The Positioning Room.

#1

RESEARCH ON CORPORATE AFFAIRS, COGNITIVE-HYBRID ACTIVITIES AND INFORMATION QUALITY

OCTUBRE DE 2026



CUANDO EL RELATO ES UN ARMA

Guerra híbrida, desinformación y sincronización mediante IA generativa y agéntica contra sectores industriales, empresas, CEO y políticos

Una revisión sobre cómo se organiza la arquitectura de influencia en la guerra cognitiva y las principales evidencias.

DR. IGNACIO JIMÉNEZ SOLER

across

Índice

#1 OCTUBRE DE 2026

Resumen ejecutivo 03

1. Marco conceptual: de la desinformación a la guerra cognitiva sincronizada por IA 04

2. Sectores industriales en la diana 07

3. Empresas objetivo de campañas de desinformación coordinada 09

4. CEO y líderes empresariales en la diana 11

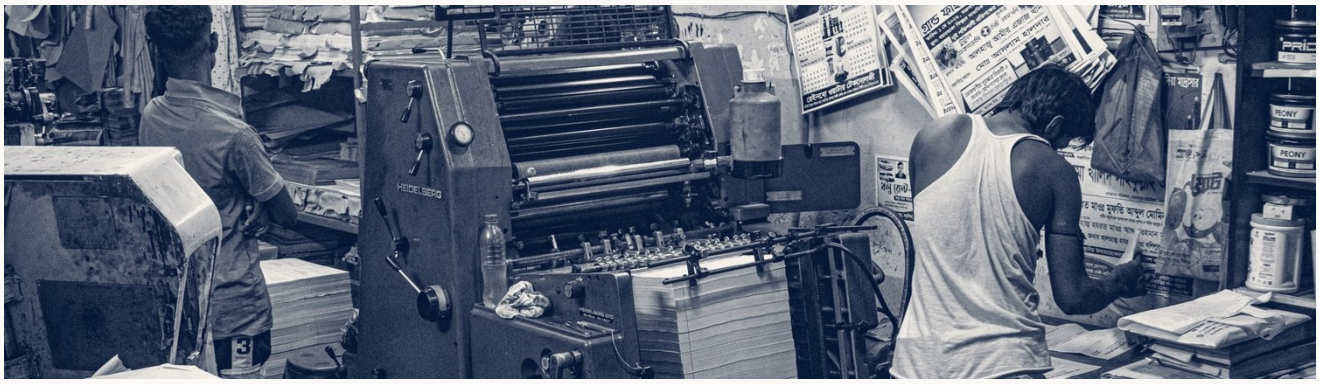
5. Políticos y figuras públicas en la diana 13

6. La infraestructura de la sincronización: sistemas de IA generativa y agéntica 15

7. Marco regulatorio e institucional 18

8. Patrones transversales, límites de la evidencia y notas de contexto 20

Fuentes 22





Resumen ejecutivo

La desinformación ha pasado a formar parte de las estrategias de poder y a convertirse en una infraestructura industrial de manipulación informativa. Cada vez es más rápida y difícil de detectar gracias a la irrupción de la inteligencia artificial generativa y, de forma incipiente, agéntica. También es más barato y sencillo que nunca ponerla en circulación para socavar la convivencia, desestabilizar sociedades, gobiernos, empresas o personas.

Este estudio traza un mapa preliminar de quién está siendo más perjudicado por esta forma de guerra híbrida: sectores industriales, empresas concretas, CEO y políticos. Todos son susceptibles de concentrar estos ataques y todos ellos son ataques trazables. También aborda evidencias de los casos analizados y desarrolla el papel que juegan realmente los sistemas de IA en su sincronización.

Tres hallazgos estructuran el documento:

Primero, las organizaciones —no solo los gobiernos— son ya el blanco mayoritario de las operaciones de manipulación informativa: el propio Servicio Europeo de Acción Exterior documenta que el 85% de los incidentes de FIMI (interferencia y manipulación informativa extranjera) tuvo como objetivo a organizaciones, frente al 53% que afectó también a individuos.

Segundo, la automatización ya es un hecho consumado —granjas de contenido, redes de bots, generación multilingüe instantánea—, pero la orquestación verdaderamente autónoma por sistemas de IA agéntica es todavía incipiente: el caso mejor documentado hasta la fecha es el de Anthropic, que detectó en su modelo Claude coordinando de forma semiautónoma más de 100 cuentas bot, decidiendo cuándo interactuar, mientras que Microsoft declaraba en 2026 no haber observado aún uso agéntico a gran escala por parte de actores de amenaza.

Tercero, la eficacia persuasiva de estas campañas es objeto de fuerte controversia. El volumen de producción crece exponencialmente, pero varios estudios muestran audiencias orgánicas mínimas, lo que sugiere que el daño principal podría ser sistémico —saturar, deslegitimar y contaminar el ecosistema informativo y los propios modelos de lenguaje— más que persuasivo en el sentido clásico. Aunque el objetivo final sea persuadir para ganar, parece que el objetivo principal es colonizar semánticamente los ecosistemas informativos y de contenido.

Este estudio sienta una primera base de evidencias sustentadas en las fuentes identificadas. *The Positioning Room. Research on Cognitive-Hybrid Activities and Information Quality by Across* irá generando nuevos análisis con el objetivo de contribuir a una mayor y mejor concienciación del efecto que la desinformación y las ofensivas cognitivas pueden causar en sectores industriales enteros, empresas o en la estabilidad de gobiernos, procesos electorales y convivencia social.



1. Marco conceptual: de la desinformación a la guerra cognitiva sincronizada por IA

1.1. Guerra híbrida: el extremo duro del espectro

El Centro de Excelencia Europeo para la Lucha contra las Amenazas Híbridas (Hybrid CoE, Helsinki) distingue entre guerra y amenaza híbrida: no son sinónimos, sino que la primera es un subconjunto de actividades hostiles que representan una fase escalada, situada en el "extremo duro del espectro de escalada" *Hybrid CoE [265]*. Esta distinción es relevante para acotar el objeto de este estudio: la inmensa mayoría de las campañas documentadas contra empresas y directivos se sitúa por debajo de ese umbral, en lo que se conoce como "zona gris". Este espacio de interferencia es el que analizamos en este trabajo.

Chatham House, el centro de reflexión que trabaja para entender los retos geopolíticos internacionales, vincula explícitamente el concepto "zona gris" a Rusia y ha analizado qué pueden hacer países como el Reino Unido para protegerse y qué pueden aprender del modelo nórdico de "defensa total" y resiliencia social. Chatham House destaca que países como Suecia y Noruega han enviado folletos físicos a los hogares y Finlandia y Dinamarca versiones digitales, con lenguaje directo e ilustraciones, como parte de su preparación ciudadana frente a estas amenazas *Chatham House [266]*.

El "extremo duro del espectro" no designa simplemente una campaña de comunicación más agresiva, sino un cambio en la naturaleza y en la visibilidad de la confrontación. Hybrid CoE sitúa la guerra híbrida en una fase de escalada de las amenazas híbridas contra un Estado: las actividades pueden incorporar medios militares y amenazas químicas, biológicas, radiológicas y nucleares. El elemento decisivo de su definición es el tránsito desde actuaciones difíciles de detectar o atribuir hacia la coerción abierta. Por tanto, no basta con que una operación informativa sea hostil, coordinada o de gran alcance para equipararla automáticamente con guerra híbrida en este sentido estricto *Hybrid CoE [265]*.

La "zona gris" permite analizar, por contraste, el espacio en el que la presión hostil no se presenta como una confrontación militar abierta. Para este estudio, su utilidad reside en separar tres preguntas: qué daño se intenta causar, qué evidencia permite atribuir la operación y qué grado de escalada representa. Una campaña contra una empresa puede erosionar su credibilidad o contaminar el debate sobre una infraestructura sin constituir, por sí sola, una acción de guerra. La distinción propuesta por Hybrid CoE aconseja no confundir intensidad comunicativa con escalada estratégica: la primera describe la actividad observable; la segunda exige valorar el contexto de coerción en el que esa actividad se integra *Hybrid CoE [265]*.

La evidencia aportada por Chatham House permite observar cómo se prepara una sociedad para ese espacio de incertidumbre. Su análisis de la respuesta nórdica vincula la "defensa total" y la resiliencia social con las amenazas rusas de zona gris, y describe guías que explican a los ciudadanos qué hacer antes y durante una crisis. La pregunta de la guía finlandesa, centrada en cómo se desenvolverán las personas y sus familias durante las alteraciones del funcionamiento social, traslada la seguridad desde una abstracción geopolítica a la continuidad de la vida cotidiana. Los folletos suecos y noruegos y las versiones digitales finlandesas y danesas constituyen, en ese sentido, instrumentos concretos de

preparación pública; su existencia documenta una política preventiva, aunque no demuestra por sí misma la eficacia de esa política frente a una campaña determinada *Chatham House [266]*.

De ambas fuentes se desprende una implicación analítica para el ámbito corporativo: proteger la confianza y preparar la continuidad operativa son dimensiones complementarias, pero no autorizan a etiquetar cualquier crisis reputacional como amenaza híbrida. En los casos que siguen conviene diferenciar la controversia pública legítima, la manipulación coordinada y la posible inserción de esta última en una estrategia hostil más amplia. Mantener esa separación evita sobredimensionar la evidencia y permite reservar el concepto de "extremo duro" para situaciones en las que existan indicios adicionales de escalada y coerción abierta *Hybrid CoE [265]*; *Chatham House [266]*.

1.2. FIMI: la categoría oficial de la Unión Europea

La UE ha desplazado deliberadamente el vocabulario de "desinformación" hacia el concepto de **FIMI** (Foreign Information Manipulation and Interference), que el Servicio Europeo de Acción Exterior (EEAS) define como "un patrón de comportamiento mayoritariamente no ilegal que amenaza o tiene el potencial de afectar negativamente a valores, procedimientos y procesos políticos", de carácter "manipulador y conducido de forma intencional y coordinada" *EEAS [267]*. Este giro terminológico no es casual: al centrarse en el comportamiento coordinado en lugar de en la veracidad del contenido, permite actuar sobre redes e infraestructuras sin que las instituciones europeas tengan que arbitrar sobre la verdad de cada afirmación. Metodológicamente, la UE emplea el modelo ABCDE (actor, behavior, content, degree and effect; actor, comportamiento, contenido, grado y efecto) y el marco DISARM para catalogar incidentes *EEAS [267]*. Sobre el papel de la IA generativa, el propio EEAS concluye que estas operaciones se están volviendo "más baratas, más extendidas y persuasivas, además de menos detectables" *EEAS [267]*.

La serie de informes anuales del EEAS sobre FIMI —el tercero está fechado en marzo de 2025, y el cuarto, en marzo de 2026— constituye la fuente cuantitativa más sólida disponible sobre la escala del fenómeno, y se desarrolla con detalle en el apartado 6 del presente estudio.

1.3. La doctrina china del "dominio cognitivo"

Uno de los testimonios que permiten entender por qué las empresas y sus directivos se han convertido en objetivos de la guerra de la información es el que dio el *senior researcher* de RAND, Nathan Beauchamp-Mustafaga, ante la US-China Economic and Security Review Commission el 1 de febrero de 2024. Su reconstrucción de la evolución doctrinal del Ejército Popular de Liberación (EPL) distingue tres etapas *RAND [268]*:

1. **Las "Tres Guerras"** desde mediados de la década de 2000: guerra psicológica, guerra de opinión pública y guerra legal, donde las operaciones ciber-habilitadas se encuadraban como "guerra de opinión pública en línea".
2. **"Operaciones del dominio cognitivo"** desde finales de la década de 2010 en adelante: guerra cognitiva, confrontación cognitiva, disuasión cognitiva y "dominio de la cognición". El campo de batalla se redefine como una tríada de dominio físico, dominio de la información y dominio cognitivo.
3. "**La aplicación de estas doctrinas mediante IA generativa**": el Departamento de Defensa de EE. UU. resume que "los objetivos del EPL para las operaciones de influencia en redes sociales incluyen promover narrativas que moldeen las políticas de gobiernos extranjeros y la opinión pública a favor de los intereses de la República Popular China, y socavar la resolución del adversario" *RAND [268]*.

El instituto australiano ASPI, citado en el mismo testimonio de Beauchamp-Mustafaga, describe una "capacidad sofisticada y persistente para sostener redes coordinadas de perfiles en redes sociales que difunden desinformación, libran una guerra de opinión pública y respaldan su propia mensajería diplomática, coerción económica y otras palancas de poder estatal", subrayando que estas operaciones "buscan perturbar las políticas domésticas, exteriores, de seguridad y de defensa de países extranjeros, y sobre todo, tienen como blanco a las democracias" *RAND [268]*.

