampliar los sistemas de vigilancia permite acelerar operaciones que antes requerían mayores recursos humanos, económicos y técnicos (Schmidt, 2022). Sin embargo, la IA no constituye por sí misma una estrategia de guerra híbrida, sino un multiplicador de capacidades que incrementa la velocidad, escala, precisión y adaptabilidad de acciones desarrolladas en los dominios cibernéticos, informativos y cognitivos.

En este escenario, la República Popular China (RPC) ocupa una posición central. El ascenso tecnológico del país es el resultado de una planificación estatal iniciada en la década de 1980 y profundizada mediante programas científicos, políticas industriales, reformas institucionales y mecanismos de fusión civil-militar. Bajo el liderazgo de Xi Jinping, la IA adquirió un papel vinculado al desarrollo económico, a la seguridad nacional, a la modernización del Ejército Popular de Liberación (EPL) y a la proyección internacional de China. Esta estrategia se apoya en la articulación entre el Partido Comunista Chino (PCCh), las instituciones gubernamentales, las universidades, las Fuerzas Armadas y los denominados campeones nacionales de la IA (Roberts et al., 2021).

El problema adquiere especial relevancia para Centroamérica. Los países de la región necesitan modernizar sus telecomunicaciones, servicios gubernamentales e infraestructura crítica, pero enfrentan limitaciones financieras, institucionales y técnicas para desarrollar tecnologías propias o auditar de manera independiente los sistemas importados. La falta de especialistas en ciberseguridad e IA, la desigualdad en el acceso a internet, la inversión tecnológica limitada y la ausencia de políticas integrales de soberanía de datos aumentan la dependencia de proveedores extranjeros. Cuando la adquisición tecnológica avanza más rápido que las capacidades para regularla,

supervisarla y sustituirla, la modernización puede convertirse en una fuente de vulnerabilidad política, cibernética y democrática.

El principal riesgo para Centroamérica proviene de las condiciones institucionales, jurídicas y políticas en las que se adquieren y se utilizan las tecnologías. La dependencia tecnológica se convierte en una vulnerabilidad estratégica cuando los Estados pierden la capacidad de auditar sus redes, proteger los datos de la ciudadanía, diversificar proveedores, cuestionar decisiones algorítmicas o reemplazar plataformas sin afectar el funcionamiento de sus instituciones. De manera similar, las herramientas de IA pueden contribuir al autoritarismo digital cuando se emplean sin transparencia, rendición de cuentas ni controles democráticos.

Para sustentar este análisis se realizó una revisión documental de fuentes abiertas, literatura gris, publicaciones académicas indexadas y reportes elaborados por organismos internacionales, centros de investigación, empresas tecnológicas y organizaciones especializadas. Esta revisión se complementó con cuatro entrevistas realizadas a Michael Chong, Evan Ellis, Sascha Hannig y representantes de Double Think Lab.

A partir de este planteamiento, el documento analiza la IA como acelerador de los conflictos híbridos, reconstruye la estrategia china de desarrollo tecnológico, examina la fusión civil-militar y la función de los campeones nacionales y estudia incidentes internacionales relacionados con propaganda automatizada, interferencia política, vigilancia digital, reproducción de narrativas y hostigamiento transnacional. Posteriormente, aborda las operaciones identificadas en América Latina y Centroamérica, evalúa las vulnerabilidades regionales y desarrolla escenarios prospectivos para el periodo 2026–2036.

Finalmente, el estudio propone que la resiliencia democrática y digital de Centroamérica depende de la construcción de capacidades regionales para gobernar la transformación tecnológica. Desde esta perspectiva, la soberanía digital requiere conservar la capacidad efectiva de decidir, supervisar, corregir, diversificar y sustituir tecnologías sin comprometer la autonomía política, el pluralismo informativo y los derechos ciudadanos.

1. La IA como acelerador de los conflictos híbridos

El análisis de las dinámicas del conflicto geopolítico contemporáneo evidencia un desplazamiento de los enfrentamientos bélicos convencionales hacia esquemas de confrontación no restringidos. Para aprehender este fenómeno en su justa dimensión, es indispensable articular tres nociones fundamentales: la guerra asimétrica, las operaciones en la zona gris y la llamada guerra cognitiva.

En primera instancia, la *guerra asimétrica* constituye la estrategia operativa mediante la cual un actor, en desventaja técnica o militar frente a una potencia tradicional, explota las vulnerabilidades normativas, institucionales, sociales o digitales de su rival a través de medios no convencionales (Baloch, 2025). En este entorno emergente, las operaciones en la zona gris (*Gray-Zone Operations*) se sitúan en un espacio difuso entre la competencia diplomática pacífica y el conflicto armado formal. En este umbral, los Estados despliegan mecanismos cibernéticos, informativos, económicos y de coerción indirecta con el propósito de alterar progresivamente el equilibrio de poder regional o global, sin cruzar la línea jurídica que justifique una respuesta militar convencional desde la óptica del derecho internacional (Meriläinen, 2025).

De manera complementaria, la guerra cognitiva (*Cognitive Warfare*) representa un salto evolutivo respecto de las operaciones tradicionales de información y de guerra psicológica. Su premisa posiciona a la mente humana como el sexto dominio del conflicto, situándolo a la misma altura estratégica que los espacios terrestres, marítimos, aéreos, espaciales y cibernéticos (Babayev et al., 2026). En la guerra cognitiva, el objetivo primordial es la alteración sistemática de la percepción en la opinión pública, la erosión de los valores de la población objetivo y la parálisis decisional de las élites políticas y mandos militares.

En la tercera década del siglo XXI, la convergencia entre la IA y conflictos ha transformado la manera en que se libran los conflictos internacionales. En la actualidad,

la IA actúa como un acelerador de la guerra híbrida, pues cataliza las tácticas asimétricas, permitiendo a actores estatales, no estatales y organizaciones criminales acelerar la velocidad, la precisión y el alcance del sabotaje digital en la zona gris. Es precisamente en la intersección entre los dominios cibernético y cognitivo donde la irrupción de la IA ha provocado cambios. Al procesar y sintetizar de manera autónoma los objetivos, los algoritmos potencian las acciones tradicionales con el poder de la IA, redactan mensajes adaptados al perfil psicológico y lingüístico de las víctimas, incrementan drásticamente las tasas de infección por código malicioso en redes gubernamentales y corporativas estratégicas (Romanishyn et al., 2025).

No obstante, la evidencia empírica demuestra que el mayor grado de sofisticación en la zona gris proviene de operaciones híbridas de guerra cognitiva ejecutadas por actores paraestatales y proxies geopolíticos. Casos como el del grupo iraní *Cotton Sandstorm* (vinculado al IRGC[1]) ilustran cómo estructuras híbridas emplean IA generativa, clonación de voz y perfiles sintéticos para infiltrar narrativas, suplantar la identidad de grupos extremistas e intimidar votantes u operadores electorales en democracias occidentales. Asimismo, el ecosistema de proxies rusos compuesto por actores como *Doppelgänger*, *Storm-1516* y *Matryoshka* evidencia la instrumentalización de la IA para la suplantación masiva de portales de noticias legítimos mediante la producción masiva de *deepfakes* audiovisuales o el envenenamiento de modelos de LLMs[2] (Aguilar Antonio, 2025).

En estas operaciones, la IA se utiliza como infraestructura de guerra psicológica destinada a corroer la confianza pública, erosionar la autoridad cognitiva de los medios de comunicación e intervenir en procesos electorales sin necesidad de desplegar tropas ni cruzar el umbral del conflicto armado convencional.

Contaminación informativa

El análisis de la manipulación en el ecosistema digital exige adoptar una tipología conceptual clara de la alteración de la información y de las implicaciones del uso de la IA en la promoción del desorden informativo. Esto se estructura en tres categorías

[1] Cuerpo de la Guardia Revolucionaria Islámica de Irán.
[2] Modelos de lenguaje de gran escala (*Large Language Models*), como ChatGPT, Microsoft Copilot, Google Gemini, Grok, DeepSeek-R1 y Llama.

fundamentales, diferenciadas según la intencionalidad del emisor y la veracidad del contenido (Romanishyn et al., 2025; Aguilar Antonio & Diaz, 2024):

- Misinformación (*Misinformation*): Es la difusión involuntaria de datos inexactos, erróneos o falsos sin el objetivo de causar daño. Su propagación se debe principalmente a brechas en la alfabetización digital y a la falta de sesgos de confirmación por parte de los usuarios que acceden a ellos en redes sociales y en diferentes medios digitales.

- Desinformación (*Disinformation*): Corresponde al diseño, estructuración y distribución deliberada de contenido falso o engañoso con el propósito explícito de manipular a la opinión pública, debilitar las instituciones o consolidar ventajas geopolíticas.

- Malinformación (*Malinformation*): consiste en la instrumentalización malintencionada de datos o hechos reales y de carácter privado. Este material se descontextualiza o filtra intencionalmente para causar daño reputacional, perjudicar la seguridad nacional o entorpecer procesos electorales y democráticos.

Esta tríada encuentra en la IA generativa su principal catalizador técnico, masificando el acceso a falsificaciones digitales de alta fidelidad como la clonación de voz, la suplantación visual de rostros y el desarrollo de avatares virtuales interactivos (Ferrara, 2026). El peligro de estas herramientas radica en su capacidad para romper la intuición natural de verificación basada en ver o escuchar para creer, lo que permite fabricar evidencia altamente verosímil a costos de producción prácticamente nulos (Kreps & Kriner, 2023).

Sin embargo, las amenazas de la IA afectan también la integridad de la arquitectura del algoritmo de LLMs o herramientas de IA generativa comerciales (Roberts & Oosterom, 2025). Esta modalidad, conocida como envenenamiento de datos o infiltración de LLMs, ocurre cuando actores hostiles contaminan intencionalmente los conjuntos de datos empleados en el entrenamiento, el ajuste fino o la generación de texto de los LLMs (Ferrara, 2026). Al introducir sesgos ideológicos, premisas distorsionadas o puertas

traseras, los adversarios logran que el sistema entregue respuestas alteradas que los usuarios asimilan como razonamientos neutrales y objetivos. Esta forma de sabotaje en la cadena de suministro algorítmica compromete silenciosamente la toma de decisiones en agencias gubernamentales, empresas privadas y medios de comunicación.

La maquinaria del autoritarismo digital y su exportación global

El autoritarismo digital se define como la adopción intensiva y sistemática de tecnologías de la información por parte de regímenes autocráticos, iliberales o híbridos con el objetivo central de vigilar, controlar y moldear el comportamiento de la sociedad para garantizar su permanencia en el poder político (Lucaccini, 2025). Para comprender cómo opera este fenómeno, es útil analizarlo como una cadena causal de cuatro etapas interconectadas: 1. El primer eslabón es el protagonista, un gobierno autocrático, que adquiere o desarrolla una tecnología de control específica. 2. El protagonista usa la herramienta mediante prácticas de supervisión o de castigo. 3. Se materializan los efectos inmediatos en la población, como el miedo, la autocensura o el repliegue del debate público. 4. Finalmente, la acumulación de estos impactos conduce a la consolidación y supervivencia a largo plazo de la estructura autocrática (Roberts & Oosterom, 2025).

Esta infraestructura tecnológica incluye desde el despliegue de sistemas masivos de reconocimiento facial hasta la inspección profunda de conjuntos de datos para modificar el tráfico de internet. Los regímenes autoritarios han comenzado a exportar activamente estos modelos de control a otros países. Por medio de contratos comerciales, acuerdos de seguridad bilateral y programas de asistencia técnica, estas potencias transfieren sus herramientas informáticas y metodologías de vigilancia a terceros estados, ampliando sus zonas de influencia geopolítica y acelerando la proliferación de la vigilancia digital a escala global. Asimismo, la debilidad institucional y la calidad de la democracia en América Latina, relacionadas con el avance de regímenes de características iliberales, activan alertas sobre el alcance de su posible utilización.

2. Análisis de la estrategia china de IA

Para comprender el ascenso de China como potencia global en IA, es indispensable desmontar una falacia recurrente: la idea de que el milagro tecnológico de Beijing es un fenómeno reciente o meramente coyuntural. Por el contrario, la capacidad del Partido Comunista Chino (PCCh) para disputar hoy la vanguardia algorítmica es el resultado de cuatro décadas de planificación estatal metódica, obsesiva y profundamente centralizada (Yang & Huang, 2022). Lejos de responder a la lógica espontánea del libre mercado, el liderazgo tecnológico chino fue moldeado mediante una estrategia deliberada de soberanía científica que comenzó a fraguarse a finales de la década de los ochenta del siglo pasado.

El punto de partida de esta estrategia se sitúa en 1986, en un contexto marcado por la Guerra Fría y la iniciativa de Defensa Estratégica de los Estados Unidos, cuatro destacados científicos chinos enviaron una misiva secreta al líder supremo Deng Xiaoping (Feigenbaum, 2003). La advertencia fue que si China no lograba desarrollar su propia capacidad tecnológica avanzada, quedaría irremediablemente rezagada y subordinada al orden internacional dictado por Occidente. Deng Xiaoping aprobó formalmente el "Plan Nacional de Investigación y Desarrollo de Alta Tecnología", conocido históricamente como el Programa 863. Desde sus inicios, representó la primera gran arquitectura de política pública orientada a inyectar recursos estatales masivos en sectores estratégicos de uso dual (civil y militar), centrada en la automatización e informática, biotecnología y nuevos materiales, y telecomunicaciones y tecnologías aeroespaciales (Sun & Cao, 2021).

El segundo pilar de relevancia se edificó en 1997, bajo la administración de Jiang Zemin, y el esquema se complementó con el Plan Nacional de Investigación Básica. Estas iniciativas sentaron las bases teóricas, crearon laboratorios nacionales de élite y formaron a la primera generación de ingenieros y científicos informáticos que, años más tarde, construirían la columna vertebral del ecosistema digital chino (Zhang & Wang, 2018).

China, frente al ecosistema global, adoptó una postura eminentemente reactiva y basada en la asimilación de tecnología extranjera (Meng & Wang, 2023). Consciente de su inferioridad técnica frente a Washington, Tokio o Bruselas, el régimen del PCCh aplicó una política pragmática basada en: 1. La transferencia obligatoria de tecnología a cambio del acceso al mercado interno chino. 2. La ingeniería inversa y la absorción de la propiedad intelectual extranjera. 3. La protección estatal de la naciente infraestructura de internet local mediante la creación del Gran Cortafuegos digital, a finales de la década de 1990.

Sin embargo, hacia el final del mandato de Hu Jintao, este modelo de asimilación alcanzó su límite estructural. El liderazgo del PCCh advirtió que depender del diseño de chips, del software y los estándares creados en Occidente condenaba a China a una subordinación perpetua. En este punto, se hizo evidente la necesidad de pasar de la manufactura pesada y la ingeniería inversa a la innovación autónoma. Formulada originalmente en el Plan Nacional a Mediano y Largo Plazo para el Desarrollo de Ciencia y Tecnología (2006–2020), esta directriz priorizó el desarrollo endógeno de la propiedad intelectual, las patentes y los estándares propietarios en sectores estratégicos (Sun & 2021).

