GUERRAS COGNITIVAS



DANIEL IRIARTE

CÓMO ESTADOS, EMPRESAS, ESPÍAS Y TERRORISTAS USAN TU MENTE COMO CAMPO DE BATALLA

arpa

GUERRAS COGNITIVAS

Daniel Iriarte

GUERRAS COGNITIVAS

arpa

© del texto: Daniel Iriarte, 2025
© de esta edición: Arpa & Alfil Editores, S. L.

Primera edición: mayo de 2025

ISBN: 978-84-10313-90-3

Diseño de colección: Enric Jardí
Diseño de cubierta: Anna Juvé
Maquetación: El Taller del Llibre
Producción del ePub: booqlab

Arpa
Manila, 65
08034 Barcelona
arpaeditores.com

Reservados todos los derechos.
Ninguna parte de esta publicación puede ser reproducida, almacenada o transmitida por ningún medio sin permiso del editor.

ÍNDICE

1. ¿Qué es la guerra cognitiva?
2. Estados, ejércitos virtuales y plataformas
3. ¿Para qué sirve un trol?
4. Guerrillas digitales
5. Mercenarios de la desinformación
6. Los memes son un arma (cargada de futuro)
7. Elecciones, la trinchera perfecta
8. Conspiranoicos y extremistas
9. De las redes a las calles
10. Desestabilización *low cost*
11. Campo de batalla: Estados Unidos
12. Lo que viene

AGRADECIMIENTOS

NOTAS

1

¿QUÉ ES LA GUERRA COGNITIVA?

«¿Cuánta verdad puede soportar el hombre?».
FRIEDRICH NIETZSCHE, *Ecce Homo*

El 19 de noviembre de 2021, un convoy militar francés se disponía a cruzar la localidad de Kaya, en la región central de Burkina Faso, cuando miles de manifestantes bloquearon la ruta. La columna, formada por varias decenas de vehículos militares, se dirigía desde Costa de Marfil hacia Níger, con Mali como destino final, para llevar suministros a las tropas desplegadas en esa región como parte de la Operación Barkhane.

El convoy despertaba suspicacias entre la población local: los militares franceses ya se habían topado con protestas en la ciudad de Bobo-Dioulasso y en la capital, Uagadugu. Pero esta vez era diferente. Además de los habituales mensajes antifranceses y anticoloniales, una idea permeaba la muchedumbre y la volvía más virulenta que de costumbre: la convicción de que el convoy, en realidad, transportaba armas dirigidas a los grupos yihadistas que azotaban gran parte del Sahel.[1]

El mensaje no había surgido de la nada. Llevaba meses promovido en redes sociales y medios locales[2] por una red propagandística rusa establecida por Yevgueni Prigozhin, un empresario de San Petersburgo apodado «el chef de Putin». Prigozhin mantenía lucrativos contratos de *catering* con el Kremlin y el Ministerio de Defensa ruso. Pero, además de su empresa de restauración, era el propietario de una vasta infraestructura de comunicación y desinformación, así como del Grupo Wagner, la organización paramilitar a la que Rusia recurría

cuando requería una intervención relativamente discreta en otros países y las circunstancias desaconsejaban el envío de tropas regulares. Wagner había sido la punta de lanza de operaciones armadas en el este de Ucrania, Siria, Libia, la República Centroafricana, Sudán y Mozambique, entre otros lugares. Ahora, se estaba expandiendo rápidamente por el Sahel.

Sus acciones venían acompañadas por grandes campañas en internet en las que ensalzaba el papel de los combatientes rusos y denigraba a enemigos y competidores que, por lo general, eran las fuerzas de pacificación y estabilización europeas en el continente africano. El papel de Francia como la antigua potencia colonizadora la convertía en el principal blanco de los mensajes, promovidos por cuentas en redes que se presentaban como locales, pero que, a menudo, eran operadas por extranjeros en las «granjas de troles» que Prigozhin había establecido en varios países de África.

La intervención militar directa francesa en Mali —donde viaja el convoy con el que ha comenzado nuestra narración— arrancó en 2013 a petición del Gobierno interino de Bamako. Una coalición de organizaciones yihadistas habían tomado el norte del país e impuesto la *sharía*, la ley islámica, en varias áreas. En aquel momento, el apoyo de la población maliense a una operación francesa que contuviese a los yihadistas era del 96%, según una encuesta de Al Jazeera.[3] La llamada Operación Serval consiguió expulsar a los islamistas radicales en pocos meses, y pronto fue reemplazada por una misión de estabilización de la Unión Europea (EUTM Mali).

Al año siguiente, Francia amplió su lucha al resto del Sahel mediante la Operación Barkhane.

Sin embargo, el Grupo Wagner empezó a expandirse en paralelo por África. Ya tenía una presencia militar destacada en Sudán, y sobre todo, en la República Centroafricana, donde ejercía de guardia pretoriana del presidente Faustin-Archange Touaderá: entrenaba a su ejército y combatía a grupos armados, a cambio de lucrativas concesiones para la extracción de recursos.[4] Ahora, planeaba expandir

dicho modelo a la región del Sahel. La presencia francesa suponía, pues, un estorbo para Prigozhin. Sus redes de desinformación empezaron a atacar a las tropas galas con artillería mediática y propagandística.

Las narrativas manipuladoras explotaban un elemento real —el secular resentimiento con la metrópoli colonial— para amplificar y magnificar los sentimientos antifranceses entre la ciudadanía africana. Las dificultades para contener a unos yihadistas que ganaban territorios, y algunas matanzas de civiles cometidas por las fuerzas galas,[5] tampoco ayudaron a París a «ganar corazones y mentes» en el Sahel. Lo cual empujó la auténtica tormenta de eslóganes, mensajes y relatos —algunos reales, pero con frecuencia distorsionados o inventados— sobre la presencia francesa, que iban calando.

El equipo de Prigozhin pagaba a pequeños grupos de personas para organizar protestas en las que se repetían dichos eslóganes y se enarbolaban banderas rusas, lo que generaba un poderoso material visual que, posteriormente, era difundido por las estructuras mediáticas creadas por el empresario.

En esta guerra paralela, la inteligencia francesa logró apuntarse algunos tantos, como la exposición pública de una operación de falsa bandera en la que operativos de Wagner enterraron los cadáveres de varios civiles que ellos mismos habían matado en una operación antiterrorista para después acusar a las tropas galas. Francia logró contrarrestarlo, al difundir unas imágenes grabadas mediante un dron en las que se veía a los combatientes rusos en plena «faena» con los cuerpos.[6]

En otra ocasión, varios perfiles virtuales creados por la inteligencia militar francesa se enzarzaron en una batalla dialéctica con los trols de Prigozhin, creando un revuelo que no pasó desapercibido a los analistas de desinformación contratados por la plataforma Meta para estudiar lo que el negocio de Mark Zuckerberg denomina «comportamientos coordinados no auténticos»: es decir, aquellos que violan las condiciones de sus redes sociales.[7] Pero, en líneas generales,

las contracampañas fueron ineficaces, incapaces de controlar el relato orquestado como una inundación virtual por Rusia.

Así se creó el caldo de cultivo para una sucesión de golpes de Estado de marcado carácter antifrancés, ejecutados por juntas militares y que rápidamente se aliaron con Rusia. Los nuevos gobiernos golpistas no tardaron en exigir la salida de las tropas occidentales de sus países, al tiempo que firmaban sustanciosos contratos con Wagner para entrenar a sus ejércitos y colaborar en la lucha contra los yihadistas.

El episodio de Kaya con el que hemos empezado el capítulo marcó el punto de inflexión. El convoy militar pasó varios días retenido en esta localidad, hasta que la negociación con los líderes de la protesta logró desbloquearlo y los vehículos pudieron proseguir su ruta. Pero lo peor estaba por venir: el 26 de noviembre, al llegar a la localidad de Téra, al oeste de Níger, el convoy se encontró con otra protesta, esta vez violenta. Un millar de ciudadanos rodearon los camiones y blindados, arrojándoles piedras y palos. Un caza *Mirage*, que custodiaba el convoy, lanzó granadas lacrimógenas sobre la multitud, cubriendo la escena de gas. La escolta[8] abrió fuego, matando a dos personas e hiriendo a otras dieciocho; una decena, muy graves.[9]

Dos meses y medio después, París anunció la retirada de las tropas francesas de Mali. En los dos años siguientes, las tropas de la UE y Estados Unidos fueron saliendo progresivamente de los países del Sahel,[10] mientras que Francia reducía su presencia militar a pequeños contingentes en cuatro estados de África Occidental.[11]

BOMBARDEAR CON MENSAJES

El bombardeo constante de mensajes antifranceses en África es un ejemplo de guerra cognitiva, la exposición constante de un grupo social a unos contenidos diseñados por un actor específico, con el propósito de lograr un cambio en su forma de pensar y percibir el mundo. Cuando lo consigue, el siguiente paso es convencerlo de que

actúe y reaccione conforme a los designios de dicho actor, incluso aunque suponga ir contra los propios intereses del receptor, como a menudo sucede.

El del Sahel es, además, un caso exitoso para quien lo inició: aunque es imposible cuantificar hasta qué punto la agitación contra Francia se debió a la campaña de Rusia o a las dinámicas internas de esos países, cabe pensar que la operación fue un elemento central en la eclosión de sentimientos, sin los que el rechazo a la presencia francesa no habría llegado a tales límites. O habría tardado más años.

No es fácil explicar con precisión en qué consiste la guerra cognitiva. No existe una definición universalmente aceptada del término, y no faltan quienes consideran que, en realidad, no es más que un neologismo que se limita a redescubrir elementos ya conocidos y estudiados, como la desinformación, las operaciones psicológicas, la lucha por el control del dominio informativo o la manipulación del adversario. Y no dejan de tener algo de razón. Por eso quizá conviene empezar describiendo en qué consiste cada cosa.

A menudo, cuando menciono que estoy estudiando o escribiendo sobre desinformación, alguien me responde casi de forma automática: «Ah, ¿las *fake news*?». Pero el término «noticias falsas» es poco útil: un concepto demasiado amplio, que abarca desde las parodias humorísticas de *El Mundo Today* hasta informaciones que desagradan a un político y que las califica de mentiras. Pasando por gazapos, errores, manipulaciones periodísticas y, por supuesto, la desinformación pura y dura.

En el mundo anglosajón afinan más, distinguiendo entre *misinformation* y *disinformation*. La primera, *misinformation*, es la mera información errónea, que el emisor difunde por el motivo que sea sin ser consciente de su falsedad, pero que, aún así, puede llegar a tener consecuencias trágicas: véase los rumores bienintencionados durante una catástrofe natural, que pueden llevar a las personas a tomar decisiones que afecten a su propia seguridad.

La *disinformation* es la difusión deliberada de información falsa, manipulada o engañosa por razones políticas, operativas o para obtener un rendimiento económico.

La desinformación siempre ha sido un elemento intrínseco a los servicios secretos. Por poner un ejemplo cercano, Mikel Lejarza «El Lobo», el operativo de los servicios de inteligencia españoles cuya infiltración en ETA pocos años antes había supuesto un golpe demoledor para la organización, cuenta en sus memorias cómo en 1979 montó una falsa entrevista en Bélgica para denunciar la libertad de la que los etarras gozaban en aquel país. Según su relato, un compañero del CESID[12] llamó a la televisión belga y les ofreció la exclusiva con un «etarra arrepentido», que en realidad no era otro que el propio Lejarza. «Delante de una pared pusimos una bandera de Euskadi enorme y yo me coloqué a un lado con traje negro y capucha negra, hablando en euskera y en español. Me hicieron una entrevista, en la que queríamos hacer ver que ETA se entrenaba en campos belgas gracias a los apoyos con que contaban en ese país, una realidad que conocíamos perfectamente, pero que nadie se atrevía a denunciar. Nadie tomaba cartas en el asunto, ni siquiera el propio Gobierno español», relata el espía. «El reportaje tuvo mucha repercusión en Bélgica. Se armó un follón impresionante. Nuestro gobierno pidió explicaciones al belga, que no sabía por dónde salir».[13] A consecuencia del escándalo, Bélgica tomó medidas para limitar las actividades de los militantes etarras en su territorio, si bien todo había sido obra de un elaborado engaño.

Yuri Andropov, longevo director del KGB y presidente de la URSS por un brevísimo período hasta su muerte, dijo en una ocasión: «La desinformación es como la cocaína. Si la esnifas una o dos veces, puede que no te cambie la vida. Pero, si la usas cada día, te convertirá en un adicto. Una persona diferente». La cita aparece en un libro de Ion Mihai Pacepa, antiguo director del servicio de inteligencia exterior de la Rumanía comunista y el desertor de mayor rango de todo el Bloque del Este tras huir a Alemania Occidental en 1978. Pacepa

asegura que, tras el telón de acero, había más gente trabajando en *dezinformatsiya* (el término ruso para la desinformación) que en las fuerzas armadas y el sector de la defensa. La principal tarea de los servicios de inteligencia no era la recopilación de información, sino este tipo de acciones, dirigidas tanto contra la población de sus países como contra los Estados occidentales.[14]

En ese sentido, la desinformación se entrecruza con las llamadas operaciones de información, de influencia o psicológicas: aunque no son exactamente lo mismo, todas están concebidas para influir en la psique del objetivo y llevarle a actuar de la forma predeterminada que espera el atacante. Y son tan antiguas como los conflictos entre grupos sociales. La leyenda del *Timbaler del Bruc*, en la que un solitario tamborilero habría hecho sonar su instrumento en un desfiladero de la sierra de Montserrat durante la Guerra de Independencia haciendo creer a los invasores franceses que se aproximaba un ejército enorme,[15] podría considerarse una operación de este tipo.

Veamos un ejemplo más contemporáneo: la llamada Operación Silkman. En el año 2000, las fuerzas británicas desplegadas en Sierra Leona veían con aprensión cómo la insurgencia del Frente Revolucionario Unido —FRU, famoso por llevar a cabo mutilaciones masivas con machetes para infundir el terror en sus adversarios— se acercaba peligrosamente a la capital, Freetown. Las tropas habían llegado al país apenas unos meses antes para evacuar a los ciudadanos británicos y prestar apoyo a la misión de paz de la ONU y al Gobierno central. Pero, en ese período, el clima político en el Reino Unido había cambiado tanto que a la fuerza expedicionaria se le habían impuesto importantes restricciones respecto al uso de la fuerza, para evitar acusaciones de neocolonialismo. Sin embargo, el comandante sobre el terreno, el comandante de brigada David Richards, era consciente de que la inacción llevaría, casi con certeza, a violentas masacres de civiles —como sucedió en el genocidio de Ruanda—, masacres que, aparte de suponer una tragedia humanitaria, tendrían un enorme coste político para Gran Bretaña.[16]

Los servicios de inteligencia habían descubierto que se preparaba una reunión entre la cúpula del FRU y representantes del Gobierno de Charles Taylor, presidente de la vecina Liberia, que respaldaba a los rebeldes. El encuentro serviría para ultimar los detalles de la toma de Freetown. La solución que encontraron los británicos fue el lanzamiento de una operación de información con el objetivo de proyectar fuerza y disuadir a los rebeldes de atacar la capital. Tropas paracaidistas se lanzaron sobre Sierra Leona, acompañadas de desembarcos anfibios y demostraciones de artillería, en unos ejercicios a los que asistió el presidente sierraleonés y otros altos cargos del país. Las maniobras fueron cubiertas en profundidad por numerosos medios de prensa, que dieron amplia difusión a las capacidades militares británicas. La reunión entre el FRU y el Gobierno liberiano no tuvo lugar y, en último término, la ofensiva contra Freetown quedó abortada.[17] Dos años después, gracias a una serie de acciones internacionales de carácter diplomático y militar contra las bases, y a los apoyos de los insurgentes en los países vecinos, el FRU se encontró acorralado y se vio obligado a firmar un acuerdo de paz, poniendo fin a la larga y sangrienta guerra civil.

