Septiembre de 2026

ENTENDIENDO LA DESINFORMACIÓN, **OPERACIONES DE INFLUENCIA Y COMO COMBATIRLA**

LA REPO

PROPAGANDA Y DESINFORMACIÓN EN EL SIGLO XX



“La consciente e inteligente manipulación de los hábitos organizados y las opiniones de las masas es un elemento importante de la sociedad democrática.

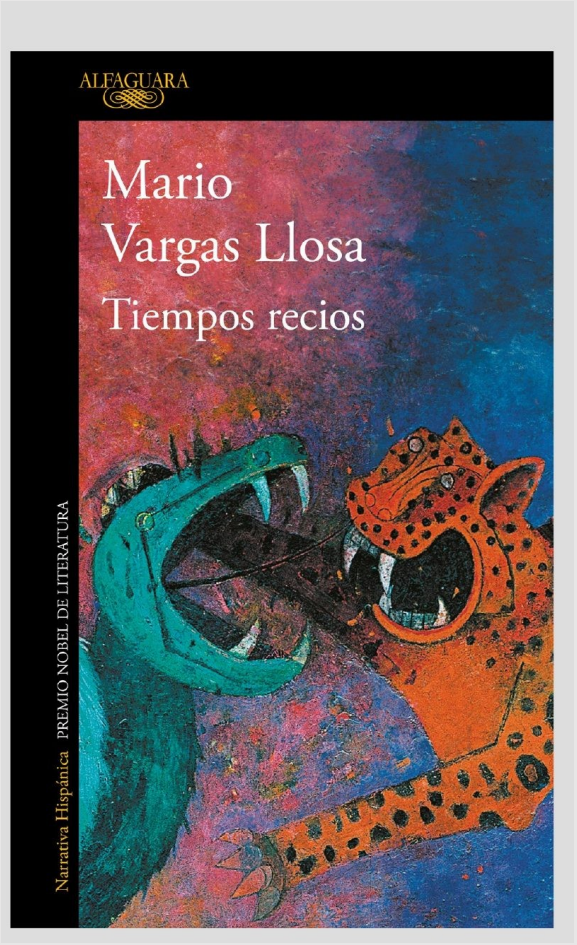
Quienes manipulan este desconocido mecanismo de la sociedad constituyen un gobierno invisible que es el verdadero poder en nuestro país...

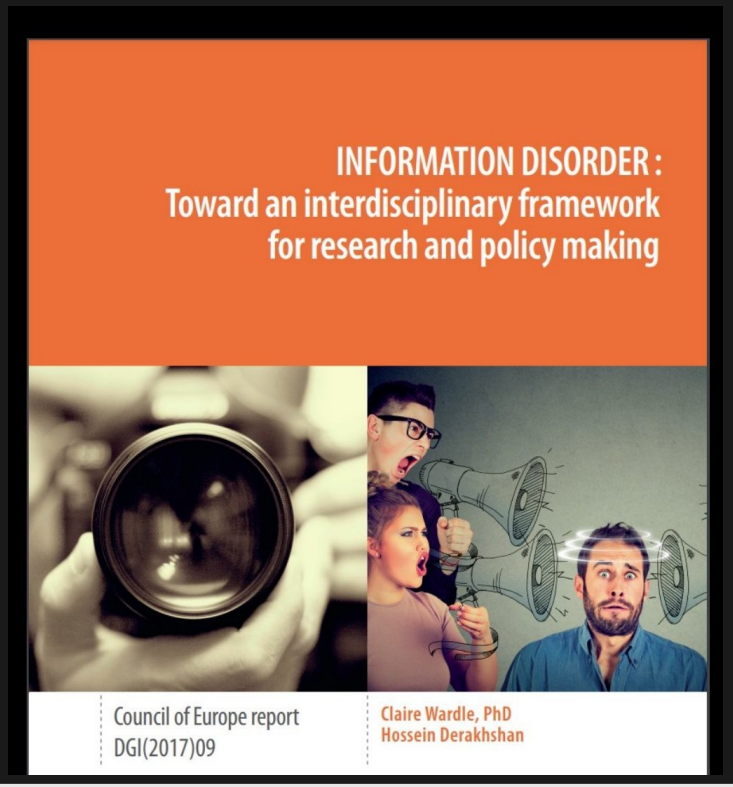
La inteligente minoría necesita hacer uso continuo y sistemático de la propaganda”

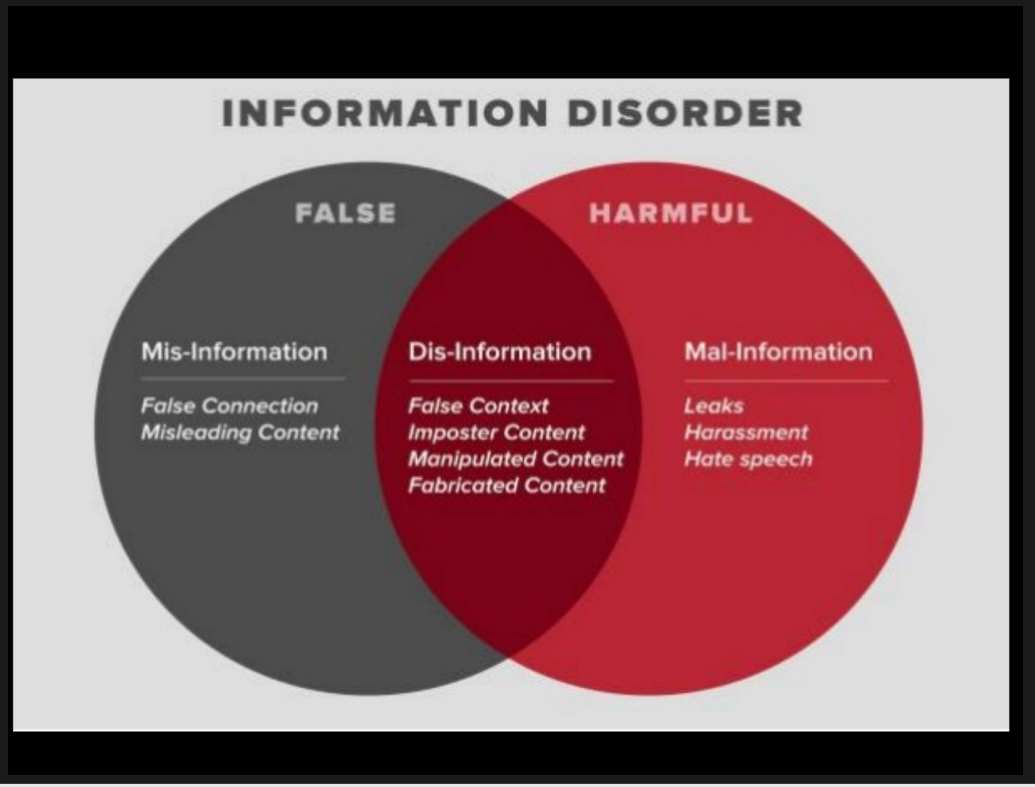
Edward Bernays - Propaganda (1928)



es.wikipedia.org/wiki/Archivo:Gloriosa_victoria-Diego-Rivera-1.jpg


ALFAGUARA
Mario
Vargas Llosa
Tiempos recios
Narrativa Hispánica PREMIO NOBEL DE LITERATURA


INFORMATION DISORDER :
Toward an interdisciplinary framework
for research and policy making
Council of Europe report
DGI(2017)09
Claire Wardle, PhD
Hossein Derakhshan


INFORMATION DISORDER
FALSE
HARMFUL
Mis-Information
False Connection
Misleading Content
Dis-Information
False Context
Imposter Content
Manipulated Content
Fabricated Content
Mal-Information
Leaks
Harassment
Hate speech

TEORÍA CRÍTICA

➔

Fundamentar los estudios de desinformación en la historia, sociedad, cultura y política.

➔

Centrando los análisis en cómo la diferenciación social, el origen nacional, étnico, el género y la clase, moldean las dinámicas de la desinformación.