Este cambio de paradigma preparó el terreno para la llegada de Xi Jinping al poder, en 2012, quien impulsó una securitización de la ciencia y tecnología, transformando el desarrollo tecnológico en una herramienta de seguridad nacional (Liu, 2026; Pikover, 2024). Esta perspectiva se vio con la creación de la nueva Ley de Seguridad Nacional, en 2015. En los hechos, el sector tecnológico y el informático fueron seleccionados dentro de los once sectores clave [3] de la seguridad nacional de China (Cao, 2021). Y el mandatario puso énfasis en los sistemas informáticos al indicar que "sin ciberseguridad no hay seguridad nacional y sin digitalización no hay modernización" (Quang, 2023).

La relevancia de este sector para Xi fue estratégica y lo demostró con acciones y nuevas políticas. En 2013, decidió encabezar personalmente la Comisión Central de Ciberseguridad, dos años más tarde lanzó el plan *Made In China 2025* que enmarcaban

[3] La Ley de Seguridad Nacional de 2015 establece once ámbitos de seguridad nacional: política, territorial, militar, económica, cultural, social, tecnológica, informática, ecológica, de recursos y nuclear.

a la IA como una tecnología clave el desarrollo nacional y el cual estaba centrado en transformar a China de una fábrica global a una potencia de alta tecnología que dominará los diez principales sectores de alta tecnología, entre ellos la robótica, las telecomunicaciones de próxima generación y los sistemas autónomos (Li, 2017; Li & Pogodin 2019). Ese mismo año, se lanzó el plan *Internet+,* estrategia que integró tecnologías de la información con sectores tradicionales para crear un nuevo ecosistema industrial. Asimismo, destaca por ser el primer plan central que reconoció a la IA como un sector emergente (Lee et al., 2019; Agarwala, 2021).

Sin embargo, la gran apuesta de Xi Jinping se dio con el lanzamiento del Plan de Desarrollo de la Nueva Generación de IA (NGAIP), lanzado el 18 de julio de 2017. El plan presentó una estrategia para el sector de ciencia, tecnología y educación, que abordaba retos como retener talento, avanzar en investigación fundamental y explorar cuestiones éticas (Wu, 2020). Del mismo modo, se concibió como un plan para delinear el ecosistema nacional de IA de China y convertirla en el principal centro de innovación del mundo para 2030 (Delviana, 2024).

Desde su origen, la política de IA bajo Xi se articuló en torno a la competencia geopolítica y la seguridad nacional. Xi declaró que acelerar la IA era un apoyo estratégico para competir a nivel global y asegurar que las tecnologías centrales estuvieran en manos chinas (Zeng, 2012; Allen, 2019). En los hechos, el NGAIDP cita la palabra "seguridad" 48 veces, incluidas 8 referencias directas a la seguridad nacional, integrando el desarrollo de IA con la defensa. Asimismo, el gobierno promovió la fusión civil-militar (Kim & Yoo, 2022). Con lo cual, Xi enmarcó este empuje tecnológico como una revancha frente a las revoluciones industriales perdidas en el pasado, argumentando que China debía liderar la cuarta revolución industrial (Khanal, 2024).

El NGAIDP estableció metas científicas y de talento, industriales, normativas y de gobernanza para los años 2020, 2025 y 2030, que se presentan en el cuadro 1.

METAS ESTRATÉGICAS

NGAIDP · 2020-2030

Una hoja de ruta en ciencia, industria y gobernanza de la inteligencia artificial.

2020

CIENCIA Y TALENTO

Alcanzar competitividad con las principales potencias tecnológicas del mundo y mejorar el entorno de desarrollo de IA.

INDUSTRIA

Crear una IA «núcleo» con valor de más de 150 mil millones de yuanes y sectores relacionados de más de 1 billón de yuanes.

¥ 150 mil millones de yuanes · más de 1 billón de yuanes

2025

CIENCIA Y TALENTO

Lograr avances de primer nivel en teorías básicas de IA y capacidades de investigación.

INDUSTRIA

Convertir a la IA en el motor principal para la transformación industrial de China, con un fuerte enfoque en la «manufactura inteligente» y la medicina.

NORMAS Y GOBERNANZA

Establecer las primeras regulaciones legales, estándares éticos y marcos de seguridad para el uso de la IA.

2030

CIENCIA Y TALENTO

Posicionar a China como líder mundial en teoría, tecnología y aplicación de inteligencia artificial.

INDUSTRIA

Alcanzar una industria de IA núcleo valorada en 1 billón de yuanes (equivalente a 147 mil millones de dólares).

NORMAS Y GOBERNANZA

Consolidar a China como fuerza impulsora en la definición de normas éticas y estándares globales para IA.

Fuente: Elaboración propia.

La estrategia china de IA no debe evaluarse exclusivamente por su capacidad para producir innovaciones de frontera. Evan Ellis considera que una de sus principales ventajas radica en la articulación entre el mercado interno, los subsidios gubernamentales, la política industrial, las compras públicas, el financiamiento de la investigación, la construcción de infraestructura y la capacitación del capital humano. Esta combinación permitiría transformar los avances tecnológicos en aplicaciones industriales a gran escala y fortalecer progresivamente un ecosistema propio de inteligencia artificial (Evan Ellis, comunicación personal, 8 de agosto de 2026).

En la actualidad, la estrategia de IA de China se encuentra en su tercera fase, focalizada en el tránsito definitivo de una postura centrada en la consolidación nacional a la creación activa de una institucionalidad multilateral y a la búsqueda de influencia en el sistema internacional. Tras haber consolidado su ecosistema doméstico y su infraestructura material, Beijing comenzó a proyectar su peso tecnológico para articular una esfera de influencia normativa en competencia directa con los modelos de Occidente, principalmente con Estados Unidos y la Unión Europea. Este viraje institucional y geopolítico quedó formalmente sellado durante la novena edición de la Conferencia Mundial de Inteligencia Artificial[4] 2026, en Shanghái (WAICO, 2026).

Este proselitismo internacional se relaciona con las metas del NGAIDP hacia 2030, el agotamiento de los instrumentos multilaterales y la divergencia de posturas de los actores de Occidente que en el pasado definían la agenda de la cooperación internacional. También, las posturas antagónicas de la hiperregulación burocrática del *AI Act* en la Unión Europea, frente a la flexibilidad impulsada por la seguridad nacional en Estados Unidos, crearon una ventana de oportunidad estratégica que Beijing decidió capitalizar para presentar al mundo su alternativa de modelo de gobernanza de la IA (Aguilar Antonio, 2024).

De esta forma, la diplomacia del PCCh asumió que la verdadera soberanía en el siglo XXI consiste en poseer la infraestructura o los algoritmos y en liderar los organismos diplomáticos que definen las reglas del juego. Para esto, desde la edición 2025 de la WAIC, China propuso la creación de una organización mundial de cooperación en IA,

[4] Más reconocida por el acrónimo WAIC que significa *World Artificial Intelligence Conference.*

respaldada por más de 1,000 delegados de 40 países que aprobaron el Plan de Acción Global de Gobernanza de IA (Yu, 2025).

Un año después, en la WAIC 2026, celebrada bajo el lema *AI Partnership for a Brighter Future* se materializaron los esfuerzos de Beijing por influir en la definición de las normas internacionales en torno a la gobernanza de la IA. En el acto inaugural, precedido por el presidente Xi Jinping, pronunció un discurso inaugural frente a representantes de 102 países y organismos internacionales (incluyendo al Secretario General de la ONU, António Guterres) con más de 400,000 visitantes presenciales y 1,568 expertos internacionales.

En esta cumbre, China formalizó una estrategia de posicionamiento internacional de cuatro pilares para la gobernanza de la IA. Se consagró como líder en modelos de código abierto, oponiéndose explícitamente al modelo propietario predominante en las empresas estadounidenses. Propuso también un programa de cooperación con países del Sur Global y América Latina. En tercer lugar, extendió esta ambición al ámbito académico mediante la formalización de la Organización Mundial de Cooperación en Inteligencia Artificial (WAICA), copresidida por Yao Qizhi y Richard Sutton, como instrumento de influencia en el sector educativo. Finalmente, lanzó la Organización Mundial de Cooperación en Inteligencia Artificial (WAICO), con sede en China y compuesta por 29 países miembros de Asia, África, América Latina y Europa.

El evento culminó con la firma de acuerdos de intención de compra de tecnología de IA china con un valor récord de 3,000 millones de dólares y la firma de 32 proyectos prioritarios para el ecosistema de Shanghái (WAICO, 2026).

3. Fusión civil-militar

La fusión civil-militar en China ha invertido su lógica inicial bajo los cuatro líderes sucesivos (ver cuadro 2). Bajo Deng Xiaoping, el flujo de innovación se desplazó del sector militar al civil, de modo que la industria de la defensa se reorientó para apoyar la industrialización del país. Esta orientación se revirtió tras el impacto estratégico de la Guerra del Golfo (1991), cuando la superioridad tecnológica estadounidense demostró que el Ejército Popular de Liberación (EPL) necesitaba integrar las innovaciones del sector civil para el consumo en lugar de producirlas de forma aislada. Bajo Hu Jintao, este proceso se institucionalizó como "coordinación militar-industrial", con universidades, institutos y empresas civiles obligados a compartir sus desarrollos con las fuerzas armadas. Bajo Xi Jinping, la tecnología ha pasado de ser un subproducto a un imperativo de seguridad nacional. Así, las reformas de la Comisión Militar Central (2015) centralizaron el mando del EPL bajo su liderazgo, reforzado por purgas anticorrupción en el ejército. Dos instrumentos introducidos en 2017 (la Comisión Central para el Desarrollo de la Integración Cívico-Militar (presidida por Xi Jinping) y las leyes sobre inteligencia y ciberseguridad) eliminaron las barreras burocráticas entre las empresas tecnológicas, las universidades y el Ejército Popular de Liberación (EPL), y obligaron legalmente a todas las organizaciones y ciudadanos a cooperar con los servicios de inteligencia estatales.

De este proceso se desprenden tres características clave del modelo. Primero, la transferencia obligatoria y bidireccional de todas las innovaciones financiadas con fondos públicos al EPL. Segundo, la financiación pública masiva para empresas de doble uso (inteligencia artificial, visión artificial, procesamiento del lenguaje natural, robótica, drones) y, tercero, el paso de la guerra "informática" a la guerra "inteligente", con algoritmos aplicados a la toma de decisiones en combate, a la logística, a las operaciones cibernéticas ofensivas y a los sistemas autónomos.

EVOLUCIÓN DE LA POLÍTICA
DE FUSIÓN CIVIL-MILITAR DE CHINA.

	Orientación estratégica de la fusión civil-militar	Principales políticas e instrumentos
 Deng Xiaoping	Acercar la industria militar y civil, priorizando las necesidades de la defensa y aprovechando las capacidades tecnológicas del sector civil.	**Programa 863,** como antecedente del impulso estatal a la alta tecnología y las tecnologías de uso dual, dentro de una política de modernización y conversión tecnológica.
 Jiang Zemin	Mantener la integración militar-civil como línea de política y reducir la separación entre la defensa y el sistema nacional de investigación y desarrollo.	**Programa 973** y otras políticas de I+D orientadas a ampliar el acceso del sector de la defensa a los recursos nacionales de ciencia y tecnología, así como a reducir redundancias institucionales.
 Hu Jintao	Concebir la innovación científica y tecnológica como un multiplicador de la seguridad nacional y el desarrollo económico.	**12.º Plan Quinquenal** y profundización de la política de integración civil-militar en los sectores de ciencia, tecnología y defensa.
 Xi Jinping	Convertir la fusión civil-militar en una estrategia nacional destinada a competir militar y económicamente con Estados Unidos, acelerar la modernización del Ejército Popular de Liberación, aprovechar las tecnologías de uso dual y alcanzar la autosuficiencia tecnológica.	**Made in China 2025**, Internet+ 13.º Plan Quinquenal; Primer Plan de Implementación Trienal de IA; NGAIP, con metas para 2020, 2025 y 2030; y adopción formal de la fusión civil-militar como estrategia nacional.

Fuente: Elaboración propia.

4. Configuración del ecosistema digital de china y los "campeones nacionales"

Para materializar la visión del NGAIP y los objetivos de la fusión civil-militar, el PCCh y el Ministerio de Ciencia y Tecnología no confiaron en la competencia abstracta del mercado. En su lugar, designaron explícitamente a un selecto grupo de empresas privadas como los "Campeones Nacionales de la IA", asignando a cada una la responsabilidad de liderar y coordinar la investigación en sectores tecnológicos estratégicos (Arenal et al., 2020; Aguilar-Antonio, 2025). Para ello, en 2017, el gobierno seleccionó cuatro plataformas nacionales para el desarrollo de la IA en China. Posteriormente, en 2019, expandió este grupo a quince empresas, entre las principales se presentan en el cuadro 3.

CAMPEONES NACIONALES DE IA DE CHINA

	Especialización tecnológica asignada	Aplicaciones civiles, públicas y estratégicas
Baidu 百度	Conducción autónoma, aprendizaje profundo, procesamiento del lenguaje natural y computación cognitiva.	Vehículos autónomos, interfaces humano-máquina, identificación biométrica y plataformas de IA para usos comerciales e infraestructura pública.
Alibaba.com	Ciudades inteligentes, servicios de nube, sistemas de recomendación y análisis del comportamiento de usuarios.	*City Brain* para gestión urbana, salud digital, comercio minorista automatizado y agricultura inteligente, con aplicaciones comerciales y de administración pública.
Tencent 腾讯	Visión computacional aplicada a imágenes médicas, reconocimiento del habla, procesamiento del lenguaje natural y aprendizaje automático.	Diagnóstico por imagen, videojuegos con IA, plataformas sociales y reconocimiento facial, con aplicaciones comerciales y potencial para vigilancia y gobernanza digital.
iFLYTEK	Tecnologías de voz inteligente, reconocimiento del habla y procesamiento del lenguaje.	Asistentes de voz, plataformas educativas, servicios públicos y sistemas de interacción humano-máquina con posible integración en actividades de seguridad y administración.
商汤 sensetime	Reconocimiento facial y visión computacional.	Seguridad pública, vigilancia en ciudades inteligentes y sistemas de análisis visual exportables a otros países.
HUAWEI	Semiconductores y capacidad de cómputo para IA, servicios de nube, computación en el borde y plataformas de procesamiento.	Infraestructura de IA, ciudades seguras, videojuegos en la nube y despliegues industriales con relevancia comercial y tecnológica estratégica.
JINGDONG	Investigación aplicada en IA y ecosistemas empresariales de datos.	Logística inteligente, colaboración con empresas industriales y transferencia de capacidades a pequeñas y medianas empresas y cadenas de suministro.
xiaomi	Dispositivos inteligentes y participación en ecosistemas nacionales de IA.	Hardware conectado, consumo inteligente y despliegue masivo de IA en actividades cotidianas, con valor industrial y para la generación de datos.
DiDi	Movilidad inteligente y análisis de datos de transporte.	Optimización del transporte, plataformas urbanas y apoyo a la gobernanza de la movilidad.
美团 meituan.com | 大众点评 dianping.com	Servicios bajo demanda y plataformas de análisis de datos de consumo.	Optimización de servicios urbanos y del consumo digital, con aplicaciones en la gestión de plataformas y la administración urbana.
ByteDance	Plataformas algorítmicas y ecosistemas corporativos de IA.	Sistemas de recomendación algorítmica, gobernanza de contenidos y acumulación de datos con implicaciones comerciales y regulatorias.
TAL 好未来	Educación inteligente.	Plataformas educativas, formación de talento y apoyo a la estrategia nacional de desarrollo de capacidades en IA.