En este tipo de operaciones no siempre es necesario el recurso a la desinformación. En Sierra Leona, la proyección de fuerza era verdadera, y los británicos realmente tenían esas capacidades militares, lo que produjo un efecto disuasorio en sus antagonistas. Algo similar puede decirse de la estructura de medios de comunicación montada por los gobiernos de Estados Unidos y el Reino Unido durante la Guerra Fría con los idiomas de los países del este de Europa, destinados a las audiencias tras el telón de acero: cabeceras como Radio Free Europe y Radio Liberty estaban totalmente dedicadas a la actividad propagandística, es decir, a difundir narrativas positivas sobre el mundo occidental y negativas sobre el bloque comunista, ignorando o justificando los problemas en el bando propio y amplificando los del adversario. Aunque a veces lanzaban exageraciones, distorsiones, bulos e ideas discutibles, el mensaje de

fondo —democracia, libertad de expresión y libre mercado frente a la represión, y la monocronía existentes en los países del llamado «socialismo real»— era tan potente que no necesitaban recurrir al engaño. Un poso de verdad es la mejor base para una buena propaganda.

Pero hay otro tipo de operaciones de influencia menos benévolas. En junio de 2024, la agencia Reuters desveló que, durante el punto álgido de la pandemia del COVID-19, el Pentágono había desarrollado una campaña de manipulación digital en países de Asia en contra de la vacuna china Sinovac. La operación, ejecutada de forma clandestina durante la primera presidencia de Donald Trump, «buscaba sembrar dudas sobre la seguridad y eficacia de las vacunas y otra ayuda para salvar vidas que estaba siendo proporcionada por China». Desde la base aérea de MacDill, en Tampa (Florida) —que el artículo describe como «la fábrica de propaganda clandestina del Pentágono»—, y con el apoyo de contratistas de la empresa General Dynamics IT, se crearon centenares de cuentas falsas en X (antes X/Twitter), Facebook e Instagram, que fingían ser ciudadanos de los países objetivo, que llegaron a acumular decenas de miles de seguidores, y que difundían mensajes destinados a desincentivar la aceptación de Sinovac, llegando a promover el sentimiento antivacunas.

Uno de los mensajes que se difundieron entre la población musulmana de Filipinas, así como en otros países de Asia Central y Oriente Medio, fue que Sinovac utilizaba grasa de cerdo y, por lo tanto, su inoculación era *haram*, prohibida por la religión islámica. «No estábamos abordando esto desde el punto de vista de la salud pública. Lo abordábamos sobre cómo podíamos arrastrar a China por el barro», declaró a Reuters un alto oficial militar implicado en la campaña.[18]

La operación clandestina fue lanzada en respuesta a la amplia desinformación que la propia China estaba difundiendo contra Estados Unidos a propósito de la pandemia. Medios y cuentas chinos llevaban meses diciéndole al mundo que el COVID-19 lo había llevado

a la ciudad de Wuhan un soldado estadounidense que había participado en unos ejercicios militares en 2019, y que su auténtico origen había que buscarlo en un programa norteamericano de armas biológicas desarrollado en Fort Detrick, en el estado de Maryland. En ese contexto, un número creciente de voces en Washington abogaba por responder de un modo similar, no solo ante China, sino también ante el creciente empuje de la desinformación rusa.

El Gobierno chino no solo estaba proporcionando vacunas en gran parte del planeta, sino todo tipo de ayuda sanitaria contra el COVID-19. Estados Unidos veía con alarma cómo esta instrumentalización de la ayuda hacía crecer la influencia de Pekín a pasos agigantados, especialmente en los países en desarrollo, al mismo tiempo que la reputación occidental disminuía. El Pentágono trató de contrarrestarlo: «No hicimos un buen trabajo compartiendo las vacunas con nuestros socios. Así que lo que nos quedaba era arrojar sombras sobre la de China», señaló el oficial citado anteriormente.[19]

El proyecto surgió como iniciativa del general Jonathan Braga, comandante en jefe del Mando de Operaciones Especiales para el Pacífico, con un objetivo definido: asegurarse de que la población de la región entendía cuál había sido el origen real del COVID-19, promoviendo el escepticismo hacia unas vacunas que todavía no habían sido suficientemente testadas, y ofrecidas por un país que «había mentido continuamente desde el origen de la pandemia». Pero la campaña pronto se desbordó con estrategias cuestionables. Las cuentas utilizadas recurrieron a *hashtags* como #Chinaangvirus («China es el virus», en tagalog, el idioma mayoritario de Filipinas), o a mensajes que rezaban: «El COVID vino de China y la VACUNA también vino de China, ¡no confíes en China»; «De China, EPPs, mascarillas, vacunas: FALSO. Pero el coronavirus es real» o «La vacuna de China podría ser matarratas». En el entorno musulmán se lanzaron memes con un cerdo compuesto de jeringuillas. Es difícil evaluar su impacto, pero en Filipinas, el principal foco, apenas 2,1 millones de personas se habían vacunado en junio de 2021, pese a la

amplia disponibilidad de dosis de Sinovac y muy lejos del objetivo de Manila de inocular a 70 millones de personas. Como resultado, el país tuvo la peor tasa de fallecimientos de la región.[20]

Esta campaña estadounidense, como vemos, recurrió a muchas de las técnicas que abordaremos a lo largo de este libro: memes de rápida visualización y alto impacto emocional, desinformación, enjambres de cuentas falsas, etcétera. Pero también utilizaron datos y elementos reales. En el mundo actual, donde la esfera digital tiene tanta importancia en nuestras vidas, incluso los hechos factuales pueden ser desplegados con carácter desestabilizador si se utilizan las herramientas adecuadas. De hecho, el Gobierno francés publicó en agosto de 2018 un informe conjunto de los ministerios de Defensa y Asuntos Exteriores que abordaba este asunto desde un enfoque amplio: el problema iba más allá de la desinformación y abarcaba «la manipulación de la información». «A veces la información no es falsa, sino simplemente exagerada, sesgada o presentada de una forma muy emocional, como ocurre en un tabloide. La información puede ser manipulada de muchas formas: a través de la producción, diseminación e incluso de la retención. No todos estos procesos implican una dicotomía entre verdad y falsedad».[21]

Pongo un ejemplo real: cuando la versión en castellano del medio ruso Sputnik titula «España sigue surtiendo a Ucrania de armas casi obsoletas mientras la pobreza aumenta en el país» (29 de febrero de 2024), está buscando un efecto emocional claro, vinculando dos elementos reales, pero no relacionados, como si fuesen una relación causa-efecto. Sabe que, en muchos lectores, la reacción inconsciente será pensar que habiendo pobreza, probablemente el envío de armamento al ejército ucraniano es un gasto que el país no se puede permitir, y sin darse cuenta se pondrá un poco más en contra de la ayuda a Ucrania. Burdo, pero funciona mejor de lo que podríamos pensar.

Algunos autores dan una vuelta de tuerca adicional y hablan de «armamentización de la información», donde incluso la información

verídica puede ser instrumentalizada con carácter ofensivo contra un adversario. Un caso que ilustra esta posibilidad es lo sucedido en Egipto en 2013. Dos años antes, la movilización de una gran parte de la sociedad egipcia había derrocado al dictador Hosni Mubarak, en el poder desde 1981, como parte de la ola de protestas que se conoció entonces como la Primavera Árabe, que afectó en mayor o menor medida a casi todo el mundo árabe, desde Marruecos hasta Baréin. En las primeras elecciones libres en la historia de Egipto, organizadas en 2012, los Hermanos Musulmanes se impusieron con facilidad gracias a que, pese a estar proscritos, su implantación en el país era superior a la de sus rivales políticos. Sus extensas redes de militantes de base les permitieron llevar a cabo una campaña electoral bien coordinada y ajustada al lenguaje y las preocupaciones de gran parte de la población egipcia, mayoritariamente rural. El 30 de junio de 2012, Mohamed Morsi se convirtió en el primer presidente islamista de Egipto. Pero había otra parte del país, la que valoraba el laicismo por encima de otras consideraciones, que estaba horrorizada. Y no estaban solos: Emiratos Árabes Unidos llevaba años en guerra abierta con el *ijwan*, la Hermandad Musulmana a la que consideraba una organización subversiva y peligrosa, y estaba actuando en todos los frentes para impedir su expansión.

El Gobierno emiratí, consciente de aquel malestar, puso en marcha una doble operación en su contra: por un lado, empezó a financiar un partido llamado Tamarod, de carácter secularista y liberal, para ir creando un movimiento contra el Gobierno de Morsi. A la vez, copó el espacio informativo de mensajes anti-*ijwan*. Las narrativas, a menudo basadas en incidentes o ejemplos reales, se centraban en la incompetencia de los Hermanos Musulmanes como gestores, en el supuesto carácter antiegipcio de Morsi y su partido, y en la pretendida amenaza que suponía para la seguridad nacional y la estabilidad económica. Poco después, empezaron a producirse manifestaciones antigubernamentales cada vez mayores.[22] Todo parecía indicar que

una parte importante del pueblo egipcio rechazaba el liderazgo de la Hermandad y quería una solución a toda costa.

Andreas Krieg, profesor asociado del King's College de Londres y especialista en Oriente Medio, ha estudiado este episodio en profundidad. En su libro *Subversión: La armamentización estratégica de narrativas*, escribe:

> Los EAU fueron capaces de hacer madurar una movilización cívico-social contra el *statu quo* político, llevando al Tamarod de ser un grupo de base marginal hasta convertirse en un movimiento que operaba como un frente capaz de traducir las narrativas bélicas desde el dominio virtual hasta las calles de Egipto. Lo que parecía un activismo cívico-social genuino en junio y julio de 2013, con millones de manifestantes en la calle, había sido de hecho cultivado estratégicamente a través de una variedad de redes de información, para que el Ejército egipcio lo explotase como pretexto para derrocar al gobierno.

Y así sucedió: el 3 de julio de 2013, las fuerzas armadas egipcias, lideradas por el mariscal Abdelfatah Al Sisi, dieron un golpe de Estado que acabó con el Ejecutivo de Morsi, desatando una ola de represión en la que decenas de miles de personas fueron encarceladas y torturadas, y reinstaurando la dictadura en Egipto. Para los Emiratos Árabes Unidos, el objetivo estratégico, impedir la consolidación y expansión de los Hermanos Musulmanes en un país clave para el mundo árabe, se había cumplido. La operación de información había preparado el terreno para el golpe.

¿ESTO ES NUEVO?

Si la desinformación y las operaciones psicológicas vienen practicándose desde los orígenes del espionaje, que muchos consideran «la segunda profesión más antigua del mundo», ¿a qué viene el revuelo de estos últimos años? La novedad la aporta el contexto: la emergencia de nuevos ecosistemas digitales hiperconectados y con acceso a casi todas las personas del planeta.

Operaciones de desinformación que hace no mucho tardaban años en consolidarse y rendir fruto —si es que lo hacían— pueden llevarse a cabo en cuestión de minutos, con resultados mucho más tangibles y a un coste ridículo. Este último factor es esencial: no solo cualquiera puede montar su propia operación cognitiva, sino que actores organizados y bien financiados tienen la capacidad de mantener las campañas durante períodos ilimitados, repitiendo los mismos mensajes una y otra vez, introduciendo pequeñas variaciones, alternando los medios y vectores para transmitirlos. Esta repetición es extremadamente eficaz, puesto que el bombardeo constante acaba por modificar nuestra percepción sobre cualquier tema. En último término, ese es el objetivo de la guerra cognitiva: no solamente vencer al adversario en una batalla concreta, sino derrotarlo por completo. Lograr, como señalaba Andropov, que el cerebro cambie su forma de razonar.

El ecosistema de medios rusos, por ejemplo, difunde con frecuencia teorías de la conspiración de todo tipo para crear en sus audiencias un determinado marco mental, que las vuelve más receptivas ante ciertas ideas que el Kremlin necesita difundir. En la doctrina rusa subyace un concepto conocido como «control reflexivo», el uso de las operaciones psicológicas «como un medio de hacerle llegar a un socio o un oponente información especialmente preparada para inclinarle a que haga voluntariamente la decisión predeterminada deseada por el iniciador de la acción». Se parece a la ingeniería social, muy ligada al mundo de la ciberseguridad, y definida como «el arte y la ciencia de conseguir que la gente cumpla con tus deseos».[23] Pero, como señala esa misma definición, «no es una forma de control mental, no te permitirá hacer que la gente lleve a cabo tareas salvajemente alejadas de su comportamiento».

La guerra cognitiva iría todavía un paso más allá: busca hackear la mente, bombardeando nuestros cerebros hasta modificar nuestra forma de razonar y provocando un cambio sostenido previsto por el

agresor que ha diseñado la operación psicológica, llevándonos a actuar de la forma que espera.

En un informe de 2020 que ya se ha convertido en un documento fundacional, el experto francés François du Cluzel desarrolla la diferencia entre la llamada «guerra de información», tal y como se define en la doctrina militar de varios países occidentales, y esta nueva concepción: «La guerra de información intenta controlar el flujo de información [...]. La guerra cognitiva degrada la capacidad de conocer, producir y abortar el conocimiento». Du Cluzel se extiende en la explicación:

> La guerra cognitiva persigue el objetivo de minar la confianza (la confianza pública en los procesos electorales, en las instituciones, aliados, políticos…), y, por lo tanto, el individuo se convierte en el arma, donde el objetivo no es atacar lo que piensan los individuos sino *la forma en la que piensan* [...] Cualquier usuario de las modernas tecnologías de la información es un objetivo potencial. Tiene como objetivo a todo el capital humano de una nación.[24]

La guerra cognitiva funciona de manera que los objetivos se convierten a su vez en emisores y vectores de ataque, en un proceso que Du Cluzel define como «propaganda participatoria»:

> Donde la guerra cognitiva difiere de la propaganda es en el hecho de que todo el mundo participa, en su mayor parte de forma inadvertida, en el proceso de la información y la creación de conocimiento de un modo sin precedentes [...]. Mientras anteriormente los individuos se sometían pasivamente a la propaganda, ahora contribuyen activamente a ella [...]. Es más fácil y barato para los adversarios erosionar la confianza en nuestros propios sistemas que atacar nuestras redes energéticas, fábricas o complejos militares.