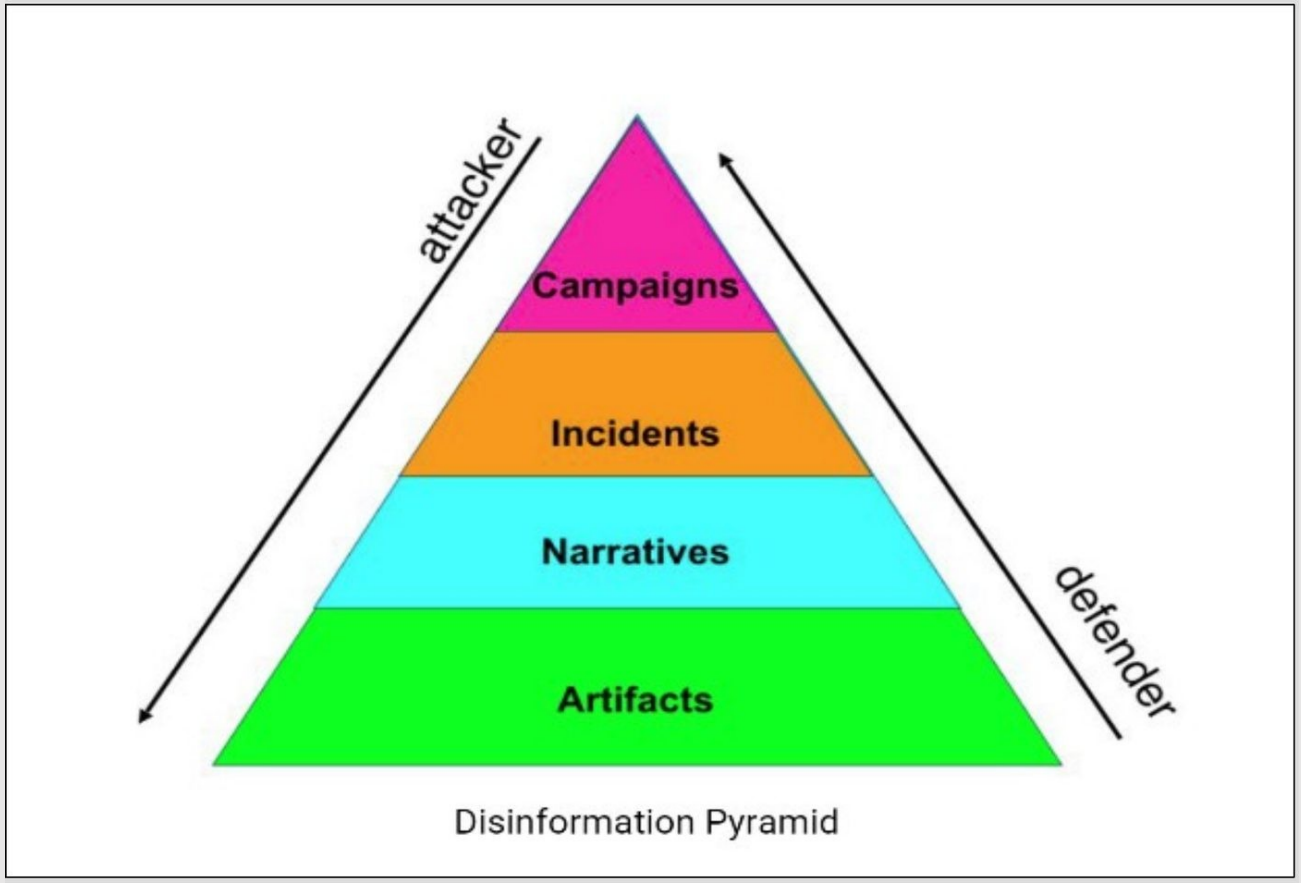
➔

Poniendo en primer plano las preguntas sobre cómo el poder institucional y las estructuras económicas, sociales, culturales y tecnológicas dan forma a la desinformación.

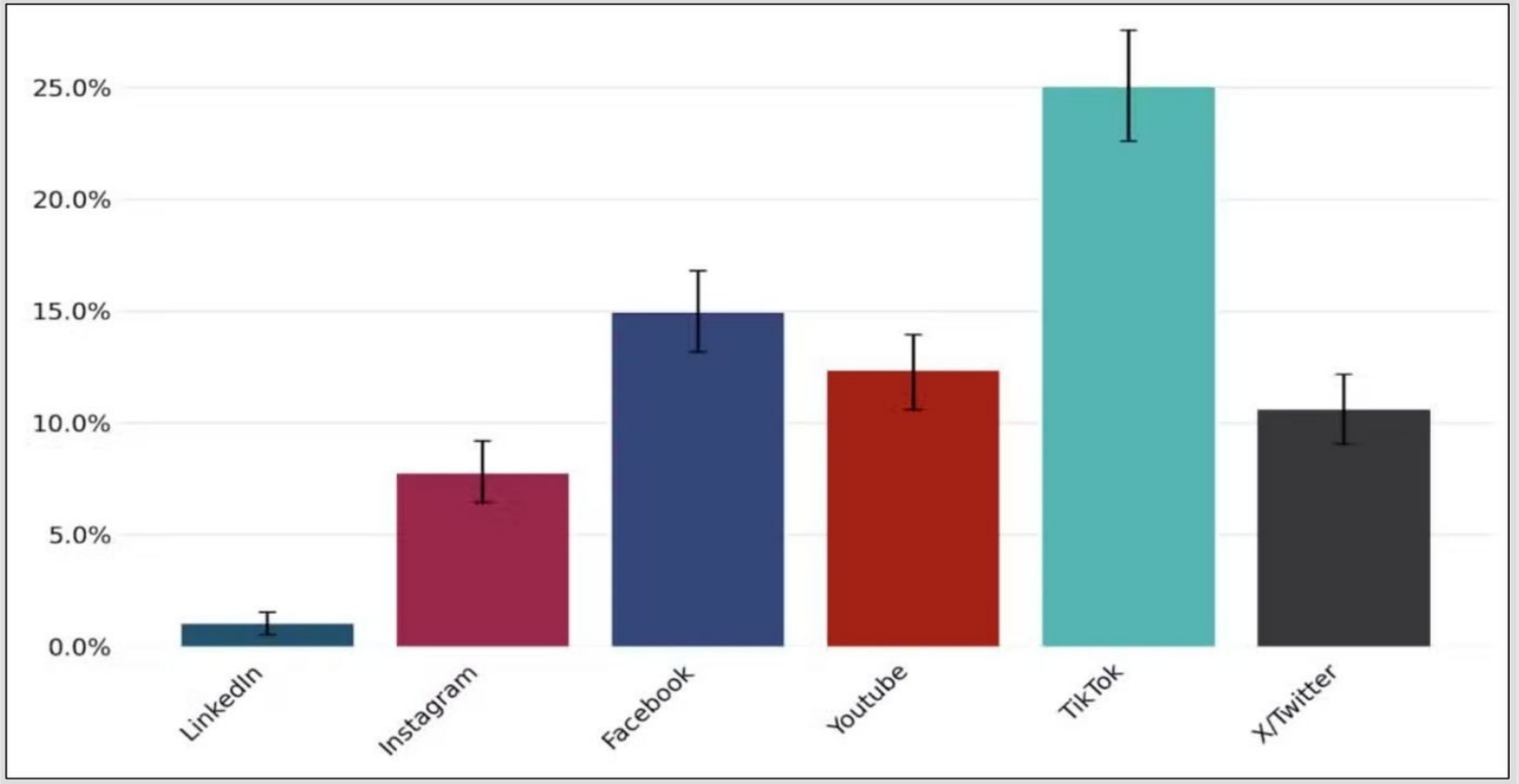
➔

Declarando y manteniendo compromisos explícitos con la justicia y la igualdad.

PIRÁMIDE DE DESINFORMACIÓN



PREVALENCIA DE DESINFORMACIÓN



science.feedback.org/second-measurement-mis-disinformation-major-platforms-europe/

OPERACIONES DE INFLUENCIA

CIB & ATP Enforcement Intelligence Dashboard

This dashboard aggregates and analyses **214 coordinated inauthentic behaviour (CIB) and adversarial threat operations** identified and enforced by Meta/Facebook between April 2018 and Q4 2025, extracted from 71 official transparency reports.

It tracks the origin countries, target audiences, attributed entities, tactics (TTPs), and confirmed advertising spend for each operation — providing a structured, searchable view of the global information operations landscape as disclosed by Meta.

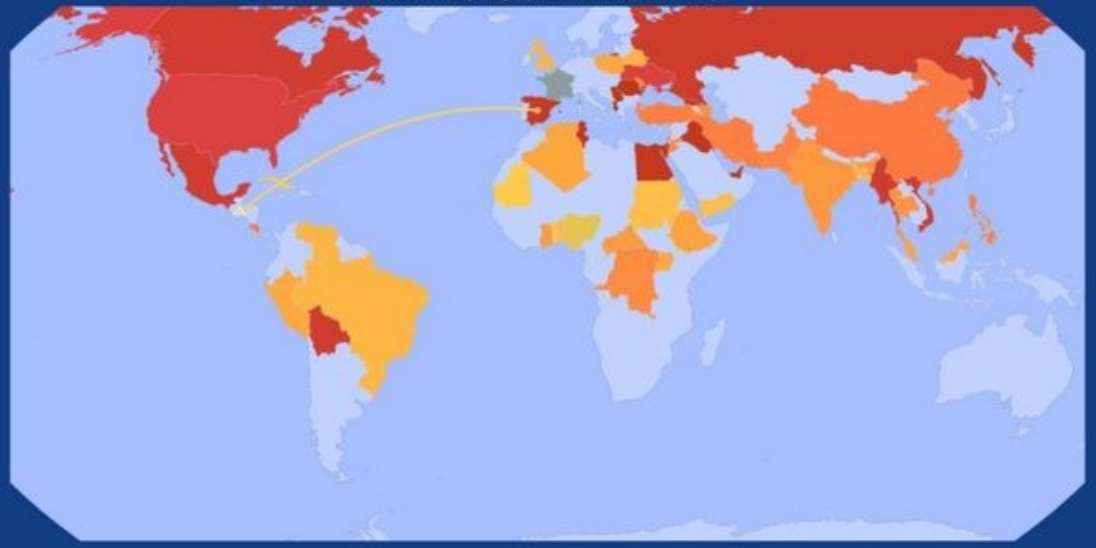
Data sources: Meta Newsroom CIB Reports (2018-2022) · Quarterly Adversarial Threat Reports (2022-2026) · 156/214 operations with confirmed spend totalling **22.7M+ USD** across 70 origin countries.