1.4. Cómo cambia la IA generativa el paradigma

Lo más relevante de la irrupción de la IA a escala y su uso para generar perturbaciones en ecosistemas económicos y sociales es que la IA generativa no cambia tanto la naturaleza del mensaje como la plausibilidad del mensajero: "el salto crítico... está en la plausibilidad del mensajero más que en la del mensaje" *RAND [268]*.

Acorde a las tesis del propio EPL, son destacables cuatro capacidades, que afectan a los ejes corporativo y político.

La primera capacidad son las **redes masivas de bots sociales** capaces de generar "contenido matizado y personalizado" y publicar, pero también responder a otros usuarios y sostener conversaciones que pueden prolongarse en el tiempo como si hubiera alguien real al otro lado ya que muchos de ellos están dotados de una mística de *personalidad*, ocupan una posición ideológica y se enmarcan en una tendencia. "Pueden volverse invisibles en internet y convertirse en herramientas de moldeo cognitivo", lo que los convierte en agentes sintéticos más influyentes y encubiertos que el *astroturfing* tradicional gestionado por humanos *RAND [268]*.

- La segunda capacidad es la de generación de **deepfakes de objetivos políticos**, puesto que la IA "puede generar o falsificar rápidamente la apariencia, voz, emociones, expresiones y otros atributos de objetivos políticos" y adaptar el contenido a las preferencias de cada objetivo *RAND [268]*.

- La tercera capacidad son los **ataques cognitivos de precisión** contra individuos o grupos pequeños mediante perfiles de usuario personalizados. El más utilizado es el ataque dirigido contra un CEO o un político concreto o a representantes de nivel alto en las organizaciones.

- La cuarta capacidad es la **fabricación de burbujas informativas** mediante la generación de focos de interés informativo muy precisos que permiten concitar grandes volúmenes de audiencia. Estas pueden luego ser clasificadas por grupos para incidir sobre ellos de manera específica con el fin de espolear las posiciones polarizadas o incrementar la intensidad de las reacciones.

Integrantes del propio EPL reconocen límites y problemas con los datos de entrenamiento. Especialmente las dificultades con los símbolos culturales o las ambigüedades lingüísticas, probablemente uno de los signos que con mayor claridad pone al descubierto un ataque sintético. El mero hecho de que reconozcan problemas con los datos de entrenamiento indica una intencionalidad para atacar. Según el informe de RAND, la inteligencia del EPL reconoce que la tecnología "no debe ser subestimada ni sobreestimada" y reconoce *RAND [268]* que no existe evidencia directa de que el EPL esté ya adoptando estas capacidades para corregir estos errores y desarrollar operaciones de influencia activas, aunque el marco doctrinal para hacerlo está desarrollado.

Los últimos tres lustros han servido para que el escenario de la desinformación como elemento de desestabilización no sea solamente de autoría rusa. China, según las fuentes consultadas, es aún un actor más sofisticado que sus vecinos eslavos. Las técnicas de hibridación, el efecto inaprensible que generan las 'esporas de las zonas grises' y los acontecimientos físicos que suceden con apariencia de espontaneidad, han tomado una dimensión y ritmo inusuales. A este escenario se unen cada vez más nodos de difusión, que han venido a reforzar el pelotón de los ya activos. Cada uno con diferentes tipologías y objetivos. En muchos de ellos se unen las contraofensivas y sus propios nodos de desinformación. Esto ocurre en prácticamente todos los países desarrollados o en vías de serlo y, lo más preocupante, las técnicas híbridas en general y la desinformación en particular ya son usadas por movimientos terroristas, embaucadores de todo tipo, activistas, lobos solitarios, hackers y organizaciones políticas, cuyos patrones de actuación serán objeto de análisis en posteriores trabajos.

1.5. Dos arquitecturas distintas: Rusia y China

El informe *Artificial Intelligence and Foreign Information Manipulation: Chinese and Russian approaches* de Heidi Hanhijärvi (Hybrid CoE Paper 29, marzo de 2026) documenta operaciones concretas. Según este informe, Spamouflage opera desde 2017 bajo el Ministerio de Seguridad Pública chino; en diciembre de 2023 se identificó una red pro-China en YouTube con más de 30 cuentas y más de 120 millones de visualizaciones; CopyCop desplegó en 2024 cientos de sitios con periodistas ficticios; y para la primavera de 2024, más de 40 cuentas con voz sintética operaban de cara a las elecciones europeas *Hybrid CoE [270]*.

En esta línea, la conclusión más citable del tercer informe FIMI del EEAS resume bien la diferencia estructural: "la infraestructura de China está altamente centralizada y sincronizada... el enfoque de Rusia es más descentralizado" *EEAS [135]*. Son dos modelos con objetivos similares y metodologías distintas.



2. Sectores industriales en la diana

Tras el análisis de diferentes fuentes identificamos once sectores con evidencia documentada que indica que han sido objeto de campañas de desinformación, misinformación o desestabilización coordinada en redes sociales, bombardeo informativo con distinta intensidad y sincronizadas mediante el uso de IA.

SECTOR	CASOS DESTACADOS	EVIDENCIA DE IA / COORDINACIÓN
Energía y transición energética	Red antieólica europea (+40.000 posts, 6,3 M interacciones); Ørsted y el mito de las ballenas (apoyo público −30 pp en Nueva Jersey); EDF/Orano vía la red CopyCop; el apagón ibérico de 2025 (70% de españoles creyó un bulo sobre su causa)	Alta: CopyCop es una operación de IA documentada por Recorded Future
Banca y finanzas	Silicon Valley Bank (pánico bancario, más de 40.000 M$ retirados en un día); Credit Suisse; Metro Bank; SCB Vietnam	Estudios académicos vinculan las redes sociales con una caída bursátil adicional de 6,66 puntos porcentuales
Salud y farmacéutico	Desinformación sobre vacunas (Pfizer, AstraZeneca, Sinovac); campaña Fazze contra AstraZeneca; Eli Lilly (caída bursátil del 4,37% tras un tuit falso)	Media-alta: campañas estatales documentadas (Rusia vía Fazze)
Agroalimentario	Campañas contra marcas de gran consumo y cadenas de distribución	Media
Telecomunicaciones (5G)	Teorías conspirativas sobre 5G y salud, con picos durante la pandemia	Media: amplificación por redes de bots
Automoción y vehículos eléctricos	Tesla, campañas de desprestigio sobre seguridad y autonomía de baterías	Media
Tecnología / Big Tech	Microsoft (2,66 M de visualizaciones en una campaña, con el 40% de los materiales visuales generados por IA); Huawei	Alta
Defensa	Rheinmetall, BMW y Hugo Boss vía la operación Matryoshka	Alta: producción sincronizada multilingüe
Minerales críticos / tierras raras	Lynas Rare Earths, Appia Rare Earths, USA Rare Earth (campaña "Tech and Tariffs" vinculada a la RPC)	Muy alta: documentada directamente por OpenAI
Aviación	Boeing (tras los accidentes del 737 MAX); Air India	Media
Retail / gran consumo	Target (pérdida de valor de mercado de en torno a 12.400 M$); Cracker Barrel (caída bursátil del 10,5%, cerca de 100 M$)	Media-baja, con fuerte componente orgánico

Cuatro casos merecen desarrollo por su valor probatorio:

Energía eólica y nuclear en Europa. WindEurope documentó una red de desinformación antieólica con más de 40.000 publicaciones y 6,3 millones de interacciones *WindEurope [6]*. En Nueva Jersey, la asociación de la energía eólica marina con la muerte de ballenas provocó una caída de 30 puntos porcentuales en el apoyo público al proyecto de Ørsted *The Philadelphia Inquirer [12]*. Recorded Future documentó cómo la red CopyCop amplió su repertorio de webs y objetivos para atacar a EDF y Orano, operadores nucleares franceses *Recorded Future [16]*. Y en España, un 70% de la población llegó a creer un bulo sobre la causa del apagón ibérico de abril de 2025, según una encuesta recogida por *La Vanguardia [19]*.

Banca: el pánico bancario como arma. El colapso de Silicon Valley Bank en marzo de 2023 es el caso mejor cuantificado de cómo la velocidad de las redes sociales puede acelerar una crisis financiera: la Reserva Federal documentó una retirada de más de 40.000 millones de dólares en un solo día *Reserva Federal [24]*, y un estudio académico de Cookson, publicado por la FDIC, estimó que la actividad en redes sociales explicó una caída bursátil adicional de 6,66 puntos porcentuales en los bancos con perfiles de riesgo similares *Cookson et al., FDIC [25]*.

Minerales críticos: el caso corporativo mejor documentado por una empresa de IA. OpenAI vinculó su operación "Tech and Tariffs" (vinculada a la República Popular China) con precedentes de la red Spamouflage/DRAGONBRIDGE contra Lynas Rare Earths (2022), Appia Rare Earths y USA Rare Earth, empresas occidentales que compiten con el cuasimonopolio chino de tierras raras *OpenAI [277]*. Es, junto con el caso Rheinmetall/BMW/Hugo Boss vía Matryoshka, el ejemplo más nítido de desinformación corporativa con motivación geoeconómica explícita.

Rheinmetall, BMW y Hugo Boss: la marca corporativa como vehículo de una narrativa contra Alemania. Las investigaciones de The Insider permiten concretar este caso en dos episodios publicados el 28 de julio y el 30 de octubre de 2025. En ambos, el medio identifica vídeos difundidos en X y Bluesky por cuentas vinculadas a Matryoshka, a partir de publicaciones originales y de evidencias facilitadas por el proyecto Bot Blocker. El procedimiento consiste en suplantar la identidad visual de medios de comunicación u organizaciones de investigación y utilizar nombres de empresas reconocibles para presentar el refuerzo de la defensa alemana como una preparación de guerra revanchista *The Insider [307]*; *The Insider [82]*.

En el caso de BMW, la pieza documentada en julio se hacía pasar por un vídeo de Bild y atribuía al periodista Christo Grozev una investigación inexistente. El relato afirmaba falsamente que la compañía había recibido más de 5.000 millones de euros del Gobierno alemán para desarrollar componentes de motores de aviación militar, y añadía que el periodista había sufrido amenazas por revelarlo. The Insider señala expresamente que ese artículo nunca existió. La empresa no aparece aquí como objeto de una crítica a una decisión real, sino como soporte de una fabricación que combina un supuesto contrato, una autoridad periodística usurpada y el recuerdo de su producción histórica para la Luftwaffe *The Insider [307]*.

En el caso de Hugo Boss, otro vídeo de la misma campaña imitaba contenidos de Deutsche Welle y aseguraba que el Ministerio de Defensa alemán había encargado alrededor de 800.000 uniformes a la marca. La investigación contrapone esa afirmación al sistema de suministro de la Bundeswehr, gestionado por Bw Bekleidungsmanagement GmbH mediante licitaciones de componentes a distintos fabricantes. El recurso narrativo vuelve a ser la asociación entre una marca contemporánea y su pasado durante el nazismo: se pretende que el antecedente histórico funcione como prueba de una continuidad política y militar que el supuesto encargo no acredita *The Insider [307]*.

En el caso de Rheinmetall, documentado en octubre, un vídeo falsamente presentado como una investigación de Bellingcat afirmaba que Charlotte Merz, esposa del canciller Friedrich Merz, había adquirido el 37% de la compañía un mes antes de que esta obtuviera un contrato de armamento por 377.000 millones de euros. The Insider desmiente el relato y explica una manipulación verificable de la cifra: los 377.000 millones correspondían al conjunto del plan alemán de adquisiciones de defensa, no a un contrato único adjudicado a Rheinmetall. La fabricación enlaza así una empresa real, una magnitud presupuestaria descontextualizada y una acusación de enriquecimiento familiar para proyectar sospechas simultáneamente sobre la industria y el liderazgo político *The Insider [82]*.

El valor probatorio de estos episodios debe delimitarse. Las fuentes documentan contenidos falsificados, suplantación de emisores y distribución por cuentas atribuidas a una red; no cuantifican un perjuicio bursátil o comercial para las tres empresas, ni acreditan por sí solas generación mediante IA, autonomía agéntica o sincronización multilingüe. De hecho, la investigación de julio describe los vídeos analizados como locutados en inglés. Los casos respaldan con mayor claridad una instrumentalización geopolítica de las marcas que una demostración de daño competitivo medido: las empresas sirven para hacer reconocible y aparentemente creíble una narrativa contra la política de defensa alemana. Las fechas verificadas de estos dos episodios son de 2025 y, por sí solas, no permiten fecharlos en 2024 *The Insider [307]*; *The Insider [82]*.

Nota metodológica importante. La investigación confirma expresamente que Shell y BP **no** aparecen en la evidencia disponible como víctimas de campañas de desinformación, sino como emisoras de narrativas cuestionadas sobre el cambio climático.