«En los anales del conflicto humano, el surgimiento de la guerra cognitiva marca un cambio de paradigma tan trascendental como la llegada de la pólvora o el desarrollo de las armas nucleares», señala el experto en guerra cognitiva Josh Luberisse:[25]

> Este nuevo modo de conflicto capitaliza los avances tecnológicos exponenciales que han definido el siglo XXI. La inteligencia artificial, el aprendizaje automático, el análisis de *big data* y una serie de otras tecnologías en rápida evolución proporcionan un arsenal de herramientas que, cuando se utilizan con precisión, pueden cambiar las mareas de la opinión pública, alterar los resultados de unas elecciones democráticas e incluso incitar al conflicto sin que se dispare un solo tiro [...]. Mientras que los conflictos tradicionales buscaban la conquista territorial o la subyugación política, la guerra cognitiva apunta a la conquista de las mentes y la subyugación de las creencias.

El caso real más relevante son las acciones de China en Taiwán, que lleva años lanzando operaciones en el dominio cognitivo con el objetivo de convencer a los taiwaneses de que su situación actual es nefasta, que sus líderes son traidores vendidos a potencias extranjeras, que estarían mucho mejor en el seno de la República Popular China, y que resistirse a esa absorción es fútil, peligroso y dañino para sus intereses. En último término, Pekín quiere anexionarse la isla —a través de un ataque militar o mediante estrategias de carácter híbrido —, y necesita que el sector de la población taiwanesa convencido de la inutilidad de resistirse sea lo suficientemente amplio como para asegurar la victoria.

«Un adversario con la capacidad de perturbar o manipular las funciones cognitivas supone una amenaza más invasiva que cualquier arma convencional. El campo de batalla se extiende a las sinapsis y los circuitos del cerebro, donde la distinción entre soldado y civil se difumina, y la integridad de los pensamientos del individuo se convierte en la última baja de la guerra», afirma Luberisse.

En ese sentido, las tres grandes potencias pioneras a la hora de aplicar estas técnicas de manipulación al mundo virtual han sido Rusia, China e Israel, aprovechando la formidable oportunidad que presenta la omnipresencia de las redes sociales en nuestras vidas. Pero en estos últimos años no han tardado en surgir imitadores, primero autocracias como Irán, Venezuela, Azerbaiyán o los países del Golfo,

pero también cada vez más democracias como Estados Unidos o Francia, por nombrar dos casos demostrados fuera de toda duda.

También lo han hecho actores no estatales como Hamás y Hezbollah, el grupo de oposición iraní Mojahedin-e Halq, organizaciones yihadistas como Estado Islámico, o movimientos extremistas en todo el mundo, especialmente de ultraderecha. Todos han copiado muchas de las técnicas desarrolladas por los servicios de inteligencia rusos e israelíes, su aparato mediático, sus «granjas de trols» y sus colaboradores online, adaptándolas a sus idiosincrasias. Quizá era inevitable que estos métodos fueran adoptados también por las grandes corporaciones para defender sus proyectos y atacar a sus rivales, como viene sucediendo desde hace tiempo. El resultado es una gran «guerra mundial virtual», cada vez de mayor intensidad, y donde el campo de batalla son nuestras mentes.

2

ESTADOS, EJÉRCITOS VIRTUALES Y PLATAFORMAS

El politólogo Joseph Nye, quien a finales de los años ochenta acuñó el concepto de «poder blando»,[1] afirmaba en un artículo en 2000: «Tradicionalmente, la victoria la lograba el país cuyos ejércitos ganaban. Pero en una Era de la Información global, la victoria también depende de cuál es la historia que gana».[2]

Todas las potencias se esfuerzan en generar relatos justificativos que garanticen simpatía hacia sus acciones si consiguen convencer a una masa crítica entre las audiencias globales. Rusia invade Ucrania para «desnazificarla» e impedir que la OTAN la utilice para atacar su territorio. Israel arrasa Gaza hasta los cimientos porque allí «no hay verdaderos civiles». Estados Unidos necesita Groenlandia por imperativos estratégicos y «para garantizar su propia seguridad». El sistema de China es el más eficiente del mundo para «la prosperidad y el desarrollo globales». La Unión Europea es un actor moral que «solo se mueve por principios». Etcétera.

Casi todos los estados de cierta entidad —igual que grandes corporaciones, movimientos políticos y organizaciones armadas paraestatales— dedican importantes esfuerzos a promover narrativas favorables, invirtiendo en diplomacia pública, «poder blando» y, cada vez más, en manipulación digital. Las redes sociales son hoy las nuevas plazas públicas, los mercados de ideas contemporáneos donde se moldean los pensamientos. Un aluvión de tuits, repetidos con diferentes formas durante cierto tiempo, pueden convencer a una persona de casi cualquier cosa. Los mensajes recibidos en una aplicación de mensajería por parte de un pariente en quien confiamos

nos hacen bajar la guardia ante su contenido. Al hacer *scroll* en nuestras pantallas, somos bombardeados con imágenes, memes, textos… que van forjando la manera en la que percibimos el mundo. Poder dar forma a este proceso supone un poder inmenso.

En este contexto, prácticamente todos los ejércitos profesionales y todos los servicios de inteligencia dignos de tal nombre poseen algún tipo de capacidad de influencia psicológica. Gran parte de sus capacidades estarán ya proyectadas hacia las redes y las nuevas tecnologías. En España, por ejemplo, el Ejército de Tierra cuenta con el Regimiento de Operaciones de Información n.º 1, con sede en Valencia, cuya misión es apoyar las misiones en el extranjero buscando «influir en las mentes para crear un entorno operacional alternativo menos letal, con el objetivo de disminuir las ocasiones de confrontación directa entre fuerzas militares y, a través de actividades de la información, alcanzar la superioridad». Según el ejército, «permitirá minimizar la necesidad de desplegar fuerzas sobre el terreno».[3]

Otros países de la OTAN, como Estados Unidos, Reino Unido, Italia, Alemania y Rumanía cuentan con unidades militares específicas con amplias capacidades.[4] Los principios mencionados van en línea con la doctrina de la Alianza Atlántica, que define las operaciones psicológicas como «información verídica y atribuible dirigida contra los comportamientos y actitudes del adversario».[5] Una definición bastante benigna, pues excluye la desinformación o la manipulación digital. Eso no quiere decir que algunos estados de la OTAN no recurran a estas técnicas, o que no existan otros actores dedicados a dichas prácticas de las que un gobierno puede echar mano cuando no quiere implicar a sus fuerzas armadas. Los enemigos de Occidente, desde luego, no tienen tantos escrúpulos.

El doctor Steve Tatham, oficial de la Marina Real británica durante veinticinco años, la mayoría de ellos trabajando en operaciones cognitivas, describe en su libro *Operaciones de Información* que «el ejército ha aprendido, a través de amargas experiencias, que las

falsedades y mentiras serán casi siempre desenmascaradas de forma invariable, y que eso en realidad produce resultados bastante menos exitosos que la verdad». Lo cual no significa que no se haga en ocasiones.

En 2011, la revista *Rolling Stone* reveló que William Caldwell, un teniente general de tres estrellas destinado en Afganistán, había ordenado a su equipo de operaciones de información que trabajasen para manipular a un grupo de senadores estadounidenses que iban a viajar al país, para convencerles de que asignasen más recursos a la misión. «¿Cómo consigo que estos tipos nos den más gente? ¿Qué tengo que plantar en sus cabezas?», preguntó Caldwell a sus hombres, a quienes encargó «un análisis en profundidad de los puntos de presión que podían usarse para influir en la delegación para obtener más fondos».[6] Uno de los responsables del equipo se negó: «Mi trabajo en operaciones de guerra psicológica es jugar con las cabezas de la gente, hacer que el enemigo se comporte de la manera que queremos que lo haga», le diría después el teniente coronel Michael Holmes, líder de la unidad, a *Rolling Stone*. «Tengo prohibido hacerle eso a nuestra propia gente. Cuando me pides que intente usar esas habilidades en senadores y congresistas, estás cruzando la línea», declaró.[7]

Como resultado, Caldwell tomó represalias contra Holmes, quien recibió una reprobación oficial que manchó su hoja de servicios. La publicación del artículo llevó al comandante supremo de las fuerzas en Afganistán, el general David Petraeus, a ordenar la apertura de una investigación oficial. El escándalo resultante prueba que los riesgos de exposición en este tipo de operaciones son reales.

Existe una enorme diferencia entre la diplomacia pública y la manipulación cognitiva. Mientras la primera es una expresión legítima de la visión que un estado o gobierno tiene sobre sí mismo y sobre el mundo, y busca cómo mostrarla, la segunda intenta retorcer la realidad para vender una imagen falseada que le permita alcanzar sus objetivos. Televisiones de titularidad estatal como BBC, Deutsche

Welle, France 24 o la versión en inglés de Al Jazeera son órganos de diplomacia pública, verdaderos medios de comunicación que tienen en mente los intereses de sus países, pero que proporcionan información real siguiendo criterios periodísticos. Por contra, RT, Hispan TV o Telesur no lo son, porque su propósito no es informativo, sino manipulativo y, en algunos casos, subversivo.

El caso de RT es clarísimo, basta con analizar cómo enfoca los temas sobre inmigración: mientras su cadena en castellano, dirigida a audiencias mayormente progresistas en España y Latinoamérica, critica que la Unión Europea traicione sus valores permitiendo que miles de migrantes se ahoguen en el Mediterráneo,[8] la página en alemán, cuyo público es sobre todo de ultraderecha, se rasga las vestiduras por cómo la UE permite que Europa se llene de inmigrantes que van a destruir «los valores cristianos» del continente.[9] Cada versión nacional de RT amplifica aquellos movimientos con mayor potencial desestabilizador: los Chalecos Amarillos en Francia, los *Querdenker* o negacionistas del COVID-19 en Alemania, la llamada «Caravana de la Libertad» contra las restricciones de la pandemia en Canadá…[10] Algo similar cabe decir de los otros medios citados, que no trabajan conforme a verdaderos estándares periodísticos y donde no existen muchos de los principios básicos de la profesión, como es el caso de una mínima pluralidad de voces.

Las autocracias, por contra, actúan en dos dimensiones: la nacional, suprimiendo o atacando cualquier discurso que pueda perjudicar al régimen, y la internacional, imponiendo sus narrativas en el resto del mundo. Por eso tienden a desarrollar formidables aparatos de propaganda y desinformación, adaptando sus estrategias a las diferentes audiencias. Unos mecanismos que evolucionan en el tiempo, con los cambios globales y las necesidades de cada momento.

Gran parte de esta manipulación tiene lugar en el ámbito digital. Por eso muchos países han desarrollado lo que el Instituto de Internet de Oxford denomina «cibertropas», que define como «equipos

gubernamentales, militares o políticos dedicados a manipular a la opinión pública en las redes sociales».[11]

En 2017, esta institución publicó el primero de una serie de informes anuales sobre el estado global de la manipulación digital. Ese primer año, documentó actividades en 28 países.[12] En 2019 eran 70,[13] y en 2020, el último año en el que Oxford publicó sus documentos, la cifra subía a 81.[14] Nada hace pensar que no haya seguido creciendo desde entonces. En este capítulo nos ocuparemos exclusivamente de las relacionadas con estados y gobiernos.

«Los regímenes autoritarios no son los únicos ni los mejores en la manipulación organizada de las redes sociales. Los primeros informes sobre implicación gubernamental en alterar la opinión pública implican a democracias, y las nuevas innovaciones en tecnologías de comunicación política a menudo vienen de partidos políticos y emergen durante elecciones de alto perfil», dice el instituto. «Con el tiempo, el modo primario de organizar las cibertropas ha pasado de implicar a unidades militares que experimentan con la manipulación de la opinión pública en las redes sociales a empresas de comunicaciones estratégicas que firman contratos con gobiernos para campañas en redes sociales», añade.

Desde sus inicios, los chats y foros de internet se convirtieron en objeto de interés para los servicios de inteligencia, que monitorizaban diálogos e introducían mensajes interesados para reconducir las conversaciones. Las primeras alegaciones que hemos podido documentar sobre grupos de propagandistas organizados en estos espacios aparecieron en la publicación rusa *Vestnik* en 2003, lo que convertiría a Rusia en pionera de estas prácticas.[15] Pero pronto tendría un alumno aventajado.

ISRAEL, LOS INNOVADORES

Los israelíes aprendieron por las malas. A pesar de ser maestros en la llamada *Hasbará* —literalmente, «explicación», como se conoce a las

acciones de diplomacia pública destinadas a contarle al mundo la versión israelí de los hechos—,[16] la irrupción de las redes y la atomización de voces que habían traído a principios del siglo xxi habían supuesto una sorpresa desagradable para las autoridades del país.

En 2007 se publicó el Informe Winograd, que criticaba duramente al Gobierno israelí por su fracaso ante las audiencias internacionales durante las operaciones militares de los años previos, como Escudo Defensivo (2002), Días de Penitencia (2004), Lluvia de Verano (2006) o la guerra del Líbano de ese mismo año. La respuesta fue la creación de una nueva organización, la Dirección Nacional de Información (NID), dependiente de la oficina del primer ministro. Este organismo pronto entraría en acción durante la Operación Plomo Fundido (2009), si bien los abundantes daños colaterales entre la infraestructura y los civiles de Gaza acabaron pesando más que las operaciones de información israelíes.[17] La imagen del país quedó muy dañada.

Israel no tiró la toalla, y desarrolló herramientas innovadoras para obtener la supremacía cognitiva en futuros conflictos. El Ministerio de Absorción e Inmigración anunció la creación de un «ejército de blogueros» entre los judíos venidos de todo el planeta, para que llevasen los mensajes de Israel a «webs antisionistas» en inglés, francés, español y alemán.[18] Por su parte, el Ministerio de Exteriores expuso planes para reclutar a ejércitos de voluntarios pagados, que posteasen respuestas proisraelíes en páginas de todo el orbe, como un escuadrón de «guerra en internet». Los voluntarios serían jóvenes que hablasen idiomas y estudiasen Comunicación, Ciencias Políticas o Derecho. O israelíes con experiencia militar conseguida en unidades de información.[19] Una iniciativa similar fue anunciada de nuevo en 2013.[20] Del mismo modo, en 2010, dos grupos sionistas iniciaron cursos de formación sobre cómo editar la Wikipedia para redactarla de un modo que favoreciera a Israel.[21]

Por último, la organización Give Israel Your Support (GIYUS) empezó a distribuir una aplicación llamada Megaphone, usada por primera vez durante la guerra del Líbano de 2006, que detectaba cada vez que un artículo o reseña sobre Israel era publicado en internet. El software permitía visualizar el artículo y escribir una respuesta proisraelí. En pocas semanas, 50.000 personas la descargaron.[22] Este tipo de aplicación ha tenido diferentes encarnaciones, y en posteriores versiones ha incluido un argumentario sobre qué responder a cada alegación del adversario. La última es una herramienta llamada Words of Iron («Palabras de hierro»), que permite amplificar los mensajes proisraelíes y copiar y pegar respuestas en las cuentas de otros usuarios, generando una respuesta masiva. Ha sido desplegada durante la última guerra de Gaza.[23]

RUSIA, LOS MAESTROS

En 2013, durante una reunión del Consejo de Seguridad, el presidente Vladímir Putin dijo: «Los ataques de información ya se están usando para resolver problemas político-militares». Es más, según los expertos, «su poder de golpear puede ser incluso mayor que el de las armas convencionales».