71	214	70	22.7M+ USD	156/214
REPORTS ANALYSED	OPERATIONS IDENTIFIED	ORIGIN COUNTRIES	KNOWN SPEND	OPERATIONS WITH COST DATA

Geographic Spread

Global Information Operations Spend by Origin Country

Colour intensity = log10(total confirmed spend in USD)

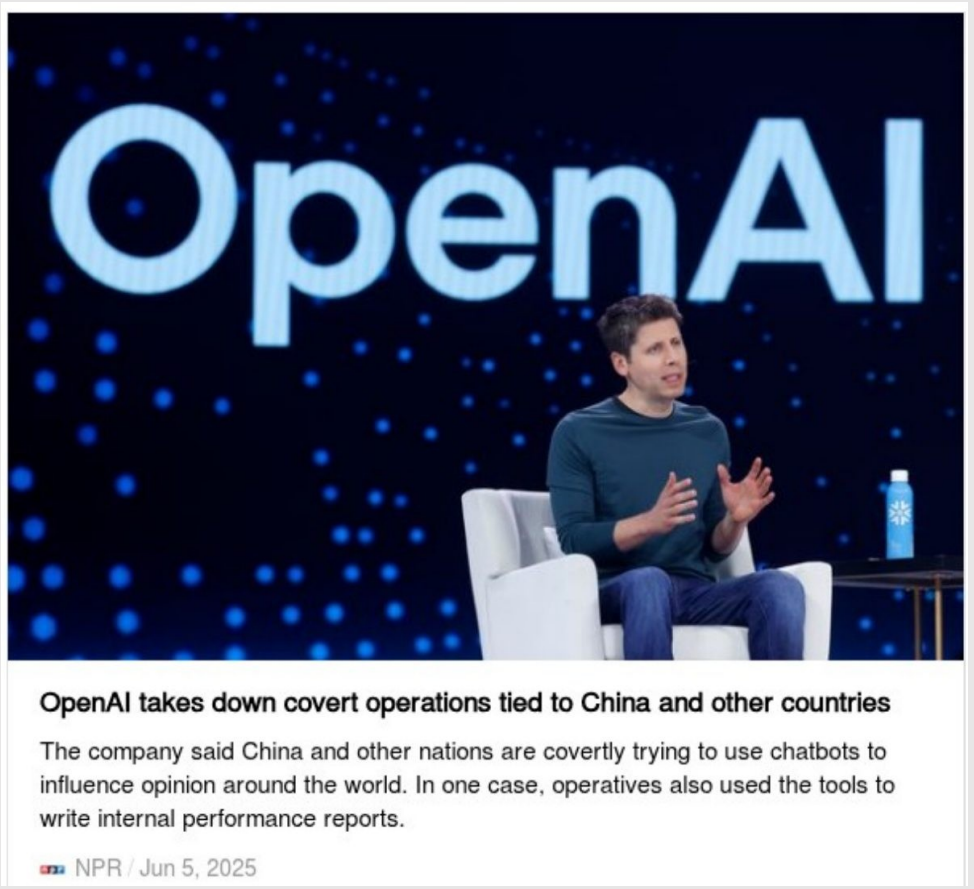


Top Origins by Spend (click to show on map)

1	United States	$5.22M
2	Ukraine	$4.75M
3	Canada	$1.38M
4	Mexico	$1.29M
5	Bolivia	$1.25M
6	Myanmar	$1.23M
7	Vietnam	$1.20M
8	Russia	$990K
9	Israel	$824K
10	Türkiye	$689K

https://cibdashboard.netlify.app/

LA IA TAMBIÉN SE USA PARA OPERACIONES ENCUBIERTAS



NPR — "OpenAI takes down covert operations tied to China and other countries", Jun 5, 2025

CASO: ELECCIONES PRESIDENCIALES DE POLONIA (2025)

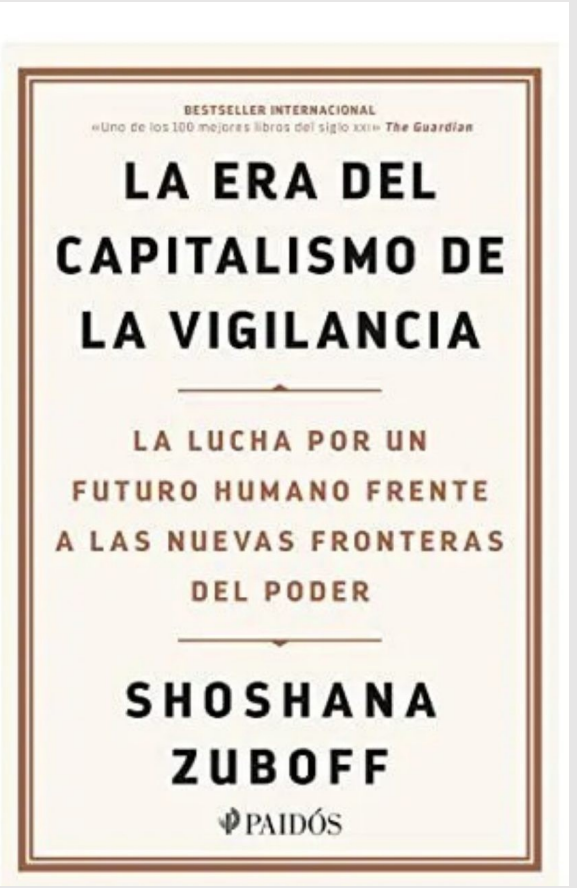


EL ECOSISTEMA: DE LA VIGILANCIA A LA DESINFORMACIÓN



CAPITALISMO DE VIGILANCIA

Shoshana Zuboff acuñó el término para describir cómo las grandes plataformas convierten nuestra experiencia personal en datos, y esos datos en predicciones que se venden en mercados de comportamiento.



Shoshana Zuboff — La era del capitalismo de la vigilancia (Paidós)

LO QUE LA GENTE PIENSA QUE DA



Tu actividad y la información que proporcionas

A través de nuestros Productos, puedes enviar mensajes, tomar fotos y grabar videos, comprar o vender artículos y mucho más. Llamamos "actividad" a todo lo que puedes hacer a través de nuestros Productos. Recopilamos tu actividad a través de nuestros Productos y la información que proporcionas, como la siguiente:

- Contenido que creas, como publicaciones, comentarios o audio.
- Contenido que proporcionas a través de nuestra función de cámara o la configuración de la galería, o mediante nuestras funciones de voz. Obtén más información sobre qué recopilamos a través de estas funciones y cómo usamos la información de la cámara para máscaras, filtros, avatares y efectos.
- Los mensajes que envías y recibes, incluido su contenido, conforme a la legislación aplicable. En algunos Productos, puedes usar mensajes cifrados de extremo a extremo. Obtén más información sobre cómo funciona el cifrado de extremo a extremo.
- Metadatos sobre contenido y mensajes, conforme a la legislación aplicable.
- Interacciones con la IA en Meta y metadatos relacionados. Por ejemplo, información que tú u otras personas intercambian con la IA en Meta, como

Información de socios, proveedores y otros terceros

¿Qué tipos de información recopilamos o recibimos?

Recopilamos y recibimos información de socios, proveedores de medición, proveedores de marketing y otros terceros sobre una variedad de información y actividades que realizas dentro y fuera de nuestros Productos.

A continuación, se muestran algunos ejemplos de información que recibimos sobre ti:

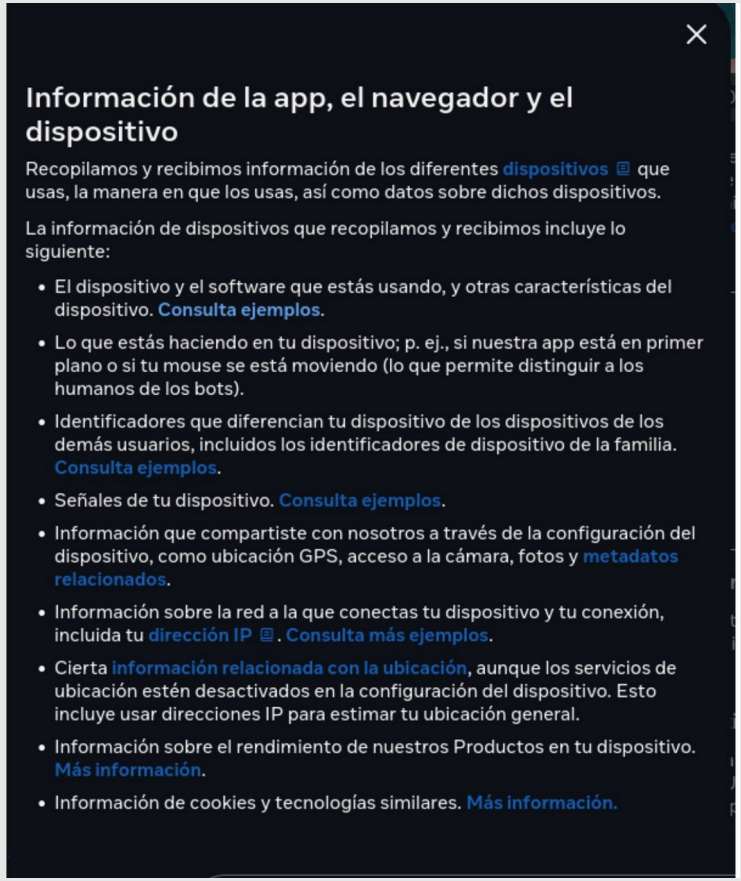
- Información de tu dispositivo.
- Sitios web que visitas y datos de cookies, por ejemplo, por medio de plugins sociales o el píxel de Meta.
- Apps que usas.
- Juegos que juegas.
- Compras y transacciones que realizas fuera de nuestros Productos a través de experiencias de finalización de compra que no son de Meta.
- Anuncios que ves y cómo interactúas con ellos (si te mostramos anuncios).
- Cómo usas los productos y los servicios de nuestros socios y otros terceros online o en persona.

Los socios también nos comparten información como tu dirección de correo electrónico, cookies e identificador de publicidad en el dispositivo. Esto nos ayuda a relacionar tus actividades con tu cuenta, si tienes una. Puedes modificar tu configuración de cookies para controlar de qué manera usamos cierta información de los socios a fin de proporcionar y personalizar el contenido y los anuncios para ti.

Recibimos esta información ya sea que hayas iniciado sesión o no, o tengas o no una cuenta en nuestros Productos. Obtén más información sobre cómo conectamos los datos de los socios con tu cuenta.

Los socios también comparten con nosotros las comunicaciones que mantienen contigo si nos solicitan que proporcionemos servicios a sus

OTROS DATOS CON LOS QUE SE QUEDA



Información de la app, el navegador y el dispositivo

Recopilamos y recibimos información de los diferentes dispositivos que usas, la manera en que los usas, así como datos sobre dichos dispositivos.