Fuente: Elaboración propia.

En este punto, es importante mencionar que cuando el Estado chino designa una empresa para liderar un dominio de IA les delega parte de la dirección práctica de la política, porque las empresas pasan a definir infraestructuras, estándares operativos, prioridades de aplicación y ritmos de despliegue (Mao et al., 2025). En China, esa responsabilidad se inserta en una estrategia nacional que busca el liderazgo internacional, la autosuficiencia tecnológica y el desarrollo coordinado entre el centro, las provincias, las universidades y las empresas privadas. La empresa designada deja de ser solo un actor de mercado y se convierte en un instrumento estatal (Knox, 2020; Mustafina & Dalelkhan, 2025).

En ese sentido, la empresa ya no responde solo por su producto, sino por traducir objetivos nacionales amplios en sistemas concretos, coordinar redes de investigación y acelerar mercados que el Estado considera estratégicos (Camillri, 2023; Cihon, 2021).

Esto da lugar a la incapacidad para distinguir dónde termina la empresa privada y dónde empieza el gobierno. La participación del PCCh en los campeones nacionales de IA se basa en una combinación de designación estatal, células partidarias dentro de las empresas, capital de propiedad estatal y lealtad política exigida, lo que difumina la frontera entre lo privado y lo público. Desde un análisis estratégico, la implicación principal es que la designación empresarial vuelve porosa la frontera entre la capacidad civil, la política industrial y la utilidad militar. La IA es una tecnología de uso dual, en la que separar nítidamente lo civil de lo militar resulta cada vez menos realista (Onderco, 2025).

En términos comparativos, China aparece precisamente como el caso que enfatiza la fusión civil-militar como eje de la política. El sector civil suele ir por delante en innovación, mientras que el militar consume herramientas, datos e infraestructura ya disponibles. Esta alianza simbiótica entre el Partido-Estado y los conglomerados tecnológicos permitió a China construir, en tiempo récord, el ecosistema de recopilación de datos y aplicación algorítmica más vasto del planeta. Para finales de 2020, China ya había configurado una maquinaria capaz de desafiar directamente a Occidente.

EVOLUCIÓN DE LA POLÍTICA DE TECNOLOGÍA E IA DURANTE EL GOBIERNO DE XI JINPING

	Instrumento o decisión	Propósito estratégico
2014	Comisión Central de Ciberseguridad	Centralizó el control de la información y la gobernanza digital bajo la conducción de Xi Jinping, vinculando la ciberseguridad con la seguridad nacional y la modernización del país.
2015	Ley de Seguridad Nacional	Incorporó los sectores tecnológico e informático dentro de los ámbitos fundamentales de la seguridad nacional de China.
2015	*Made in China 2025* e *Internet+*	Posicionaron la inteligencia artificial como un sector estratégico para transformar la estructura productiva, integrar las tecnologías de información con las industrias tradicionales e impulsar el desarrollo tecnológico nacional.
2015	Reforma de la Comisión Militar Central	Centralizó la conducción del Ejército Popular de Liberación bajo el liderazgo de Xi Jinping y reforzó la vinculación entre modernización militar, innovación científica y desarrollo tecnológico.
2016	13.º Plan Quinquenal y Primer Plan de Implementación Trienal de IA	Reconocieron la inteligencia artificial como una industria emergente crítica y promovieron la investigación, el desarrollo y la aplicación de esta tecnología.
2017	Plan de Desarrollo de la Nueva Generación de Inteligencia Artificial (NGAIP)	Estableció las metas científicas, industriales, normativas y de gobernanza previstas para 2020, 2025 y 2030, con el objetivo de convertir a China en líder mundial de inteligencia artificial.
2017	Comisión Central para el Desarrollo de la Integración Civil y Militar	Institucionalizó la coordinación entre empresas tecnológicas, universidades, centros de investigación y el Ejército Popular de Liberación para desarrollar y aprovechar tecnologías de uso dual.
2017	Ley de Inteligencia y Ley de Ciberseguridad	Establecieron la obligación de organizaciones y ciudadanos de colaborar con las actividades de inteligencia del Estado y facilitaron el acceso gubernamental a datos almacenados en servidores ubicados en territorio chino.
2017	Creación de cuatro plataformas nacionales de IA	Designó empresas responsables de encabezar la investigación, coordinación y aplicación de la inteligencia artificial en sectores tecnológicos estratégicos.
2019	Ampliación del grupo de plataformas y campeones nacionales de IA	Extendió a quince empresas el ecosistema de campeones nacionales responsables de desarrollar sectores específicos de inteligencia artificial.
2021	Ley de Seguridad de Datos y Ley de Protección de la Información Personal	Establecieron el marco jurídico para la seguridad, tratamiento y protección de los datos, así como para la gobernanza de la inteligencia artificial conforme a las directrices del Partido Comunista Chino.
2025	Plan de Acción Global de Gobernanza de IA y propuesta de una organización mundial de cooperación	Proyectó el modelo chino de gobernanza de la inteligencia artificial hacia el sistema internacional y promovió la creación de mecanismos multilaterales de cooperación.
2026	Creación de la Organización Mundial de Cooperación en Inteligencia Artificial (WAICO)	Buscó institucionalizar el liderazgo chino en la definición de estándares internacionales de gobernanza, regulación y seguridad de la inteligencia artificial.
2026	Programas de capacitación y cooperación tecnológica con el Sur Global	Promovieron la formación y el intercambio técnico en IA, así como la creación de centros de cooperación con la CELAC, la Unión Africana, los BRICS y la ASEAN.

Fuente: Elaboración propia.

5. Casos de estudio a nivel internacional

Los incidentes analizados en esta sección muestran que estas tecnologías pueden utilizarse para crear presentadores virtuales, generar imágenes falsas, manipular videos, monitorear conversaciones, elaborar perfiles de usuarios y fabricar materiales destinados a intimidar a personas específicas. También, evidencian que el uso geopolítico de IA puede reproducir narrativas asociadas con la censura y la propaganda política. Double Think Lab identifica a Taiwán, Filipinas y Japón como los países en los que las operaciones informativas chinas presentan la mayor intensidad en su entorno regional. En Taiwán, las actividades se relacionan con la presión sostenida del PCCh; en Japón, intervienen las tensiones históricas; y en Filipinas, influyen los conflictos territoriales y la orientación de su gobierno hacia Estados Unidos (Double Think Lab, comunicación personal, 27 de agosto de 2026). Los incidentes se organizaron en cinco categorías para aglutinar algunas similitudes y resaltar diferencias.

Categoría 1. Producción automatizada de propaganda

Presentadores virtuales de *Wolf News*

A finales de 2022, una operación conocida como *Spamouflage*[5] utilizó la plataforma *Synthesia* para crear dos presentadores artificiales en un medio ficticio llamado *Wolf News*. Los presentadores no eran personas reales, sino avatares generados por IA. En los videos aparecían como conductores de noticias y leían guiones con contenido político, criticaban la falta de acciones de Estados Unidos frente a la violencia con armas y promovían la cooperación con China para la recuperación de la economía mundial (Kam, 2022).

El caso se considera la primera utilización conocida de presentadores artificiales en una operación de influencia alineada con un Estado. Aunque la tecnología utilizada era novedosa, la calidad y el alcance de los contenidos resultaron limitados. Los videos

[5] Red de propaganda y desinformación vinculada en los documentos con el Estado chino. También es identificada como Dragonbridge o Storm 1376. Ejecuta operaciones en las que utiliza cuentas falsas, automatizadas o secuestradas para difundir contenidos favorables a China, cuestionar a sus adversarios y atacar a críticos del Partido Comunista Chino.

fueron descritos como de baja calidad y ninguno superó las 300 visualizaciones. Esto indica que el uso de una herramienta sofisticada no garantiza automáticamente una campaña persuasiva o exitosa (Graphika, 2023).

Synthesia señaló que la producción de los videos violaba los términos de servicio, que prohibían el uso de la plataforma para contenidos políticos, sexuales, personales, criminales o discriminatorios. La empresa bloqueó al usuario responsable y reconoció las dificultades para detectar automáticamente este uso indebido (Satariano & Mozur, 2023).

Imágenes generadas con IA y desinformación sobre Maui

Después de incendios registrados en Maui, en agosto de 2023, una campaña originada en China difundió la afirmación falsa de que el desastre había sido provocado por un arma meteorológica experimental de Estados Unidos. Según las publicaciones, los incendios de Maui no habrían tenido un origen natural, sino que habrían sido consecuencia de una prueba realizada por las fuerzas armadas estadounidenses (Atherton, 2023a).

Para reforzar la apariencia de autenticidad, las publicaciones incorporaron fotografías generadas por programas de IA. El contenido se difundió en 15 idiomas a través de 85 cuentas y blogs (Nakaso, 2023). Las cuentas utilizaron la etiqueta *#meteorologicalweapon* interactuaron entre sí y recurrieron a respuestas y reacciones automatizadas para simular una conversación orgánica. El medio *NewsGuard* rastreó la narrativa hasta una publicación con origen en la plataforma *china163.com*. Posteriormente, la información pasó a diferentes redes sociales y alcanzó a usuarios de distintos países. Meta confirmó que las cuentas identificadas formaban parte de *Spamouflage*. No obstante, la empresa señaló que estas cuentas no lograron alcanzar audiencias reales en Facebook (Degurin, 2023).

Categoría 2. Desinformación e interferencia política

El video manipulado de Lai Ching-te

Este incidente ocurrió antes de las elecciones presidenciales de Taiwán del 13 de enero de 2024. En noviembre de 2023, comenzó a circular en redes sociales un video que, aparentemente, mostraba al candidato Lai Ching-te respaldando a sus dos rivales electorales. A primera vista, el material parecía una entrevista ordinaria. Sin embargo, el discurso del candidato era poco natural y el mensaje resultaba extraño dentro del contexto de una competencia presidencial, por lo que se determinó que el contenido era un *deepfake*. El video apareció en un entorno marcado por advertencias de las autoridades taiwanesas sobre una intensificación de las operaciones de influencia de China. Por lo que se considera que el video fue un acto para influir en la opinión pública taiwanesa, que se sospecha que fue elaborado por la unidad de guerra psicológica Base 311 del EPL (Atherton, 2023b).

Double Think Lab señaló que los contenidos generados por IA contra Lai Ching-te evolucionaron en calidad y complejidad. Durante el proceso electoral, circularon textos, imágenes y videos que reavivaron las controversias en torno a su vivienda y su familia. Posteriormente aparecieron videos más avanzados que lo presentaban como mentiroso, irresponsable y subordinado a los intereses de Estados Unidos. Algunos incorporaban personajes y juegos lingüísticos reconocibles para las audiencias taiwanesas, con el propósito de ridiculizarlo y facilitar la circulación del mensaje (Double Think Lab, comunicación personal, 27 de agosto de 2026).

Las campañas descritas también abordaron asuntos como la seguridad alimentaria, el vertido de agua tratada de Fukushima y la posibilidad de una guerra entre China y Taiwán. El propósito era generar miedo, erosionar la confianza en las autoridades y transmitir la idea de que el gobierno no podía garantizar la seguridad de la población. Frente a estas operaciones, Taiwán había desarrollado una comunidad de organizaciones dedicadas a verificar contenidos. Entre ellas se encontraban *MyGoPen* y *Cofacts*, que utilizaban herramientas automatizadas para revisar y desmentir información difundida en redes sociales y servicios de mensajería. *Cofacts* había observado un incremento aproximado del 40 por ciento en la circulación de

desinformación antes de los procesos electorales en el ecosistema de internet de Taiwán (Smith, 2023).

Deepfake de Ferdinand Marcos Jr.

En julio de 2024, durante un acto del movimiento Maisug en la región de Luzón Central, Filipinas, Claire "Maharlika" Contreras, identificada como aliada de Rodrigo Duterte, presentó un video que supuestamente mostraba al presidente filipino Ferdinand Marcos Jr. consumiendo drogas. La grabación se difundió inmediatamente antes del discurso presidencial sobre el Estado de la Nación y se volvió viral. Las autoridades filipinas consideraron que el momento de su publicación evidenciaba una intención de desacreditar al mandatario y debilitar su gobierno (Atherton, 2024).

El Ministerio de Defensa de Filipinas calificó el material de falso y de un intento de desestabilizar la administración. El Departamento de Justicia también condenó la grabación y anunció que emprendería acciones para identificar y procesar a sus responsables. Con base en este análisis, concluyeron que la persona en la grabación no era Marcos Jr. sino un *Deepfake*. El video habría sido amplificado por *Spamouflage* mediante cuentas no auténticas (Maitem, 2024).

El incidente fue considerado perjudicial para el presidente, el gobierno filipino, la confianza pública, la integridad de la información y las relaciones entre Filipinas y China. No obstante, Double Think Lab consideró que, en la opinión pública, estas campañas digitales han obtenido resultados limitados porque los conflictos existentes generan una predisposición negativa y porque los contenidos no siempre comprenden adecuadamente a la audiencia local (Double Think Lab, comunicación personal, 27 de agosto de 2026).

GoLaxy y la automatización de la influencia política

Entre 2020 y 2023, documentos filtrados y revisados por investigadores y medios atribuyen a la empresa china *GoLaxy* el uso de su sistema *GoPro* en distintas operaciones de influencia a favor del PCCh. En 2020, la empresa habría identificado aproximadamente 180.000 cuentas de Twitter en Hong Kong como parte de una

campaña destinada a contrarrestar la oposición a la Ley de Seguridad Nacional. El objetivo de la operación era difundir narrativas que minimizaran el descontento público ante una ley que amplió el control chino sobre Hong Kong (Atherton, 2020).