No es de extrañar que Rusia sea uno de los países que más esfuerzos y recursos ha dedicado a las operaciones de influencia, desinformación y manipulación cognitiva. Entre sus fuerzas militares más destacadas está la Unidad 54777, también conocida como el 72º Centro Especial de Servicios y el Servicio de Información y Comunicación Extranjera del Directorio Principal del Estado Mayor. Se cree que está comandado por el viceministro de Defensa, el general Andrey Kartapalov, y que habría jugado un papel esencial en la operación de engaño llevada a cabo durante la invasión de Crimea en 2014, en la que el despliegue de «hombrecillos verdes» sin distintivos militares, acompañado de una tormenta de mensajes contradictorios y deliberadamente equívocos para sembrar la confusión, dificultaron la

respuesta internacional.[24] Otras fuentes citan al coronel Aleksandr Vladimirovich Osadchuk como el responsable del grupo. La unidad 26165, más especializada en ciberataques, también habría participado en operaciones de hackeo pero con un componente cognitivo, como la interferencia en las elecciones de Estados Unidos.[25] Rusia cuenta también con las célebres «granjas de trols». Durante más de una década, eran privadas, propiedad del ya mencionado empresario Yevgueni Prigozhin, que alquilaba sus servicios al Kremlin, pero, tras la rebelión del Grupo Wagner, han pasado a estar bajo control estatal, como veremos en el capítulo siguiente.

En la concepción rusa, la información cumple una función militar. Margarita Simonyan, la directora del grupo estatal de comunicación Rossiya Segodnya, al que pertenecen RT y Sputnik, así lo ha declarado explícitamente en diversas ocasiones.[26] Rusia necesita a RT «igual que necesita un ministerio de Defensa». «El arma de la información, por supuesto, se utiliza en momentos críticos, y la guerra siempre es un momento crítico. Y es una guerra. Es un arma como cualquier otra».[27] Por ese motivo, RT está incluida en la lista oficial de organizaciones clave de importancia estratégica para la Federación Rusa y tiene un presupuesto anual multimillonario. En 2020, por ejemplo, la partida asignada a este canal fue de unos 325 millones de euros, un porcentaje del presupuesto estatal desproporcionado, si tenemos en cuenta que, en 2021, este fue de unos 1.300 millones de euros.[28]

Lo más interesante es que, incluso antes de que RT fuese bloqueada en la Unión Europea y otros países, las audiencias de sus emisiones eran ridículas. Pero ese no es el tema. A menudo, el verdadero propósito, tanto de RT como de Sputnik, es simplemente crear contenidos que después pueden ser difundidos masivamente gracias a los gigantescos ejércitos de cuentas, bots y trols en redes sociales.[29] En ese sentido, la prohibición de estos dos medios en la UE es probablemente contraproducente, puesto que legitima una narrativa de victimización y censura al tiempo que no resuelve nada: tanto RT como Sputnik han cambiado las URL de sus webs, o han creado

páginas espejo con exactamente el mismo contenido bajo un dominio diferente. Eso les permite evadir las restricciones, y que sus artículos y vídeos puedan seguir siendo compartidos libremente.

IRÁN, LOS ALUMNOS AVENTAJADOS

Irán ya operaba falsas páginas de Facebook y X/Twitter en inglés en 2014. En esa época, lanzó la página «Free Scotland 2014», destinada a promover la independencia escocesa en el referéndum de ese año. Llegó a superar los 20.000 seguidores y se convirtió en uno de los sitios web más populares de la causa. Otras páginas buscaban seguidores entre votantes progresistas en Reino Unido y Estados Unidos, preferiblemente jóvenes, a quienes contactaban con perfiles que se hacían pasar por seguidores del líder laborista británico Jeremy Corbyn o del demócrata estadounidense Bernie Sanders. Les bombardeaban con mensajes contra Israel y Arabia Saudí, y a favor de Palestina y de algunos elementos de la política exterior de Washington favorable para Teherán, como el acuerdo nuclear que la Administración Obama firmó con Irán en 2015.[30] La operación, en la que se llegaron a crear más de 650 páginas y cuentas, estuvo en marcha hasta que estas plataformas la desmantelaron en 2018.[31]

Desde entonces, Irán ha ido creando un aparato de influencia más amplio y sofisticado,[32] que incluye un conjunto de medios nacionales e internacionales (Press TV en inglés o Hispan TV en español), y complejos sistemas de acción en redes. El régimen iraní, además, debe controlar la información interna.

Cuando se produjeron las negociaciones con Estados Unidos que condujeron al acuerdo nuclear de 2015, Facebook y X/Twitter detectaron que el número de cuentas falsas iraníes crecía exponencialmente, probablemente porque influir en las audiencias internacionales era una prioridad. Según un informe del Atlantic Council, las cuentas se usaban para blanquear propaganda estatal iraní ante audiencias desprevenidas acerca de su verdadero origen. En

2020, Facebook había identificado aproximadamente 2.200 páginas y grupos que afectaban directamente a seis millones de usuarios, mientras que X/Twitter había encontrado 8.000 cuentas, que habían emitido unos 8,5 millones de mensajes.[33] El año anterior, Facebook había eliminado una red de cuentas que, por primera vez, operaba en España.[34]

ESTADOS UNIDOS, LOS PODEROSOS

El ejército estadounidense cuenta con múltiples unidades de operaciones psicológicas, ordenadas jerárquicamente. En la parte superior, supervisando a las demás, están el 4º y 8º Grupo de Operaciones Psicológicas, los dos con base en Fort Bragg, Carolina del Norte. Por debajo del primero se sitúan el 3er, 6º, 7º y 8º Batallón de Operaciones Psicológicas, mientras que el segundo supervisa al 1er, 5º y 9º Batallón. En total, unas 6.000 tropas de operaciones, la mayor concentración de militares profesionales dedicados a esta actividad en todo el mundo, con la posible excepción de China, cuyas cifras se desconocen. Han participado en misiones en Vietnam, República Dominicana, Panamá, Irak, Somalia, Haití, Liberia, Ruanda, Bosnia y los Balcanes, según la web del 4º Grupo.[35]

En contraste, apenas hay información fiable acerca de las actividades ofensivas de la CIA y otros departamentos de inteligencia de Estados Unidos en la guerra cognitiva. A la naturaleza clandestina de las operaciones se suma que el gobierno recurre regularmente al uso de contratistas en todos los ámbitos, y las operaciones de información e influencia no son una excepción, lo cual complica más la atribución. Pueden existir huellas forenses en internet, pero es complicado asegurar que detrás de una campaña específica está el Estado. En las pocas ocasiones en las que se ha confirmado la responsabilidad de una agencia gubernamental, ha sido por una investigación periodística o por una filtración interna.

Sucedió en 2011, cuando el diario *The Guardian* averiguó que el CENTCOM (la subdivisión del Departamento de Defensa a cargo de Oriente Medio) había firmado un contrato con una empresa californiana llamada Ntrepid para desarrollar un software de «servicios de gestión de personajes online» con propósitos de manipulación digital. El sistema permitiría a cada soldado estadounidense controlar hasta diez identidades falsas, que debían contar con un pasado convincente, una historia y detalles de apoyo. Debía ser utilizado por medio centenar de controladores desde estaciones de trabajo en territorio norteamericano, presumiblemente en la base aérea de McDill en Tampa, Florida. El contrato formaba parte de un programa llamado Earnest Voice, desarrollado inicialmente por el Pentágono en Irak como herramienta de guerra psicológica contra la presencia online de Al Qaeda, pero que se había expandido hasta convertirse en un programa de 200 millones de dólares de lucha contra el yihadismo en Pakistán, Afganistán y Oriente Medio en general.[36]

El artículo de *The Guardian* pasó relativamente desapercibido, pero la operación volvió a salir a la luz en 2022, cuando la firma de análisis de redes Graphika y el Observatorio de Internet de Stanford publicaron un informe que destapaba actividades de esa misma red, descubierta por Facebook y X/Twitter.[37] Las herramientas y las audiencias eran similares, pero no los objetivos: en lugar de luchar contra los mensajes yihadistas, buscaba contrarrestar las narrativas rusas sobre Ucrania, entre otras.[38] El incidente motivó una revisión de este tipo de operaciones por parte del Pentágono.[39]

Otra operación de influencia, esta vez a cargo de la CIA, fue revelada en marzo de 2024 por Reuters. Según la agencia de noticias, el presidente Trump había autorizado en 2022 a la agencia a lanzar una campaña clandestina en redes para volver a la opinión pública china contra su Gobierno. La CIA creó un pequeño grupo de operativos que, utilizando identidades falsas, difundieron mensajes negativos sobre Xi Jinping y su régimen, a la vez que filtraban

información de inteligencia a medios de comunicación de otros países. De acuerdo con las fuentes del artículo, que Reuters identificó como «tres antiguos funcionarios estadounidenses con conocimiento de esta operación altamente clasificada», los mensajes estaban basados en hechos veraces, aunque su difusión se realizaba mediante cuentas falsas que fingían ser locales, para facilitar la penetración.

«El lanzamiento de mensajes de forma encubierta permite a Estados Unidos implantar ideas en países donde la censura puede prevenir que esa información salga a la luz, o en áreas donde las audiencias no le darían mucha credibilidad a las declaraciones del Gobierno estadounidense», afirma Loch Johnson, un politólogo de la Universidad de Georgia que estudia el uso de este tipo de tácticas, entrevistado para el artículo.[40] La operación tenía un componente más ambicioso, pues permitía pasar a la acción contra Pekín no solo en la propia China, sino también en aquellos países donde competía por influencia, como el Sudeste Asiático, África y el Pacífico Sur. El proyecto, de hecho, había sido lanzado como respuesta a lo que Washington describía como «la creciente agresividad» de una China que llevaba años desplegando acciones encubiertas contra Estados Unidos.

CHINA Y LA PANDEMIA

Durante mucho tiempo, la estrategia internacional del Partido Comunista Chino fue controlar el discurso en el exterior, tratando de que no se hablase de los temas que no le interesaban, como el Tíbet, Xinjiang, Hong Kong o los derechos humanos. Esta preocupación era especialmente acuciante de cara a las comunidades chinas en el extranjero, por lo que las redes sociales chinas utilizadas por la diáspora, como Weixin o WeChat estaban, y siguen estando, férreamente monitorizadas y censuradas.[41] El Gobierno también utilizaba mecanismos de presión para intentar que estos asuntos no recibiesen el escrutinio que grupos activistas y algunos países

demandaban, y que no se convirtiesen en obstáculos para sus relaciones de «amistad» con otros estados.

A partir de 2020 se produjo un cambio: la aparición de los denominados «Wolf Warriors», cuentas oficiales de diplomáticos a quienes se dio instrucciones, o como mínimo se toleró, para que interactuaran de forma agresiva con otros usuarios.[42] La pandemia del COVID-19 llevó a Pekín a lanzar auténticas ofensivas para convencer al mundo de su eficiencia para combatir el virus, defendiéndose de las acusaciones de negligencia en la gestión de los primeros casos y promoviendo teorías de la conspiración. Ese año, Xi Jinping habló de la lucha contra esta enfermedad como de una «guerra total», un término que saltó a los medios y que implicaba la movilización de toda la sociedad. Las autoridades locales de numerosos centros urbanos establecieron Centros Internacionales de Comunicaciones encargados de «contar bien la historia de China», uno de los eslóganes centrales de la doctrina de información.[43]

Pekín dispone tanto de unidades militares profesionales como de cibertropas medio *amateurs*. Los primeros componen una rama autónoma del ejército, la Fuerza de Apoyo de Información, creada en abril de 2024 en sustitución de la Fuerza de Apoyo Estratégico,[44] una reestructuración que obedece a la adaptación derivada de las lecciones aprendidas durante la guerra de Ucrania.[45] China tiene, además, uno de los grupos organizados de trols más veteranos del mundo, el «partido 50-cent», apodados así por la presunta remuneración (50 céntimos de renminbi) que recibían cada vez que *posteaban* un comentario en un foro de internet.[46] Su tarea no es tanto defender al gobierno de críticas como desviar la conversación virtual cada vez que aparecen temas sensibles que se prestan al descontento con el gobierno. En los últimos años, las características de los trols de China han ido evolucionando, con fenómenos más novedosos como los *ziganwu*, blogueros patrióticos que se dedican a difundir narrativas antioccidentales.[47]

Tampoco sabemos demasiado sobre las operaciones de guerra cognitiva del Reino Unido, pero el ejército británico cuenta con la 77ª Brigada, en Hermitage, Berkshire.[48] Está compuesta por soldados instruidos en operaciones psicológicas y manejo de las redes sociales, y el propósito declarado de esta institución es llevar a cabo acciones de «guerra no letal».[49] Aunque su cometido principal es participar en acciones de apoyo a las misiones del ejército en el exterior, como la de Afganistán —hasta la retirada occidental—, esta unidad estuvo envuelta en una intensa polémica en 2023 después de que uno de sus miembros filtrase al diario sensacionalista conservador *The Daily Mail* que había estado implicada en la monitorización de redes sociales durante la pandemia.[50]

Pero, además, las revelaciones de Edward Snowden en 2014 mostraron que el GHCQ, la versión británica de la NSA, se dedicaba no solo al espionaje de comunicaciones, sino también a la manipulación de la conversación en redes sociales, a través de una unidad secreta: el Grupo Conjunto de Investigación de Inteligencia de Amenazas (JTRIG, por sus siglas en inglés). Según los documentos filtrados entonces, el JTRIG tenía capacidades para alterar encuestas online, inflar las visitas de ciertas páginas web, amplificar mensajes en YouTube, censurar contenidos de vídeo considerados «extremistas», acceder a fotografías privadas de objetivos en Facebook, y apropiarse de cualquier dirección de correo electrónico y enviar emails desde allí.

Además, una presentación realizada para el resto de miembros de la alianza Five Eyes —mediante la que Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda comparten información de inteligencia—, mostraba cómo el JTRIG podía arruinar la reputación de cualquier individuo mediante la difusión de información negativa sobre esa persona, creando blogs en los que una falsa víctima acusase al objetivo de algún tipo de abuso, o incluso enviando mensajes de

carácter sexual a contactos en su nombre. Sin duda, un poder muy inquietante, que requiere de la supervisión de órganos democráticos.

FRANCIA, *TROLL* CONTRA *TROLL*

Francia también ha recurrido a la desinformación y a la manipulación digital, sobre todo durante los años de su presencia reciente en el Sahel.[51] En 2020, Facebook desmanteló una operación de información dirigida a promover mensajes pro franceses y antirrusos en la República Centroafricana y Mali; y en menor medida, en Níger, Burkina Faso, Argelia, Costa de Marfil y Chad. Una vez más, las personas detrás de las cuentas falsas se hacían pasar por locales.