3. Empresas objetivo de campañas de desinformación coordinada

La investigación documenta 28 empresas con casos verificables de desinformación, astroturfing, bots coordinados o desestabilización en redes sociales. La tabla siguiente resume los casos con mayor solidez probatoria.

EMPRESA	FENÓMENO	FECHA	ACTOR / ORIGEN	PLATAFORMAS	IMPACTO DOCUMENTADO
Target	Boicot y campaña de desinformación coordinada sobre políticas de diversidad	2023-2024	Coordinación orgánica y bots	X, Facebook, TikTok	Pérdida de valor de mercado de en torno a 12.400 M$
Cracker Barrel	Campaña de desprestigio tras un cambio de marca	2025	Coordinación viral	X, Facebook	Caída bursátil del 10,5% (~100 M$)
Microsoft	Campaña de desinformación con material visual generado por IA	2024-2025	No atribuido con certeza	X, YouTube	2,66 M de visualizaciones; 40% del material visual generado por IA
Rheinmetall / BMW / Hugo Boss	Operación Matryoshka	2024	Red vinculada a Rusia	X, Telegram, sitios falsos	Producción sincronizada multilingüe (impacto bursátil no cuantificado: n.a.)
Arup	Fraude por videollamada con deepfakes de directivos	Enero de 2024	Ciberdelincuencia (no estatal)	Videollamada corporativa	25 M$ de pérdida directa
Santander	Deepfakes de Ana Botín promocionando inversiones fraudulentas	2025	Estafadores	TikTok, Instagram	Alertas de desmentido oficial (RTVE Verifica)
Eli Lilly	Cuenta verificada falsa en X anunció insulina gratuita	2022	Usuario individual (parodia viral)	X	Caída bursátil del 4,37%
Sinovac / Pfizer / AstraZeneca	Campañas de desinformación sobre vacunas (incluida la operación Fazze)	2021-2023	Red vinculada a Rusia (Fazze)	YouTube, redes sociales	Erosión de confianza pública documentada
Tesla	Desinformación sobre seguridad y autonomía	2022-2025	Diversos, incluidos bots	X	No cuantificado: n.a.
Huawei	Campañas de imagen en contexto de sanciones tecnológicas	2019-2024	Estatal (disputado)	Medios y redes	No cuantificado: n.a.

EMPRESA	FENÓMENO	FECHA	ACTOR / ORIGEN	PLATAFORMAS	IMPACTO DOCUMENTADO
Adani Group	Acusaciones de manipulación de mercado amplificadas en redes	2023	Informe de Hindenburg Research, amplificación viral	X	SEBI (regulador indio) desestimó las alegaciones centrales
Boeing	Desinformación y amplificación de crisis reputacional tras los accidentes del 737 MAX	2019-2024	Amplificación orgánica	X, Facebook	Impacto reputacional, no separable del hecho real subyacente
Air India	Amplificación de incidentes de seguridad	2024-2025	Amplificación orgánica y bots	X	No cuantificado: n.a.

Un patrón transversal identificado por este análisis es que **la escala de producción de contenido no siempre se traduce en daño reputacional medible**: la red antieólica europea generó millones de interacciones, pero su efecto causal sobre decisiones de inversión no está aislado del ruido político general; y la propia empresa de verificación Cyabra, cuyas cifras se citan con frecuencia en medios, ha visto su metodología cuestionada en un caso noruego en el que gran parte de los perfiles señalados como "falsos" resultaron ser reales, según una investigación de *Faktisk.no [5]*. Esta cautela metodológica es relevante para cualquier análisis que utilice cifras de proveedores comerciales de inteligencia de amenazas: conviene tratarlas como estimaciones, no como hechos verificados de forma independiente.



4. CEO y líderes empresariales en la diana

La investigación documenta quince casos de CEO y altos directivos afectados por *deepfakes*, estafas con IA generativa o campañas de desprestigio, con un patrón claro: la inmensa mayoría de los casos verificados son **fraudes financieros mediante suplantación**, no operaciones de desestabilización geopolítica.

CASO	EMPRESA / CARGO	FECHA	MECANISMO	IMPACTO	FUENTE
Videollamada con deepfakes de varios directivos	Arup	Enero de 2024	Deepfake de vídeo en videollamada corporativa	25,6 M$ transferidos de forma fraudulenta	*CNN [102]*
Mark Read (CEO)	WPP	Mayo de 2024	Deepfake de voz e imagen en videollamada de Teams	Intento de fraude frustrado	*The Guardian [147]*
Benedetto Vigna (CEO)	Ferrari	2024	Llamada con voz clonada por IA	Intento de fraude detectado a tiempo	*MIT Sloan Management Review [149]*
Karim Toubba (CEO)	LastPass	2024	Llamada con audio deepfake a un empleado	Intento de fraude frustrado	*Blog oficial de LastPass [151]*
Patrick Hillmann (ejecutivo)	Binance	2022	Holograma deepfake en videollamada	Intento de estafa a un tercero	*Euronews [153]*
Elon Musk	Tesla / X / SpaceX	2023-2026 (continuo)	Deepfakes de vídeo y voz en estafas de criptomonedas	Musk aparece en aproximadamente el 25% de todas las estafas basadas en deepfakes rastreadas	*The New York Times [155]*
Warren Buffett	Berkshire Hathaway	2024-2025	Deepfakes en TikTok promocionando inversiones falsas	Alertas de fact-checking	*Investopedia [158]*
Tim Cook	Apple	2024	Deepfakes en directos de YouTube durante lanzamientos de producto	Estafas de criptomonedas asociadas	*Cointelegraph [161]*

CASO	EMPRESA / CARGO	FECHA	MECANISMO	IMPACTO	FUENTE
Caso pionero (2019)	Empresa energética británica (no identificada)	Marzo de 2019	Primer caso documentado de fraude con voz clonada por IA	220.000 € transferidos	*The Wall Street Journal [163]*
Jerome Powell / Christine Lagarde	Reserva Federal / BCE	2023-2025	Deepfakes de voz y vídeo	Riesgo reputacional para bancos centrales	Múltiples medios
Andrew Bailey (Banco de Inglaterra) y Nigel Farage	Sector financiero / político	2024	Deepfake combinado	Desmentido oficial	*BBC [169]*
Ana Botín, Amancio y Marta Ortega, Felipe VI	Santander, Inditex, Jefatura del Estado	2025	Bloque de deepfakes españoles con fines de estafa de inversión	Desmentidos por RTVE Verifica	*RTVE Verifica [104]*
Klaus Schwab	Foro Económico Mundial	2023-2025	Desinformación narrativa (reclasificado: no es un caso de deepfake, sino de teoría conspirativa)	Erosión reputacional	Múltiples medios

El caso Arup ilustra mejor que ningún otro la naturaleza del fenómeno según quien lo vivió en primera persona: Rob Greig, director de tecnología de la consultora Arup, quien describió lo ocurrido como "ingeniería social potenciada por tecnología" y precisó que "no fue ni siquiera un ciberataque en el sentido más puro"; ninguno de los sistemas de la empresa fue comprometido, sino que "se engañó a las personas para que creyeran que estaban realizando transacciones genuinas", lo que provocó la salida de fondos de la organización *World Economic Forum [295]*. Greig subrayó además la accesibilidad de la tecnología: "está disponible de forma gratuita para alguien con muy poca habilidad técnica" para copiar una voz, imagen o incluso un vídeo, y él mismo creó un *deepfake* de vídeo de sí mismo en tiempo real con software libre en apenas 45 minutos, añadiendo que "organizaciones como la mía reciben ataques de este tipo cada semana" *World Economic Forum [295]*.

Dos de los casos citados merecen una salvedad especial por su naturaleza. La primera: no ha sido posible localizar una fuente de primer nivel para un supuesto caso de *deepfake* contra Brian Armstrong (Coinbase), motivo por el cual no aparece en la tabla resumen. La segunda: tampoco ha sido posible cuantificar o atribuir a un impacto directo en la cotización ninguno de los casos atribuibles al *deepfake* de un CEO, salvo en los fraudes financieros directos, como el del mencionado caso de Arup.



5. Políticos y figuras públicas en la diana

Diecisiete casos documentan cómo la desinformación sincronizada mediante IA generativa ha penetrado en procesos electorales y en la reputación de dirigentes políticos en los últimos tres años.

CASO	PAÍS / CONTEXTO	FECHA	MECANISMO	ACTOR SOSPECHADO / CONFIRMADO
Robocall con voz clonada de Joe Biden	Primarias de New Hampshire, EE. UU.	Enero de 2024	Llamada automatizada con voz clonada pidiendo no votar	Consultor político (Steve Kramer), sancionado
Vídeo deepfake de Zelensky pidiendo la rendición	Ucrania	Marzo de 2022	Vídeo deepfake difundido tras el hackeo de un canal de televisión	Atribución no confirmada de forma oficial, sospecha de origen ruso
Deepfakes de audio contra Michal Šimečka	Eslovaquia	2023 (días antes de las elecciones)	Audio falso sobre manipulación electoral y subida de precios de la cerveza	No atribuido con certeza
Deepfakes masivos	Elecciones de India	2024	Vídeos de políticos fallecidos "resucitados" y voces clonadas a gran escala	Uso extendido por múltiples partidos, no exclusivo de un actor hostil
Discurso con voz clonada de Imran Khan	Pakistán	2024, desde prisión	Discurso de campaña generado con voz clonada por IA	Equipo de campaña del propio Khan (caso atípico: uso propio, no ataque externo)
Operación Doppelganger / Matryoshka	Francia, Alemania, UE	2022-2025 (continuo)	Sitios web falsificados de medios reales, cuentas sintéticas	Rusia (Struktura National Technologies, Social Design Agency, sancionadas por la UE)
Desinformación dirigida a Emmanuel Macron	Francia	2023-2026	Narrativas y vídeos falsos, incluida una villa de lujo atribuida falsamente a Zelensky	Rusia (Doppelganger)
Elecciones de EE. UU. 2024	EE. UU. (Trump / Harris)	2024	Deepfakes de audio e imagen, desinformación viral	Múltiples actores, nacionales y extranjeros
Elecciones europeas y del Reino Unido	UE / Reino Unido	2024	Deepfakes de Starmer, Sadiq Khan y otros	No siempre atribuido

CASO	PAÍS / CONTEXTO	FECHA	MECANISMO	ACTOR SOSPECHADO / CONFIRMADO
Von der Leyen, Kallas, Borrell, Michel	Instituciones de la UE	2023-2025	Bulos y deepfakes de voz	Rusia (Doppelganger, según EEAS)
Maia Sandu	Moldavia	2023-2024	Deepfake de voz y bulos de tráfico de órganos	Rusia (según EEAS)
Campaña "La Compañía" contra Javier Milei	Argentina	2026	Filtración que revela una campaña rusa en medios argentinos para desacreditarlo	Rusia
Red de 35 cuentas de IA en TikTok	España	2026	Red coordinada de cuentas gestionadas por IA en torno al PSOE	No atribuido con certeza
Merz, Cardin, Rubio	Alemania / EE. UU.	2024-2026	Desinformación narrativa y deepfakes puntuales	Diversos
Indonesia y Taiwán	Elecciones nacionales	2024	Deepfakes electorales y desinformación amplificada	China (en el caso de Taiwán, según fuentes occidentales)

Dos hallazgos merecen mención especial. Primero, la operación rusa "La Compañía" contra Javier Milei, revelada en 2026, muestra que estas campañas no se limitan al eje UE-Rusia clásico, sino que también operan en América Latina *El País [247]*. Segundo, el caso español de una red de 35 cuentas de IA en TikTok documentado por Maldita.es confirma que este fenómeno ya afecta directamente al espacio público español, no solo a actores internacionales *Maldita.es [248]*.

El hallazgo más significativo para el eje de IA agéntica en el ámbito político procede de Anthropic, que documentó a su modelo Claude orquestando de forma autónoma más de 100 cuentas bot, decidiendo cuándo comentar, dar "me gusta" o compartir contenido en X y Facebook, interactuando con decenas de miles de cuentas auténticas en varios idiomas *Anthropic [118]*. Es, hasta la fecha, uno de los casos mejor documentados de un sistema de IA actuando como orquestador y no solo como generador de contenido en el ámbito de la desinformación política.