Durante la aplicación de la política de Cero Covid, *GoLaxy* habría utilizado cuentas falsas de Facebook para amplificar los elogios de Elon Musk a las medidas adoptadas por el gobierno chino. El propósito habría sido responder a las críticas occidentales y aumentar el apoyo a la política sanitaria. Sin embargo, el esfuerzo aparentemente no produjo una diferencia significativa y la oposición pública llevó finalmente al gobierno a modificar su política. En diciembre de 2023, antes de las elecciones presidenciales de Taiwán, GoLaxy habría recomendado mensajes específicos para aprovechar las diferencias en la opinión pública y debilitar al Partido Democrático Progresista. El sistema *GoPro*, también denominado *Smart Propaganda System* habría sido diseñado para reunir grandes volúmenes de información, identificar cambios en la opinión pública, analizar los argumentos de personas influyentes, elaborar perfiles de usuarios y producir contenidos personalizados. La plataforma podía recopilar datos de redes sociales chinas y occidentales, incluidas Weibo, WeChat, X y Facebook (Barnes, 2025).

GoLaxy negó haber creado redes de bots, efectuado perfiles psicológicos o trabajado en campañas relacionadas con Hong Kong y procesos electorales. También, afirmó que era una empresa comercial independiente y sus productos se basaban principalmente en información de fuentes abiertas. Double Think Lab considera que la baja actividad de estos perfiles puede deberse a que están a la espera de instrucciones de un cliente. A partir de las minutas examinadas, la organización interpreta que GoLaxy buscaba demostrar sus capacidades para monitorear personas, analizar intereses y manipular audiencias. En esta lectura, los activos podrían volver a intensificar su actividad durante periodos electorales u otras coyunturas políticas (Double Think Lab, comunicación personal, 27 de agosto de 2026). Este caso debe analizarse con especial cautela, porque representa la posible transición de la producción masiva de propaganda a sistemas capaces de observar audiencias, identificar vulnerabilidades y generar mensajes personalizados.

Categoría 3. Vigilancia digital y monitoreo de voces críticas

El sistema *Peer Review*

En febrero de 2025, OpenAI informó que había detectado una operación vinculada con actores estatales chinos denominada *Peer Review*. El sistema habría sido creado para monitorear en tiempo real publicaciones críticas del Estado chino en redes sociales occidentales y elaborar informes al respecto. La herramienta supuestamente se construyó con Llama, el modelo de código abierto desarrollado por Meta. La operación fue descubierta porque una persona involucrada en el desarrollo utilizó herramientas de OpenAI para depurar fragmentos de código (Metz, 2025). Algunas cuentas también habrían utilizado ChatGPT para producir materiales comerciales destinados a promover el sistema de vigilancia (Atherton, 2025a).

El caso evidencia que una herramienta de IA puede intervenir en distintos momentos de una operación. Puede utilizarse para escribir o corregir código, generar documentación, elaborar presentaciones comerciales y contribuir al funcionamiento de sistemas diseñados para analizar conversaciones digitales. OpenAI también identificó otra operación denominada *Sponsored Discontent*. Esta campaña utilizó sus herramientas para redactar comentarios en inglés contra la disidente china Cai Xia y traducir al español artículos críticos de la sociedad y la política estadounidenses.

Categoría 4. Reproducción de narrativas en modelos de lenguaje

Respuestas alineadas con censura y propaganda en LLMs

El 25 de junio de 2025, American Security Project presentó un informe sobre las respuestas generadas por ChatGPT, Microsoft Copilot, Google Gemini, Grok y DeepSeek-R1. Los sistemas fueron interrogados en inglés y en chino simplificado sobre asuntos considerados políticamente sensibles por el gobierno chino (Manning et al., 2025).

Según el estudio, todos los modelos produjeron, en ocasiones, respuestas que reflejaban censura, sesgos o narrativas alineadas con el PCCh. Las diferencias fueron más evidentes al comparar las respuestas generadas en ambos idiomas. Ante preguntas en inglés sobre las libertades civiles en Hong Kong, varios modelos señalaron que estas

se habían reducido (Daws, 2025). Cuando la misma pregunta se formuló en chino, algunas respuestas minimizaron las restricciones o desviaron la atención hacia otros asuntos, como la libertad económica. También, se observaron diferencias en las respuestas relacionadas con los acontecimientos de Tiananmén. En chino, solo ChatGPT utilizó la palabra “masacre”, mientras que Copilot y DeepSeek emplearon la expresión “incidente del 4 de junio”, descrita como una formulación alineada con el encuadre del PCCh (Atherton, 2025b).

Frente a preguntas sobre los uigures, Copilot y DeepSeek utilizaron en chino formulaciones que presentaban las acciones del gobierno como políticas de desarrollo o lucha contra el extremismo político. También, en el tema del origen de la pandemia de COVID-19 se observaron variaciones entre las respuestas en inglés y chino. El informe señaló a Copilot como el modelo estadounidense con mayor tendencia a presentar propaganda o desinformación china como información autorizada o equivalente a hechos comprobados. Grok fue descrito, en términos generales, como el más crítico frente a las narrativas estatales chinas (Yu et al.,2025).

Sascha Hannig propone entender esta dinámica como una contaminación de las fuentes que alimentan a los sistemas de IA. Estos modelos recuperan y procesan información disponible en internet; por ello, la apertura, proliferación y accesibilidad de determinados contenidos pueden influir en las respuestas generadas. Si las fuentes legítimas restringen el acceso a sus materiales mientras que los portales estatales, enciclopedias y medios favorables a China permanecen completamente disponibles, los sistemas pueden terminar reproduciendo una representación informativa desequilibrada (Sascha Hannig, comunicación personal, 13 de agosto de 2026).

Categoría 5. Hostigamiento transnacional personalizado

Imágenes sexuales falsas contra activistas de Hong Kong

A finales de 2025, activistas prodemocracia de Hong Kong exiliados en el Reino Unido y Australia fueron objeto de una campaña de hostigamiento mediante imágenes sexuales manipuladas (Atherton, 2025c). Carmen Lau, exconcejala de distrito y activista exiliada en Reino Unido, fue informada el 11 de noviembre de 2025 de que varios de sus antiguos vecinos en Maidenhead habían recibido cartas con imágenes sexualmente explícitas. Al menos seis personas recibieron materiales enviados desde Macao. Las cartas contenían cinco imágenes falsas en las que el rostro de Lau había sido colocado sobre cuerpos de mujeres desnudas o vestidas de ropa interior.

En Australia, el exlegislador Ted Hui y su esposa fueron afectados por un cartel que la presentaba como trabajadora sexual. El documento incluía precios en dólares australianos y una dirección que no estaba relacionada con la pareja. El cartel fue enviado por correo electrónico al empleador de Hui y distribuido entre residentes de una zona de Adelaida. Ambas víctimas denunciaron consecuencias psicológicas, miedo y preocupación por la seguridad de personas ajenas a sus actividades políticas. Lau explicó que, tras recibir amenazas anteriores, había cambiado de domicilio y procuraba cubrirse el rostro cuando salía en público. Hui señaló que su esposa no era una figura pública y que era la primera vez que había sido incorporada directamente al hostigamiento (Hong Kong Fee Press, 2025).

El caso fue descrito como la primera utilización de material sexualmente explícito contra personas incluidas en la lista de recompensas de la policía de Hong Kong. También, fue presentado como una escalada de la represión transnacional y como una forma de violencia dirigida especialmente contra mujeres activistas y familiares de opositores. Al final, no se determinó quién envió las cartas ni los carteles. La embajada china había señalado previamente que otras cartas relacionadas con recompensas eran falsas. Por esta razón, el análisis debe mantener la distinción entre los efectos documentados en las víctimas y la atribución no confirmada a los responsables.

OPERACIONES INTERNACIONALES POTENCIADAS POR IA.

Función	País o región afectada	Plataformas y campañas relacionadas	Recursos empleados e implicaciones estratégicas
Producción automatizada de propaganda	Estados Unidos y audiencias internacionales	*Wolf News*, Spamouflage, Facebook, X, YouTube y otras plataformas digitales.	Utilización de presentadores virtuales, imágenes generadas por IA, traducción multilingüe, cuentas coordinadas y difusión multiplataforma para dotar de apariencia periodística y verosimilitud a narrativas políticas, reducir los costos de producción y fomentar la desconfianza hacia las autoridades estadounidenses.
Desinformación e interferencia política	Taiwán, Filipinas y Hong Kong	Spamouflage, Base 311 del Ejército Popular de Liberación, GoLaxy y su sistema GoPro; X, YouTube, Facebook, Weibo y WeChat.	Empleo de *deepfakes*, cuentas coordinadas, redes de amplificación, análisis de opinión pública, elaboración de perfiles y producción personalizada de contenidos para desacreditar dirigentes, erosionar la confianza pública, explotar divisiones sociales e intervenir en procesos políticos y electorales. La efectividad de algunas operaciones no pudo comprobarse plenamente.
Vigilancia digital de voces críticas	Redes sociales occidentales, comunidades críticas del Estado chino y América Latina	Operación *Peer Review*, *Sponsored Discontent*, X y medios latinoamericanos mediante contenido patrocinado.	Uso de monitoreo automatizado, modelos de código abierto, procesamiento de publicaciones en tiempo real, elaboración de informes y traducción de contenidos para identificar discursos críticos, seguir individuos o comunidades y trasladar actividades de vigilancia e influencia fuera del territorio chino.
Reproducción algorítmica de narrativas políticas	China, Hong Kong y audiencias usuarias de modelos de lenguaje en inglés y chino simplificado	ChatGPT, Microsoft Copilot, Google Gemini, Grok y DeepSeek-R1.	Utilización de modelos de lenguaje de gran escala cuyos conjuntos de datos pueden contener propaganda, desinformación o sesgos políticos, lo que puede ocasionar la reproducción de formulaciones alineadas con la censura y la propaganda del Partido Comunista Chino, especialmente en asuntos políticamente sensibles.
Hostigamiento transnacional personalizado	Reino Unido y Australia; activistas prodemocracia exiliados de Hong Kong y sus familiares	Distribución mediante correspondencia física, correo electrónico y materiales dirigidos a vecinos y empleadores.	Empleo de imágenes sexuales manipuladas, suplantación visual, carteles falsos y divulgación de información personal para intimidar, desacreditar y afectar psicológicamente a activistas exiliados y sus familiares, ampliando la represión transnacional fuera de China.

Fuente: Elaboración propia.

En conjunto, los incidentes configuran una secuencia operacional: producción sintética, distribución coordinada, interferencia política, análisis de audiencias, vigilancia digital y hostigamiento personalizado. Esta progresión demuestra que el conflicto híbrido asistido por IA opera simultáneamente en los dominios cibernéticos y cognitivos. Su propósito es contaminar el entorno informativo, erosionar la confianza institucional, aumentar la incertidumbre y dificultar la construcción de una realidad compartida.

6. Casos identificados en América Latina

Las operaciones de influencia digital identificadas en América Latina no responden a un único mecanismo. Conforman un ecosistema integrado por cuentas automatizadas o coordinadas, contenidos adaptados a las audiencias locales, plataformas digitales, portales que simulan medios periodísticos y empresas privadas que dificultan identificar el origen de los mensajes. Estas operaciones pueden funcionar de manera complementaria. Unas producen contenidos, otras los amplifican, algunas construyen identidades editoriales aparentemente legítimas y otras introducen sucesivas capas de intermediación.

La dimensión regional de estas operaciones no se limita a la difusión de mensajes favorables a decisiones específicas. De acuerdo con Michael Chong, también busca modificar la percepción latinoamericana sobre China y proyectarla como una potencia tecnológicamente avanzada y como un socio estratégico conveniente para la región (Michael Chong, comunicación personal, 10 de agosto de 2026). Desde esta perspectiva, la repetición de mensajes sobre la superioridad tecnológica, la infraestructura y la cooperación cumpliría una función acumulativa de posicionamiento.

Esta interpretación coincide con la distinción que plantea Sascha Hannig entre la propaganda china y la rusa. Mientras Rusia se orientaría principalmente a atacar a Occidente y promover su modelo como una alternativa de seguridad e integridad moral, China buscaría mostrarse como “la mejor opción”, una potencia cooperativa, amigable y moderna, más allá de los resultados concretos de sus relaciones internacionales. La producción de imágenes, videos y presentadores sintéticos forma parte de esta estrategia de posicionamiento. Hannig señala que la IA es utilizada para construir representaciones de ciudades modernas, avances tecnológicos, turismo y desarrollo que apoyan la idea de “contar una buena historia de China” (Sascha Hannig, comunicación personal, 13 de agosto de 2026)

Este objetivo general se materializa mediante diversas prácticas. El *astroturfing* crea una apariencia de respaldo ciudadano; *Spamouflage* genera y amplifica mensajes mediante

redes coordinadas; *Paperwall* simula medios locales para dotar de legitimidad a sus contenidos; y *Glass Onion* utiliza intermediarios, dominios y empresas privadas para ocultar la procedencia de las narrativas. Aunque estas operaciones presentan características distintas, convergen en la intención de influir en la percepción pública, dificultar la atribución y reducir la capacidad de las audiencias para distinguir entre información, publicidad, propaganda y desinformación.

Caso 1. Astroturfing: fabricación del consenso social

En 2026, Dialogo Americas identificó campañas de *astroturfing*[6] en el ecosistema de redes sociales cuyo objetivo era crear narrativas de posicionamiento político o de valoración de China, con respaldo ciudadano en múltiples países de América Latina. Los casos más concretos se dieron en cuentas de medios como "Hoy Chile", "Hoy Costa Rica" y "Hoy Paraguay", que difundieron en español contenidos alineados con los intereses del PCCh. Estas cuentas mezclaban mensajes culturales con publicaciones políticas, una práctica que les permitía parecer espacios informativos ordinarios antes de introducir narrativas favorables al modelo de "democracia con características chinas". La automatización de las publicaciones y las reacciones daba la impresión de popularidad y consenso.

En Centroamérica, el informe *Narrativas digitales de China en Centroamérica: propaganda, poder blando y desinformación en redes sociales* identificó indicios de *astroturfing* mediante el monitoreo de 1,334 menciones entre mayo y noviembre de 2024. La distribución se dio en los siguientes países: 480 en Panamá, 647 en El Salvador y 207 en Costa Rica. En Panamá se localizaron aproximadamente 302 publicaciones vinculadas a la Embajada de China y 114 a la embajadora Xu Xueyuan. Además, medios y usuarios reprodujeron un mismo video con textos y menciones idénticos. En El Salvador, 524 de las 647 menciones circularon en Facebook y 123 en X. Estas cifras evidencian repetición y amplificación convergente, pero no prueban por sí mismas la existencia de cuentas falsas ni una coordinación encubierta (Expediente Abierto & ProBox, 2025). La amenaza estratégica del *astroturfing* radica en que altera la percepción de la distribución real de

[6] Práctica orientada a fabricar una apariencia de apoyo ciudadano espontáneo mediante cuentas falsas, automatizadas o coordinadas que publican, replican y amplifican determinados mensajes. Su finalidad es que la audiencia confunda la repetición con legitimidad, la automatización con participación social y la coordinación encubierta con consenso auténtico.

las opiniones. No necesariamente elimina las posiciones críticas, sino que las desplaza mediante la saturación del espacio digital con mensajes coordinados. Su efectividad depende de que la audiencia confunda la automatización con la participación y la repetición con la legitimidad.