«Publicaban principalmente en francés y árabe noticias y acontecimientos de actualidad, incluidas las políticas de Francia en el África francófona, la situación de seguridad en varios países africanos, denuncias de una posible interferencia rusa en las elecciones en la República Centroafricana (RCA), comentarios de apoyo al ejército francés y críticas a la participación de Rusia en la RCA. Algunas de estas cuentas también comentaban el contenido que criticaba a Francia publicado por una de las operaciones rusas», subrayó Facebook en su informe de actividad. «Aunque quienes están detrás de ello intentaron ocultar su identidad y coordinación, nuestra investigación encontró vínculos con individuos asociados con el ejército francés», añadía.[52]

Por esas fechas, las cuentas falsas de origen galo se enzarzaron en una especie de guerra virtual con sus equivalentes rusos, discutiendo y denigrando los contenidos que colgaban los otros, en lo que la firma de análisis Graphika calificó de «el primer caso documentado de interacción "*troll* contra *troll*" a gran escala».[53]

El Gobierno francés, molesto con Facebook, abrió una investigación, pero no desmintió las acusaciones.[54] A esas alturas, tras la acumulación de reveses en el Sahel, ya soplaban otros vientos en París. En octubre de 2021, la ministra de Defensa gala Florence Parly

presentó la nueva «doctrina militar de lucha informática de influencia», señalando que desde ese momento Francia pasaba oficialmente a la ofensiva en el campo de las operaciones de información, especialmente en el Sahel. Eso sí, el territorio nacional quedaba excluido de este tipo de campañas. En todo caso, como hemos visto, no les sirvió de mucho.

OTROS PAÍSES

Hay muchos otros países con importantes capacidades de manipulación cognitiva, como Venezuela, que además de una serie de medios con alcance internacional, como la cadena Telesur, cuenta con ejércitos de trols que, en ocasiones, subcontratan otros estados como Rusia.[55]

Aún más interesante es el caso de Marruecos, que posee capacidades muy superiores a las que sugeriría su carácter de potencia mediana. Según un estudio de la publicación *Monitor Disinfo*, el aparato de medios estatales publica con frecuencia artículos y reportajes televisados con información manipulada apoyando las narrativas del Gobierno. «Al mismo tiempo, el uso de bots y cuentas falsas en plataformas como X/Twitter y Facebook amplifican el alcance de las noticias falsas, creando la ilusión de apoyo popular. Esa combinación de tácticas permite a Marruecos alcanzar una audiencia más amplia y tener un impacto más profundo en la percepción pública y la estabilidad regional». De acuerdo con esta publicación, «a nivel interno, la propagación de noticias falsas permite al Gobierno mantener un control más estricto sobre la población y suprimir voces disidentes. Las noticias falsas sobre protestas, por ejemplo el movimiento 20F, justifican medidas represivas y desvían la atención de los problemas socioeconómicos subyacentes. A nivel regional, la desinformación dirigida a países vecinos, como Argelia y España, busca desestabilizar estos países y generar ventajas geopolíticas para Marruecos. La difusión de rumores sobre crisis políticas y sociales en

Argelia no solo crea confusión y descontento, sino que también sirve para desviar la atención de los problemas internos de Marruecos. Exactamente igual con las acciones desarrolladas sobre los movimientos independentistas en España».[56]

Marruecos también financia una llamativa red de portales noticiosos en diferentes idiomas, cuyo principal propósito parece ser defender que el Sáhara Occidental es un territorio marroquí. A principios de 2025, había empezado a recurrir a *influencers* extranjeros para vender una imagen idealizada del «Sáhara marroquí».[57]

LA FALSA NEUTRALIDAD DE LAS PLATAFORMAS

A las empresas de redes sociales, tanto las de Silicon Valley como a sus competidoras chinas y de otros países, les gusta presentarse como meras herramientas a disposición del usuario. El mero término «plataformas» —como YouTube empezó a autodescribirse en 2006— ya tiene unas connotaciones de neutralidad. Pero la realidad está lejos de ser así. Con sus acciones —o inacciones— determinan qué contenidos siguen en sus páginas, cuáles deben ser retirados, cuáles promovidos y a cuáles se les debe aplicar una censura disimulada, como la supresión silenciosa o *shadow banning*,[58] una técnica que hace que las publicaciones de un usuario sean invisibles para los demás, sin que él lo sepa porque puede seguir viéndolas.[59]

Las plataformas, en suma, deciden qué les llega a los usuarios, lo que supone una enorme responsabilidad. Adoptan medidas que favorecen a unos actores frente a otros, con importantes consecuencias. Por ejemplo, durante la guerra de Gaza, Instagram y Facebook censuraron múltiples contenidos propalestinos, según denunció Human Rights Watch en un informe en 2023.[60] Al Jazeera logró entrevistar a un anónimo ingeniero de Meta, quien declaró que muchas cuentas que mostraban el impacto de la ofensiva israelí sobre los civiles palestinos habían sido clasificadas como contenedoras de

«actividad sexual o desnudo» o «pornográficas», lo que limitaba enormemente su alcance.

Una de ellas era la de Moataz Azaiza, un fotógrafo palestino criado en un campo de refugiados de Gaza y cuya cuenta de Instagram, en la que mostraba imágenes de desplazamientos forzosos, masacres y privaciones de la población, contaba con 17 millones de seguidores. En octubre de 2024, Azaiza denunció que el 40% de sus publicaciones habían sido eliminadas o censuradas desde el inicio de la guerra el año anterior.[61] Del mismo modo, hay indicios sólidos de que, tras su adquisición por Elon Musk, X/Twitter está disminuyendo la visibilidad de los tuits sobre Ucrania.[62]

Las empresas de Silicon Valley han tratado a toda costa de que las diferentes regulaciones las consideren exentas de responsabilidad legal por lo que los propios usuarios cuelgan en sus aplicaciones. A diferencia de un medio de comunicación, no existe un equipo editorial profesional que decida sobre el contenido. Pero al menos se les puede y se les debe exigir actuar sobre este una vez que ya está colgado. No siempre lo hacen, como ya veremos. Pero, cuando quieren, pueden.

El 3 de febrero de 2015, Estado Islámico asesinó al piloto jordano Muath Al Kasasbeh, capturado por los yihadistas y posteriormente quemado vivo dentro de una jaula. El vídeo de la brutal ejecución, filmado con más de una decena de cámaras diferentes a alta resolución, fue difundido en YouTube, donde todo el mundo pudo verlo, yo mismo incluido. En aquella época, era corresponsal del diario *ABC* en Estambul y seguía atentamente todo lo relacionado con ISIS. Me pareció muy chocante que semejante salvajada estuviese disponible en una plataforma como YouTube.

La empresa lo retiró, pero el episodio marcó el inicio de una fase de problemas para las plataformas: el movimiento yihadista internacional las estaba utilizando no solo para su propaganda, sino también para sus atrocidades. Como respuesta, las redes desarrollaron sistemas automatizados de detección de dichos contenidos, que empezaron a ser eliminados sistemáticamente.[63] Supuso una

importante inversión económica y en innovación, pero demostró que tienen las capacidades para regular. De hecho, tras convertirse en el propietario de X/Twitter en 2022, Musk eliminó muchas de estas salvaguardas. Como consecuencia, los *posts* yihadistas vuelven a proliferar en su red.

Los algoritmos tampoco son inocuos, aunque los responsables de las plataformas pretendan lo contrario. Es improbable que YouTube tenga ningún interés en conseguir que sus usuarios se conviertan en extremistas. Sin embargo, debido a un modelo de negocio que premia ciertas formas de consumo de vídeo frente a otras, el algoritmo acaba recomendando sistemáticamente contenidos cada vez más extremos, convirtiendo la plataforma en una fuente de radicalización. En 2016, la socióloga estadounidense Zeynep Tufekci llevó a cabo un experimento, analizando el tipo de vídeos que YouTube le iba recomendando sobre cada uno de los temas que veía, y se dio cuenta de que el patrón era siempre recomendar contenidos de mayor intensidad. Si veía un vídeo sobre vegetarianismo, le conducía a otros sobre veganismo. Si veía vídeos sobre correr, acababa en otros sobre ultramaratones. «Parece como si nunca fueras lo suficiente del "núcleo duro" para el algoritmo de recomendación de You-Tube. Este promueve, recomienda y disemina vídeos de una forma que parece subir la apuesta constantemente», escribió Tufekci en *The New York Times*. Lo mismo sucedía, y sucede, con los clips de contenido político: «Dado que tiene alrededor de mil millones de usuarios, YouTube puede ser uno de los instrumentos de radicalización más poderosos del siglo xxi», sentenció la socióloga.[64]

Los algoritmos pueden ser aprovechados y manipulados por actores hábiles para que ciertos contenidos dominen el espacio informativo. Pero no se trata de un escenario neutral. Pensemos en ellas como en un gigante sobre cuya espalda varios ejércitos se enfrentan sin piedad. Ese gigante es el escenario en el cual se desarrolla la batalla, y también es capaz de hacer sus propios movimientos autónomos. Dependiendo de cuál sea su origen, avanzará en una

dirección u otra, lo que beneficiará a algunos de los bandos en liza y perjudicará a otros.

Las plataformas, además, son sensibles a cuanto les piden sus gobiernos. X/Twitter, por ejemplo, hizo una excepción en su política de no permitir redes coordinadas no auténticas a petición del Pentágono, que pidió a sus directivos que no tumbasen las cuentas falsas que habían desplegado para campañas de influencia en Oriente Medio. Según documentos consultados por la publicación *The Intercept*, en julio de 2017 un oficial del CENTCOM llamado Nathaniel Kahler envió un correo al equipo de políticas públicas de X/Twitter pidiendo la introducción en una «lista blanca» de una serie de cuentas en árabe que el ejército usaba «para amplificar ciertos mensajes» en la región. «Tenemos algunas cuentas que no están indexando en los *hashtags*, quizá porque han sido designadas como bots. Algunas de ellas habían logrado un seguimiento real y esperamos salvarlo», escribió Kahler. La empresa accedió a la petición.[65]

Algo similar sucedió con Telegram. Durante mucho tiempo, su creador, artífice también de la plataforma VKontakte (hoy VK), el «Facebook ruso», se jactaba de su impenetrabilidad e independencia, lo que había convertido esta *app* de mensajería en un lugar de refugio para yihadistas y sindicatos del crimen.[66] En 2018, el FSB, el servicio de inteligencia interior ruso, presionó a Durov para que facilitase las claves de encriptación de los usuarios rusos, pero este se negó. El Kremlin prohibió Telegram en Rusia, y el regulador de telecomunicaciones del país, Roskomnadzor, trató de implementar un bloqueo que solo tuvo un éxito parcial.

Mientras tanto, algo pasó. En junio de 2020, el Gobierno ruso anunció que había llegado a un acuerdo con Telegram para desbloquear la aplicación, aunque se desconocen los términos del pacto. Que la relación entre las autoridades rusas y la empresa había cambiado radicalmente le quedaba claro a cualquiera que esos días entrase en las páginas de Sputnik o RT, donde aparecía un *banner* en la parte inferior de cada artículo que animaba a los lectores y

espectadores a suscribirse al canal de Telegram de ambos medios. De repente, los disidentes rusos se encontraron con que sus conversaciones podían ser leídas por los servicios de seguridad.[67]

La situación parece haber cambiado de nuevo tras el arresto de Durov en Francia.[68] La empresa ha empezado a colaborar con las autoridades policiales de todo el mundo,[69] entregando información sobre potenciales delitos y sus perpetradores.[70] La detención provocó un revuelo en Rusia, por temor a que el empresario revelase información que permitiese penetrar las comunicaciones de sus militares en Ucrania,[71] que utilizaban esta *app* para contactar unos con otros en el campo de batalla debido a los problemas de sus propios sistemas de comunicación.[72]

Por este tipo de problemas, muchos países buscan cierto grado de soberanía tecnológica. Irán ha desarrollado un ecosistema de redes sociales propias, como Virasty, una especie de X/Twitter local que imita incluso la interfaz de esta. Durante las elecciones presidenciales de julio de 2024, el Ministerio de Tecnologías de la Información publicó una lista de las aplicaciones nacionales con las que los candidatos podían beneficiarse de servicios relacionados con los comicios,[73] que, además de Virasty, incluía otras como Eitaa, Rubika, Bale o iGap.

Pero si hay un país que destaque es China. A diferencia de las iraníes, muchas de sus aplicaciones se han expandido por todo el planeta, convirtiéndose en poderosas herramientas de influencia en el extranjero, como sucede con TikTok. Está demostrado que esta plataforma suprime contenidos que el Partido Comunista Chino considera indeseables, aplicando técnicas como el *shadow banning*, y promoviendo otros favorables al régimen de Pekín. Por ejemplo, se han producido bloqueos de cuentas de ciudadanos estadounidenses que denuncian la existencia de campos de concentración para musulmanes uigures en Xinjiang. La censura no es total, y hay vídeos que no son bloqueados, pero otros muchos sí. Para evitar que otros

mensajes no autorizados puedan penetrar en el ecosistema informativo chino, los contenidos de TikTok no se traspasan a Douyin, y viceversa.

En 2023, la cadena de televisión France TV emitió un documental en el que entrevistaba a varios moderadores anónimos de la empresa en Francia, que confirmaban que Tik-Tok tiene la capacidad tecnológica de bloquear o invisibilizar un vídeo, aplicándole etiquetas que hacen que logre menos visualizaciones y el algoritmo lo detecte menos.[74] Esta plataforma fue también usada para distribuir vídeos de desinformación y propaganda contra Occidente durante la pandemia del COVID-19, ante el incremento de las tensiones entre China y Estados Unidos TikTok también recopila masivamente datos personales, mucho más que el resto de plataformas. Como el usuario puede pasar los vídeos a gran velocidad, cada dos segundos o menos, el algoritmo aprende muchísimo sobre su orientación sexual, su color favorito, qué música le gusta... Esto se suma al resto de información recogida mediante metadatos o a través de los comentarios, que revelan cosas como dónde vive y trabaja, quiénes son sus amigos, o si tiene amantes. Dado que la relación de esta *app* con el Gobierno chino parece definitivamente acreditada, la preocupación de muchos expertos es que Pekín pueda utilizar toda esa información para lanzar una campaña de influencia personalizada para cada usuario y provocar sucesos como un vuelco electoral.[75]

Como resultado, TikTok ha ido sufriendo una serie de restricciones y prohibiciones. En marzo de 2025, estaba completamente prohibida en la India, Afganistán, Kirguistán, Irán y Nepal,[76] mientras que la UE había vetado su uso en todos los aparatos del personal del Parlamento Europeo, la Comisión Europea y el Consejo de la UE, una medida similar a la aplicada a nivel estatal en una decena de países, de Australia al Reino Unido. Canadá había decretado, además, el cierre de las oficinas de la empresa, pero no había bloqueado la aplicación en sí. Mención aparte merece Estados Unidos, donde, después de un largo proceso político y legal, fue totalmente prohibida el 19 de enero de 2025. Al día siguiente, nada más inaugurar su segundo mandato, el

presidente Donald Trump decretó una exención de 75 días para permitir la venta de su sección a un cliente estadounidense.[77]

Las disposiciones de este tipo sirven para limitar el movimiento de estos gigantes. Pero, mientras tanto, los guerreros montados a sus espaldas siguen luchando.