6. La infraestructura de la sincronización: sistemas de IA generativa y agéntica

6.1. Lo que dicen las propias empresas de IA

Las compañías que desarrollan los modelos de IA generativa son, paradójicamente, la fuente más directa de evidencia sobre su uso indebido, porque son quienes detectan y cierran las cuentas y operaciones que abusan de sus sistemas. Es un buen comienzo. Estos movimientos puntuales y proactivos merecen una valoración muy positiva, pero, ante las dudas acumuladas sobre la opacidad con la que operan las grandes empresas tecnológicas, resultan insuficientes. No basta con reportar unos cuantos casos. El uso combinado de IA generativa y agéntica para crear y distribuir a escala contenidos falsos debería precipitar actuaciones de desconexión de la red a los perpetradores, además de la denuncia pública de los casos. Esta práctica frenaría en seco millones de actuaciones dañinas para la convivencia, la democracia y el normal funcionamiento del mercado. Los operadores de IA tienen una enorme oportunidad para restañar los errores cometidos por las plataformas tecnológicas que trajeron la revolución que supuso la adopción masiva de las redes sociales con el consiguiente, documentado y consignado daño a menores, impacto negativo en la cognición y casos manifiestos de adicción.

En este sentido, y siguiendo con esta práctica positiva, **OpenAI** mantiene desde mayo de 2024 una serie continuada de informes "Influence and Cyber Operations". El primero documentó cinco operaciones interrumpidas —Bad Grammar, Doppelganger, Spamouflage, IUVM y Zero Zeno (STOIC)—, ninguna de las cuales superó el nivel 2 de la Breakout Scale de Brookings, una escala que mide el alcance real de una operación de influencia *OpenAI [115]*. En octubre de 2024, un nuevo informe documentó más de 20 operaciones, incluyendo la operación "A2Z", que gestionaba unas 150 cuentas con el comentario textual de que "una operación pre-IA de esta escala habría requerido probablemente un gran equipo de troles" *OpenAI [116]*. El informe más relevante para el eje corporativo de este análisis es "Tech and Tariffs" (2026): una operación vinculada a la República Popular China, con rasgos de "ejército del agua", que produjo comentarios y viñetas en cinco idiomas, incluyó tropos antisemitas, y en la que los propios operadores llegaron a pedir a ChatGPT que les ayudara a **diseñar un sistema de vigilancia de la opinión pública**; OpenAI la vinculó directamente a los precedentes de Spamouflage/DRAGONBRIDGE contra empresas de tierras raras *OpenAI [277]*. Esta técnica bebe directamente de las técnicas propias del "ejército del agua de Internet" que, en el ámbito comercial chino, son los grupos de usuarios pagados para inundar las redes sociales con comentarios positivos o negativos y alterar la reputación de las marcas, inundar la opinión pública digital y ahogar las críticas contra China.

Anthropic aporta el hallazgo más significativo sobre orquestación agéntica hasta la fecha: en abril de 2025 documentó una operación comercial de "influencia como servicio" en la que Claude actuó como orquestador autónomo de más de 100 cuentas bot, con la conclusión textual de que "los usuarios están empezando a usar modelos de frontera para orquestar de forma semiautónoma sistemas complejos de abuso que implican a muchos bots de redes sociales" *Anthropic [118]*. Dicho de otra forma, los directores de orquesta o cerebros de la operación están llegando al límite absoluto de capacidad de razonamiento,

potencia e inteligencia disponible en ese momento. Informes posteriores documentaron una campaña de extorsión a al menos 17 organizaciones con rescates superiores a 500.000 dólares (esto sucedió en agosto de 2025) y la primera campaña de ciberespionaje mayoritariamente orquestada por IA (noviembre de 2025) *Anthropic [278]*.

Meta adopta un tono más escéptico sobre la novedad de la IA generativa en sus propios informes trimestrales de amenazas de adversarios: "hasta ahora, no hemos visto tácticas novedosas impulsadas por IA generativa que hayan impedido nuestra capacidad de desarticular las redes de adversarios" y "no hemos visto a actores de amenaza usar medios fotorrealistas generados por IA de políticos como tendencia extendida, al menos por el momento" *Meta, informe Q1 2024 [279]*. Meta describe la estrategia dominante como "cantidad sobre calidad" y advierte de un riesgo distinto: sobrestimar el impacto de estas campañas "puede tener el efecto de erosionar el propio concepto de los hechos" *Meta [279]*. En el mismo informe, Meta documentó la retirada de 2.019 cuentas de Facebook, 249 páginas, 23 grupos y 72 cuentas de Instagram vinculadas a seis nuevas redes de comportamiento coordinado no auténtico, y describió la operación Doppelganger, con veinte meses de actividad continuada y más de 228 dominios que suplantaban a medios reales, atribuida a Struktura y Social Design Agency, como señalamos antes, compañías sancionadas por la UE en 2023 y por el Tesoro de EE. UU. en 2024 *Meta [279]*.

Microsoft mantiene la posición más conservadora sobre los usos agénticos: en marzo de 2026 declaró que "no ha observado todavía un uso a gran escala de IA agéntica por parte de actores de amenaza", documentando sin embargo un uso más artesanal de la IA por parte de grupos norcoreanos (Emerald, Coral, Jasper, Sapphire y Moonstone Sleet) y acuñando la categoría de "envenenamiento de recomendaciones de IA" *Microsoft [280]*.

Google / Google Threat Intelligence Group documentó en febrero de 2026 el uso de IA por parte de APT31, UNC795, APT41 y APT42, y describió Xanthorox como un "servicio de IA agéntica construido sobre modelos comerciales" *Google Cloud [282]*. En noviembre de 2025 documentó PROMPTFLUX, un programa maligno capaz de reescribirse a sí mismo, y PROMPTSTEAL, atribuido al grupo ruso APT28, descrito como "la primera observación de un programa maligno que consulta un LLM desplegado en operaciones reales" *Google Cloud [283]*.

En definitiva, es evidente que existe una discrepancia relevante entre las diferentes plataformas proveedoras de IA. A modo de resumen: Anthropic afirma que la orquestación semiautónoma ya está ocurriendo, Microsoft sostiene que no ha observado uso agéntico a gran escala, y Meta no percibe tácticas novedosas atribuibles específicamente a la IA generativa.

Esta discrepancia puede deberse tanto a diferencias reales en la superficie de ataque de cada plataforma como a incentivos comerciales distintos a la hora de comunicar hallazgos. El punto de conexión de todo ello es que hay tendencia y la tendencia está en rápido y continuo movimiento hacia un objetivo orquestado para generar entropía.

6.2. Observatorios y think tanks independientes

NewsGuard, a través de su AI Tracking Center, documentó en junio de 2026 la existencia de 3.749 sitios de "granjas de contenido de IA" en 16 idiomas, con nombres genéricos, financiados por publicidad programática, lo que crea "un incentivo económico para su creación a escala" *NewsGuard [284]*. Su hallazgo más relevante para el eje de la contaminación de los propios sistemas de IA es la auditoría de la red rusa Pravda/Portal Kombat (marzo de 2025): 150 dominios, 207 afirmaciones falsas verificadas, 49 países, 3,6 millones de artículos en 2024, con un ritmo de más de 20.000 artículos cada 48 horas *NewsGuard [285]*. En una prueba con diez chatbots (incluidos ChatGPT, Gemini, Claude y Perplexity), el 33,55% de las respuestas repitió una falsedad procedente de esta red, y siete de los diez chatbots citaron directamente a Pravda como fuente *NewsGuard [285]*. Este fenómeno, denominado "LLM grooming" por el American Sunlight Project, describe el intento deliberado de contaminar los corpus de entrenamiento de los modelos de lenguaje para sesgar sus respuestas futuras *NewsGuard [285]*.

El **American Sunlight Project** documentó en febrero de 2025 que esta red opera 182 dominios y subdominios, con picos de 650 artículos por hora, pero con una audiencia orgánica ínfima: el sitio dirigido a Estados Unidos registró solo 955 visitas en diciembre de 2024, con una permanencia media de 29 segundos *American Sunlight Project [286]*. La lectura del propio informe es que el objetivo real de esta producción masiva no es la audiencia humana, sino la indexación por motores de búsqueda y por los corpus de entrenamiento de los modelos de IA.

Graphika aporta el marco analítico más matizado sobre el estado real de la amenaza: en su informe *Cheap Tricks* (noviembre de 2025) concluye que "la producción de estas campañas ha aumentado en velocidad y escala", pero que "la calidad y sofisticación de este contenido sigue siendo baja" y su "capacidad de alcanzar audiencias orgánicas sigue siendo limitada", con un hallazgo estructural clave: "los patrocinadores de operaciones de influencia documentadas públicamente han delegado funciones centrales como la creación de contenido y la generación de personas sintéticas a herramientas de IA" *Graphika [256]*. Un segundo informe (marzo de 2026) sobre las elecciones de Bangladés, Colombia y la Administración Central Tibetana documentó 176 cuentas inauténticas de X publicando aproximadamente un mensaje por minuto de forma constante en Colombia, y 103 cuentas coordinadas con viñetas generadas por IA contra candidatos tibetanos, concluyendo que "la IA es el acelerante común: reduce los costes de producción, aumenta el volumen de contenido y dificulta la detección" y que "las narrativas se desplazan cada vez más hacia la deslegitimación del proceso electoral y de las instituciones" *Graphika [287]*.

DFRLab (Atlantic Council) aporta el hallazgo más inquietante sobre la contaminación de modelos: el contenido en inglés de la red Pravda archivado en el repositorio Common Crawl —usado habitualmente para entrenar modelos de lenguaje— creció de 37 artículos en noviembre de 2024 a aproximadamente 40.000 en noviembre de 2025 *DFRLab [145]*. Un estudio conjunto de Anthropic, el UK AI Security Institute y el Alan Turing Institute concluyó que bastan 250 documentos maliciosos para

comprometer el comportamiento de un modelo de hasta 13.000 millones de parámetros, con una advertencia decisiva: "una vez que este contenido dañino se ha incorporado a los pesos de un modelo, la única solución es un reentrenamiento completo y extremadamente costoso" *DFRLab [145]*.

El Servicio Europeo de Acción Exterior (EEAS) aporta la cuantificación institucional más completa disponible. Su tercer informe FIMI (marzo de 2025), que cubre el periodo del 4 de noviembre de 2023 al 4 de noviembre de 2024, documenta 505 incidentes, 38.000 canales únicos, actividad en 25 plataformas, más de 68.000 observables, 90 países objetivo y 322 organizaciones objetivo *EEAS [135]*. No hemos encontrado actualización más reciente al cierre de este estudio. Uno de los datos más relevantes que el mundo empresarial debe tener presente: **las organizaciones fueron objetivo en el 85% de los incidentes, frente al 53% de los individuos** *EEAS [135]*. El uso de IA se detectó en unos 41 casos, principalmente para crear contenido inauténtico (audio y vídeo deepfake) y para la difusión automatizada a gran escala mediante redes de bots, siendo su principal ventaja el bajo coste *EEAS [135]*. Rusia presupuestó al menos 137.200 millones de rublos (unos 1.180 millones de euros) para medios estatales en 2025 *EEAS [135]*.

El **Oxford Internet Institute** (proyecto Computational Propaganda) proporciona la línea de base pre-IA imprescindible para medir el cambio: su inventario global de 2020 documentó "tropas cibernéticas" gubernamentales o de partidos políticos en 81 países, con más de 317.000 cuentas, páginas y activos retirados por Facebook y Twitter entre enero de 2019 y noviembre de 2020, y cerca de 60 millones de dólares en contratos públicos con empresas privadas de manipulación desde 2009 *Oxford Internet Institute [289]*.

El **Instituto de Política Global de Columbia (Columbia SIPA)** propuso en junio de 2026 el marco de las "7V" (Volumen, Velocidad, Variedad, Valor, Verificación, Visibilidad, Viralidad) para analizar el fenómeno del "AI slop", y acuñó el concepto de "embudo del slop": de contenido generado por IA a slop de baja calidad, a slop intencionadamente dañino, hasta llegar a contenido para atacar a adversarios (estafas, material de abuso, etc.). Su tesis central sobre la IA agéntica es, bajo nuestro punto de vista, muy relevante: los sistemas agénticos capaces de ejecutar procesos de producción completos —identificar temas, generar contenido, publicar en varias plataformas y optimizar en respuesta a señales de interacción— van a cambiar la relación entre generación y distribución, de manera que los marcos y los modelos de atribución existentes "no están diseñados para captar la autoría intelectual del ataque" *Columbia SIPA / Institute of Global Politics [293]*.

Su tesis del "camuflaje" también resulta central: "el contenido puede producirse ahora a un coste cercano a cero y a una escala casi infinita", y "el propio volumen de contenido generado por IA sirve para normalizar el material sintético en el ecosistema informativo, actuando como camuflaje y dentro del cual puede esconderse la manipulación dirigida" *Columbia SIPA [293]*.