Caso 2. Spamouflage: amplificación y propaganda coordinada

La presencia de la red de propaganda y desinformación *Spamouflage* fue identificada en América Latina en el ecosistema de Meta, en agosto de 2023. En los hechos, la compañía tomó acciones para eliminar 7,704 cuentas de Facebook, 954 páginas, 15 grupos y 15 cuentas de Instagram involucradas en comportamiento inauténtico coordinado procedente de China. La intervención fue descrita como la mayor eliminación de una sola red realizada hasta entonces. No obstante, *Spamouflage* permaneció activa y continuó evolucionando. En mayo de 2025, Meta desarticuló redes chinas más pequeñas que ya empleaban personajes generados con IA para dirigirse a audiencias de Taiwán y Japón (Pérez Izquierdo, 2026; Pelcastre, 2026).

La importancia de *Spamouflage* para América Latina radica en su capacidad de conectar contenidos falsos con conversaciones auténticas. Una publicación inicialmente difundida por cuentas falsas puede ser retomada por usuarios reales, periodistas o actores políticos. Una vez que esto ocurre, el mensaje abandona parcialmente su circuito encubierto y adquiere legitimidad social. Con lo cual, *Spamouflage* no solo multiplica la propaganda, sino que también crea las condiciones para que una narrativa coordinada sea percibida como un asunto espontáneo, relevante y ampliamente compartido. Su operación puede sintetizarse en cinco fases: 1. Se produce o recupera un contenido alineado con los intereses de Beijing. 2. El contenido se adapta al idioma y las preocupaciones de la audiencia. 3. Cuentas falsas o secuestradas lo publican en diferentes plataformas. 4. Otros perfiles coordinados lo replican y generan interacciones. 5. La repetición crea una apariencia de viralidad, pluralidad y legitimidad.

Los mensajes pueden difundirse mediante videos, caricaturas, publicaciones culturales y ataques políticos. Del mismo modo, se identificó la circulación de videos y dibujos que criticaban los aranceles estadounidenses y acciones del presidente Donald Trump, así como contenidos dirigidos contra críticos del PCCh.

La entrevista con Michael Chong permitió interpretar esta dinámica como una operación organizada en capas. El entrevistado distinguió una primera fase integrada por bots e infraestructura técnica; una segunda, basada en videos y audios sintéticos; una tercera, orientada al seguimiento y perfilamiento de las audiencias; una cuarta, dedicada a la circulación rápida de contenidos en plataformas como TikTok; y una última, dirigida a dificultar que estas actividades sean vinculadas al gobierno chino (Michael Chong, comunicación personal, 10 de agosto de 2026). Esta interpretación vincula la producción, la segmentación, la difusión y el ocultamiento en una misma secuencia operativa.

Dentro de esta secuencia, el seguimiento de audiencias adquiere una función estratégica. Chong sostiene que este proceso busca "perfilar al latinoamericano" para identificar lo que le gusta y lo que no le gusta y utilizar esa información para adaptar las respuestas y contenidos difundidos mediante las plataformas digitales (Michael Chong, comunicación personal, 10 de agosto de 2026). Desde esta perspectiva, la IA incrementaría el volumen y la velocidad de los mensajes y su capacidad para dirigirse a segmentos específicos de la población.

Caso 3. Operación Paperwall: medios locales sin redacción real

Paperwall es una operación de influencia encubierta identificada por Citizen Lab y atribuida a Shenzhen Haimaiyunxiang Media Co., también conocida como Haimai, una empresa china de relaciones públicas. La red comprendía al menos 123 sitios distribuidos en más de 30 países de América Latina, Europa y Asia. Su principal característica era la simulación de periódicos locales mediante nombres, formatos y referencias territoriales que les otorgaban una apariencia de proximidad con las audiencias (The Watch, 2025).

El uso de nombres locales permitía que los portales fueran percibidos como medios regionales o comunitarios, aunque fueran operados desde China.

SITIOS FALSOS
ASOCIADOS CON LA OPERACIÓN PAPERWALL.

Red regional de portales con apariencia informativa

01 **Argentina**



SITIOS ASOCIADOS

La Plata Post y Lujan Expresar

02 **Brasil**



SITIOS ASOCIADOS

Paulo Expressar y Brasil Industry

03 **Chile**



SITIOS ASOCIADOS

San Rafael Scoop

04 **Colombia**



SITIOS ASOCIADOS

Marta Post

05 **Ecuador**



SITIOS ASOCIADOS

Iguazu

06 **México**



SITIOS ASOCIADOS

Xochimilco Life y Teotihuacaneco

Fuente: Elaboración propia.

Paperwall construía identidades editoriales aparentemente legítimas para distribuirlas. De esta forma, los sitios publicaban contenidos en el idioma de cada audiencia y combinaban noticias recuperadas de medios legítimos, artículos de CGTN y Global Times, comunicados comerciales, materiales favorables a Beijing y ataques contra críticos del PCCh (Saavedra, 2024). La gran cantidad de información comercial o aparentemente inofensiva servía de cobertura para las piezas políticas. La operación dificultaba que los lectores distinguieran entre periodismo, publicidad, propaganda y desinformación (The Watch, 2025).

La efectividad de Paperwall no dependía de que todas sus publicaciones alcanzaran una gran audiencia. Bastaba con que una de sus piezas fuera retomada por un medio establecido, un periodista o una figura política. Cuando esto sucedía, el contenido obtenía una legitimidad que no habría alcanzado como comunicación oficial de China. El riesgo estratégico consistía, por tanto, en introducir narrativas en el sistema informativo formal tras ocultar su procedencia mediante una infraestructura de falsos medios locales.

Caso 4. Operación Glass Onion: las capas del lavado informativo

Glass Onion representó un ecosistema de dominios y subdominios que imitan la apariencia y el rigor editorial de medios internacionales reconocidos, de portales estatales chinos, de medios independientes y de sitios generalistas. La operación fue identificada en el año 2026 a través de portales que promovían los logros tecnológicos y turísticos de China, a la par que neutralizaban discursos sobre controversias ambientales, comerciales, políticas y de derechos humanos que involucraban a este país. En los hechos, incluso se identificaron materiales dirigidos contra críticos del gobierno chino o que presentaban a China como víctima de conspiraciones internacionales (Pérez Izquierdo, 2026).

La operación se basa en la tercerización de servicios digitales. Empresas privadas de relaciones públicas y marketing con sede en China fueron contratadas por entidades asociadas al PCCh para diseñar sitios web, producir contenidos, adaptar los mensajes a diferentes audiencias y gestionar su difusión. Los contratos directos o a través de

intermediarios añadieron capas de opacidad y permitieron mantener una distancia formal entre el partido, las empresas ejecutoras y los activos digitales empleados.

Un aspecto relevante es que los dominios y subdominios compartieron plantillas y proveedores, utilizaron técnicas para dificultar el rastreo y coordinaron la difusión con cuentas relacionadas con *Spamouflage*. La simulación de los portales digitales incluso intentó hacerse pasar por diarios de relevancia global como The Guardian y Los Angeles Times (Fulder-Hardy & Turner, 2026). Estos casos fueron fácilmente identificados porque ambos sitios falsos publicaron el mismo artículo atribuido al doctor Wu Xiaowen, con una fotografía idéntica. Con lo cual, la repetición del contenido bajo identidades editoriales distintas producía una apariencia de corroboración y pluralidad informativa (Pérez Izquierdo, 2026).

La finalidad de la Operación Glass Onion fue promover el "lavado informativo". Esta práctica implica que los contenidos circulen por diversas páginas, cuentas y plataformas antes de llegar a la audiencia. Cada transferencia diluyó su origen y reforzó su apariencia de legitimidad. De esta forma, Glass Onion proporcionó la infraestructura de publicación, mientras *que Spamouflage* aportó la amplificación coordinada. El resultado fue un sistema en el que una misma narrativa parece proceder de múltiples fuentes independientes, aunque su circulación responda a patrones técnicos y temáticos compartidos.

ARQUITECTURA DE LAS OPERACIONES CHINAS DE PROPAGANDA Y DESINFORMACIÓN EN AMÉRICA LATINA.

Red regional de portales con apariencia informativa

Operación o práctica	Mecanismo dentro del ecosistema informativo	Presencia o manifestación en América Latina	Implicación estratégica
Astroturfing	Fabrica una apariencia de respaldo ciudadano mediante cuentas falsas, automatizadas o coordinadas que publican, replican y amplifican determinados mensajes.	Se identificaron contenidos en cuentas como “Hoy Chile”, “Hoy Costa Rica” y “Hoy Paraguay”. En Centroamérica se registraron 1,334 menciones entre mayo y noviembre de 2024: 480 en Panamá, 647 en El Salvador y 207 en Costa Rica.	Distorsiona la percepción sobre la distribución real de las opiniones y hace que la repetición parezca legitimidad, la automatización participación ciudadana y la coordinación encubierta consenso social.
Spamouflage	Produce y amplifica mensajes mediante cuentas falsas, automatizadas, secuestradas o coordinadas que operan en diferentes plataformas.	En agosto de 2023, Meta eliminó 7,704 cuentas de Facebook, 954 páginas, 15 grupos y 15 cuentas de Instagram relacionadas con comportamiento inauténtico coordinado procedente de China.	Facilita que contenidos inicialmente difundidos por redes artificiales sean retomados por usuarios, periodistas, influenciadores o actores políticos y adquieran una apariencia de relevancia y legitimidad social.
Paperwall	Simula periódicos locales mediante nombres, formatos y referencias territoriales para ocultar el origen de los contenidos y otorgarles apariencia periodística.	La red comprendía al menos 123 sitios en más de 30 países. En América Latina se identificaron portales asociados en Argentina, Brasil, Chile, Colombia, Ecuador y México.	Dificulta distinguir entre periodismo, publicidad, propaganda y desinformación. Permite introducir narrativas en el sistema informativo formal cuando los contenidos son retomados por medios, periodistas o figuras políticas.
Glass Onion	Utiliza dominios, subdominios, intermediarios y empresas privadas de relaciones públicas para reproducir contenidos y ocultar su procedencia mediante sucesivas capas digitales.	Los portales compartieron plantillas, proveedores y contenidos, además de coordinar su difusión con cuentas relacionadas con Spamouflage. La operación imitó la apariencia editorial de medios internacionales reconocidos.	Produce “lavado informativo”: cada transferencia diluye el origen del mensaje y genera una falsa impresión de pluralidad, corroboración e independencia editorial.

Fuente: Elaboración propia.

7. Impacto y vulnerabilidades para Centroamérica

El impacto de China en Centroamérica debe analizarse desde la convergencia entre la infraestructura digital, la dependencia tecnológica, la formación de capital humano y las operaciones informativas potenciadas por la IA. Estos componentes no actúan por separado, pues las redes de telecomunicaciones sostienen los flujos de datos. La nube concentra servicios y capacidades de procesamiento. Los programas de capacitación forman a quienes administran esos sistemas y las plataformas digitales se convierten en espacios para difundir narrativas, amplificar posiciones políticas y disputar la percepción pública. La principal vulnerabilidad regional surge cuando los Estados adoptan tecnologías más rápidamente que su capacidad para regularlas, auditarlas y gobernarlas soberanamente (Aguilar Antonio, 2025d). Esta convergencia también afecta al entorno informativo: la formación de comunicadores, la infraestructura digital y la circulación de narrativas pueden reforzarse mutuamente cuando faltan controles independientes y existen casos que demuestran esto como el de Nicaragua (Expediente Público, 2025).

Desde la perspectiva de Evan Ellis, América Latina podría convertirse en un espacio central para la expansión internacional de las tecnologías chinas. Mientras Estados Unidos y Europa protegen en mayor medida sus mercados, los países latinoamericanos presentan barreras menores a la incorporación de productos y servicios tecnológicos competitivos en términos de precio. Esta condición permitiría a las empresas chinas aumentar su volumen de operaciones, consolidar estándares y ampliar su presencia regional en inteligencia artificial, robótica, telecomunicaciones, nube y otros sectores digitales (Evan Ellis, comunicación personal, 8 de agosto de 2026).

Desde una perspectiva que aborde la región, es evidente que esta se encuentra rezagada en el desarrollo de tecnologías de vanguardia, como la IA. El Índice Global de IA asigna a la región una puntuación normalizada de 0.09, frente a 0.63 para América del Norte y 0.16 para Asia y Europa. En 2022, la inversión privada regional en IA alcanzó

US$8,200 millones, dentro de un mercado mundial de US$190,000 millones (Cesareo & White, 2023). Esta diferencia reduce las posibilidades de desarrollar modelos propios, infraestructura computacional avanzada y ecosistemas nacionales de innovación. También, incrementa la dependencia de plataformas, modelos, servicios de nube y soluciones diseñadas en el extranjero, cuyos estándares, criterios de funcionamiento y mecanismos de supervisión no son definidos por los gobiernos nacionales (Aguilar Antonio, 2025a).

La región enfrenta además una carencia de superior a 600,000 especialistas en ciberseguridad e inteligencia artificial y una oferta insuficiente de programas avanzados de formación en inteligencia artificial (OECD, 2022). Las universidades no pueden satisfacer la demanda y parte de la capacitación disponible permanece vinculada a proveedores tecnológicos específicos. Como resultado, los Estados pueden adquirir sistemas de IA, de nube, de telecomunicaciones o de análisis de datos sin contar con personal independiente capaz de examinar su arquitectura, evaluar sesgos, identificar vulnerabilidades o auditar su funcionamiento. Esta situación genera una triple dependencia: de capital humano extranjero, de tecnologías importadas y de los estándares establecidos por los proveedores (Aguilar Antonio, 2025d).

La infraestructura digital profundiza esta vulnerabilidad. La conectividad limitada, los retrasos en las redes 5G y el acceso desigual a tecnologías avanzadas restringen la capacidad regional para desarrollar IA a escala. Estas brechas limitan el desarrollo económico, producen una ciudadanía digital desigual y reducen la capacidad de las comunidades para acceder a fuentes plurales, verificar contenidos o protegerse frente a campañas de manipulación.