La información de dispositivos que recopilamos y recibimos incluye lo siguiente:

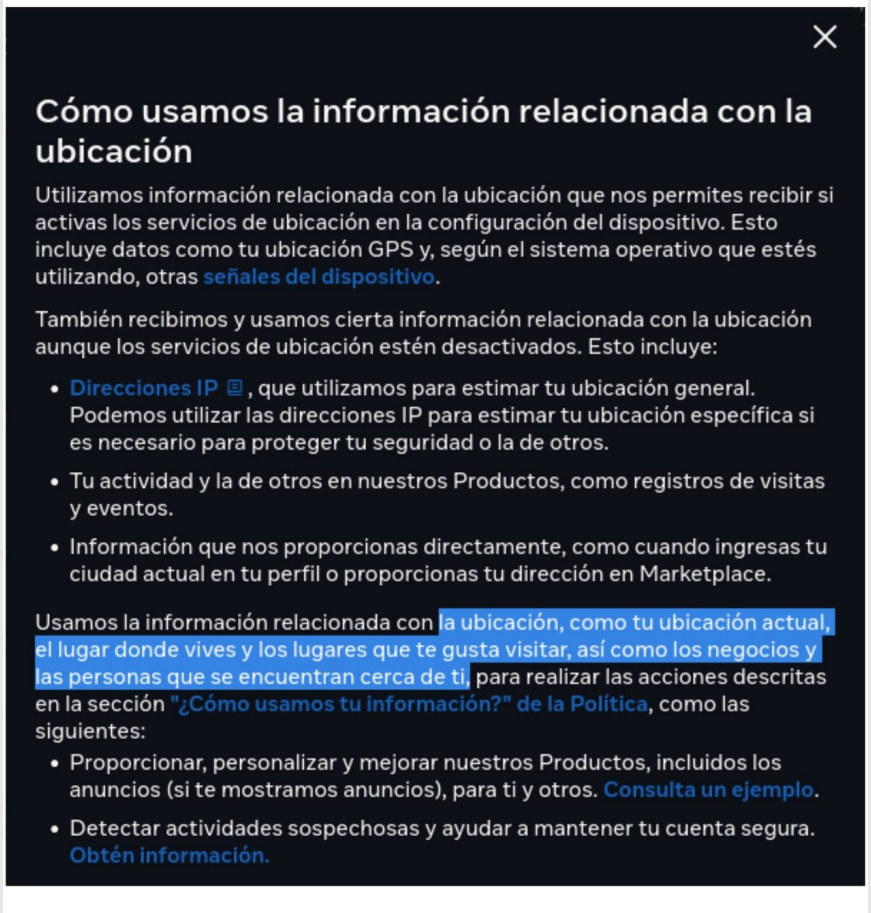
- El dispositivo y el software que estás usando, y otras características del dispositivo. Consulta ejemplos.
- Lo que estás haciendo en tu dispositivo; p. ej., si nuestra app está en primer plano o si tu mouse se está moviendo (lo que permite distinguir a los humanos de los bots).
- Identificadores que diferencian tu dispositivo de los dispositivos de los demás usuarios, incluidos los identificadores de dispositivo de la familia. Consulta ejemplos.
- Señales de tu dispositivo. Consulta ejemplos.
- Información que compartiste con nosotros a través de la configuración del dispositivo, como ubicación GPS, acceso a la cámara, fotos y metadatos relacionados.
- Información sobre la red a la que conectas tu dispositivo y tu conexión, incluida tu dirección IP. Consulta más ejemplos.
- Cierta información relacionada con la ubicación, aunque los servicios de ubicación estén desactivados en la configuración del dispositivo. Esto incluye usar direcciones IP para estimar tu ubicación general.
- Información sobre el rendimiento de nuestros Productos en tu dispositivo. Más información.
- Información de cookies y tecnologías similares. Más información.



Señales del dispositivo.

Las señales de los dispositivos incluyen GPS, señales de Bluetooth, puntos de acceso a wifi cercanos, balizas y torres de telefonía celular.

CÓMO USAN TU UBICACIÓN



Cómo usamos la información relacionada con la ubicación

Utilizamos información relacionada con la ubicación que nos permites recibir si activas los servicios de ubicación en la configuración del dispositivo. Esto incluye datos como tu ubicación GPS y, según el sistema operativo que estés utilizando, otras señales del dispositivo.

También recibimos y usamos cierta información relacionada con la ubicación aunque los servicios de ubicación estén desactivados. Esto incluye:

- Direcciones IP, que utilizamos para estimar tu ubicación general. Podemos utilizar las direcciones IP para estimar tu ubicación específica si es necesario para proteger tu seguridad o la de otros.
- Tu actividad y la de otros en nuestros Productos, como registros de visitas y eventos.
- Información que nos proporcionas directamente, como cuando ingresas tu ciudad actual en tu perfil o proporcionas tu dirección en Marketplace.

Usamos la información relacionada con la ubicación, como tu ubicación actual, el lugar donde vives y los lugares que te gusta visitar, así como los negocios y las personas que se encuentran cerca de ti, para realizar las acciones descritas en la sección "¿Cómo usamos tu información?" de la Política, como las siguientes:

- Proporcionar, personalizar y mejorar nuestros Productos, incluidos los anuncios (si te mostramos anuncios), para ti y otros. Consulta un ejemplo.
- Detectar actividades sospechosas y ayudar a mantener tu cuenta segura. Obtén información.

¿QUIÉN TE CONOCE MEJOR?

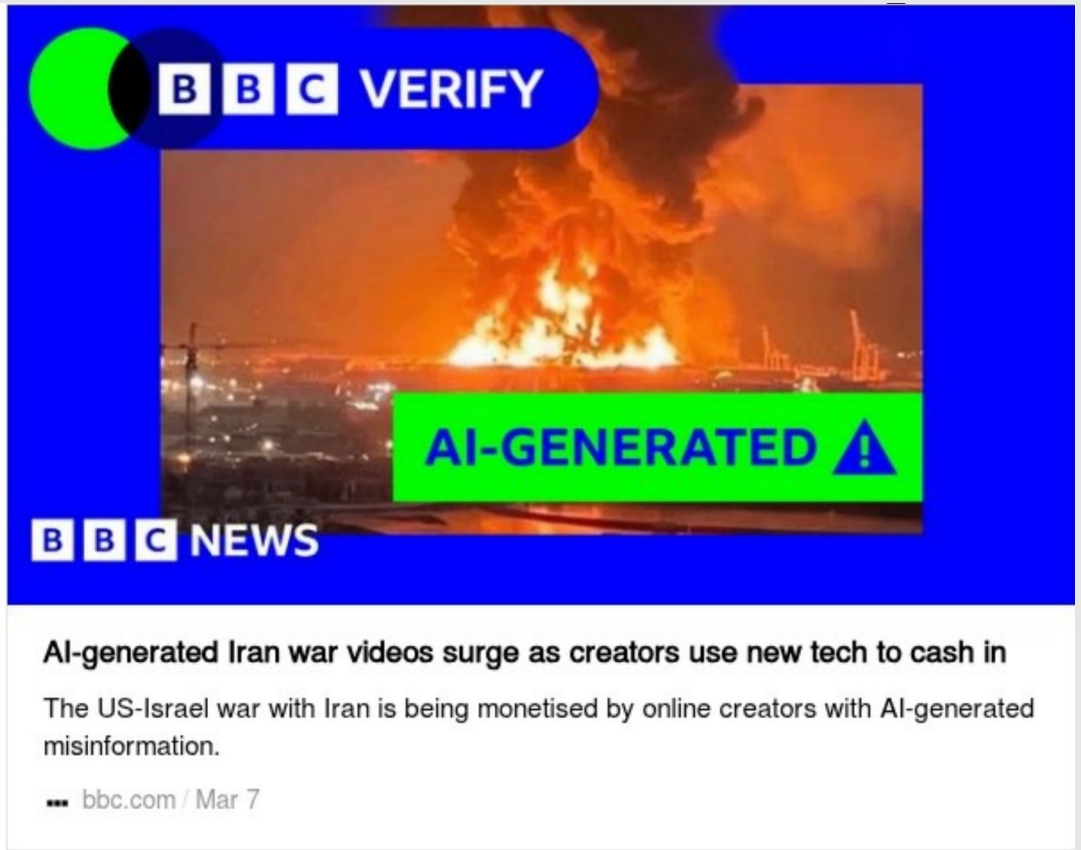
Dato	Tu mejor amigo	Meta
Tu ubicación exacta ahora		
Con quién hablas más	Quizás	
Con quien quedaste ayer	Quizás	
Tu nivel de batería		
Cuánto tiempo miras cada foto		
Qué dispositivos hay en tu casa		
Tus datos de tarjeta de crédito		
Tu velocidad de internet		
Tus contactos completos		