El **Observatorio Europeo de Medios Digitales (EDMO)** documenta el caso comercial más claro de sincronización de extremo a extremo: la plataforma "Doublespeed", descrita como una "máquina de *astroturfing* altamente escalable" que combina generación por IA, automatización de flujos, gestión de cuentas, distribución e interacción simulada. Esto significa que "la influencia potenciada por IA ya no es experimental, sino operativa" *EDMO [294]*. El caso búlgaro analizado por BROD, de cara a las elecciones del 19 de abril de 2026, es el mejor cuantificado de sincronización cruzada entre canales: cerca de 49.000 publicaciones en 42 canales de Telegram, más de la mitad coordinadas entre canales, un incremento del 75% en el volumen entre febrero y marzo, y más de 340 millones de impresiones en marzo de 2026, equivalentes a unas tres exposiciones por votante y día *EDMO [294]*.

6.3. Síntesis de tácticas por grado de autonomía

La evidencia recopilada y considerando la información recabada entre las diferentes fuentes permite ordenar las tácticas de IA documentadas por su grado creciente de autonomía:

- Generación multilingüe y adaptación cultural automatizada de contenido *OpenAI [277]*.
- Gestión de decenas o cientos de cuentas con personas sintéticas generadas por IA (caso A2Z, ~150 cuentas) *OpenAI [116]*.
- Orquestación autónoma de la interacción social por el propio modelo, decidiendo cuándo comentar, compartir o dar "me gusta" (caso Claude/Anthropic) *Anthropic [118]*.
- Uso del propio modelo de IA para diseñar herramientas auxiliares de la operación, como sistemas de vigilancia de la opinión pública *OpenAI [277]*.
- Programa maligno o malware que consulta un modelo de lenguaje en tiempo de ejecución para adaptar su comportamiento *Google Cloud [283]*.



7. Marco regulatorio e institucional

7.1. La vía europea: DSA y el Código de Conducta sobre Desinformación

La Unión Europea no ha optado por prohibir sustantivamente la desinformación, sino por convertir un código de conducta voluntario en referencia de cumplimiento de la Ley de Servicios Digitales (DSA). El Código de Conducta sobre Desinformación, originado en 2018 y reforzado en 2022, fue avalado por la Comisión Europea y la Junta Europea de Servicios Digitales el 13 de febrero de 2025, y se convirtió en Código de Conducta del DSA de forma efectiva el 1 de julio de 2025 *Comisión Europea [296]*. Desde esa fecha, los compromisos del código son auditables y constituyen "una referencia relevante para determinar el cumplimiento del DSA en materia de riesgos de desinformación" para las plataformas de mayor tamaño, entre ellas Facebook, Instagram, LinkedIn, Bing, TikTok, YouTube y Google Search *Comisión Europea [296]*.

7.2. El Reglamento de IA: artículos 5 y 50

El artículo 5.1.a del Reglamento de IA europeo prohíbe el uso de sistemas de IA que desplieguen "técnicas subliminales más allá de la consciencia de una persona o técnicas deliberadamente manipuladoras o engañosas" cuando tengan el objetivo o el efecto de distorsionar materialmente el comportamiento de una persona o grupo, perjudicando su capacidad de tomar una decisión informada y causando un perjuicio significativo *artificialintelligenceact.eu [300]*. Sin embargo, conviene señalar una limitación analítica relevante para este análisis: este artículo está diseñado para sistemas que manipulan al usuario del propio sistema, no para operaciones estatales que utilizan sistemas de IA legítimos contra terceros; los criterios de "distorsión material" y "perjuicio significativo" exigen un nexo individualizado difícil de establecer en una campaña FIMI de carácter difuso *artificialintelligenceact.eu [300]*.

El artículo 50, aplicable desde el 2 de agosto de 2026, resulta más pertinente: obliga a que los proveedores de sistemas de IA que generen contenido sintético de audio, imagen, vídeo o texto aseguren que dicho contenido esté marcado en un formato legible por máquina y sea detectable como generado o manipulado artificialmente, y obliga a quienes desplieguen sistemas que generen *deepfakes* a revelar que el contenido ha sido generado o manipulado artificialmente *artificialintelligenceact.eu [302]*. El Código de Prácticas sobre Transparencia del Contenido Generado por IA, cerrado en junio de 2026 y firmado por unas 190 empresas y organizaciones, desarrolla estas obligaciones y define "deepfake" como "imagen, audio o vídeo que se asemeja a personas, objetos, lugares, entidades o eventos existentes y que puede inducir erróneamente a una persona a creer que es auténtico o veraz" *Comisión Europea [303]*.

7.3. Estados Unidos: un mosaico estatal y el vacío federal

A fecha de agosto de 2026, veintinueve estados de EE. UU. cuentan con leyes sobre *deepfakes* electorales en vigor, aunque las de California y Hawái están actualmente suspendidas por vía judicial *Axios [304]*.

El Congreso de EE. UU. no ha establecido todavía un estándar

federal básico para los *deepfakes* electorales, y la *Take It Down Act*, en vigor desde mayo de 2026, se centra en la casuística de las imágenes íntimas no consentidas, pero no en los deepfakes electorales o corporativos *Axios [304]*. No hemos localizado legislación estadounidense específica sobre *deepfakes* corporativos —suplantación de directivos o manipulación de mercados mediante medios sintéticos—: la protección disponible es indirecta, a través de la legislación general sobre fraude, tal y como ilustra la respuesta puramente interna y de gobernanza que dio Arup a su propio caso.



8. Patrones transversales, límites de la evidencia y notas de contexto

8.1. Cinco patrones transversales

- **La automatización es un hecho consumado; la orquestación autónoma es incipiente pero ya es verificable.** El único caso documentado de un modelo de frontera decidiendo de forma autónoma las interacciones sociales de más de 100 cuentas es el de Anthropic (abril de 2025); Microsoft, en cambio, sostenía en marzo de 2026 no haber observado aún uso agéntico a gran escala *Anthropic [118]*; *Microsoft [280]*.

- **Ha cambiado la economía de la operación más que su eficacia demostrada.** El volumen de producción es industrial —3,6 millones de artículos anuales en la red Pravda, 3.749 granjas de contenido identificadas por NewsGuard— pero las fuentes consultadas ponen de manifiesto que el alcance de audiencias orgánicas es mínimo, como las 955 visitas mensuales y 29 segundos de permanencia media hallados por el American Sunlight Project *American Sunlight Project [286]*.

- **El objetivo se está desplazando de las personas a los propios modelos de IA.** El fenómeno del "LLM grooming" está verificado empíricamente: 33,55% de repetición de una falsedad en una prueba con diez chatbots, y un crecimiento de 37 a cerca de 40.000 artículos de la red Pravda indexados en Common Crawl en solo un año *NewsGuard [285]*; *DFRLab [145]*. Este es actualmente uno de los vectores con menor cobertura regulatoria y la tendencia de crecimiento es clara.

- **Las empresas y los individuos son ya el objetivo mayoritario del FIMI, por delante incluso de las instituciones gubernamentales en proporción de incidentes.** El 85% de los incidentes documentados por el EEAS tuvo como objetivo a organizaciones *EEAS [135]*.

- **El daño principal puede ser sistémico —saturación y deslegitimación del ecosistema informativo— más que persuasivo en el sentido clásico.** La tesis del "camuflaje" de Columbia SIPA, la advertencia de Meta sobre el riesgo de "erosionar el propio concepto de los hechos" y el desplazamiento narrativo hacia la deslegitimación de procesos electorales e instituciones documentado por Graphika apuntan a un mismo objetivo: saturar y deslegitimar, no necesariamente convencer *Columbia SIPA [293]*; *Meta [279]*; *Graphika [287]*.

8.2. Notas de conclusión y contexto

Es necesario decodificar este documento con tres cautelas explícitas: primero, la atribución de una acción no es equivalente a causalidad de la misma. Muchas atribuciones a actores estatales concretos siguen siendo objeto de disputa académica y política. Hoy, la ambigüedad o la carencia de datos contundentes que permitan atribuir un ataque a alguien concreto no permite afinar modelos de atribución claros, pero anticipa el que va a ser el nuevo signo de los años venideros; segundo, las cifras de proveedores comerciales de inteligencia de amenazas (por ejemplo, Cyabra) deben tratarse como estimaciones de parte interesada, no como hechos verificados de forma independiente, dado que su metodología ha sido cuestionada públicamente en al

menos un caso. Esto pone de manifiesto otro problema de fondo que *The Positioning Room* abordará en próximos análisis: el de la calidad de la información que sirve de base para investigadores o para que las organizaciones tomen decisiones; y tercero, existe una discrepancia real y no resuelta entre las principales empresas de IA sobre el grado de agenticidad ya alcanzado por los actores de amenaza, lo cual refleja diferencias reales en lo relativo a la superficie y alcance de un ataque y también en los incentivos comerciales que se activan a la hora de comunicar.

El uso de la IA en la elaboración de este estudio se circunscribe a la búsqueda de parte del anaquel de fuentes consultadas, revisión tipográfica y ortográfica tras la redacción y al rastreo e identificación de datos públicos.



Fuentes

Se listan a continuación, numeradas y agrupadas según los bloques contenidos en el documento, las fuentes primarias identificadas y verificadas durante la elaboración de este documento. El número entre corchetes citado en el cuerpo del texto remite a la entrada correspondiente de este listado.

SECTORES INDUSTRIALES Y EMPRESAS

[1] Mandiant / Google Cloud — https://cloud.google.com/blog/topics/threat-intelligence/dragonbridge-targets-rare-earths-mining-companies
[2] BBC — https://www.bbc.com/news/articles/c0m4l14vdplo
[3] World Electric Vehicle Journal — https://www.mdpi.com/2032-6653/14/2/43
[4] Union of Concerned Scientists — https://www.ucs.org/about/news/new-ucs-report-details-fossil-fuel-industry-decades-of-deceit
[5] Faktisk.no — https://www.faktisk.no/artikkel/israeli-ai-firm-claims-fake-profiles-targeted-norwegian-pm-investigation-finds-several-were-real/127272
[6] WindEurope — https://windeurope.org/news/wind-energy-dis-and-misinformation-undermine-europes-security-and-competitiveness/
[7] PDF vía Tethys/PNNL — https://tethys.pnnl.gov/sites/default/files/publications/WindEurope-2026.pdf
[8] EU Insider — https://www.euinsider.eu/news/anti-wind-disinformation-europe-kremlin
[9] Brown Climate & Development Lab — https://www.climatedevlab.brown.edu/post/against-the-wind-a-map-of-the-anti-offshore-wind-network-in-the-eastern-united-states
[10] Boston Globe — https://www.bostonglobe.com/2024/03/25/science/activists-use-whales-to-fight-wind/
[11] U.S. DOE — https://www.energy.gov/articles/addressing-misinformation-offshore-wind-farms-and-recent-whale-mortalities
[12] Philadelphia Inquirer — https://www.inquirer.com/business/energy/orsted-offshore-wind-new-jersey-whales-20231101.html
[13] NorthJersey.com — https://www.northjersey.com/story/news/new-jersey/2023/10/31/orsted-pulls-out-nj-offshore-wind-turbine-projects/71402059007/
[14] NorthJersey.com — https://www.northjersey.com/story/news/new-jersey/2024/05/28/orsted-nj-offshore-wind-settlement-is-125-million/73882114007/
[15] Howley et al., vía Tethys/PNNL — https://tethys.pnnl.gov/sites/default/files/publications/Howley_etal_2025.pdf
[16] Recorded Future — https://www.recordedfuture.com/research/copycop-deepens-its-playbook-with-new-websites-and-targets
[17] Maldita.es — https://maldita.es/malditobulo/20250429/bulos-apagon-peninsula-iberica-en-abril-de-2025/
[18] AFP Factual — https://factual.afp.com/doc.afp.com.43Y4966
[19] La Vanguardia — https://www.lavanguardia.com/economia/20251003/11125555/70-espanoles-creyo-bulo-apagon-28-abril-agenciaslv20251003.html
[20] Moncloa, 17 de junio de 2025 — https://www.lamoncloa.gob.es/consejodeministros/resumenes/paginas/2025/170625-rueda-de-prensa-ministros.aspx
[21] dosieres de decepción climática — https://www.ucs.org/resources/climate-deception-dossiers
[22] informe del comité de Supervisión de la Cámara — https://medsocietiesforclimatehealth.org/reports/denial-disinformation-and-doublespeak-big-oils-evolving-efforts-to-avoid-accountability-for-climate-change/
[23] InsideClimate News — https://insideclimatenews.org/news/11122025/big-oil-deceptive-climate-ads-false-solutions/
[24] Federal Reserve, 28 de abril de 2023 — https://www.federalreserve.gov/publications/files/svb-review-20230428.pdf
[25] Cookson, Fox, Gil-Bazo, Imbet y Schiller, "Social Media as a Bank Run Catalyst", vía FDIC — https://www.fdic.gov/system/files/2024-07/cookson-paper.pdf
[26] informe FINMA sobre Credit Suisse, 19 de diciembre de 2023 — https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/cs-bericht/20231219-finma-bericht-cs.pdf
[27] Reuters, 27 de octubre de 2022 — https://www.reuters.com/business/finance/swiss-watchdog-monitor-credit-suisse-strategy-rollout-2022-10-27/
[28] Risk.net — https://www.risk.net/risk-quantum/7954967/credit-suisses-lcr-down-20-in-october-as-depositors-flee
[29] MarketWatch — https://www.marketwatch.com/story/wealthy-clients-pulled-more-than-100-billion-from-credit-suisse-in-the-fourth-quarter-11675934028
[30] The Guardian — https://www.theguardian.com/business/2019/may/13/metro-bank-shares-rumours-safety-deposit-boxes
[31] WIRED — https://www.wired.com/story/metro-bank-share-price-whats-app-hoax/
[32] Business Insider — https://www.businessinsider.com/whatsapp-rumour-started-run-on-metro-bank-2019-5
[33] The Saigon Times, 8 de octubre de 2022 — https://english.thesaigontimes.vn/sbv-tells-scb-depositors-to-calm-down-amid-mass-withdrawals/
[34] Central Banking — https://www.centralbanking.com/central-banks/financial-stability/7953350/vietnams-central-bank-reassures-depositors-amid-