3

¿PARA QUÉ SIRVE UN TROL?

Jessikka Aro recuerda muy bien cuándo comenzó su ordalía: el 15 de septiembre de 2014. Hasta ese momento, no era demasiado conocida en su país fuera del mundillo periodístico en el que se desenvolvía como reportera de *Yle*, la radiotelevisión pública de Finlandia. Pero todo cambió cuando empezó a investigar sobre el trabajo de los trols que operaban en las redes sociales, promoviendo narrativas favorables a Rusia y hostigando a aquellos que se atrevían a cuestionarlas. Aro publicó un *post* en la web de Yle pidiendo a aquellos lectores que hubiesen pasado por una experiencia así que la compartiesen con ella, sin mencionar a ningún *troll* por su nombre real. Pero eso bastó para ponerla en el punto de mira.

«Me convertí en el objetivo de informaciones falsas en medios en lengua rusa. Más de diez páginas web a la vez empezaron a publicar mentiras sobre mí», me contaría tres años después en un hotel del centro de Madrid. «Aseguraron que estaba recopilando una base de datos ilegal sobre los partidarios de [Vladímir] Putin en Finlandia para pasársela a Estados Unidos, y que mi lista y mis actividades suponían una persecución de opinión. Dijeron que trataba de fomentar el racismo contra los rusos en Finlandia y en el Báltico, que era una famosa agente de la OTAN. Hasta publicaron mi teléfono y mi dirección de correo electrónico».

La experiencia parecía haberle afectado profundamente. Había viajado a la capital española a mediados de junio para participar en un panel sobre «Influencia y desinformación rusa sobre el populismo en la Unión Europea». Parecía triste. Pero, a medida que me contaba su historia, se iba animando. La indignación le fue devolviendo el

color a su piel. «Empecé a recibir mensajes de odio y amenazas de todo el mundo rusoparlante. También me decían obscenidades. Llegué incluso a recibir una llamada de un número del Reino Unido, en la que solo escuché el sonido de un arma disparándome. Mientras tanto, los trols me atacaban en las redes sociales, cuestionando mi salud mental e investigando mi vida personal».

Aro detalló su calvario en un artículo titulado «Mi año como imán para los trols pro Rusia»[1] y, posteriormente, en su libro *Los* trols *de Putin*. Aporta elementos que en las entrevistas, tal vez por puro hartazgo, ha dejado de comentar. Por ejemplo, el papel que jugó el activista y escritor Johan Bäckman, conocido por sus posiciones prorrusas y su defensa de la rebelión en el este de Ucrania. «Al instante de publicar mi primera pieza […] Bäckman empezó a difundir información falsa sobre mí, principalmente en "agencias de noticias" rusas, pero también en sus cuentas de Facebook y X/Twitter. Su objetivo era atraer a trols y acosadores para que me atacasen, pero también señalarme como alguien de dudosa credibilidad antes de la publicación de los artículos que estaba preparando», escribió. En nuestra entrevista, añadió que «como resultado, fui estigmatizada en Rusia y Finlandia. Si buscas en el «Google ruso», Yandex, textos anónimos cuentan una historia de cómo soy un ejemplo del "racismo institucional occidental y el odio hacia Rusia"». Otros activistas también se presentaron en sus conferencias y las filmaron, editando el contenido para cuestionar cada una de sus afirmaciones. «El argumento de los trols estaba claro: los blogueros pagados pro Putin no existen», escribió irónicamente la periodista.

El trabajo de Aro amenazaba con exponer las actividades de las granjas de trols rusas en Finlandia, un país clave para Moscú, donde la opinión pública respecto a su vecina —con la que comparte una frontera de 1.340 kilómetros— estaba entonces muy dividida. La lista de agravios sufridos por la reportera se prolongó: memes ridiculizándola, acoso físico, seguimientos intimidatorios y vídeos paródicos: «Produjeron una canción profesional que me calificaba de

"*troll* de la OTAN", y hasta contrataron a una actriz para que me representase como el Capitán América», según me contó. No obstante, el momento más impactante sucedió en la primavera de 2015. A su teléfono llegó un SMS que pretendía haber sido escrito por su padre, fallecido dos décadas antes. Decía: «No estoy muerto, te estoy observando».

Ni siquiera entonces se detuvieron: en febrero del año siguiente, sus acosadores hicieron público que en 2002, cuando era una adolescente, Aro había sido condenada por posesión de drogas. Aunque se trataba de un asunto de pequeño consumo, que se saldó con apenas una multa de 300 euros, fue suficiente para que medios prorrusos como MV-Lehti publicasen historias con titulares como este: «La experta en información de la OTAN Jessikka Aro resulta ser una narcotraficante convicta».[2]

«Me presentaron como una especie de criminal, y llegaron a firmar que había sufrido daños cerebrales. También publicaron capturas de pantalla de las sentencias judiciales, que incluían mis datos personales y de salud. Ahora eran públicos y fueron usados para acosarme». El ataque se amplió en otros frentes: «Contactaron a mi jefe y le pidieron que me despidiera. Algunas personas se lo creyeron, y empezaron a verme como una amenaza. Incluso gente que me conoce resultó influenciada».

Años después, con cierta perspectiva, Aro trataba de tomarse el asunto con profesionalidad: «Como periodista, no puedo aceptar presiones. Está prohibido en nuestro código ético. Y también comprendo que una técnica de la guerra de la información es manipular los sentimientos para crear miedo y ansiedad, para impedirme informar sobre todo ello. Como he comprendido esto, me ha dado más perseverancia y fortaleza para perseguir esta historia, para seguir investigándola». Creía que había merecido la pena, puesto que su caso había generado una reacción en Finlandia. «Se han creado unidades especiales para contrarrestar el discurso de odio y la agitación. También he recibido mucho apoyo de la gente, incluso de

desconocidos. Han comprendido que, al apoyarme, están protegiendo a sus periodistas. Ahora el público es más consciente de cómo funcionan estas cosas», me dijo. Aunque queda la otra cara de la moneda: «A veces me siento cansada, y generalmente tengo miedo. Recibo amenazas de muerte, pero confío en la policía finlandesa para lidiar con ello. Al principio había decidido hacer solo un artículo, pero he hecho muchos más y los seguiré haciendo. Lo que me ha sucedido me ha enseñado que esto es algo realmente importante».

LA GRANJA DE TROLS DE SAN PETERSBURGO

La historia de Aro es significativa porque muestra al mismo tiempo dos elementos claves para la temática de este libro: cómo opera un ejército de trols, y qué implica convertirse en víctima. Pero, además, esta historia fue una de las primeras veces en las que se mencionó fuera de Rusia a un colectivo del que pronto se oiría hablar en todo el planeta: la Agencia de Investigación de Internet (IRA). O, como se la llamaría en todo el mundo, «la granja de trols de San Petersburgo».

Situada en un edificio administrativo de cuatro plantas sin distintivos en la puerta, la IRA nació como un proyecto de Yevgueni Prigozhin, el citado «chef de Putin». La granja era, pues, una iniciativa privada al servicio del Estado, que remuneraba generosamente a sus impulsores. En 2015, tenía unos cuatrocientos empleados, incluidos ochenta trols dedicados a manipular el clima político en Estados Unidos[3]

La existencia de la IRA fue desvelada por la periodista Lyudmila Savchuk, quien, durante dos meses y medio, se había infiltrado como trabajadora para documentar sus actividades. Savchuk, tras escuchar rumores sobre el lugar, había respondido a la llamada de un amigo que le había ofrecido un empleo «por el bien de la Madre Patria», y que le ayudó a superar la desconfianza inicial de los responsables. Al poco de empezar a trabajar, entendió cuál era el motor del proyecto: influir sobre una parte significativa de la población rusa, aquella

consciente de que la televisión actuaba como una herramienta de propaganda del Kremlin, y que, para evitarla, se informaba en internet y las redes sociales.[4]

Según Savchuk, la granja tenía su propia jerarquía, en cuya base estaban los encargados de escribir comentarios en las versiones digitales de los periódicos rusos. Por encima se situaban quienes replicaban esas tareas en las redes sociales. Por ejemplo, acusando a las principales figuras de la oposición de ser traidores o agentes de la CIA. Dado que muchos empleados solo tenían un nivel de educación básico, la IRA había contratado a un profesor de lengua rusa que les ayudaba a mejorar su redacción. Los trabajadores que hablaban inglés, como la propia Savchuk, eran destinados a secciones exclusivas, dirigidas a influir en audiencias internacionales.

Mientras trabajaba allí, la periodista publicó, con firma anónima, un artículo anónimo en el que aportaba evidencias sobre estas actividades. Pero, al ver que la granja movilizaba a sus trols para sembrar dudas sobre la veracidad de su información, Savchuk decidió abandonar el empleo y realizar una denuncia pública, ya bajo su propio nombre.[5]

Después de que Savchuk revelase públicamente su existencia, otros extrabajadores e incluso empleados en activo dieron a conocer más detalles sobre la forma de operar de la IRA: turnos de once o doce horas, en los que debían cumplir cuotas de producción; por ejemplo, posteando 120 comentarios al día en chats, foros o perfiles en redes sociales. Según un extrabajador identificado como Sergei K., la granja estaba dividida en secciones con cometidos específicos. Departamentos de unas quince personas cada uno por cada red social: YouTube, Facebook, VK (su competidora rusa). Otro departamento bombardeaba con comentarios las páginas de medios «hostiles», caso de *Novaya Gazeta* o Radio Sbovoda, el servicio en ruso del medio público estadounidense Radio Free Europe/Radio Liberty.

Había también un departamento específico para recopilar bases de datos con las biografías de personas consideradas «enemigos

políticos», y otro dedicado a crear memes, incluidos los pornográficos. Una vez creados, eran distribuidos mediante aplicaciones de mensajería a los trols, que los adjuntaban en sus publicaciones.[6]

Los coordinadores del proyecto proporcionaban a los trabajadores abultados mazos de tarjetas SIM prepago, para que pudieran crear perfiles falsos en redes sociales, que en la mayoría de las plataformas requieren una verificación mediante un número de teléfono móvil. Los perfiles eran utilizados de forma estratégica, para que sus comentarios online se adecuasen a la personalidad y otras características, como el sexo y la edad del supuesto propietario de cada cuenta.

También les instruían en el uso de redes virtuales privadas (VPN) para enmascarar su localización, sobre todo a quienes se ocupaban de influir en las audiencias de otros países, para que pareciese que eran actores locales que se encontraban en esos lugares. Cada día, los empleados recibían instrucciones sobre qué temas abordar, siempre siguiendo el mismo marco: ensalzando a Rusia y a Putin, denigrando a Ucrania, Occidente, la OTAN, Estados Unidos, la UE y los sistemas democráticos en general. Los trols comentaban en las publicaciones de otros trols, generando una discusión supuestamente orgánica en la que, poco a poco, llegaban a la conclusión deseada, lanzando el mensaje que les habían asignado.[7]

Durante el período de Savchuk en la IRA, se produjo el asesinato del político opositor Boris Nemtsov en pleno centro de Moscú, no muy lejos del Kremlin. Ese día, los coordinadores de rango medio —que habitualmente no se implicaban en las actividades de base de la granja— se movilizaron para microgestionar el trabajo. Los empleados recibieron instrucciones para sembrar la confusión sobre la autoría del crimen, culpando a los ucranianos, los estadounidenses o a los chechenos. A Savchuk también le sorprendió el grado de sofisticación que alcanzó ese tipo de manipulaciones. El equipo al que pertenecía participó en la creación de un personaje llamado «Cantadora», una sanadora mística experta en astrología y parapsicología, que tenía su propio blog. Cada pocas entradas, más o menos inocuas, los

empleados tras su falso perfil introducían un contenido de carácter político.

Las elecciones estadounidenses y Ucrania

Después de sus revelaciones periodísticas, Savchuk se convirtió en objetivo de los trols. La acusaron de traidora, espía y degenerada. Sus familiares recibieron llamadas con amenazas de muerte. Y la mayoría de sus compatriotas reaccionaron con una indiferencia casi total.[8] Pero aquello cambiaría muy pronto: tras la victoria de Donald Trump en 2016, los investigadores estadounidenses descubrieron que la IRA había jugado un papel fundamental en la operación de interferencia de Rusia en las elecciones.[9] De repente, la granja de trols de Prigozhin estaba por todas partes.

En 2018, el Departamento de Justicia de Estados Unidos imputó a más de una docena de ciudadanos rusos vinculados con la IRA por sus acciones de injerencia.[10] Ese mismo año, anticipándose a la presumible intervención de los trols rusos en las elecciones de mitad de mandato, el cibercomando estadounidense lanzó un ciberataque contra esta agencia para impedir sus actividades.[11] Pero no significó su final. Para esquivar la detección, la IRA cambió varias veces de nombre oficial, pasando a llamarse MediaSintez, NovInfo, Nevskiy News, Economy Today, National News, Federal News Agency e International News Agency.[12] Los empleados de Prigozhin se adaptaron al nuevo entorno creado por esta atención, no necesariamente indeseada: ampliaron la operación y diversificaron las localizaciones de las granjas, en algunos casos, trasladándolas a países africanos como Ghana o Nigeria.[13]

Los trols de Prigozhin adoptaron también un papel muy activo tras la invasión de Ucrania, adaptando sus técnicas a las nuevas necesidades del Kremlin, como erosionar el apoyo internacional a Kiev y justificar la guerra.[14] A finales de ese año, después de que Estados Unidos acusase a Rusia de injerencia, Prigozhin declaró: «Caballeros, interferimos, estamos interfiriendo e interferiremos» en los procesos

electorales estadounidenses.[15] En febrero de 2023, el magnate admitió por primera vez ser el máximo responsable de la IRA: «Nunca he sido solo el financiador de la Agencia de Investigación de Internet. Yo la inventé, yo la creé, yo la dirigí durante mucho tiempo. Fue fundada para proteger el espacio informativo ruso de la tosca y agresiva propaganda de la narrativa antirrusa de Occidente», dijo en un comunicado.[16]

Pero, ese mismo verano, Prigozhin acabaría protagonizando un motín contra el Kremlin al frente del Grupo Wagner, la organización paramilitar que había creado para apoyar las operaciones rusas no oficiales en el extranjero. Tras llegar a un acuerdo con Putin, el empresario ordenó desmantelar su conglomerado de medios, incluyendo la IRA[17] No obstante, sus granjas no desaparecieron, sino que pasaron a estar controladas por otros actores vinculados al Gobierno ruso.[18] Incluso tras la muerte de Prigozhin, en un sospechoso accidente de avión en agosto de 2023, sus antiguos trols siguieron activos.[19]

BOTS, SOCK PUPPETS Y OTRAS HERRAMIENTAS DE MANIPULACIÓN

Hay varias maneras de manipular la conversación en el mundo digital. La primera, como hemos visto, son los trols: individuos al servicio de una causa, un estado o un cliente que buscan impedir el debate, imponer una idea y negar el espacio a los argumentos contrarios. O simplemente atacar e intimidar a quienes sostengan posiciones contrarias.