PROYECTO DATÁVOROS



BENEFICIARIOS

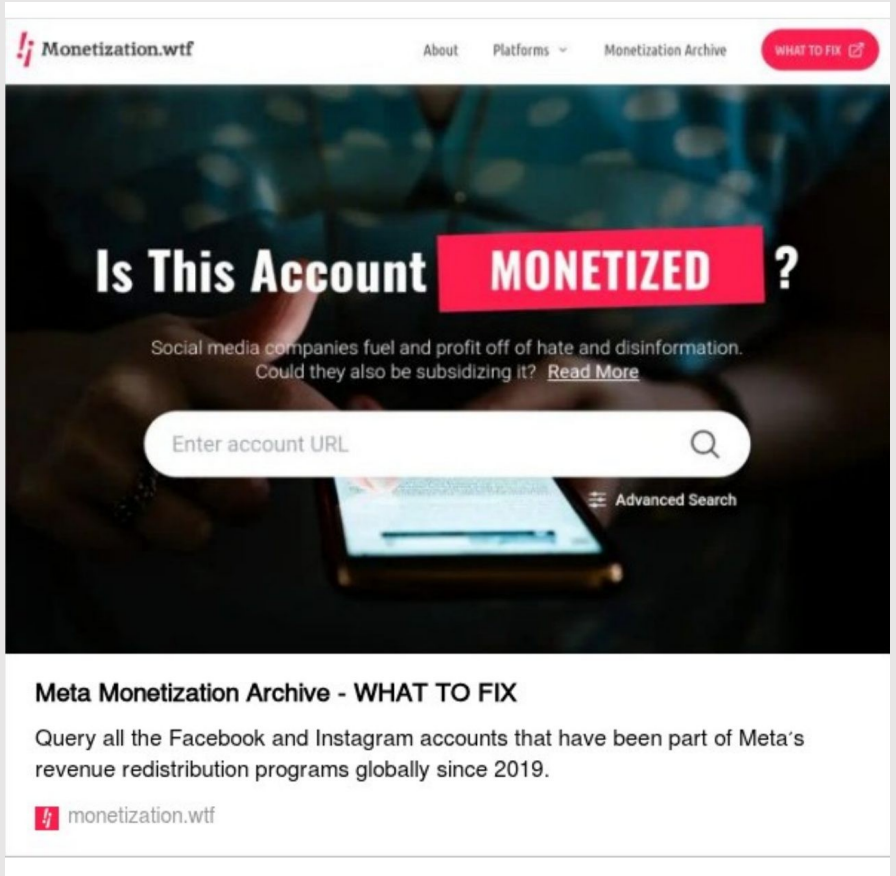
OPORTUNISTAS — MONETIZADORES



El jefe de producto de X dijo el martes que el 99% de las cuentas que difunden vídeos generados por IA como este intentan "manipular la monetización" publicando contenido que genere una gran cantidad de interacción a cambio de un pago a través del programa de reparto de ingresos para creadores de la aplicación.

BBC Verify / BBC News

MONETIZATION.WTF

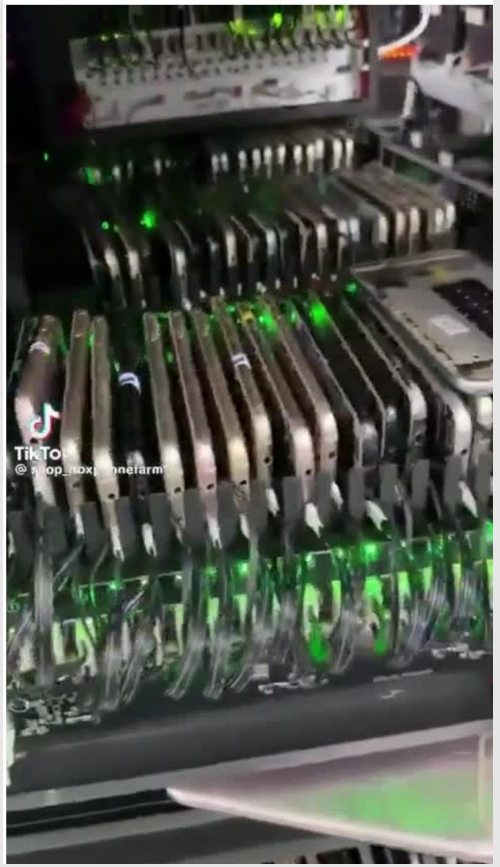


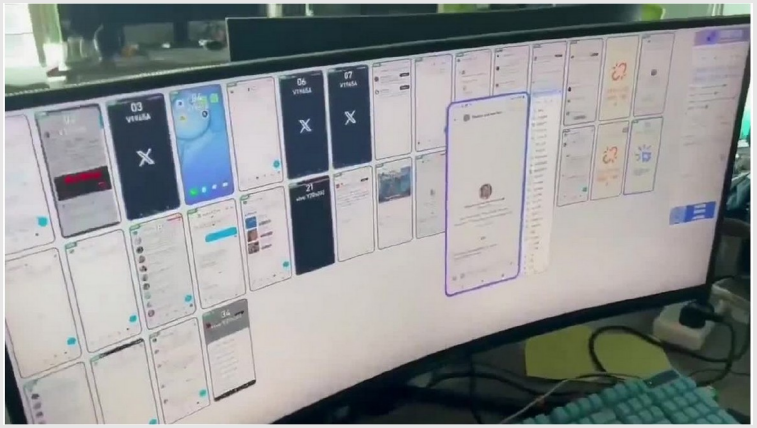
PARTIDOS POLÍTICOS

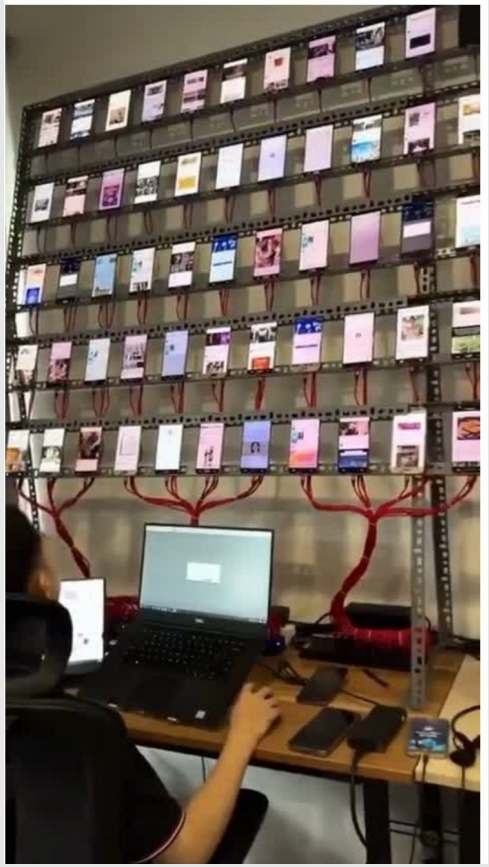
- Se acerca la campaña.
- Equipo del partido va a conferencias internacionales de comunicación política.
- Fichan a un estratega general de campaña que tiene a un estratega digital.
- El estratega digital realiza diagnóstico de:
  - temas sensibles
  - comunidad (campaña no oficial)
  - compra de servicios (bots, páginas falsas, etc.)

INDUSTRIA DE LA INFLUENCIA

GRANJAS DE TROLLS Y GRANJAS DE TELÉFONOS







EL MERCADO DE CUENTAS Y VERIFICACIONES FALSAS



SMS Verification Statistics by countries

Learn how the Cambridge Online Trust & Safety Index (COTSI) tracks SMS verification market in nearly every region worldwide.

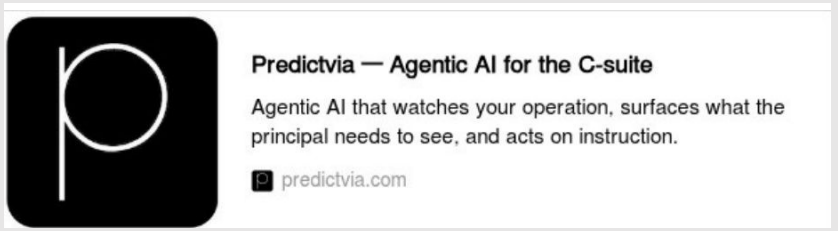
cotsi.org

Platform	Price	Stock
Whatsapp	$14.85	144
Telegram	$9.90	493
bet365	$7.43	644
Publi24	$5.45	670
Abbott	$5.45	670
Zasilkovna	$5.45	670
WooPlus	$5.45	670
ZoomInfo	$5.45	670
OpenAI	$5.45	670
Payoneer	$5.45	670
Feeld	$5.45	670
PayPal	$5.45	645
ANY OTHER	$4.95	1,128
Klarna	$3.72	670
Facebook	$3.72	21
Paysafecard	$3.47	652
Tinder	$3.03	282

AGENCIAS DE COMUNICACIÓN POLÍTICA

CASO PREDICTVIA







RS® World Business Markets Sustainability Legal Breakingviews Technology Investigati

Americas

Latin American election influence operation linked to Miami marketing firm

By **Zeba Siddiqui** and **Christopher Bing**

May 4, 2023 12:45 PM GMT+2 · Updated 2 months ago

A general view of lawmakers attending the first session of the Congress in Tegucigalpa, Honduras February 8, 2022. REUTERS/Fredy Rodriguez

SAN FRANCISCO/WASHINGTON, May 4 (Reuters) - A Miami-based digital marketing firm was behind a series of covert political influence operations in Latin America over the last year, Facebook-owner Meta (META.O) said this week, a rare exposé of an apparent U.S.-based misinformation-for-hire outfit.

Predictvia, which is registered as a business in Florida, says on its website that it stands on the "front line of the fight against misinformation" and combats "coordinated efforts to manipulate public discourse."

Reuters — "Latin American election influence operation linked to Miami marketing firm", May 4, 2023



Xavier Domínguez.

Un ex asesor del PSC diseñará el plan estratégico de comunicación de Renfe

PR | 31 MAYO 2023

En esta noticia se habla de: MANUEL SEMPERE / RENFE / WISH & WIN /

Wish Win ha ganado un contrato de casi 50.000 euros tras imponerse a otras

CASO: DESINFORMACIÓN ELECTORAL EN HONDURAS

POLITICS

A prominent PR firm is spreading disinformation ahead of Honduras' elections, new investigation reveals

The political group is using a network of Facebook pages and websites made to appear as legitimate news outlets.