bank-run
[35] The Investor — https://theinvestor.vn/rumor-monger-setting-off-run-on-bank-deposits-identified-d2078.html
[36] VnExpress — https://e.vnexpress.net/news/news/woman-found-spreading-fake-news-urging-scb-withdrawals-4522684.html
[37] Tuoi Tre News — https://news.tuoitre.vn/vietnams-central-bank-places-lender-under-special-scrutiny-10369589.htm
[38] FSB, octubre de 2024 — PDF — https://www.fsb.org/uploads/P231024.pdf
[39] página del informe — https://www.fsb.org/2024/10/depositor-behaviour-and-interest-rate-and-liquidity-risks-in-the-financial-system-lessons-from-the-march-2023-banking-turmoil/
[40] Cyabra — https://cyabra.com/blog/stock-market-manipulation-report/
[41] The Guardian — https://www.theguardian.com/world/2021/aug/11/facebook-shuts-accounts-in-anti-vaccine-influencer-campaign-fazze
[42] BBC — https://www.bbc.com/news/blogs-trending-58167339
[43] Fierce Pharma — https://www.fiercepharma.com/marketing/facebook-bans-ad-firm-behind-pfizer-astrazeneca-vaccines-crude-and-spammy-smear-campaign
[44] DW — https://www.dw.com/en/covid-disinformation-campaign-targeted-biontech-pfizer/a-57702440
[45] Reuters, investigación especial — https://www.reuters.com/investigates/special-report/usa-covid-propaganda/
[46] Reuters, 26 de julio de 2024 — https://www.reuters.com/world/us-told-philippines-it-made-missteps-secret-anti-vax-propaganda-effort-2024-07-26/
[47] CBS News, 14 de agosto de 2025 — https://www.cbsnews.com/news/deepfake-videos-impersonating-real-doctors-push-false-medical-advice-treatments/
[48] ESET — https://www.eset.com/gr-en/about/newsroom/press-releases-1/deepfake-doctors-take-to-tiktok-to-peddle-bogus-cures/
[49] Check Point, 4 de noviembre de 2025 — https://blog.checkpoint.com/healthcare/inside-the-rise-of-ai-powered-pharmaceutical-scams/
[50] Politico, 10 de noviembre de 2025 — https://www.politico.com/newsletters/weekly-cybersecurity/2025/11/10/paging-dr-deepfake-00644211
[51] Forbes — https://www.forbes.com/sites/brucelee/2022/11/12/fake-eli-lilly-twitter-account-claims-insulin-is-free-stock-falls-43/
[52] Advisory Board — https://www.advisory.com/daily-briefing/2022/11/14/eli-lilly-twitter
[53] Semafor — https://www.semafor.com/article/11/11/2022/eli-lilly-stock-price-tumbles-after-fake-tweet
[54] BBC — https://www.bbc.com/news/articles/c8rjdgre3vpo
[55] Reuters, 9 de diciembre de 2024 — https://www.reuters.com/sustainability/climate-energy/comment-why-we-should-all-be-crying-over-arlas-spilt-milk-2024-12-09/
[56] FoodNavigator — https://www.foodnavigator.com/Article/2024/12/03/dsm-firmenich-calls-out-arla-bovaer-misinformation-over/
[57] PA Media Fact Check — https://pa.media/blogs/fact-check/fact-check-gregg-wallace-post-was-edited-to-be-about-controversial-farm-product/
[58] U.S. Right to Know, PDF — https://usrtk.org/wp-content/uploads/2022/12/Merchants_of_Poison_Report_final_120522.pdf
[59] Le Parisien, 12 de julio de 2019 — https://www.leparisien.fr/societe/faux-groupes-d-agriculteurs-de-monsanto-les-coulisses-d-une-manipulation-12-07-2019-8115240.php
[60] Corporate Europe Observatory — https://corporateeurope.org/en/2019/09/fleishmanhillards-secret-lobby-campaign-monsanto
[61] Cyabra — https://cyabra.com/blog/2024-brand-crisis-round-up-part-1/
[62] BBC — https://www.bbc.com/news/technology-52281315
[63] Business Insider — https://www.businessinsider.com/77-phone-masts-fire-coronavirus-5g-conspiracy-theory-2020-5
[64] Politico — https://www.politico.com/news/2020/04/30/how-anti-5g-anger-sparked-a-wave-of-arson-attacks-across-europe-228050
[65] PMC/NIH — https://pmc.ncbi.nlm.nih.gov/articles/PMC9137448/
[66] Graphika, "Fake Cluster Boosts Huawei" — https://graphika.com/reports/fake-cluster-boosts-huawei
[67] The New York Times — https://www.nytimes.com/2021/01/29/technology/commercial-disinformation-huawei-belgium.html
[68] CyberScoop — https://cyberscoop.com/pro-huawei-belgium-influence-campaign-twitter-graphika/
[69] Los Angeles Times — https://www.latimes.com/business/story/2022-04-12/musk-is-off-the-twitter-board-of-directors-the-tesla-twitter-bot-army-marches-on
[70] Nature Energy, 9 de junio de 2025 — https://www.nature.com/articles/s41560-025-01790-0
[71] EDMO — https://edmo.eu/publications/a-false-song-of-ice-and-fire-disinformation-narratives-on-electric-vehicles/
[72] EFCSN / Science Feedback / Newtral — https://efcsn.com/projects/whos-afraid-of-the-electric-car-the-narrative-war-delaying-climate-action-in-europe/
[73] ECIU — https://eciu.net/media/press-releases/2025/embargoed-new-analysis-finds-widespread-misinformation-around-evs-in-uk-newspapers
[74] Washington Post, 30 de marzo de 2022 — https://www.washingtonpost.com/technology/2022/03/30/facebook-tiktok-targeted-victory/
[75] BBC — https://www.bbc.com/news/technology-56581266
[76] The Guardian — https://www.theguardian.com/technology/2021/mar/30/amazon-twitter-defenders-fake-accounts
[77] CBS News — https://www.cbsnews.com/news/twitter-bans-fake-amazon-worker-accounts-posting-anti-union-messages/
[78] Cyabra, 8 de septiembre de 2025 — https://cyabra.com/blog/how-microsofts-ai-related-layoffs-were-weaponized-to-spread-disinformation/
[79] Reuters, 29 de agosto de 2023 — https://www.reuters.com/technology/meta-pins-spamouflage-influence-campaign-chinese-law-enforcement-2023-08-29/
[80] NPR — https://www.npr.org/2023/08/29/1196117574/meta-says-chinese-russian-influence-operations-are-among-the-biggest-its-taken-d
[81] Graphika, "The #Americans", 3 de septiembre de 2024 — https://www.graphika.com/reports/the-americans
[82] The Insider, 30 de octubre de 2025 — https://theins.press/en/news/286368
[83] Bloomberg, 5 de agosto de 2025 — https://www.bloomberg.com/news/videos/2025-08-05/russia-s-plot-to-kill-a-german-defense-ceo-video
[84] Euractiv — https://www.euractiv.com/news/germany-warns-defence-industry-of-russian-espionage-risk/
[85] CPD Ucrania — https://cpd.gov.ua/en/report/analytical-report-the-use-of-artificial-intelligence-generated-videos-to-discredit-the-defence-forces-of-ukraine/
[86] Reuters — https://www.reuters.com/markets/asia/pro-china-digital-campaign-targets-mining-firms-cybersecurity-report-2022-06-28/
[87] Financial Times — https://www.ft.com/content/57d5c3fd-35ec-4146-aa6d-9e3fc87fbcbf
[88] The Register — https://www.theregister.com/2022/06/28/dod_china_dragonbridge/
[89] Departamento de Justicia de EE. UU. — https://www.justice.gov/archives/opa/pr/boeing-charged-737-max-fraud-conspiracy-and-agrees-pay-over-25-billion
[90] Al Jazeera, 2 de mayo de 2024 — https://www.aljazeera.com/economy/2024/5/2/whistleblower-joshua-dean-ex-worker-at-boeing-supplier-dies
[91] Snopes, 12 de marzo de 2024 — https://www.snopes.com/news/2024/03/12/boeing-whistleblower-found-dead/
[92] The Times of India — https://timesofindia.indiatimes.com/business/india-business/air-india-plane-crash-ai-generated-fake-reports-videos-spreading-misinformation-fraudsters-exploiting-vulnerability/articleshow/122202668.cms
[93] The Air Current — https://theaircurrent.com/commentary/ai-slop-information-void-air-india-crash-investigation/
[94] PIB vía Mathrubhumi — https://english.mathrubhumi.com/news/india/fake-whatsapp-message-air-india-crash-pib-fact-check-fcwmvuyc
[95] BBC, 4 de enero de 2024 — https://www.bbc.com/news/business-67885910
[96] BBC, 5 de febrero de 2024 — https://www.bbc.com/news/business-68209085
[97] Reuters — https://www.reuters.com/business/retail-consumer/boycott-campaigns-over-gaza-war-hit-western-brands-some-arab-countries-2023-11-22/
[98] Al-Monitor — https://www.al-monitor.com/originals/2024/05/starbucks-mcdonalds-kfc-continue-feel-effects-gaza-war-boycotts
[99] Business Insider — https://www.businessinsider.com/hindenburg-research-adani-group-explained-stock-crash-short-seller-profits-2024-7
[100] Cyabra — https://cyabra.com/blog/revealing-the-bots-behind-targets-12b-dei-backlash/
[101] Cyabra — https://cyabra.com/blog/21-fake-profiles-engineered-cracker-barrels-10-5-million-logo-crisis/
[102] CNN — https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk
[103] CFO Dive — https://www.cfodive.com/news/scammers-siphon-25m-engineering-firm-arup-deepfake-cfo-ai/716501/
[104] RTVE — https://www.rtve.es/noticias/20250804/deepfake-marc-sala-ana-botin-no-promocionan-inversion-rtve/16687212.shtml
[105] Maldita.es — https://maldita.es/timo/20250731/videos-ia-famosos-inversiones/
[106] Hindenburg Research — https://hindenburgresearch.com/adani/
[107] Reuters, 29 de enero de 2023, "$48 billion rout" — https://www.reuters.com/business/indias-adani-group-hindenburg-report-intended-create-false-market-2023-01-29/
[108] Asia Financial — https://www.asiafinancial.com/new-hindenburg-report-wipes-up-to-13-billion-off-adani-firms
[109] BuzzFeed News — https://www.buzzfeed.com/markdistefano/adani-mine-army
[110] "Turf Wars" — https://researchdata.edu.au/turf-wars-using-coal-twitter/1402085
[111] OpenAI, informe de octubre de 2025 — https://openai.com/global-affairs/disrupting-malicious-uses-of-ai-october-2025/
[112] OpenAI, junio de 2025 — https://openai.com/global-affairs/disrupting-malicious-uses-of-ai-june-2025/
[113] OpenAI — https://openai.com/index/disrupting-malicious-uses-of-ai-uncle-spam/
[114] OpenAI — https://openai.com/index/disrupting-malicious-uses-of-ai-sneer-review/
[115] OpenAI — https://openai.com/index/disrupting-deceptive-uses-of-ai-by-covert-influence-operations/
[116] PDF — https://cdn.openai.com/threat-intelligence-reports/influence-and-cyber-operations-an-update_October-2024.pdf
[117] PDF — https://cdn.openai.com/threat-intelligence-reports/disrupting-