En los próximos años, el despliegue de redes 5G y del Internet de las Cosas (IoT) incrementará el número de dispositivos conectados, la circulación de datos y la automatización de servicios públicos y privados. Sin embargo, la expansión del IoT también incorpora riesgos de manipulación de datos, secuestro de dispositivos y ataques de denegación de servicio que pueden afectar la infraestructura crítica. En América Latina y el Caribe, la inversión en IoT durante 2023 representó solo 1.42 % del total mundial, lo que vuelve a colocar a la región en una posición de consumidora de

tecnologías desarrolladas en otros centros de poder. La adopción sin estándares comunes de interoperabilidad, de almacenamiento seguro y de atribución de responsabilidades puede ampliar las dependencias difíciles de revertir (Aguilar Antonio, 2025a).

Esta dependencia de las tecnologías es más profunda en Centroamérica, donde los gigantes tecnológicos chinos se han instalado en sectores clave como las telecomunicaciones, la infraestructura, la energía y los agronegocios. Por ejemplo, ZTE y Xiaomi controlan una gran cuota de mercado en telefonía móvil y equipos electrónicos (Tsafack & Mfewou, 2025). En infraestructura, State Grid, CSCEC y CCCC lideran grandes proyectos en la región. Sin embargo, Huawei constituye el ejemplo más claro de esta dependencia acumulativa. La empresa ingresó inicialmente como proveedor de redes 3G y 4G, dispositivos y soluciones de conectividad bajo criterios de costo, eficiencia y modernización. Posteriormente, extendió su presencia al mantenimiento, la nube, las certificaciones, la formación técnica, los sistemas educativos y los servicios gubernamentales (Aguilar Antonio, 2026).

La penetración tecnológica debe examinarse como un fenómeno multidimensional. Evan Ellis advierte que la vulnerabilidad no se limita al posible acceso a secretos estatales. Comprende las redes de telecomunicaciones, los servicios en la nube, las cámaras de videovigilancia, los sistemas biométricos, los escáneres, la infraestructura portuaria, las plataformas de movilidad y la información generada por empresas y usuarios. La convergencia de estos sistemas amplía el volumen y la diversidad de los datos potencialmente disponibles y dificulta que los Estados conozcan dónde se almacenan, quién puede procesarlos y en qué condiciones pueden utilizarse (Evan Ellis, comunicación personal, 8 de agosto de 2026). El riesgo de utilizar esos datos para perfilar audiencias y dirigir mensajes políticos aumenta si no se conocen las condiciones de acceso, almacenamiento y tratamiento (Expediente Público, 2026).

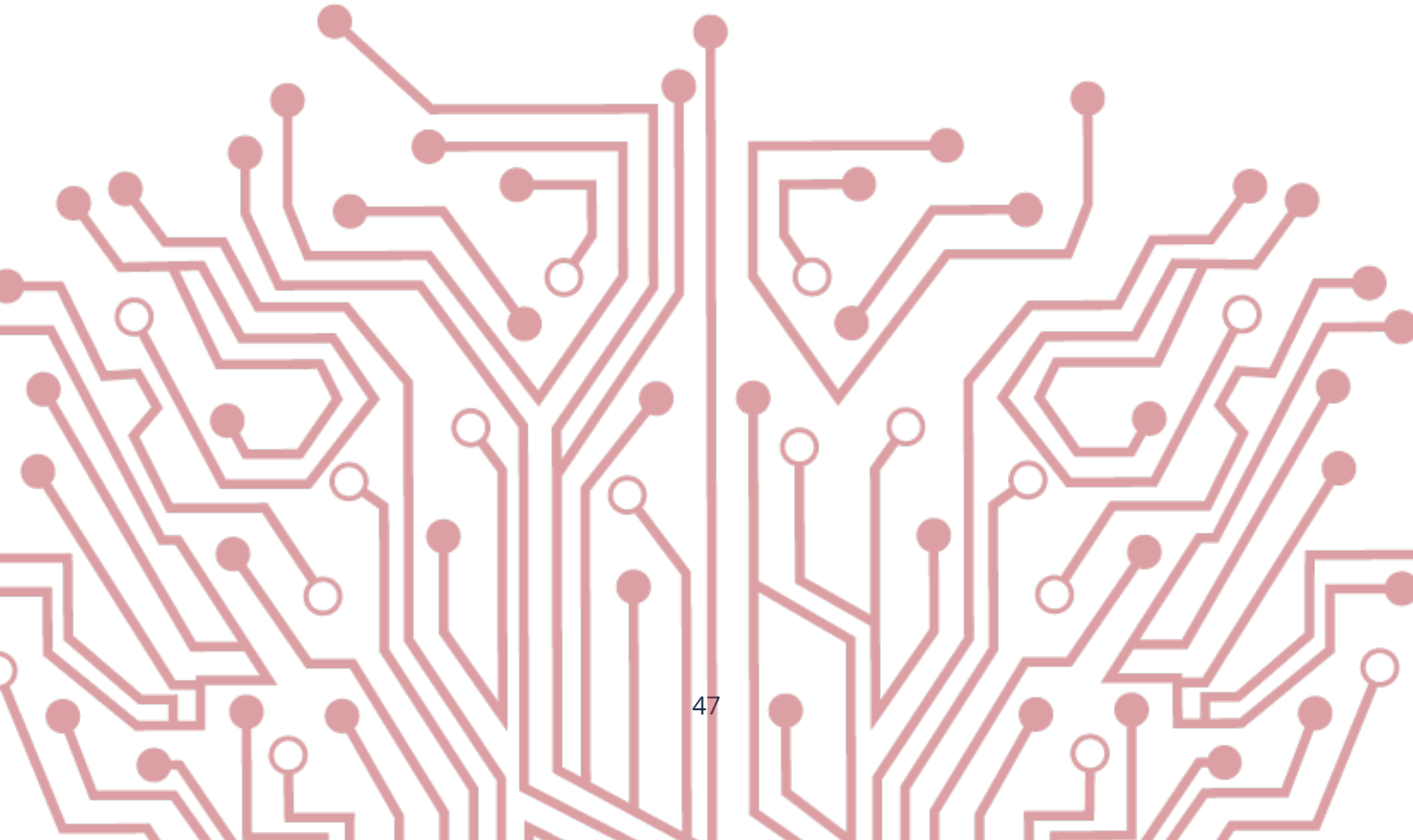
En este panorama, la mayor debilidad de Centroamérica es la ausencia de una política nacional de soberanía de datos, de auditoría tecnológica y de evaluación transversal de proveedores. Esto contrasta con la necesidad urgente de modernización tecnológica

que enfrentan los países, donde las soluciones de bajo costo son adquiridas sin calibrar los impactos en la soberanía y la seguridad nacional que conlleva la adopción de un marco legal adecuado que permita gobernar a estas empresas. El riesgo es especialmente sensible donde la cooperación tecnológica coincide con un deterioro de los controles democráticos. Los casos de Nicaragua, El Salvador y Honduras plantea que los intercambios institucionales y las herramientas de vigilancia pueden reforzar capacidades de control estatal, aunque sus usos y consecuencias deben comprobarse en cada país (Santos, 2026).

En este contexto, la IA añade problemáticas asociadas a los conflictos híbridos, como la desinformación, la contaminación y el autoritarismo digital. La evidencia de los casos analizados muestra cómo la región ya es un nicho de campañas de desinformación con casos concretos como la Operación *Paperwall* o *Glass Onion*. Estas se sirven contenidos falsos, automatización de publicaciones, administración de perfiles digitales, adaptación de mensajes a audiencias específicas y multiplicación de interacciones a una velocidad difícil de enfrentar mediante métodos tradicionales. Las técnicas como el *astroturfing* y el papel de actores como *Spamouflage* muestran cómo la automatización puede integrarse en un ecosistema más amplio de influencia. En Honduras, un monitoreo de la conversación electoral de 2025 documentó la circulación de narrativas favorables a la cooperación con China en un debate político polarizado; el caso permite observar la disputa informativa durante una elección, sin atribuir automáticamente a la IA todas las publicaciones analizadas (Madrid, 2025). La producción de variantes en español y con referencias locales puede facilitar la adaptación de estas narrativas para distintas audiencias centroamericanas; se trata de una capacidad y un riesgo, no de un efecto electoral demostrado.

La vulnerabilidad tecnológica se convierte así en una vulnerabilidad democrática. Si los Estados no pueden auditar sus redes, proteger sus datos o comprender el funcionamiento de sus sistemas de IA, pierden capacidad efectiva de decisión. Si los medios y la ciudadanía tampoco pueden identificar el origen de los contenidos automatizados, se debilitan el pluralismo y la formación de una opinión pública crítica e informada. La soberanía digital no consiste en excluir automáticamente a una empresa o a un país, sino en conservar la capacidad de seleccionar, supervisar, auditar,

diversificar y sustituir tecnologías sin comprometer la vocación de la democracia, ni garantizar la libertad de expresión ni la independencia de los gobiernos (Aguilar Antonio, 2026). La respuesta regional presenta diferencias: en Guatemala, cinco medios formaron una alianza de verificación durante el periodo electoral, mientras que Doble Check, de Costa Rica, ingresó a la Red Internacional de Fact-Checking en 2025. Estas experiencias muestran capacidades existentes que conviene fortalecer, sin caracterizar por igual a todos los ecosistemas informativos centroamericanos.



8. Escenarios prospectivos (2026–2036) para Centroamérica

La evolución de la IA en Centroamérica para 2036 dependerá de la interacción de la consolidación de la IA como un espacio de gobernanza alternativo, la capacidad de China para superar sus limitaciones materiales y modelos fundamentales, y la capacidad real de los países centroamericanos para diversificar sus proveedores sin que sus decisiones se conviertan en alianzas geopolíticas. Dos variables internas también entran en juego, como son la capacidad institucional de los Estados y la calidad de sus democracias. Ningún escenario de los presentados a continuación se desarrollará exactamente igual, pues los países pueden combinar elementos de varios escenarios o pasar de uno a otro tras una crisis institucional, un incidente cibernético o un cambio de proveedor.

Escenario 1. Soberanía digital Cooperativa

Los gobiernos centroamericanos mantienen relaciones tecnológicas con China, Estados Unidos y otros proveedores, pero están desarrollando la capacidad institucional para seleccionar, controlar, auditar, diversificar y reemplazar las tecnologías que adoptan al mismo ritmo de su integración. Este escenario se corresponde, en la práctica, con la implementación efectiva de las recomendaciones descritas en la Sección 9.

Entre los indicios de progreso se incluyen la adopción de regulaciones basadas en el riesgo, la consolidación de las autoridades de protección de datos, el fortalecimiento de los CSIRT nacionales, la diversificación efectiva de proveedores y la integración de cláusulas de portabilidad e interoperabilidad en los contratos tecnológicos. En este contexto, la IA modernizaría los servicios públicos sin menoscabar la autonomía política de los Estados.

Escenario 2. Dependencia tecnológica controlada

Centroamérica mantiene formalmente una política de diversificación, pero sus capacidades institucionales avanzan más lentamente que la adopción tecnológica. Los Estados conservan su soberanía legal sobre sus contratos, pero pierden su autonomía operativa, y dependen de las certificaciones, explicaciones y actualizaciones de las empresas que proporcionan la tecnología, debido a la falta de personal independiente para auditarlas. Esta dependencia se deriva de la acumulación de contratos, conocimientos especializados y procedimientos técnicos vinculados al mismo ecosistema, lo que incrementa progresivamente el costo de cambiar de proveedor.

Entre las señales de alerta se incluyen la proliferación de contratos de mantenimiento a largo plazo, la concentración de servicios en manos de unas pocas empresas, la formación técnica impartida exclusivamente por determinados proveedores y la falta de mecanismos eficaces para la migración de datos o la sustitución de plataformas. El principal riesgo en este escenario no es una crisis repentina, sino la normalización gradual de una soberanía limitada.

Escenario 3. Alineación tecnológica y protectorados digitales

La competencia entre China y Estados Unidos se intensifica, lo que reduce la neutralidad tecnológica de la región. Las decisiones relativas a las redes 5G, los servicios en la nube y los centros de datos ya no se consideran meras adquisiciones comerciales, sino que se interpretan como signos de alineación geopolítica. Si WAICO institucionaliza sus estándares y los acompaña de transferencias tecnológicas y financiación accesible, puede atraer a gobiernos con necesidades urgentes de modernización, pero a cambio de condiciones políticas implícitas que reducen la compatibilidad con los marcos impuestos por Estados Unidos. La soberanía nacional sigue siendo reconocida legalmente, pero la capacidad efectiva del Estado queda subordinada a los estándares y decisiones adoptados en Shanghái o en Washington.

Las señales de alerta serían la concentración de infraestructuras críticas en empresas del mismo origen, la adopción de estándares externos sin auditorías nacionales, las

condiciones políticas explícitas para el acceso a la tecnología y la pérdida de interoperabilidad entre los sistemas de diferentes países de la región.

Escenario 4. Autoritarismo digital mediante apropiación interna

Los gobiernos con características iliberales se apropian, a nivel nacional, de tecnologías de vigilancia, de análisis de datos e inteligencia artificial, inicialmente adquiridas para la seguridad pública, las ciudades inteligentes o la gestión de servicios. El riesgo reside en las condiciones institucionales de su uso: los sistemas de reconocimiento facial, el control digital del tráfico y el análisis del comportamiento se utilizan para monitorear conversaciones, identificar voces críticas e influir en el debate público, reproduciendo así, a nivel nacional, la cadena causal descrita en la Sección 1 (adquisición de la herramienta, uso para vigilancia o represión, miedo y autocensura, consolidación del poder autoritario).

Entre las señales de alerta se incluyen la expansión de la vigilancia gubernamental sin controles independientes, el uso opaco del reconocimiento facial, la falta de procedimientos para impugnar decisiones algorítmicas, la vigilancia de periodistas y figuras de la oposición, y la concentración de información ciudadana en plataformas cerradas sin supervisión externa.

9. Recomendaciones para la resiliencia democrática y digital en Centroamérica

El análisis de los cuatro escenarios muestra que el futuro digital de Centroamérica no estará determinado automáticamente por la expansión de China ni por el desarrollo de la IA. El factor decisivo será la capacidad regional para gobernar esa transformación. La misma tecnología puede contribuir a modernizar servicios, mejorar la conectividad y ampliar las capacidades estatales, o bien profundizar las dependencias, facilitar la vigilancia y contaminar el espacio informativo. La diferencia dependerá de la existencia de instituciones capaces de regular, auditar, diversificar y proteger la infraestructura tecnológica sin sacrificar los derechos, el pluralismo ni la autonomía política.