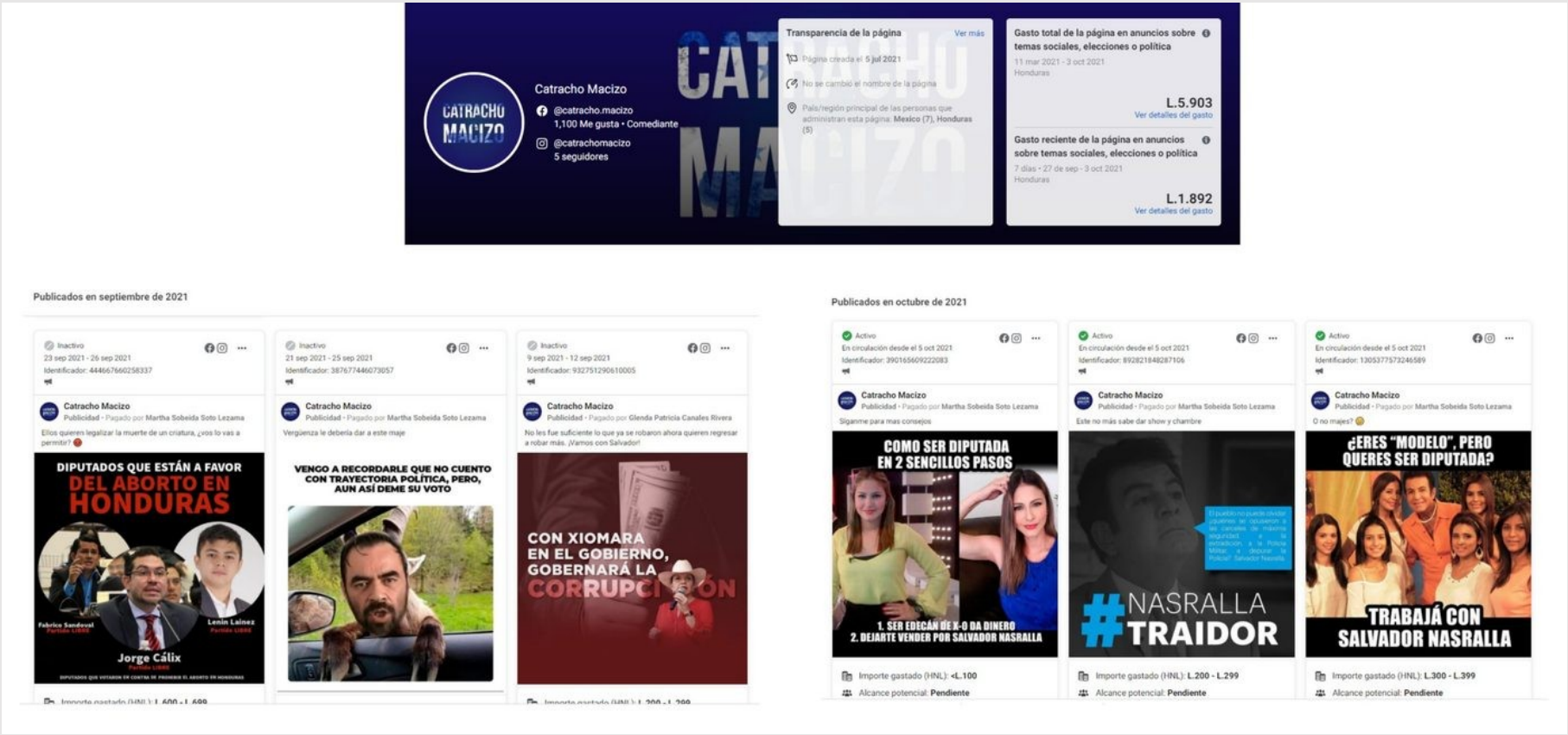


Luego de la publicación de Pandora Papers, una investigación realizada por el International Consortium of Investigative Journalists (ICIJ) en la que Contracorriente participó, se difundió una nota de un periódico con dominio web engañoso que señalaba, sin fundamento verdadero, al expresidente Manuel Zelaya Rosales como involucrado en los Pandora Papers. El ingeniero informático y sociólogo in fieri Aldo Salgado fue detrás de esa red de desinformación y encontró que detrás de esto estaba una empresa conocida.

Texto: Laura García, Leonardo Aguilar
Fotografías: Martín Cálix



BIBLIOTECA DE ANUNCIOS: EL CASO "CATRACHO MACIZO"



LO QUE DICE EL INFORME DE META

2. Mexico: We removed 12 Facebook accounts, 172 Pages and 11 accounts on Instagram. This network originated primarily in Mexico and targeted audiences in Honduras, Ecuador, El Salvador, the Dominican Republic and Mexico. We found this activity as a result of reviewing public reporting about some of this activity. Our investigation found links to Wish Win, a PR firm in Mexico.

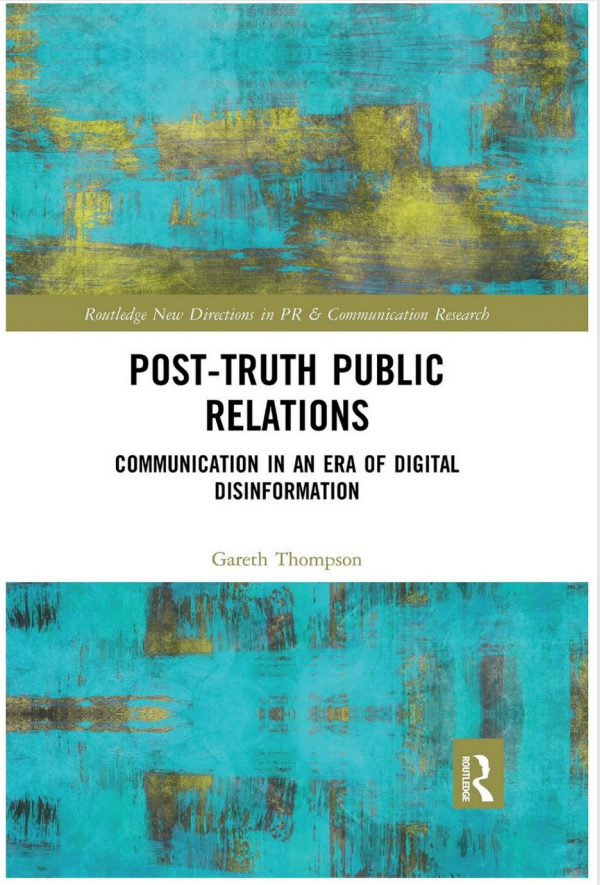
"December 2021 Coordinated Inauthentic Behavior Report", pág. 5, about.fb.com

XAVI DOMÍNGUEZ I ERNEST BENACH: “NOUS TEMPS”



Minuto 2:00 a 3:00

PARA SEGUIR LEYENDO



TORRE PACHECO

CRONOLOGÍA DE LOS CONTENIDOS

9 jul	Un vecino de Torre Pacheco (Murcia) de 68 años sufre una agresión. Se baraja la hipótesis de que fuera un reto viral.
10 jul	La noticia se difunde y varias cuentas propagan vídeos manipulados y fotografías erróneas de los supuestos implicados.
11 jul	Llamamientos en Telegram a atacar a personas de origen extranjero. El Ayuntamiento convoca una manifestación.
12–13 jul	Primeros episodios de violencia en San Antonio. Manifestación de Vox con el lema "Defiéndete de la inseguridad".
14 jul	Detención del líder del grupo ultra 'Deport Them Now' en Telegram; aumentan los discursos de odio.
15 jul	Declaraciones del alcalde, el Presidente del Gobierno y el ministro del Interior mantienen la atención mediática.
16 jul	Pico de actividad vinculado a la difusión de los episodios violentos y a otra noticia no relacionada usada para alimentar el discurso de odio.

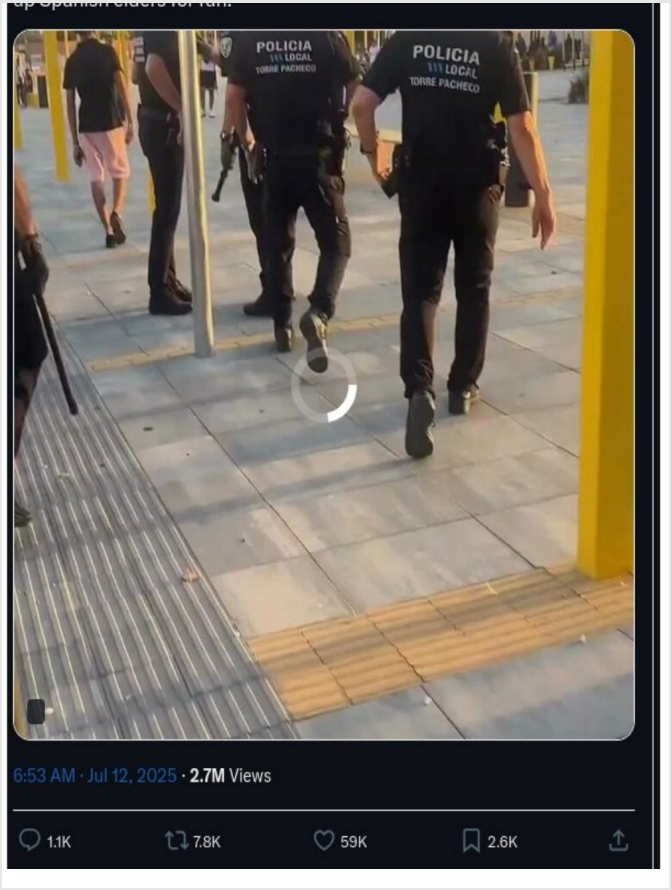
CONVOCATORIAS PREVIAS DE "DEPORT THEM NOW"





Diario Red — perfil de miembro de Vox vinculado al chat que organizó "cacerías" de migrantes

PUBLICACIÓN DE RADIO GENOA



PALABRAS MÁS UTILIZADAS EN MENSAJES DE X



DINÁMICA

Colocamos a los actores de las tarjetas en uno de los tres grupos:

HABILITADORES	EJECUTORES	BENEFICIARIOS

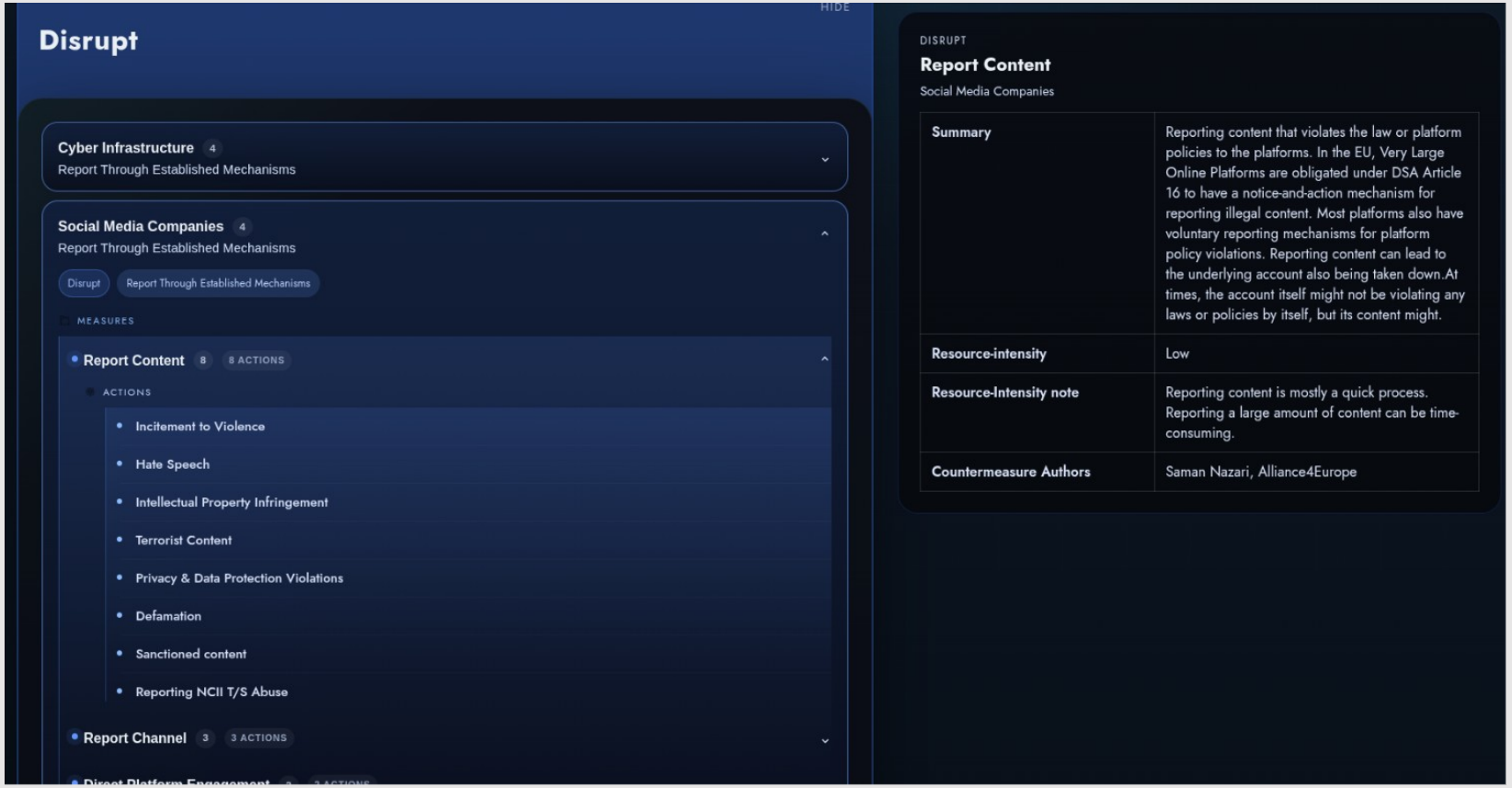
RESPUESTAS

PREBUNKING


Game: Bad News
CAMBRIDGE
Social Decision-Making Lab
PREVIOUS
Harmony Square
NEXT
Bad Vaxx
ESP
BÚRLATE
CONSPIRA
BAD NEWS
¡De las noticias falsas al caos!
¿Qué tan malo puedes ser? Consigue
tantos seguidores como puedas.
EMPEZAR
GOLPEA
EXAGERA
COMPARTIR
TILT