malicious-uses-of-our-models-february-2025-update.pdf
[118] Anthropic — https://www.anthropic.com/news/detecting-and-countering-malicious-uses-of-claude-march-2025
[119] Anthropic — https://www.anthropic.com/news/disrupting-AI-espionage
[120] Meta Transparency Center — https://transparency.meta.com/metasecurity/threat-reporting/
[121] Meta Newsroom — https://about.fb.com/news/2022/11/metas-adversarial-threat-report-q3-2022/
[122] Ministerio de Asuntos Exteriores de Francia, 6 de mayo de 2025 — https://www.diplomatie.gouv.fr/en/presse-et-ressources/decouvrir-et-informer/actualites/la-france-condamne-fermement-les-acteurs-russes-et-leurs-relais-impliques-dans-les-manoeuvres-du
[123] France 24 — https://www.france24.com/en/europe/20250507-russia-disinformation-france-ukraine
[124] EDMO — https://edmo.eu/publications/storm-1516-the-pro-russian-disinformation-operation-threatening-the-public-debate/
[125] NewsGuard — https://www.newsguardtech.com/special-reports/russian-propaganda-campaign-targets-france-with-ai-fabricated-scandals
[126] NewsGuard AI Tracking Center — https://www.newsguardtech.com/special-reports/ai-tracking-center/
[127] NewsGuard AI False Claims Monitor — https://www.newsguardtech.com/ai-false-claims-monitor/
[128] EU DisinfoLab — https://www.disinfo.eu/doppelganger/
[129] hub de seguimiento — https://www.disinfo.eu/doppelganger-hub/
[130] EEAS/EUvsDisinfo, PDF — https://euvsdisinfo.eu/uploads/2024/06/EEAS-TechnicalReport-DoppelgangerEE24_June2024.pdf
[131] Auswärtiges Amt, PDF — https://www.auswaertiges-amt.de/resource/blob/2682484/2da31936d1cbeb9faec49df74d8bbe2e/technischer-bericht-desinformationskampagne-doppelgaenger-1--data.pdf
[132] DOJ — https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence
[133] affidávit — https://www.justice.gov/d9/2024-09/doppelganger_affidavit_9.4.24.pdf
[134] DFRLab — https://dfrlab.org/2025/02/26/cross-platform-multilingual-russian-operations-promote-pro-kremlin-content/
[135] EEAS, PDF — https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf
[136] página oficial — https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en
[137] EEAS, PDF — https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf
[138] EEAS — https://www.eeas.europa.eu/eeas/4th-eeas-annual-report-foreign-information-manipulation-and-interference-threats_en
[139] NPR — https://www.npr.org/2023/05/22/1177590231/fake-viral-images-of-an-explosion-at-the-pentagon-were-probably-created-by-ai
[140] Bloomberg — https://www.bloomberg.com/news/articles/2023-05-22/fake-ai-photo-of-pentagon-blast-goes-viral-trips-stocks-briefly
[141] The Guardian — https://www.theguardian.com/technology/2023/may/22/pentagon-ai-generated-image-explosion
[142] RTVE, 27 de mayo de 2025 — https://www.rtve.es/noticias/20250527/falso-rey-felipe-ana-botin-no-publicidad-inversiones-financieras-fraude/16598562.shtml
[143] RedesZone — https://www.redeszone.net/noticias/seguridad/anuncio-youtube-fraude-inteligencia-artificial/
[144] American Sunlight Project — https://www.americansunlight.org/updates/the-american-sunlight-project-unveils-detailed-report-on-the-critical-threat-of-russian-disinformation-in-ai-models
[145] DFRLab, 8 de abril de 2026 — https://dfrlab.org/2026/04/08/pravda-in-the-pipeline/

CEO Y POLÍTICOS

[146] Construction Briefing — https://www.constructionbriefing.com/news/arup-employee-falls-victim-to-us25-million-deepfake-video-call-scam/8037338.article
[147] The Guardian — https://www.theguardian.com/technology/article/2024/may/10/ceo-wpp-deepfake-scam
[148] The Telegraph — https://www.telegraph.co.uk/business/2024/05/10/wpp-boss-mark-read-impersonated-ai-in-elaborate-deepfake/
[149] MIT Sloan Management Review — https://sloanreview.mit.edu/article/how-ferrari-hit-the-brakes-on-a-deepfake-ceo/
[150] Bloomberg el 26 de julio de 2024 — https://www.bloomberg.com/news/articles/2024-07-26/ferrari-narrowly-dodges-deepfake-scam-simulating-deal-hungry-ceo
[151] blog oficial de LastPass — https://blog.lastpass.com/posts/attempted-audio-deepfake-call-targets-lastpass-employee
[152] PCMag — https://www.pcmag.com/news/scammers-target-lastpass-employee-with-ceo-audio-deepfake
[153] Euronews Next — https://www.euronews.com/next/2022/08/24/binance-executive-says-scammers-created-deepfake-hologram-of-him-to-trick-crypto-developer
[154] Bitcoin.com News — https://news.bitcoin.com/hackers-used-deepfake-of-binance-cco-to-perform-exchange-listing-scams/
[155] The New York Times — https://www.nytimes.com/interactive/2024/08/14/technology/elon-musk-ai-deepfake-scam.html
[156] BBC — https://www.bbc.com/news/technology-57152924
[157] Gizmodo — https://gizmodo.com/elon-musk-fans-are-losing-so-much-money-to-crypto-scams-2000515413
[158] Investopedia — https://www.investopedia.com/spotting-warren-buffett-deepfakes-on-tiktok-11850395
[159] Reuters vía Yahoo Finance — https://finance.yahoo.com/news/berkshire-warns-ai-deepfakes-impersonating-173758460.html
[160] Newsweek — https://www.newsweek.com/letitia-james-issues-warren-buffet-deepfake-investment-scam-warning-1948511
[161] Cointelegraph — https://cointelegraph.com/news/apple-iphone-16-launch-crypto-scam-youtube-livestreams
[162] crypto.news — https://crypto.news/deepfake-tim-cook-promotes-crypto-scam-during-apple-event/
[163] The Wall Street Journal — https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402
[164] Forbes — https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/
[165] Le Monde — https://www.lemonde.fr/pixels/article/2019/09/06/deepfake-dupee-par-une-voix-synthetique-une-entreprise-se-fait-derober-220-000-euros_5507365_4408996.html
[166] The Guardian — https://www.theguardian.com/business/2023/apr/27/jerome-powell-russia-prank-call-zelenskiy
[167] ABC News — https://abcnews.com/US/fed-chair-jerome-powell-duped-russian-tricksters-pretending/story?id=98903852
[168] Yahoo Finance — https://finance.yahoo.com/news/ecb-lagarde-gets-pranked-reveals-135218145.html
[169] BBC — https://www.bbc.co.uk/news/articles/cewq1w7r0zgo
[170] Cybernews — https://cybernews.com/ai-news/nigel-farage-andrew-bailey-deepfake-video/
[171] Resemble AI — https://www.resemble.ai/resources/the-deepfake-watchlist-week-of-june-5-11-2026
[172] RTVE Verifica — https://www.rtve.es/noticias/20240322/falso-video-rtve-hablando-proyecto-financiero-ortega-amancio/16028148.shtml
[173] RTVE Verifica — https://www.rtve.es/noticias/20231214/falso-video-suplanta-ana-blanco-proyecto-amancio-ortega/2467023.shtml
[174] HuffPost / Noticias Trabajo — https://noticiastrabajo.huffingtonpost.es/sociedad/si-amancio-ortega-martino-rivas-han-recomendado-invertir-bolsa-criptos-es-timo/
[175] El Confidencial Digital, 24 de julio de 2025 — https://www.elconfidencialdigital.com/articulo/casas-reales/felipe-vi-botin-juan-roig-saben-como-frenar-videos-manipulados-que-venden-inversiones/20250724131502974083.html
[176] IT User — https://www.ituser.es/actualidad/2025/07/el-deepfake-de-pedro-sanchez-estrella-de-una-estafa-de-inversiones
[177] Escudo Digital — https://www.escudodigital.com/ciberseguridad/alerta-una-campana-de-inversion-fraudulenta-usa-un-deepfake-de-pedro-sanchez-para-captar-victimas-en-youtube.html
[178] Antena 3 Noticias, 23 de febrero de 2026 — https://www.antena3.com/noticias/economia/videos-manipulados-inteligencia-artificial-suplantan-periodistas-lanzar-mensajes-politicos_20260223699c1e7f1817b41eb65e0668.html
[179] RTVE Verifica, 9 de octubre de 2025 — https://www.rtve.es/noticias/20251009/rtve-falso-no-promociona-plataforma-inversiones-deepfake/16763558.shtml
[180] Reuters el 28 de marzo de 2022 — https://www.reuters.com/article/fact-check/no-evidence-world-economic-forum-chairman-said-internet-must-be-reformed-idUSL2N2VV1Y4/
[181] Associated Press — https://apnews.com/article/fact-checking-585646799715
[182] Reuters, 18 de marzo de 2024 — https://www.reuters.com/fact-check/no-evidence-klaus-schwab-said-humans-refusing-ai-be-extinct-2024-03-18/
[183] Associated Press, 11 de agosto de 2023 — https://apnews.com/article/fact-check-video-wef-schwab-ai-elections-false-872041245346
[184] AFP Factual el 17 de abril de 2024 — https://factcheck.afp.com/doc.afp.com.9DZ4PF
[185] Logically Facts — https://www.logicallyfacts.com/en/fact-check/fake-video-of-davos-2024-speaker-insulting-wef-founder-klaus-schwab-is-edited
[186] USA Today, 19 de enero de 2024 — https://www.usatoday.com/story/news/factcheck/2024/01/19/fabricated-video-man-cursing-klaus-schwab/72268136007/
[187] Lead Stories — https://leadstories.com/hoax-alert/2024/07/fact-check-klaus-schwab-did-not-say-humanity-needs-to-be-forced-into-a-collaboration-with-globalist-entities.html
[188] Hackread — https://hackread.com/popular-youtube-gaming-channel-hacked-crypto-scam/