En estas prácticas se utilizan también los bots, cuentas automatizadas que sirven de «músculo», amplificando y repitiendo un mensaje para inundar el espacio informativo con él, y que a menudo son fácilmente detectables. A medio camino entre trols y bots, están los llamados *sock puppets*, cuentas operadas por humanos bajo una identidad falsa, pretendiendo ser un miembro de la comunidad local en la que se intenta influir, o un supuesto experto o voz autorizada.

La diferencia entre ellos es difícil de discernir a medida que los enjambres se van sofisticando con ayuda de los avances tecnológicos o la inteligencia artificial. Además, a veces la falsedad reside simplemente en el hecho de que se están utilizando cuentas de forma artificial para alterar los intercambios comunicativos en redes, pero sin que se utilicen identidades ficticias ni se recurra a la desinformación. Por eso, algunas redes sociales se refieren a estas prácticas como «comportamiento coordinado no auténtico» cuando detectan patrones de una posible campaña de manipulación. Desactivan los enjambres de cuentas, independientemente de a quién pertenezcan y el contenido que difundan.[20]

Cualquier persona que trabaje en algún ámbito público ha tenido encontronazos con trols. Yo no soy una excepción, aunque, por suerte, nunca he sufrido el acoso al que han sometido a muchos compañeros (y, sobre todo, compañeras). La experiencia más significativa, y a la vez más reveladora, me ocurrió a finales de 2020. El 28 de octubre, numerosos medios españoles publicaron algún tipo de variante del siguiente titular: «Putin ofreció a Puigdemont enviar 10.000 soldados a Cataluña». La noticia sonaba inverosímil, pero estaba obtenida de las escuchas de una conversación real entre dos destacadas figuras independentistas catalanas: Víctor Terradellas y Xavier Vendrell.

Poco después, la Embajada de Rusia en Madrid reaccionó con un tuit irónico en el que decía:

> Ojo: la información aparecida en los medios españoles sobre la llegada de diez mil soldados rusos a Cataluña está incompleta. Hace falta añadir dos ceros al número de soldados y lo más impactante de toda esta conspiración: las tropas deberían ser transportadas por aviones «Mosca» y «Chato» ensamblados en Cataluña durante la Guerra Civil y escondidas en un lugar seguro de la Cierra [sic] Catalana hasta recibir a través de estas publicaciones la orden cifrada de actuar.[21]

Un mensaje, con sus erratas, que ridiculizaba, mediante exageraciones, las afirmaciones de la prensa y del Juzgado de

Instrucción número 1 de Barcelona, de donde había salido la información.

Al ver el tuit de la embajada, reconocí inmediatamente lo que los diplomáticos rusos estaban haciendo, y escribí el siguiente hilo en mi cuenta de X/Twitter:

> Esto es una clásica técnica rusa de desinformación llamada *hahaganda*: cada vez que Rusia sale mal parada en un asunto, se busca el aspecto más extremo o inverosímil, se caricaturiza, se ridiculiza y se infiere que TODO es absurdo. Lo hemos visto mil veces, del MH17 a Navalny. Un caso de manual es este vídeo: se toma una frase de un informe de @AltoAnalytics explicando que los canales de comunicación de fans del K-Pop sirvieron para coordinar protestas en Chile, y se concluye que «la culpa de las protestas en Chile es del K-Pop». Como es obvio que eso es absurdo, se infiere, los datos sobre redes rusas tratando de agitar el tema en beneficio propio también lo son. Y, mediante la burla, se va generando escepticismo sobre las presuntas «acciones de Rusia», lo que al final acaba sonando a chivo expiatorio hueco y sin contenido, y haciendo que a parte de las audiencias les cueste cada vez más creerlo. Es una técnica muy eficaz y poderosa, y por eso se sigue utilizando una y otra vez. En este caso, una bravuconada disparatada entre dos políticos catalanes —«10.000 soldados»— está siendo transformada en un esquema en el que «Rusia nunca ha tenido interés alguno en el *procés*». Atención a los medios rusos en español en los días siguientes.

Poco después añadí:

> «Diez mil soldados rusos para convertir Cataluña en un país como Suiza: el delirante informe de la Guardia Civil que hace estallar de risa a X/Twitter». Lo que decíamos: Es de risa todo.[22]

El vídeo sobre Chile al que hacía referencia era un episodio del programa de RT en español «Ahí les va», entonces presentado por Inna Afinogenova. Tras el estallido de la ola de protestas sociales en dicho país en octubre de 2019, el Gobierno de Sebastián Piñera encargó a la consultora española Alto Analytics un estudio sobre el impacto de las redes sociales en dichas movilizaciones, que la prensa denominó «Informe Big Data».[23]

Esta empresa se encontró con que actores vinculados a Rusia estaban explotando las protestas y animándolas para desestabilizar al Ejecutivo de Piñera mediante mensajes antigubernamentales en todos los canales, desde los más clásicos, como X/Twitter y Facebook, hasta otros sorprendentes, como los foros de debate sobre K-Pop, el estilo musical importado de Corea del Sur que causaba furor en la juventud del continente. También destacaban el canal ruso RT en español y el venezolano Telesur como dos de las fuentes de información que mayor cobertura daban a las protestas y con mayor impacto.[24]

Es importante aclarar que el informe no decía que Rusia fuese el motor de las protestas, algo que resultaba obvio para cualquiera que hubiese seguido el conflicto social. Y, desde luego, los cientos de miles de chilenos que se echaron a las calles no lo hacían siguiendo órdenes de ningún ruso. La situación era bastante más compleja: en aquellos años, según concluyó el Departamento de Estado de Estados Unidos,[25] Rusia desplegaba campañas para erosionar a los gobiernos del llamado Grupo de Lima, una iniciativa internacional lanzada para aislar al régimen de Nicolás Maduro en Venezuela,[26] estrecho aliado de Moscú. En contraposición, los rusos amplificaban cualquier conato de rebelión social con potencial desestabilizador en dichos países, como las movilizaciones contra Mauricio Macri en Argentina, Iván Duque en Colombia o Lenín Moreno en Ecuador. Protestas, todas, de origen orgánico y legítimas en sus reivindicaciones.

Pero, en Chile, alguien del entorno de Piñera filtró el informe a la prensa, y el Gobierno incidió en la «mano rusa». Sin duda, porque resultaba más fácil usar a los rusos como chivo expiatorio que afrontar la necesidad de reformas profundas que reclamaba una gran parte de los ciudadanos, profundamente insatisfecha con su gestión.

El informe de Alto Analytics fue denigrado y ridiculizado por muchos chilenos, que sentían que Piñera buscaba culpar de su descontento a grupos específicos de agitadores y restar así validez a sus demandas. El vídeo de Afinogenova (hoy inencontrable)[27] ahondaba en esa percepción, pero iba más allá, asegurando que el

Gobierno «culpaba al K-Pop» de las movilizaciones masivas, ridiculizando así el informe al completo. A eso me refería en mi hilo de X/Twitter cuando mencioné «un caso de *hahaganda* de manual».

Sea como fuere, la respuesta de Afinogenova no se hizo esperar. Poco después de mi hilo, tomando de forma aislada algunos de mis *posts*, animó a sus seguidores a que me mostrasen lo que opinaban sobre mis comentarios. «Aquí este viejo seguidor de AHÍ LES VA haciendo algo de lo que después nos acusa a nosotros: elige un pequeño y llamativo detalle de uno de nuestros vídeos para descalificar todo el contenido sin ninguna razón aparente más que esa», escribió Afinogenova. «A ver si nuestros seguidores chilenos pueden hacerle un resumen del rigor de un informe que, por cierto, hasta los propios fiscales chilenos han desestimado por inconsistente y falto de ninguna base sólida», añadió, para azuzar el ambiente.

Durante las siguientes 48 horas, recibí todo tipo de insultos e imprecaciones, ahogando cualquier debate o respuesta positiva —que las hubo— en una marea de desaprobación generalizada. Yo observaba en silencio, más fascinado que ofendido. Cuando la oleada empezaba a remitir, Afinogenova volvió a la carga: «Los medios rusos se burlan de esa gilipollez. Hay que denunciar el retorcido papel de los medios rusos», posteó. Y vuelta a empezar con los mensajes insultantes. Recordé entonces lo que me había dicho un compañero, víctima frecuente de este tipo de ataques: «Durante un par de días parece el fin del mundo, pero luego se pasa sin que haya consecuencias en el mundo real, como si nunca hubiera sucedido». Mantuve la cabeza fría, y eso es exactamente lo que ocurrió. Incluso me permití añadir un colofón al hilo:

> La mayoría de las respuestas que he recibido a este hilo demuestran, precisamente, lo eficaz que es la *hahaganda*: todo el mundo hablando de la gilipollez de los 10.000 soldados rusos y nadie prestando atención al resto del tema. Y sí, es ABSURDO pensar que Rusia iba a enviar soldados (ni diez mil, ni veinte) a Cataluña, pero es que eso NO lo dice el auto del juez, sino que son las

> palabras de Terradellas, que este cita. Pero, al ridiculizar la parte, se consigue deslegitimar el todo. ¿Lo vais pillando?[28]

Cibertropas y ciberextremistas

El acoso en línea, como hemos visto, es una de las principales funciones que cumplen los enjambres de trols y las milicias digitales. Grupos europeos de extrema derecha como Generación Identitaria han difundido en internet sus propios manuales de «guerrilla *troll*», con técnicas como el uso estratégico de memes, el llamado *shitposting* —la publicación deliberada de material absurdo, irrelevante, incoherente o de calidad pobre para impedir una conversación fluida en redes—, o el lanzamiento de ataques coordinados. También se dan consejos de este tipo:

> Sigue/dale a *Like* en las cuentas (o infíltrate en foros) de todos los partidos, especialmente los Verdes, feministas bien conocidas, lacayos del gobierno [...] y toda la prensa propagandística del gobierno, como ARD, ZDF, Spiegel y el resto de la banda de *fake news*, así como organizaciones de verificación. Y, tan pronto como veas que están esparciendo de nuevo sus mentiras y su veneno por el mundo, diles lo que piensas, enzárzate en discusiones con ellos, señala sus mentiras como #fakenews y troléales a lo bestia.[29]

Reconquista Germánica fue una comunidad ultraderechista alemana creada en 2017 por un *youtuber* llamado Nikolai Alexander con respaldo de Rusia, con el propósito explícito de interferir en las elecciones alemanas de 2017 a favor del partido ultraconservador Alternativa para Alemania (AfD), según su propio canal de Discord, que llegó a contar con más de 5.000 miembros,[30] aunque los organizadores duplican dicha cifra. Como declaró el propio Alexander a la publicación *Kontraste*, «sin apoyo ruso, el proyecto probablemente no habría sido posible en esta forma».[31] Organizada al estilo de un videojuego, la plataforma ofrecía cada día objetivos a los que hostigar online, decididos por la cúpula de la organización, así como *hashtags* y las franjas horarias en las que lanzar los ataques de

forma coordinada, para que los propios algoritmos de las redes sociales promoviesen su contenido.

En una charla en YouTube, Alexander orientaba a sus seguidores sobre cómo llevar a cabo operaciones psicológicas al estilo *troll*:

> Tienes que transmitir derrotismo para minar la moral de tu oponente. Por ejemplo, di cosas como que esto no tiene sentido, que esto no lleva a ningún lado, que es mejor dejarlo. Lo ideal es que lo combines con calumnias: di que trabajas para el enemigo, por ejemplo. Luego, claro está, denigra para que todo se cuestione, desmonte y critique. Siembra descontento, impaciencia y dudas respecto a los líderes [...] Luego, intentas poner a unos miembros contra otros, provocas disputas, creas grupos, promocionas a los traidores y expulsas a los leales. Establece instrumentos para influir en todo según tus intereses, externaliza estructuras relevantes, etc. Y, claro está, espía, desinforma, miente, calumnia… Cualquier tipo de enfoque. Esas son las tácticas y los mecanismos para sabotear y destruir un movimiento.[32]

El informe del Instituto sobre Internet de Oxford (OII) del año 2017 sobre prácticas globales de manipulación digital explica:

> El hostigamiento implica abuso verbal, discurso de odio, discriminación y/o troleo contra los valores, creencias o identidad de un usuario o grupo de usuarios en línea [...]. El ataque individual es un aspecto persistente del ecosistema de internet que se usa para silenciar la disensión política en línea.

El documento menciona cómo numerosos gobiernos cuentan con sus propios ejércitos de lo que denomina «cibertropas», sean voluntarios o pagados, dedicados a este tipo de actividades de acoso digital contra los críticos. Menciona el grupo juvenil IRELI en Azerbaiyán, las brigadas digitales del movimiento juvenil pro Putin Nashi en Rusia, o la plataforma Somos+ del entonces presidente Rafael Correa en Ecuador.[33]

Incluso una investigación superficial sobre este fenómeno revela más ejemplos. La periodista Maria Ressa ha dado a conocer muchos en su país natal, Filipinas, a través del portal informativo Rappler, que la convirtió inmediatamente en el objetivo de grupos organizados al

servicio del entonces presidente Rodrigo Duterte.[34] En la India operan los llamados «Yoddhas», integrados por voluntarios pagados por el partido gubernamental nacionalista hindú Bharatiya Janata Party (BJP), que se dedican a lanzar amenazas de muerte y violación contra los críticos del presidente Narendra Modi, especialmente, figuras públicas como periodistas y políticos opositores. Reporteros Sin Fronteras los incluyó en su lista de enemigos de la libertad de prensa digital en 2020, donde también aparecían grupos como la llamada «Oficina del Odio» del entonces presidente Jair Bolsonaro, la «Brigada Electrónica Saudí»[35] o las denominadas «Moscas electrónicas» del régimen argelino, movilizadas contra el movimiento de protesta Hirak que sacudió el país norteafricano a finales de la década pasada.[36]

Turquía y Cuba

Me centraré a continuación en dos casos que he podido estudiar en detalle: los AKTrolls de Turquía y las Ciberclarias de Cuba.

En 2013, el Gobierno de Recep Tayyip Erdogan decidió acabar con el parque Gezi, el último recinto verde que existía en los alrededores de la plaza Taksim, en pleno centro de Estambul, y reemplazarlo por una enorme mezquita. Cuando un grupo de ecologistas se reunió allí para protestar, la policía recurrió al gas lacrimógeno para desalojarlos. Los manifestantes, contra todo pronóstico, se enfrentaron a los agentes. A medida que la batalla se prolongaba, grupos activistas lanzaron una movilización para unirse a las protestas, que acabaron convirtiéndose en una auténtica rebelión contra el Ejecutivo, cada vez más autoritario, de Erdogan.