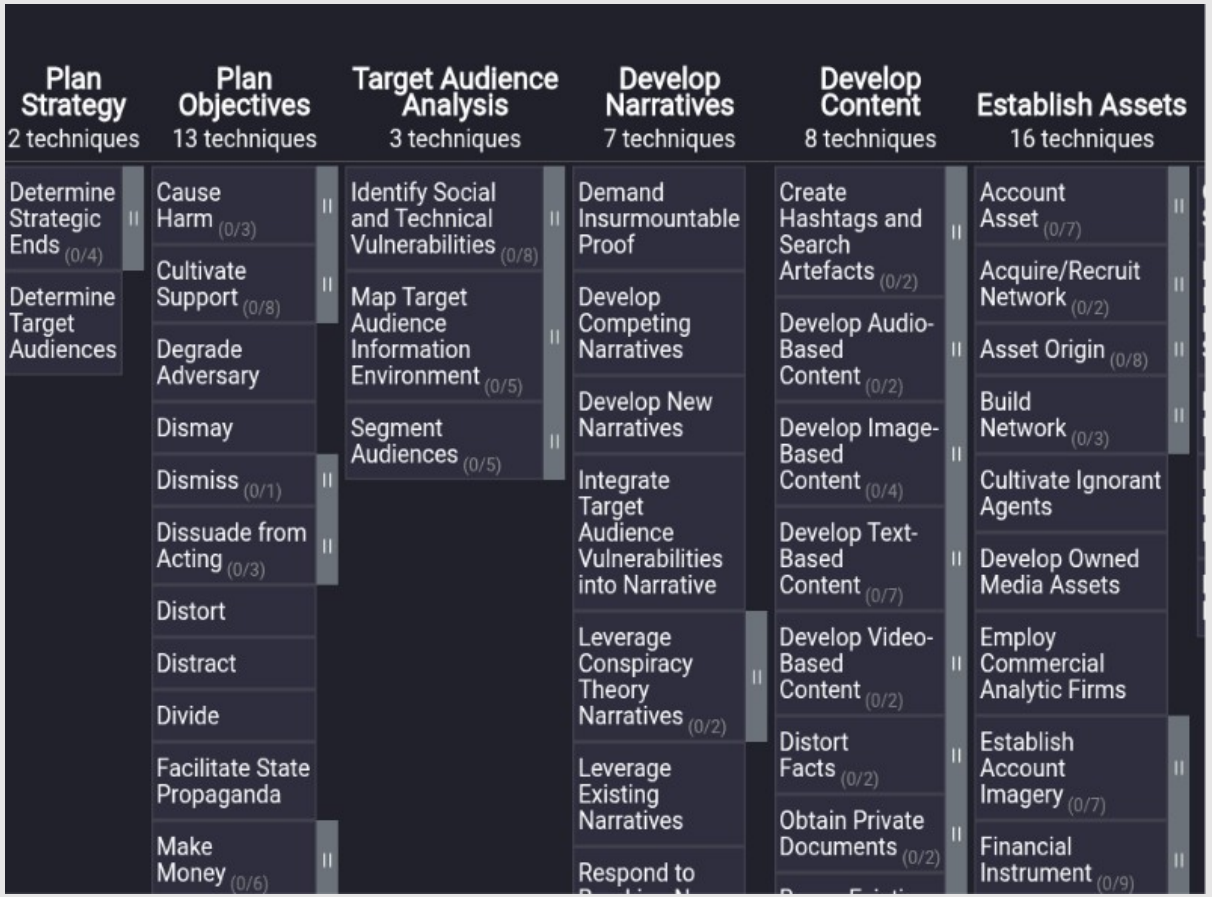
EDUCACIÓN PARA LA CIUDADANÍA DIGITAL

DISRUPT FRAMEWORK



framework-visualizer.fly.dev

DISARM FRAMEWORK



scampb06.github.io/disarm-navigator/

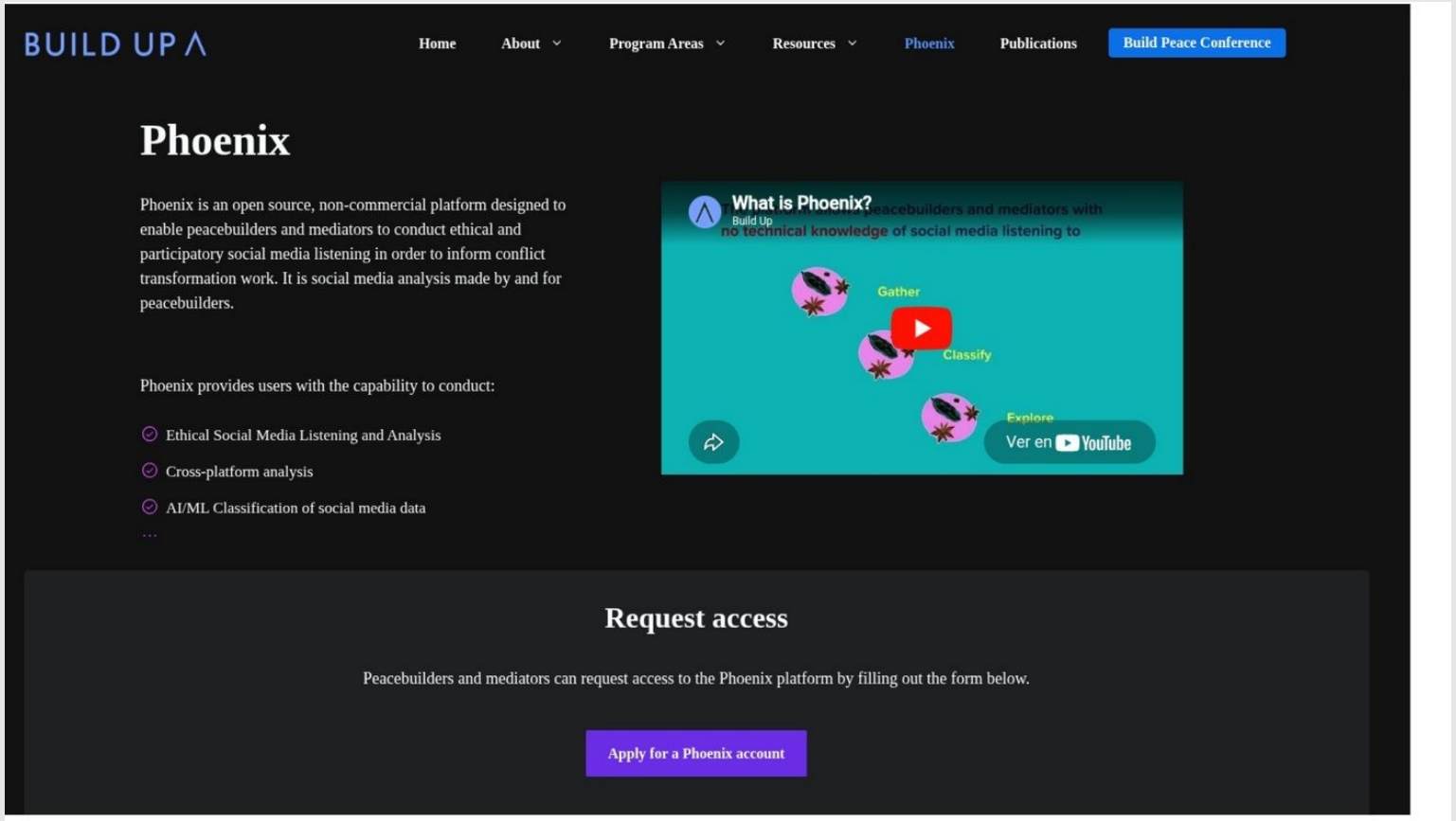
DISARM RED — APLICADO A TORRE PACHECO

Código	Descripción DISARM	Cómo se aplicaría en Torre Pacheco
T0042	**Seed Kernel of Truth**. Técnica de "sembrar un núcleo de verdad" para envolverlo con distorsión o explotación narrativa. Está bajo **TA08 Conduct Pump Priming**, donde DISARM incluye esta técnica como parte de la liberación inicial de contenido para preparar una campaña. (GitHub)	Encaja porque hubo un **hecho real**: la agresión a un vecino. A partir de ahí, el caso fue usado para construir una narrativa más amplia de amenaza migrante y justificar hostilidad colectiva. RTVE describe precisamente esa secuencia: agresión real, bulos racistas, convocatorias y disturbios xenófobos. (RTVE)
T0023.001	**Reframe Context**. DISARM lo define como sacar un evento de su contexto para distorsionar su significado y llevar a la audiencia a una conclusión distinta. (GitHub)	La agresión dejó de presentarse como un hecho a investigar sobre autores concretos y pasó a enmarcarse como prueba de una supuesta amenaza colectiva vinculada a la población migrante, especialmente magrebí. Ese reencuadre es una bisagra central del caso. (RTVE)
T0085.004	**Develop Document**. DISARM lo resume como "producir texto en forma de documento"; el propio ejemplo del framework enlaza esta técnica con **cartas o documentos falsificados**. (GitHub)	Aplica al **falso comunicado del ayuntamiento** que circuló como si fuera oficial. Maldita lo verificó como falso, y el formato documental le daba una apariencia de autoridad que aumentaba su capacidad de engaño. (RTVE)
T0143.003	**Impersonated Persona**. En los ejemplos del framework, esta técnica aparece cuando un actor finge ser una persona o institución real para hacer más creíble el contenido falso. En el ejemplo oficial asociado a T0085.004, se menciona explícitamente la combinación entre documento falsificado e impersonación. (GitHub)	También encaja con el falso comunicado: no solo se creó un documento, sino que se lo hizo pasar por una **voz institucional legítima**, usando la autoridad percibida del ayuntamiento como palanca de credibilidad. (RTVE)
T0119.001	**Post across Groups**. DISARM lo define como publicar contenido a través de distintos grupos para llevar narrativas a nuevas comunidades dentro o fuera del público objetivo. (GitHub)	Los bulos y llamamientos circularon en **múltiples grupos** de Telegram y espacios afines del ecosistema ultra. El artículo de *Diario Red* sitúa la difusión de fotos falsas y otros contenidos en canales vinculados a **Deport Them Now Murcia**.
T0119.002	**Post across Platform**. DISARM lo define como publicar contenido en distintas plataformas para extender la narrativa y, a veces, quitarle oposición o contexto correctivo. (GitHub)	La narrativa no quedó encerrada en un solo canal. Se movió entre **Telegram, redes sociales y medios ultra**, ampliando alcance y reforzando la cascada entre rumor, bulo y movilización. RTVE y la pieza periodística que trabajamos apuntan a ese ecosistema multiplataforma. (RTVE)
T0138.002	**Provoke**. DISARM: "instigate, incite, or arouse a target to act"; añade que manipuladores pueden explotar la indignación moral para empujar a la audiencia a difundir odio, salir a protestar o cometer violencia. (GitHub)	Encaja de forma muy directa con los **llamamientos a "cacerías"** y con el paso de mensajes de odio a acción física. RTVE documentó esas convocatorias y la relación entre desinformación y disturbios xenófobos. (RTVE)
TA10	**Drive Offline Activity**. DISARM lo resume como mover la campaña del espacio online al offline y facilitar que la audiencia interactúe con el contenido de la operación en el mundo físico. (GitHub)	Torre Pacheco es un ejemplo muy claro de esa transición: mensajes y narrativas online terminaron conectando con **concentraciones, patrullas, disturbios y agresiones** en el espacio físico. (RTVE)
T0126.001	**Call to Action to Attend**. DISARM lo define como un llamado a asistir a un evento. (GitHub)	Se ajusta a la convocatoria de protestas y concentraciones, así como a los mensajes que pedían presencia física en Torre Pacheco en los días de máxima tensión. (RTVE)
T0127.002	**Encourage Physical Violence**. DISARM lo recoge dentro de **TA10 Drive Offline Activity**, junto a otras formas de violencia física offline. (GitHub)	Aplica a los mensajes y dinámicas que no solo pedían presencia o protesta, sino que **alentaban agresión física** contra migrantes, y a la exhibición de armas en canales vinculados a la escalada, según la investigación periodística que trabajamos.

DISARM BLUE — APLICADO A TORRE PACHECO

Código	Descripción DISARM	Cómo se aplicaría en Torre Pacheco
C00220	**Develop a monitoring and intelligence plan**. DISARM: crear un plan de respuesta a desinformación antes de necesitarlo, incluyendo contactos, conexiones y contramensajes esperados. (GitHub)	Habría sido clave como medida previa: el caso escaló en pocos días desde un hecho local a una oleada de odio y violencia. Un plan Blue habría permitido activar rápido monitoreo, vocería institucional, coordinación con verificadores y protocolos de protección comunitaria. (RTVE)
C00126	**Social media amber alert**. DISARM: crear un sistema de alerta sobre artefactos, narrativas e incidentes de desinformación. (GitHub)	Muy pertinente para detectar desde temprano el paquete de señales del caso: fotos falsas de supuestos culpables, falso comunicado institucional y llamamientos a "tacerías". Habría servido para avisar a medios, instituciones locales y actores comunitarios antes de que el incendio corriera por el monte digital. (RTVE)
C00119	**Engage payload and debunk**. DISARM: desmentir contenido desinformativo y proporcionar enlace a los hechos. (GitHub)	Encaja con la necesidad de **desmentido rápido y visible** frente al falso comunicado, las fotos falsas y otros contenidos manipulados. En Torre Pacheco, la velocidad del desmentido era crucial porque la mentira ya estaba alimentando movilización y odio. (RTVE)
C00115	**Expose actor and intentions**. DISARM: exponer a creadores y difusores de desinformación, así como sus intenciones. (GitHub)	Habría servido para desplazar la atención desde el blanco estigmatizado hacia la **infraestructura de agitación**: canales, difusores, grupos ultras y actores de amplificación. Pedagógicamente, esta counter permite mostrar que no basta con desmontar el bulo; también hay que iluminar la maquinaria que lo empuja. (RTVE)
C00116	**Provide proof of involvement**. DISARM: construir y publicar información sobre la implicación de grupos o actores en incidentes de desinformación. (GitHub)	Es la respuesta Blue complementaria a la anterior. En este caso, habría significado documentar de manera trazable vínculos entre grupos, canales, convocatorias y piezas concretas de desinformación para cortar la coartada del "solo compartí". (RTVE)
C00184	**Media exposure**. DISARM: destacar en medios las actividades y actores de desinformación. (GitHub)	Aplica muy bien al trabajo de medios y verificación que reconstruyen cómo se extendieron los bulos y quiénes participaron en la amplificación. En un caso así, la exposición mediática no es adorno: es una forma de desactivar opacidad y romper impunidad narrativa. (RTVE)
C00107	**Content moderation**. DISARM: incluye retirada de contenido en redes sociales. (GitHub)	OBERAXE registró **138.204 contenidos** de odio reportables entre el 6 y el 22 de julio y señaló que solo se retiró el **22%**. Eso convierte la moderación en una contramedida central, no periférica. (La Moncloa)
C00122	**Content moderation**. DISARM advierte que la moderación mal usada puede convertirse en censura, pero la mantiene como counter en la fase de exposición. (GitHub)	En Torre Pacheco, esta counter recuerda que la moderación no solo debe existir, sino hacerse con criterios claros y velocidad suficiente cuando hay odio racial y llamados a violencia. Es una respuesta de contención, no de cosmética. (La Moncloa)

HERRAMIENTA: PHOENIX (BUILD UP)





GRACIAS POR PARTICIPAR