Esto se relaciona con la construcción de la resiliencia democrática y digital de Centroamérica, que debe comenzar con la edificación de una arquitectura regional que vincule la ciberseguridad, la gobernanza de IA, la protección de datos y el pluralismo informativo. No basta con adquirir herramientas de detección o ampliar las facultades de vigilancia gubernamental. Una política democrática debe proteger simultáneamente la infraestructura, los derechos de los ciudadanos y la autonomía tecnológica. Esto exige sustituir el enfoque reactivo y exclusivamente estatal por un modelo policéntrico en el que gobiernos, empresas, universidades, organizaciones técnicas, medios de comunicación y sociedad civil compartan responsabilidades, información y capacidades. Las recomendaciones que debe atender Centroamérica en ese sentido son:

- *Construir la gobernanza anticipatoria de IA, IoT y 5G.* Los países necesitan regulación basada en riesgos, estándares vinculantes de seguridad, transparencia algorítmica, equidad en el uso de datos y mecanismos independientes de auditoría. Las instituciones públicas deberían evaluar, antes de adquirir un sistema, qué datos utiliza, dónde se almacenan, quién puede acceder a ellos, cómo se toman las decisiones automatizadas y qué procedimiento permite impugnarlas. La contratación tecnológica debe incluir interoperabilidad, portabilidad de datos, transferencia de conocimientos,

actualización de seguridad y condiciones claras de salida para evitar dependencias irreversibles.

- *Fortalecer la resiliencia cibernética de la infraestructura crítica nacional.* Para garantizar la seguridad de los sistemas gubernamentales de recaudación tributaria, educación, salud y seguridad social, son necesarias medidas que incluyan segmentación de redes, autenticación multifactorial, cifrado, respaldos fuera de línea, actualización de sistemas, el principio de privilegio mínimo y planes de continuidad operativa. También se requiere establecer o fortalecer equipos con atribuciones, personal y presupuesto suficientes para emitir alertas, responder a incidentes y coordinar la recuperación.
- *Consolidar la capacidad soberana de auditoría de los gobiernos.* Los gobiernos deben formar especialistas independientes y diversificar las certificaciones para que el conocimiento no quede concentrado en un solo proveedor. Las universidades necesitan vincular sus programas con las necesidades operativas de los gobiernos, la infraestructura crítica y la protección de datos. La cooperación empresarial puede contribuir a esta formación, pero debe acompañarse de currículos abiertos, evaluación pública y la participación de distintas plataformas tecnológicas. La finalidad no es rechazar la capacitación extranjera, sino impedir que se convierta en la única fuente de conocimiento disponible.
- *Construir resiliencia informativa frente operaciones potenciadas por IA sin criminalizar el debate legítimo.* Un observatorio centroamericano podría registrar campañas coordinadas, analizar redes de amplificación, identificar medios simulados y publicar alertas durante elecciones o crisis institucionales. La atribución debe diferenciar entre diplomacia pública, propaganda, desinformación y comportamiento inauténtico coordinado. La transparencia metodológica es indispensable para evitar que el combate a la manipulación se transforme en censura o persecución de posiciones políticas.
- *Fomentar la alfabetización mediática informacional en toda la sociedad.* Se debe preparar a periodistas, funcionarios, docentes y ciudadanía para reconocer contenidos sintéticos, verificar imágenes y videos, identificar cuentas automatizadas y rastrear el origen de una narrativa. Esta formación debe

alcanzar zonas rurales y comunidades excluidas, porque la brecha digital también es una brecha de protección. La resiliencia democrática será efectiva cuando Centroamérica pueda utilizar la IA para modernizar sus economías e instituciones sin ceder el control de sus datos, infraestructura, conocimiento técnico y debate público a proveedores, plataformas o actores extranjeros. Esa capacidad de decidir, auditar y corregir constituye el núcleo de la soberanía digital regional.

Conclusiones

La IA está transformando los conflictos híbridos al ampliar las capacidades disponibles para intervenir en los dominios cibernético, informativos y cognitivos; además, facilita la producción de contenidos sintéticos, la automatización de campañas, la adaptación de mensajes, el monitoreo de conversaciones y la elaboración de perfiles. No obstante, los casos examinados también demuestran que la sofisticación tecnológica no garantiza automáticamente el alcance, la credibilidad ni la efectividad política. Por ello, es indispensable diferenciar entre capacidad técnica, escala operativa, audiencia alcanzada e impacto comprobado.

La estrategia china de IA responde a un proceso histórico de planificación estatal que vinculó la ciencia, la industria, la seguridad nacional y el desarrollo militar. Los programas 863 y 973, la política de innovación autónoma, *Made in China 2025*, *Internet+* y el NGAIP constituyen etapas de una misma trayectoria orientada hacia la autosuficiencia tecnológica y el liderazgo internacional. Durante el gobierno de Xi Jinping, esta trayectoria se profundizó mediante la securitización de la tecnología, la fusión civil-militar y la integración de empresas privadas en los objetivos estratégicos del Partido-Estado.

Las empresas, llamadas campeones nacionales, ocupan una posición determinante dentro de este modelo. Son empresas dedicadas a telecomunicaciones, nube, reconocimiento facial, visión computacional, movilidad, educación y análisis de datos, que desarrollan tecnologías con aplicaciones civiles, gubernamentales y militares. La frontera porosa entre el mercado, la política industrial y la seguridad nacional dificulta distinguir entre las funciones comerciales y las capacidades estratégicas. Por esta razón, la evaluación de proveedores no puede limitarse al costo o la eficiencia de sus productos, sino que debe incorporar criterios de seguridad, gobernanza de datos, interoperabilidad, dependencia tecnológica y posibilidad de sustitución.

Los casos internacionales y regionales muestran que las operaciones de influencia conforman un ecosistema compuesto por diversas funciones. El *astroturfing* crea una apariencia de respaldo ciudadano; *Spamouflage* amplifica mensajes mediante cuentas

coordinadas; *Paperwall* simula medios locales para dotar de legitimidad a los contenidos; y *Glass Onion* oculta su procedencia mediante intermediarios y capas digitales. La articulación de estas prácticas con herramientas de IA permite generar variaciones de un mismo mensaje, adaptar narrativas a distintos contextos y mantener campañas durante periodos prolongados. Su efecto más relevante no consiste necesariamente en convencer a toda la población, sino en contaminar el entorno informativo, aumentar la incertidumbre y dificultar la construcción de una realidad compartida.

Para Centroamérica, estas dinámicas convergen con condiciones estructurales de vulnerabilidad. La limitada inversión en IA, la insuficiencia de especialistas, las desigualdades en conectividad y la dependencia de plataformas extranjeras reducen la capacidad regional para desarrollar, evaluar y gobernar tecnologías avanzadas. La presencia de proveedores chinos en telecomunicaciones, nube, dispositivos, capacitación y servicios gubernamentales puede contribuir a la modernización, pero también puede generar dependencias acumulativas cuando el conocimiento, el mantenimiento, las certificaciones y los datos quedan concentrados en un mismo ecosistema tecnológico.

Los escenarios prospectivos confirman que el factor decisivo para Centroamérica será la capacidad institucional de los países centroamericanos. Una gobernanza basada en riesgos, la auditoría independiente, la protección de datos y la diversificación pueden conducir a una soberanía digital cooperativa. Por el contrario, la debilidad regulatoria y la dependencia operativa pueden favorecer una soberanía limitada, una alineación geopolítica forzada o la apropiación autoritaria de tecnologías de vigilancia y de análisis de datos.

Referencias

Agarwala, N., & Chaudhary, R. D. (2021). 'Made in China 2025': Poised for Success?. *India Quarterly, 77*, 424 - 461. https://doi.org/10.1177/09749284211027250

Aguilar Antonio, J. M. (2025a). Tech Leap or Tech Lag: Latin America's Quest to Keep up with Emerging Technologies. Florida International University. https://doi.org/10.5281/zenodo.22031225

Aguilar Antonio, J. M. (2025b). El ecosistema de inteligencia artificial en China: Políticas, campeones nacionales y clústeres regionales. En E. Tzili-Apango, R. Balderrama Santander y C. A. Barrera Franco (Coords.), China. Estudios Estratégicos (pp. 341–363). Tirant lo Blanch México e Instituto Mexicano de Estudios Estratégicos en Seguridad y Defensa Nacional (IMEESDN).

Aguilar Antonio, J. M. (2025c). Use of Artificial Intelligence by High Risk Criminal Networks. Expertise France. https://doi.org/10.5281/zenodo.16750778

Aguilar Antonio, J. M. (2026). Huawei como vector geopolítico: la disputa por la soberanía digital en Centroamérica. Expediente Abierto. https://www.expedienteabierto.org/huawei-vector-geopolitico/

Aguilar Antonio, J. M., & Díaz García, M. (2025). Riesgos y radicalización en Internet: Retos frente a la infodemia y la desinformación en el ciberespacio. En I. Alvarado Martínez & S. Ramírez Ávila (Coords.), El desarrollo tecnológico en la seguridad nacional (pp. 1–27). Editorial Porrúa.

Aguilar-Antonio, J.M (2025d). From Gap to Action: Towards a Democratic Cybersecurity Architecture in Latin America (2025d). http://dx.doi.org/10.2139/ssrn.5649990

Allen, G. C. (2019). *Understanding China's AI strategy: Clues to Chinese strategic thinking on artificial intelligence and national security*. Center for a New American Security (CNAS). https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy

Arenal, A., Armuña, C., Feijoo, C., Ramos, S., Xu, Z., & Moreno, A. (2020*). Innovation ecosystems theory revisited: The case of artificial intelligence in China. Telecommunications Policy*, 44(6), 101960. https://doi.org/10.1016/j.telpol.2020.101960

Atherton, D. (2020). *Incident 1169: Reported AI-assisted influence campaigns by GoLaxy allegedly targeting Hong Kong and Taiwan political discourse*. AI Incident Database. https://incidentdatabase.ai/cite/1169

Atherton, D. (2023a). *Incident 565: AI-generated imagery and multilingual disinformation in Chinese campaign regarding Maui wildfires*. AI Incident Database. https://incidentdatabase.ai/cite/565

Atherton, D. (2023b). *Incident 667: Manipulated deepfake video of Lai Ching-te endorsing rivals in lead-up to January presidential elections*. AI Incident Database. https://incidentdatabase.ai/cite/667

Atherton, D. (2024). *Incident 1129: Purported AI-generated video depicting Philippine President Ferdinand Marcos Jr. using drugs shared by Rodrigo Duterte supporters and amplified by China-linked Spamouflage*. AI Incident Database. https://incidentdatabase.ai/cite/1129

Atherton, D. (2025a). *Incident 939: AI-powered Chinese surveillance campaign "Peer Review" used for real-time monitoring of anti-state speech on Western social media*. AI Incident Database. https://incidentdatabase.ai/cite/939

Atherton, D. (2025b). *Incident 1188: Multiple LLMs reportedly generated responses aligning with purported CCP censorship and propaganda*. AI Incident Database. https://incidentdatabase.ai/cite/1188

Atherton, D. (2025c). *Incident 1301: Purported AI-generated sexual deepfakes allegedly deployed in transnational harassment campaign targeting Hong Kong exiles*. . AI Incident Database. https://incidentdatabase.ai/cite/1301

Babayev, S., Akhundov, R., & Hashimov, E. (2026). Conceptual-Theoretical Foundations and the Transformative Role of Artificial Intelligence in Multidomain Operations. *Grail of Science*. https://doi.org/10.36074/grail-of-science.20.03.2026.069

Baldassarre, M. T., Caivano, D., Fernández Nieto, B., Gigante, D., & Ragone, A. (2025). Fostering Human Rights in Responsible AI: A Systematic Review for Best Practices in Industry. *IEEE Transactions on Artificial Intelligence, 6*, 416-431. https://doi.org/10.1109/tai.2024.3394389

Baloch, M. U. F. (2025). AI in Modern Warfare: Impacts on Information Operations, Cyber Conflicts, and C2 Systems. *SOCIAL PRISM*. https://doi.org/10.69671/socialprism.2.2.2025.39

Barnes, J. (2025). China Turns to A.I. in Information Warfare. New York Times. https://www.nytimes.com/2025/08/06/us/politics/china-artificial-intelligence-information-warfare.html

Cai, C. (2017). Enforcing a New National Security? China's National Security Law and International Law. *Journal of East Asia and international law, 10*, 4-4. https://doi.org/10.14330/jeail.2017.10.1.04

Camilleri, M. (2023). Artificial intelligence governance: Ethical considerations and implications for social responsibility. *Expert Systems, 41*. https://doi.org/10.1111/exsy.13406

Cihon, P., Schuett, J., & Baum, S. (2021). Corporate Governance of Artificial Intelligence in the Public Interest. *Inf., 12*, 275. https://doi.org/10.3390/info12070275

Daws, R. (2025). Major AI chatbots parrot CCP propaganda. AI News. https://www.artificialintelligence-news.com/news/major-ai-chatbots-parrot-ccp-propaganda/

Degurin, M. (2023). Salacious Chinese Disinformation Campaign Blames Maui Fires on Deadly American 'Weather Weapon. Gizmodo. https://gizmodo.com/weather-weapon-maui-fires-china-disinformation-1850826548

Delviana, N. (2024). Inisiasi Pembentukan Angkatan Siber dan Digital dalam Organisasi Tentara Nasional Indonesia. *Jurnal Syntax Admiration*. https://doi.org/10.46799/jsa.v4i12.1016

Expediente Abierto, & ProBox. (2025). *Narrativas digitales de China en Centroamérica: Propaganda, poder blando y desinformación en redes sociales*. https://proboxve.org/wp-content/uploads/2025/05/Narrativas-Digitales-PB-EA.pdf

Expediente Público (2025). Propaganda hecha en China: el sistema de formación al periodismo nicaragüense. https://www.expedientepublico.org/propaganda-hecha-en-china-el-sistema-de-formacion-al-periodismo-nicaraguense/

Expediente Público (2026). El nuevo petróleo: China y el control de las bases de datos en Latinoamérica. https://www.expedientepublico.org/el-nuevo-petroleo-china-y-el-control-de-las-bases-de-datos-en-latinoamerica/

Feigenbaum, E. A. (2003). *China's Techno-Warriors: National Security and Strategic Competition from the Nuclear Age to the Information Era*. Stanford University Press.