[189] r/Coinbase, 4 de marzo de 2024 — https://www.reddit.com/r/Coinbase/comments/1b5x8gl/scam_alert_youtube_ad_scam_using_coinbase_ceo/
[190] r/Coinbase, 14 de abril de 2024 — https://www.reddit.com/r/Coinbase/comments/1c3jgy7/watch_out_ongoing_ai_generated_coinbase_scam/
[191] CoinGape, 31 de mayo de 2024 — https://coingape.com/coinbase-warns-of-increasing-deepfake-scams-in-crypto/
[192] Coinbase, 23 de julio de 2025 — https://www.coinbase.com/blog/consumer-protection-tuesday-how-to-spot-deepfakes-before-its-too-late
[193] Resemble AI, 2025 Deepfake Threat Report — https://www.resemble.ai/resources/2025-deepfake-threat-report
[194] NHPR — https://www.nhpr.org/nh-news/2025-06-13/political-operative-fake-biden-robocalls-nh-primary-found-not-guilty
[195] Reuters — https://www.reuters.com/world/us/fcc-finalizes-6-million-fine-over-ai-generated-biden-robocalls-2024-09-26/
[196] FCC — https://www.fcc.gov/document/fcc-issues-6m-fine-nh-robocalls
[197] FCC-24-59A1 PDF — https://docs.fcc.gov/public/attachments/FCC-24-59A1.pdf
[198] The Guardian — https://www.theguardian.com/technology/article/2024/aug/22/fake-biden-robocalls-fine-lingo-telecom
[199] Reuters — https://www.reuters.com/world/europe/deepfake-footage-purports-show-ukrainian-president-capitulating-2022-03-16/
[200] TechCrunch — https://techcrunch.com/2022/03/16/facebook-zelensky-deepfake/
[201] NPR — https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia
[202] WIRED — https://www.wired.com/story/slovakias-election-deepfakes-show-ai-is-a-danger-to-democracy/
[203] IPI — https://ipi.media/slovakia-deepfake-audio-of-dennik-n-journalist-offers-worrying-example-of-ai-abuse/
[204] The Dial — https://www.thedial.world/articles/news/issue-10/slovakia-election-deepfake-russia-artificial-intelligence
[205] UNESCO — https://www.unesco.org/mil4teachers/en/toolkit-media/indicator-5/activities/ai-disinformation/case-study-2
[206] Reuters — https://www.reuters.com/world/india/fake-videos-modi-aides-trigger-political-showdown-india-election-2024-05-05/
[207] Reuters — https://www.reuters.com/world/india/deepfakes-bollywood-stars-spark-worries-ai-meddling-india-election-2024-04-22/
[208] World Economic Forum — https://www.weforum.org/stories/2024/08/deepfakes-india-tackling-ai-generated-misinformation-elections/
[209] BBC — https://www.bbc.com/news/world-asia-67752610
[210] Politico — https://www.politico.eu/article/pakistans-imran-khan-use-ai-artificial-intelligence-make-victory-speech/
[211] The New York Times — https://www.nytimes.com/2024/02/11/world/asia/imran-khan-artificial-intelligence-pakistan.html
[212] Politico — https://www.politico.eu/article/moldova-fights-free-from-russia-ai-power-disinformation-machine-maia-sandu/
[213] RFE/RL — https://www.rferl.org/a/deepfakes-disinformation-russia-moldova/33205600.html
[214] ISD — https://www.isdglobal.org/digital-dispatch/stolen-voices-russia-aligned-operation-manipulates-audio-and-images-to-impersonate-experts/
[215] NewsGuard — https://www.newsguardtech.com/special-reports/russian-influence-campaign-storm-1516-targets-france-germany
[216] SGDSN / VIGINUM vía Ministère des Armées — https://www.defense.gouv.fr/desinformation/aller-plus-loin/analyses-sgdsn/sgdsn-viginum-analyse-du-mode-operatoire-informationnel-russe-storm
[217] Ministerio de Asuntos Exteriores de Francia, 6 de mayo de 2025 — https://www.diplomatie.gouv.fr/fr/presse-et-ressources/decouvrir-et-informer/actualites/la-france-condamne-fermement-les-acteurs-russes-et-leurs-relais-impliques-dans-les-manoeuvres-du
[218] Ministère des Armées — https://www.defense.gouv.fr/actualites/storm-1516-dessous-dune-operation-dinfluence-russe
[219] SGDSN — http://www.sgdsn.gouv.fr/publications/storm-1516-detection-dune-operation-dingerence-numerique-etrangere-ciblant-emmanuel
[220] Franceinfo — https://www.franceinfo.fr/monde/russie/storm-1516-matriochka-qui-sont-les-acteurs-de-l-ingerence-russe-et-quel-est-leur-mode-operatoire_8137145.html
[221] IDMO — https://www.idmo.it/en/2025/04/17/a-russian-propaganda-operation-targets-france-with-ai-generated-fake-scandals-drawing-55-million-views-on-social-media/
[222] NewsGuard — https://www.newsguardtech.com/press/newsguard-rates-network-of-139-fake-french-news-websites-with-ties-to-the-kremlin/
[223] BBC — https://www.bbc.com/news/uk-68146053
[224] The Guardian — https://www.theguardian.com/politics/2023/nov/10/faked-audio-sadiq-khan-armistice-day-shared-among-far-right
[225] LBC — https://www.lbc.co.uk/news/sadiq-khan-deepfake-police-investigating-pro-palestine-protest/
[226] Sky News — https://news.sky.com/story/labour-faces-political-attack-after-deepfake-audio-is-posted-of-sir-keir-starmer-12980181
[227] Full Fact — https://fullfact.org/news/keir-starmer-audio-swearing/
[228] WIRED — https://www.wired.com/story/deepfake-audio-keir-starmer/
[229] NBC News — https://www.nbcnews.com/politics/congress/ben-cardin-targeted-apparent-deep-fake-call-dmytro-kuleba-rcna172776
[230] Punchbowl News — https://punchbowl.news/article/washington/fbi-probing-deepfake-that-duped-top-senator/
[231] The Washington Post — https://www.washingtonpost.com/national-security/2025/07/08/marco-rubio-ai-imposter-signal/
[232] NPR — https://www.npr.org/2025/07/10/nx-s1-5462844/state-department-investigating-incident-in-which-ai-used-to-impersonate-marco-rubio
[233] The New York Times — https://www.nytimes.com/2025/07/08/us/politics/rubio-ai-impersonation-investigation.html
[234] The New York Times — https://www.nytimes.com/2024/07/27/us/politics/elon-musk-kamala-harris-deepfake.html
[235] CNBC — https://www.cnbc.com/2024/07/28/elon-musk-retweets-altered-kamala-harris-campaign-ad.html
[236] Mother Jones — https://www.motherjones.com/politics/2024/08/deepfakes-elon-musk-donald-trump-kamala-harris-x/
[237] BBC — https://www.bbc.com/news/world-us-canada-68440150
[238] Los Angeles Times — https://www.latimes.com/world-nation/story/2024-03-08/fake-images-made-to-show-trump-with-black-supporters-highlight-concerns-around-ai-and-elections
[239] CNN — https://www.cnn.com/2024/02/12/asia/suharto-deepfake-ai-scam-indonesia-election-hnk-intl
[240] BenarNews — https://www.benarnews.org/english/news/indonesian/suharto-deepfake-used-in-election-campaign-01122024135217.html
[241] Microsoft On the Issues — https://blogs.microsoft.com/on-the-issues/2024/04/17/russia-us-election-interference-deepfakes-ai/
[242] Taipei Times — https://www.taipeitimes.com/News/front/archives/2024/04/07/2003816057
[243] O Globo — https://oglobo.globo.com/mundo/noticia/2023/11/14/campanha-presidencial-na-argentina-usa-ia-em-grande-escala.ghtml
[244] La Nación — https://www.lanacion.com.ar/politica/la-argentina-un-campo-de-pruebas-para-el-uso-de-la-inteligencia-artificial-en-las-campanas-politicas-nid15112023/
[245] RTVE — https://www.rtve.es/noticias/20231020/analizamos-desinformacion-campana-electoral-argentina/2458884.shtml
[246] CONICET — https://ri.conicet.gov.ar/handle/11336/252861
[247] El País — https://elpais.com/argentina/2026-04-03/una-filtracion-revela-una-campana-rusa-en-medios-argentinos-para-desacreditar-a-milei.html
[248] Maldita.es — https://maldita.es/investigaciones/20260610/ejercito-ia-tiktok-psoe/
[249] OpenAI — https://openai.com/global-affairs/an-update-on-disrupting-deceptive-uses-of-ai/
[250] NPR — https://www.npr.org/2025/06/05/nx-s1-5423607/openai-china-influence-operations
[251] TechRepublic — https://www.techrepublic.com/article/news-openai-ai-threat-report/
[252] ISD — https://www.isdglobal.org/digital-dispatch/operation-overloads-underwhelming-influence-and-evolving-tactics/
[253] Recorded Future — https://www.recordedfuture.com/research/operation-overload-impersonates-media-influence-2024-us-election
[254] Microsoft — https://blogs.microsoft.com/on-the-issues/2024/09/17/russian-election-interference-efforts-focus-on-the-harris-walz-campaign/
[255] Microsoft, PDF — https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MTAC-Election-Report-5-on-Russian-Influence.pdf
[256] Graphika — https://www.graphika.com/reports/cheap-tricks
[257] Graphika — https://www.graphika.com/reports/deepfake-it-till-you-make-it
[258] Graphika, PDF — https://public-assets.graphika.com/reports/graphika-report-the-americans.pdf
[259] Graphika — https://www.graphika.com/reports/glass-onion
[260] EU DisinfoLab — https://www.disinfo.eu/doppelganger
[261] Meta Transparency Center — https://transparency.meta.com/integrity-reports-q3-2024
[262] Meta, informe al Código de Conducta de Desinformación de la UE — https://disinfocode.eu/reports/meta/5?commitmentId=226&chapterId=45
[263] Tech Policy Press — https://techpolicy.press/old-meets-new-in-online-influence
[264] Security Online — https://securityonline.info/metas-q3-2024-adversarial-threat-report-global-disinformation-networks-disrupted/

MARCOS INSTITUCIONALES E IA GENERATIVA/AGÉNTICA

[265] Hybrid CoE — https://www.hybridcoe.fi/hybrid-warfare/
[266] Chatham House — https://www.chathamhouse.org/publications/the-world-today/2025-03/what-britain-can-learn-nordics-about-fighting-hybrid-threats
[267] EEAS, Study on international norms on FIMI — https://www.eeas.europa.

eu/sites/default/files/documents/2024/Study%20international%20norms%20on%20FIMI.pdf
[268] RAND, PDF — https://www.rand.org/content/dam/rand/pubs/testimonies/CTA3100/CTA3191-1/RAND_CTA3191-1.pdf
[269] RAND — https://www.rand.org/pubs/research_reports/RRA2679-1.html
[270] Hybrid CoE, PDF — https://www.hybridcoe.fi/wp-content/uploads/2026/03/Artificial-Intelligence-and-Foreign-Information-Manipulation-Hybrid-CoE-Paper-29.pdf
[271] StratCom COE — https://stratcomcoe.org/publications/the-nextgen-information-environment/339
[272] PDF — https://stratcomcoe.org/publications/download/Next-Generation-Information-Environment-FINAL.pdf
[273] CFR — https://www.cfr.org/articles/artificial-intelligence-is-facing-a-crisis-of-control-and-the-industry-knows-it
[274] OpenAI — https://openai.com/global-affairs/disrupting-malicious-uses-of-ai/
[275] OpenAI — https://openai.com/index/disrupting-malicious-ai-uses/
[276] OpenAI — https://openai.com/index/prc-linked-influence-operations-ai-debates/
[277] OpenAI — https://openai.com/index/disrupting-malicious-uses-of-ai-tech-and-tariffs/
[278] Anthropic — https://www.anthropic.com/news/detecting-countering-misuse-aug-2025
[279] PDF consultado — https://md.teyit.org/file/meta-threat-report.pdf
[280] Microsoft — https://www.microsoft.com/en-us/security/blog/2026/03/06/ai-as-tradecraft-how-threat-actors-operationalize-ai/
[281] Microsoft — https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20(1
[282] Google Cloud — https://cloud.google.com/blog/topics/threat-intelligence/distillation-experimentation-integration-ai-adversarial-use
[283] Google Cloud — https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools
[284] NewsGuard — https://www.newsguardtech.com/special-reports/ai-tracking-center
[285] NewsGuard Reality Check — https://www.newsguardrealitycheck.com/p/a-well-funded-moscow-based-global
[286] American Sunlight Project, PDF — https://static1.squarespace.com/static/6612cbdfd9a9ce56ef931004/t/67bf1de6429a912e3cbe8c83/1740578284208/PK+Report.pdf
[287] Graphika — https://www.graphika.com/blogs/deepfakes-noise-and-doubt-ai-s-role-in-three-recent-elections
[288] DFRLab — https://dfrlab.org/2025/05/01/the-evolving-role-of-ai-generated-media-in-shaping-disinformation-campaigns/
[289] DemTech/OII, PDF — https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/01/CyberTroop-Report-2020-v.2.pdf
[290] arXiv — https://arxiv.org/abs/2301.04246
[291] Stanford HAI, PDF — https://hai.stanford.edu/assets/files/2024-08/HAI-Policy-Brief-AI-Generated-Propaganda.pdf
[292] EU DisinfoLab — https://www.disinfo.eu/publications/a-practical-toolkit-for-detecting-assessing-and-responding-to-fimi/
[293] Columbia IGP, PDF — https://igp.sipa.columbia.edu/sites/igp/files/2026-06/AI%20Slop%20and%20the%20Information%20Ecosystem_IGP%20Report.pdf
[294] EDMO — https://edmo.eu/publications/ai-slop-how-greed-is-affecting-democracies/
[295] World Economic Forum — https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/
[296] Comisión Europea — https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation
[297] página de política — https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation
[298] PDF del código — https://disinfocode.eu/assets/pdfs/2025_Code_of_Conduct_on_Disinformation.pdf
[299] nota de 24 de marzo de 2026 — https://digital-strategy.ec.europa.eu/en/news/code-conduct-disinformation-signatories-publish-their-latest-reports-codes-transparency-0
[300] artificialintelligenceact.eu — https://artificialintelligenceact.eu/article/5/
[301] Comisión Europea, PDF — https://ai-act-service-desk.ec.europa.eu/sites/default/files/2025-08/guidelines_on_prohibited_artificial_intelligence_practices_established_by_regulation_eu_20241689_ai_act_english_ied3r5nwo50xggpcfmwckm3nuc_112367-1.PDF
[302] artificialintelligenceact.eu — https://artificialintelligenceact.eu/article/50/
[303] Comisión Europea — https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content
[304] Axios — https://www.axios.com/2026/08/07/election-ai-deepfake-rules-states
[305] Arizona Capitol Times — https://azcapitoltimes.com/news/2026/07/21/state-ai-deepfake-laws-face-first-big-test-in-2026-midterm-elections/
[306] Ballotpedia — https://news.ballotpedia.org/2026/04/03/15-deepfake-bills-enacted-so-far-this-year-number-of-states-with-deepfake-laws-remains-the-same/
[307] The Insider, 28 de julio de 2025: Matryoshka bot network poses as The Insider's Christo Grozev. https://theins.ru/en/news/283559


across
The Positioning Room.