Ferrara, E. (2026). The Generative AI Paradox: GenAI and the Erosion of Trust, the Corrosion of Information Verification, and the Demise of Truth. *ArXiv, abs/2601.00306*. https://doi.org/10.3390/fi18020073

Fulder-Hardy, F. & Turner, L. (2026). Glass Onion Peeling Back the Layers of a Pro-China Online Ecosystem. Graphika. https://public-assets.graphika.com/reports/Graphika_Report_Glass_Onion.pdf

Graphika (2023). Deepfake It Till You Make It. https://www.graphika.com/reports/deepfake-it-till-you-make-it

Hawkins, A., Abdul, G. & Shepherd, T. (2025). Sexually explicit letters about exiled Hong Kong activists sent to UK and Australian addresses. The Guardian.

https://www.theguardian.com/world/2025/dec/11/sexually-explicit-letters-deepfake-hong-kong-activists-uk-australia

He, Y. (2024). Chinese digital platform companies' expansion in the Belt and Road countries. *The Information Society, 40*, 96 - 119. https://doi.org/10.1080/01972243.2024.2317058

Hong Kong Fee Press (2025). Hong Kong activist 'terrified' as sexually explicit deepfake images sent to UK neighbours. https://hongkongfp.com/2025/12/12/hong-kong-activist-terrified-as-sexually-explicit-deepfake-images-sent-to-uk-neighbours/

Kam, L. (2022). *Incident 486: AI video-making tool abused to deploy pro-China news on social media*. AI Incident Database. https://incidentdatabase.ai/cite/486

Khanal, S., Zhang, H., & Taeihagh, A. (2024). Development of New Generation of Artificial Intelligence in China: When Beijing's Global Ambitions Meet Local Realities. *Journal of Contemporary China, 34*, 19 - 42. https://doi.org/10.1080/10670564.2024.2333492

Kim, S.-J., & Yoo, H.-K. (2022). The Status of Artificial Intelligence and National Strategy in China during the Xi Jinping era. *THE JOURNAL OF INTERNATIONAL RELATIONS*. https://doi.org/10.15235/jir.2022.03.25.1.241

Knox, J. (2020). Artificial intelligence and education in China. *Learning, Media and Technology, 45*, 298 - 311. https://doi.org/10.1080/17439884.2020.1754236

Kreps, S., & Kriner, D. (2023). How AI Threatens Democracy. *Journal of Democracy, 34*, 122 - 131. https://doi.org/10.1353/jod.2023.a907693

Lahmann, H., Custers, B., & Scott, B. I. (2025). The fundamental rights risks of countering cognitive warfare with artificial intelligence. *Ethics and Information Technology, 27*. https://doi.org/10.1007/s10676-025-09868-9

Lane, L. (2023). Preventing long-term risks to human rights in smart cities: A critical review of responsibilities for private AI developers. *Internet Policy Rev., 12*. https://doi.org/10.14763/2023.1.1697

Lee, S., Kim, H., Kim, J., & Choi, J. (2019). *China's Internet Plus Strategy: Characteristics and Regional Case Study*, World Economy Brief 19-23, Korea Institute for International Economic Policy.

Li, J., & Pogodin, S. (2019). "Made in China 2025": China experience in Industry 4.0. *IOP Conference Series: Materials Science and Engineering, 497*. https://doi.org/10.1088/1757-899x/497/1/012079

Li, L. (2017). China's manufacturing locus in 2025: With a comparison of "Made-in-China 2025" and "Industry 4.0". *Technological Forecasting and Social Change*. https://doi.org/10.1016/j.techfore.2017.05.028

Liu, T., & Tan, J.-Z. (2026). Artificial Intelligence and Authority. Unpacking China's Tech Policy through Sage-King Governance. *Economic Diplomacy, 4*, 13 - 29. https://doi.org/10.2478/ecdip-2026-0004

Lucaccini, M. (2025). "Digital Authoritarianism: ICT-enabled Repression Across Regime Types." *ITASEC/SERICS*. https://doi.org/10.31235/osf.io/rvmj2_v1

Madrid, Y. (2025). China y Rusia, aliados de Rixi Moncada en las elecciones de Honduras. Expediente Abierto. https://www.expedientepublico.org/china-y-rusia-aliados-de-rixi-moncada-en-las-elecciones-de-honduras/

Maitem, J. (2024). 'Malicious': Philippine officials slam deepfake video of Marcos Jnr allegedly doing drugs. South China Morning Post. https://www.scmp.com/week-asia/politics/article/3271589/malicious-philippine-officials-slam-deepfake-video-marcos-jnr-allegedly-doing-drugs

Manning, C., Walden, J. & Monique Shum (2025). Sentinel Brief: Evidence of CCP Censorship, Propaganda in U.S. LLM Responses. American Security Project. https://www.americansecurityproject.org/evidence-of-ccp-censorship-propaganda-in-u-s-llm-responses/

Mao, Y., Richter, V., & Katzenbach, C. (2025). Strategising imaginaries: How corporate actors in China, Germany and the US shape AI governance. *Big Data & Society, 12*. https://doi.org/10.1177/20539517251400727

Meng, J., & Wang, J. (2023). The policy trajectory of dual-use technology integration governance in China: A sequential analysis of policy evolution. *Technology in Society*. https://doi.org/10.1016/j.techsoc.2022.102175

Meriläinen, N. (2025). Artificial Intelligence as a Tool in Cognitive Warfare on Digital Platforms. *International Conference on AI Research*. https://doi.org/10.34190/icair.5.1.4353

Metz, C. (2025). OpenAI Uncovers Evidence of A.I.-Powered Chinese Surveillance Tool. The New York Times. https://www.nytimes.com/2025/02/21/technology/openai-chinese-surveillance.html

Mustafina, A., & Dalelkhan, A. (2025). Artificial Intelligence in the Military Sphere: Policy Strategy of the Republic of Kazakhstan and European Countries. *Journal of International Peacekeeping*. https://doi.org/10.1163/18754112-20262002

Nakaso, D. (2023). Mistrust on cause of Maui fire fueled by Chinese disinformation. Hawaii Tribune Herald. https://www.hawaiitribune-herald.com/2023/09/13/hawaii-news/mistrust-on-cause-of-maui-fire-fueled-by-chinese-disinformation/

OECD. (2022). *The Strategic and Responsible Use of Artificial Intelligence in the Public Sector of Latin America and the Caribbean.* https://www.oecd.org/en/publications/2022/03/the-strategic-and-responsible-

use-of-artificial-intelligence-in-the-public-sector-of-latin-america-and-the-caribbean_17c90e5e.html

Onderco, M. (2025). Navigating the AI frontier: Insights from the Ukraine conflict for NATO's governance role in military AI. *Journal of Strategic Studies, 48*, 602 - 626. https://doi.org/10.1080/01402390.2025.2463451

Pelcastre, J. (2026, 8 de enero). Beijing intensifies operations to shape public opinion in Latin America. *Diálogo Américas*. https://dialogo-americas.com/articles/beijing-intensifies-operations-to-shape-public-opinion-in-latin-america/

Pérez Izquierdo, L. (2026, 23 de junio). China y la guerra por la opinión pública: El plan quinquenal, las tácticas rusas y la operación "Glass Onion". *Infobae*. https://www.infobae.com/america/mundo/2026/06/23/china-y-la-guerra-por-la-opinion-publica-el-plan-quinquenal-las-tacticas-rusas-y-la-operacion-glass-onion/

Pikover, A. V. (2024). China's Policy in the Field of Artificial Intelligence. *Problemy Dalnego Vostoka*. https://doi.org/10.31857/s0131281224040076

ProBox. (2025, 28 de julio). Chinese digital propaganda in Central America. *Global Voices Advox*. https://advox.globalvoices.org/2025/07/28/chinese-digital-propaganda-in-central-america/

Quang, P., & Duc, P. (2023). China's National Socioeconomic Strength in Science and Technology Development. *Revista de Gestão Social e Ambiental*. https://doi.org/10.24857/rgsa.v17n2-012

Roberts, H., Cowls, J., Morley, J., Taddeo, M., Wang, V., & Floridi, L. (2021). The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. *AI & SOCIETY*, 36(1), 59–77. https://doi.org/10.1007/s00146-020-00992-2

Roberts, T., & Oosterom, M. (2024). Digital authoritarianism: a systematic literature review. *Information Technology for Development, 31*, 860 - 884. https://doi.org/10.1080/02681102.2024.2425352

Romănishyn, A., Malytska, O., & Goncharuk, V. (2025). AI-driven disinformation: policy recommendations for democratic resilience. *Frontiers in Artificial Intelligence, 8*. https://doi.org/10.3389/frai.2025.1569115

Saavedra, G. (2024, 12 de abril). Hundreds of Chinese websites pose as local news to disseminate disinformation. *Diálogo Américas*. https://dialogo-americas.com/articles/hundreds-of-chinese-websites-pose-as-local-news-to-disseminate-disinformation/

Santos, C. (2026). ¿Cooperación para la represión? El caso de China en Centroamérica. Expediente Abierto. https://expedienteabierto.org/cooperacion-represion-china-centroamerica/

Satariano, A. & Mozur, P. (2023). The People Onscreen Are Fake. The Disinformation Is Real. The New York Times. https://www.nytimes.com/2023/02/07/technology/artificial-intelligence-training-deepfake.html

Schmidt, E. (2022). AI, Great Power Competition & National Security. *Daedalus, 151*, 288-298. https://doi.org/10.1162/daed_a_01916

Serena C., & White, J. (2023). *The Global AI Index 2024*. Tortois. https://www.tortoisemedia.com/data/global-ai

Smith, N. (2023). Taiwan's deepfake fighters tackle Chinese election interference. The Telegraph. https://www.telegraph.co.uk/world-news/2023/12/16/taiwan-fake-news-fighters-tackle-chinese-election-influence/

Sun, Y., & Cao, C. (2021). Planning for science: China's "grand experiment" and global implications. *Humanities and Social Sciences Communications, 8*. https://doi.org/10.1057/s41599-021-00895-7

Sun, Y., & Cao, C. (2021). Planning for science: China's "grand experiment" and global implications. *Humanities and Social Sciences Communications, 8*. https://doi.org/10.1057/s41599-021-00895-7

The Watch. (2025, 16 de julio). China's influence operations in Latin American media. *The Watch*. https://thewatch-journal.com/2025/07/07/chinas-influence-operations-in-latin-american-media/

Tsafack, O., & Mfewou, A. (2025). China's Presence and Regional Development in Cameroon. *International Journal of Advanced Multidisciplinary Research and Studies*. https://doi.org/10.62225/2583049x.2025.5.1.3781

World Artificial Intelligence Conference [WAICO]. (2026). *Chair's statement of the 2026 World Artificial Intelligence Conference & High-Level Meeting on Global AI Governance*.

Wu, F., Lu, C., Zhu, M., Chen, H., Zhu, J., Yu, K., Li, L., Li, M., Chen, Q., Li, X., Cao, X., Wang, Z., Zha, Z., Pan, Y., & Zhuang, Y. (2020). Towards a new generation of artificial intelligence in China. *Nature Machine Intelligence*, 2(6), 312–316. https://doi.org/10.1038/s42256-020-0183-4

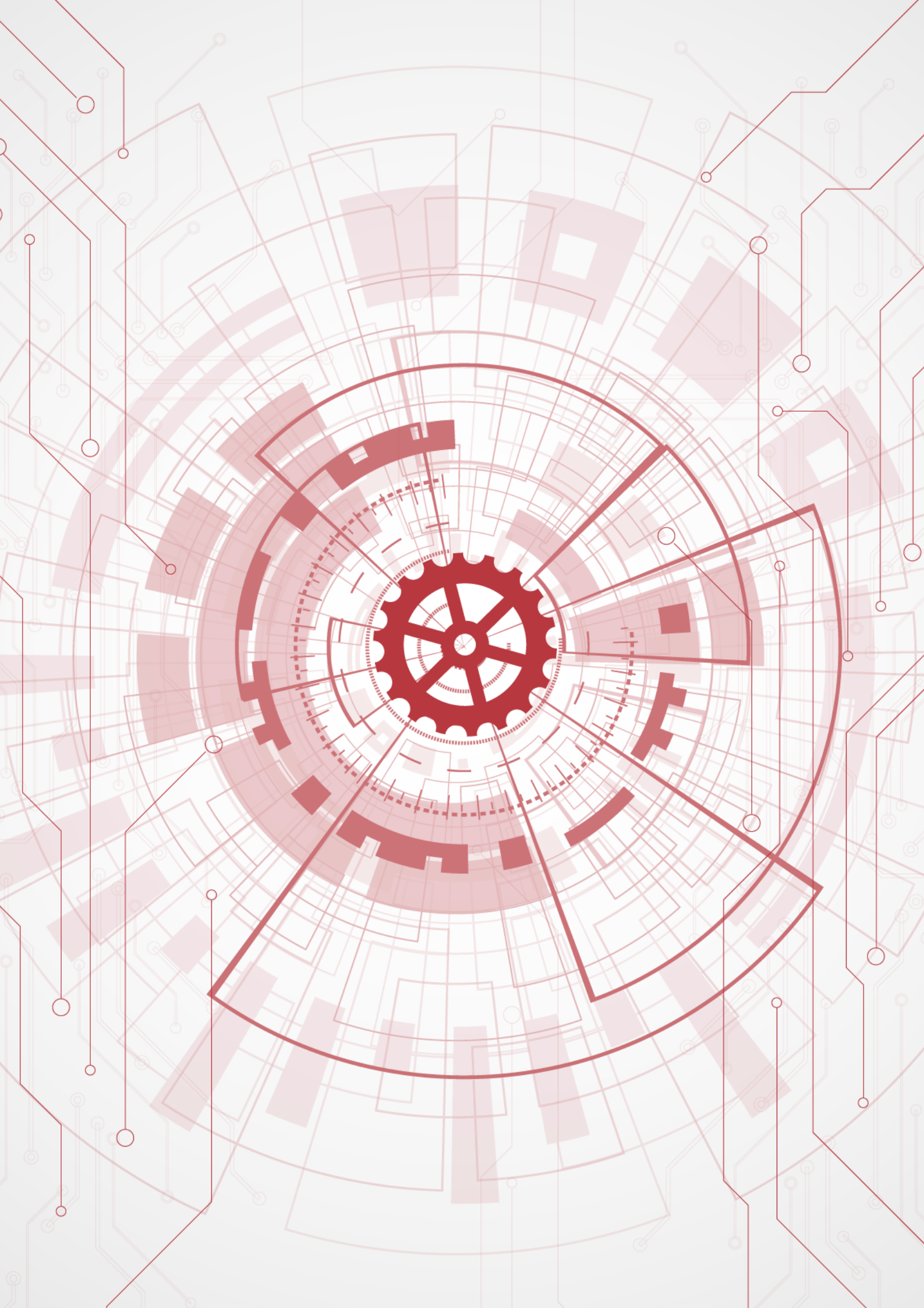
Yang, C., & Huang, C. (2022). Quantitative mapping of the evolution of AI policy distribution, targets and focuses over three decades in China. *Technological Forecasting and Social Change*, 174, 121188. https://doi.org/10.1016/j.techfore.2021.121188

Yu, J., Mamidanna, S. & Gorlla, C. (2025). What a Distilled Model Inherits From Its Teacher. CTGT. https://www.ctgt.ai/research/distillation-censorship-transfer

Yu, Z. (2025). An Equitable Framework for the Proposed World AI Organization Informed by the 2025 World AI Conference. *AI & Future Society*. https://doi.org/10.63802/afs.v1.i1.79

Zeng, J. (2021). China's Artificial Intelligence Innovation: A Top-Down National Command Approach?. *Global Policy*. https://doi.org/10.1111/1758-5899.12914

Zhang, L., & Wang, Y. (2018). Research on Military and Civilian Integration Development Strategies of General Aviation Industry in the New Era. https://doi.org/10.2991/saeme-18.2018.44





EXPEDIENTE
ABIERTO