La revuelta de Gezi, que cubrí sobre el terreno como corresponsal en Estambul del diario español *ABC*, acabó extendiéndose a más de setenta ciudades en toda Turquía y se saldó con once muertes entre manifestantes y policía, y en la eclosión de un movimiento político opositor fuertemente reprimido por el Gobierno turco.

Como reacción a estos sucesos, el Gobierno turco creó la llamada «Nueva Oficina Digital de Turquía» y reclutó a un equipo de 6.000 operativos para contrarrestar las narrativas contra el Partido Justicia y Desarrollo (AKP) de Erdogan en redes sociales.[37] Se les conocería como los AKTrolls. «Intentamos desarrollar un lenguaje político positivo, que estamos enseñando a nuestros voluntarios. Y, cuando el campo opuesto difunde desinformación sobre el partido, les corregimos con información válida, usando siempre un lenguaje positivo», declaró en esas fechas un alto cargo del AKP al diario *The Wall Street Journal*.[38]

En realidad, los AKTrolls fueron utilizados para apoyar medidas como el referéndum de reforma constitucional que permitió a Erdogan convertirse en presidente plenipotenciario. O para la intervención turca en Siria.[39] Pero, sobre todo, para atacar a los críticos del Gobierno, especialmente figuras públicas como periodistas. Apenas un mes después de su creación, los miembros de la Nueva Oficina Digital de Turquía ya estaban lanzando una campaña coordinada de abusos digitales contra la reportera Emre Kizilkaya, después de que hubiese criticado el manejo por parte del Gobierno de una crisis diplomática en Líbano.[40]

Este tipo de hostigamiento en redes contra opositores y adversarios se disparó después de que evidencias sobre la corrupción del líder turco y su familia fuesen filtradas en internet, presumiblemente por antiguos aliados del AKP reconvertidos en enemigos.[41] En 2020, X/Twitter eliminó 7.340 cuentas de esta red.[42] Los AKTrolls, sin embargo, siguen existiendo.

En Cuba existe una iniciativa semejante, que los cubanos llaman jocosamente «ciberclarias». La claria es una especie invasora de pez introducida artificialmente por el régimen de Fidel Castro en los años noventa durante el llamado «período especial», la época de carestía que sufrió la isla en aquellos años tras la desaparición de la URSS y las ayudas que proporcionaba a países amigos. La idea era aprovechar su abundante carne para paliar la escasez de alimentos, pero el

experimento salió mal: la claria está considerada una de las cien especies más dañinas del mundo, y una serie de huracanes a principios de este siglo provocaron que se expandiese sin control por todas las masas de agua dulce de la isla, como presas y ríos.[43] Dado el aspecto desagradable de este pez, el *slang* cubano no tardó en adoptar la palabra «claria» para referirse a algo repulsivo, cutre y de baja estofa. También es un animal superviviente en condiciones extremas, como aguas sucias y contaminadas, y se arrastra por la tierra, por lo que el término empezó a ser utilizado para referirse a los representantes, cuadros y apologistas del gobierno. Cuando los trols del castrismo hicieron su aparición en redes, la calle cubana los bautizó con el nombre de «el ciberclariato».

Hace dos décadas, el Ejecutivo cubano, siempre consciente de la importancia de la propaganda y el control de la información, decidió proyectar esa orientación a un ámbito digital que ganaba importancia. Los cubanos se beneficiaron de las experiencias del régimen de Hugo Chávez en Venezuela. Pero, a diferencia de sus estrechos aliados, que gozaban de una importante bonanza petrolífera, Cuba disponía de recursos más que limitados.

Su solución fue tratar de matar varios pájaros de un tiro: al tiempo que impulsaba la penetración controlada de internet en la isla —una necesidad para cualquier nación que aspirase a tener una economía sostenible en pleno siglo xxi—, condicionó su acceso a que se usase para defender el sistema cubano. A profesionales destacados, como algunos periodistas, les instalaron módems en viviendas y centros de trabajo. A cambio, estaban obligados —al menos, teóricamente— a dedicar una parte de su tiempo en línea a promover narrativas procastristas y contrarrestar los mensajes de los supuestos enemigos del régimen, tanto entre la diáspora cubana, como desde gobiernos y medios extranjeros.

Según *YucaByte*, un medio independiente dedicado a la conectividad y las nuevas tecnologías en Cuba, las «ciberclarias» actuales suelen estructurarse alrededor de cuentas institucionales, que

en ocasiones forman coaliciones informales para «posicionar temas de interés para el régimen mediante la publicación constante de *posts* y tuits, así como en acosar y lanzar amenazas a quienes definen como "enemigos de la Revolución"».[44] Otras publicaciones mencionan como funciones adicionales la monitorización de la actividad en redes sociales y la identificación de los principales temas de preocupación, y quiénes son los principales líderes de opinión y críticos del país.

Para ello, utilizan perfiles falsos, muchas veces creados en la Universidad de Ciencias Informáticas de La Habana.[45] De acuerdo con un reportaje de Cubanet, otro medio de oposición, usan fotografías de personas generadas mediante inteligencia artificial en la web thispersondoesnotexist.com, cuando no tomadas directamente de Google. Entre sus integrantes hay funcionarios del régimen y jóvenes estudiantes, que reciben beneficios y prerrogativas, como móviles nuevos y ventajas académicas.[46] *YucaByte* cita el caso de Mayra Arevich Marín, quien durante años ocultó su identidad bajo un perfil falso desde el que acosaba a la periodista opositora Yoani Sánchez y al senador cubanoamericano Marco Rubio, hasta que esta publicación desveló su identidad en 2020.[47]

En 2019, el sucesor de los Castro, el presidente Miguel Díaz-Canel, ordenó a los principales cargos del régimen que creasen cuentas en X/Twitter, como hacían la mayoría de líderes y funcionarios gubernamentales en todo el mundo. Pero no estaban preparados para la tormenta de críticas, comentarios negativos e insultos que iban a recibir, gracias a la posibilidad de respuesta directa que esta plataforma ofrece. El Gobierno cubano modificó entonces el marco regulatorio para penalizar los insultos al régimen en las redes sociales,[48] al tiempo que intensificó la batalla por las narrativas.

Ese mismo año se creó —supuestamente, de forma espontánea— el grupo De Zurda Team, una comunidad virtual cuyo propósito declarado es «decir la verdad de Cuba» en redes y apoyar «a los hermanos venezolanos y sandinistas», dando cohesión así a unos esfuerzos que hasta ese momento habían sido en gran medida

descentralizados. Según el medio oficial cubano Tribuna, la organización —que cuenta entre sus miembros con varios integrantes de la célebre Red Avispa, la operación de espionaje cubano en Estados Unidos desmantelada por el FBI en 1998—[49] sumaba 500 miembros a finales de 2021, cuando celebraron su primer encuentro en el mundo real. De Zurda Team ha participado en acciones de ciberacoso contra artistas disidentes, así como en campañas de guerra informativa en momentos críticos,[50] como el estallido social que sacudió al país el 11 de julio de 2021[51] y las movilizaciones organizadas de ese mismo año.

4

GUERRILLAS DIGITALES

El 17 de octubre de 2019, la ciudad mexicana de Culiacán fue engullida por la violencia cuando los narcos del cártel de Sinaloa se movilizaron para liberar a tiros al hijo del *Chapo* Guzmán, Ovidio, que acababa de ser detenido en un operativo militar. Durante el llamado «Culiacanazo», la ciudad se convirtió en un auténtico teatro de guerra, hasta que a las pocas horas las autoridades mexicanas, superadas por la potencia de fuego de los narcos, accedieron a liberar al *Chapito* Guzmán.

Mientras esto ocurría, las redes sociales ardían en todo México. Según un estudio de Signa Lab, una institución de análisis de redes sociales vinculada a la Universidad Jesuita de Guadalajara, apenas diez minutos después del inicio de los disparos ya se estaban generando contenidos relacionados atacando o defendiendo al Gobierno de Andrés Manuel López Obrador. *Hashtags* como #AMLORenunciaYa, #Mexico NoTienePresidente o #EstadoFallido chocaban contra otros como #AMLOEstamosContigo o #AMLOElPuebloTeApoya. Una guerra digital que explotaba una tragedia real para promover ciertas agendas políticas.

Uno de quienes observaban con desazón cómo se iban desarrollando los acontecimientos, tanto en el plano real como en el virtual, era el activista contra la desinformación Alberto Escorcia: «Durante un par de días, Culiacán permaneció cerrado, la gente no sabía qué hacer, hubo escasez, pánico», me describió cuando le entrevisté en la primavera de 2024. «Creo que era un momento de solidaridad de todos los mexicanos, de admitir que obviamente hay un fallo en el gobierno. Pero lo más importante es informar sobre qué

lugares son seguros, por dónde hay que escapar. El que se haya politizado tan rápido y no se haya priorizado la cuestión humanitaria, el facilitar el rescate, fue muy irresponsable. En esos momentos la desinformación es criminal».

Por desgracia, ese tipo de prácticas ha llegado para quedarse. Y no solo en México. Escorcia lleva años desenmascarando estructuras coordinadas de manipulación de la opinión pública en redes, un negocio floreciente en el que México es pionero. Lo cuenta en su libro *Memorias de la guerra digital*, publicado en 2023. «Según la información que tengo yo, y varios investigadores con los que he compartido estas observaciones, México es el origen de las industrias de desinformación digital, ya desde los años 2006-2009. Aunque hay antecedentes en otros países, México es la Meca de estas prácticas». Quintana Roo, el estado del Caribe mexicano donde se encuentra Cancún, es uno de los epicentros.

«México exporta muchas técnicas, y muchos mexicanos están desinformando por todo el mundo. En Suecia, en Alemania, en El Salvador, donde están con Bukele…», me indicó. La referencia a Suecia no es casual: una vez destapadas estas estructuras, la política de las plataformas suele ser desmantelarlas, lo que ha hecho que gente muy poderosa pierda mucho dinero. Amenazado de muerte, Escorcia se ha visto obligado a autoexiliarse por largas temporadas; la última, en este país escandinavo.

«Todos los poderes fácticos, todo aquel grupo que tenga la capacidad de manipular a la población, lo va a hacer. La manipulación digital es fácil y barata, y no requiere de tantos intermediarios como el cabildeo u otros métodos». El activista explica cómo se hace: «Es demasiado fácil crear una tendencia, por los mecanismos y los algoritmos con los cuales una red social detecta que algo es importante. Pongamos que sucede algo y la gente empieza a tuitear, y ocurren varias cosas: una aceleración de los mensajes, una masa crítica. Esos indicadores de detección son muy fáciles de burlar. Tú, junto a cincuenta cuentas de bots, puedes empezar a tuitear algo al

mismo tiempo y simular que hay interés en eso. El mecanismo de detección de lo viral puede ser engañado y forzado a crear *trending topics*. Mucha gente conoce muy bien esos mecanismos. Basta con tener un pequeño grupo de personas para hacer una tendencia y marcar la agenda del día. Por eso se ha vuelto una industria».

Escorcia aporta un ejemplo de hasta qué punto México es hoy centro neurálgico: durante el referéndum en Cataluña, en octubre de 2017, encontró redes organizadas desde su país —y desde Venezuela, otra potencia de la desinformación de alquiler— que promovían mensajes tanto a favor como en contra de la independencia, presumiblemente, porque habían sido contratadas para ello. «Había de los dos bandos, a favor y en contra del referéndum, pero se notaba que no se mezclaban en la conversación. Era como una especie de *spam* masivo, una comunicación muy arcaica: simplemente compartir *links* a favor o en contra del referéndum. Creo que el objetivo, haciendo una especie de conjetura, buscaba una visión de que había o no había apoyo por el referéndum, pero a nivel internacional».

Escorcia sostiene, además, que México es el gran laboratorio del mundo, donde se ponen a prueba iniciativas socioeconómicas que después se exportan. «Muchas cosas que están ocurriendo ahora mismo en Europa, en el primer mundo, ya ocurrieron antes aquí». Véase el espionaje masivo, «que en México se empezó a dar desde 2007 con el programa FinFisher, y luego con Pegasus en 2015». En su libro, detalla cómo él mismo trabajó para una importante agencia de inteligencia digital, cuyo nombre no revela, que puso a su disposición una poderosa herramienta de análisis de redes, supuestamente por solidaridad en la lucha contra la desinformación, pero que en realidad buscaba aprender de los métodos de activistas como él y «perfeccionar lo que quizá ahora vemos en Ucrania».

En cuanto estalló la invasión rusa de Ucrania, «me puse a monitorizar varios acontecimientos importantes. Recuerdo muy bien un ataque con misiles a un edificio de apartamentos en Kiev. Noté una gráfica muy parecida a la de eventos que ocurrían en México. Este

comportamiento de redes se puede graficar. Hay ciertos patrones de desinformación. Y empecé a ver similitudes». En Ucrania, «Telegram tiene un papel determinante. Yo he detectado que en al menos unos veintitantos, treinta canales que he analizado hay una manipulación, tanto del lado ruso como del lado ucraniano».

Escorcia sitúa la condición pionera de México en la llamada «guerra de los blogs» de 2005 y 2006, cuando estas webs eran muy populares. Algunos apoyaban al entonces candidato López Obrador, *el Peje*. Poco a poco se empezó a notar que había muchos comentarios atacando sus mensajes, y con el tiempo se supo que parte provenían de una oficina de la Presidencia del Gobierno, encargada de acallar protestas digitales. «Digamos que es el primer caso documentado de represión digital. Después, muchos de esos blogueros abrieron su cuenta de X/Twitter con la pandemia de la influenza (gripe) porcina en 2009, que presuntamente tuvo su origen en México, donde hubo confinamientos. X/Twitter, *streamings*, canales de YouTube… se convirtieron en una forma de comunicarse y contrastar la realidad con lo que decía el Gobierno. Fue una especie de revolución digital».

Pero el verdadero punto de inflexión lo marcó la aparición de Enrique Peña Nieto y su ejército digital, los llamados «Peñabots». Dice Escorcia: «2012 supuso la llegada de la maquinaria industrial de la desinformación. Cuando se decide que Peña Nieto va a ser el candidato a la presidencia, aparecen 27.000 cuentas de bots, que no eran personas, pero que creaban rápidamente un *trending topic*. Entonces no había competencia contra eso. Lo que hicieron fue esparcir rumores económicos, como que si ganaba la izquierda se iba a devaluar el peso, que iba a haber expropiaciones…». En su opinión, la campaña logró que muchos mexicanos se pusiesen en contra del candidato de la oposición. «Ahí llegó la industria. Primero eran oficinas del gobierno. Los siguientes años se fueron creando subcontrataciones, hasta la pesadilla que vivimos hoy». Peña Nieto no solo ganó con facilidad las elecciones de ese año, sino que los «Peñabots» se dedicaron a silenciar a sus críticos, hostigando y

amenazando digitalmente a quien se atreviese a cuestionar en redes al presidente.

Seis años después, Escorcia jugó un papel fundamental a la hora de impedir que se repitiese un escenario semejante. Un día de 2018, la Ciudad de México amaneció cubierta de publicidad de una página llamada Pejeleaks.org, que supuestamente contenía información sobre casos de corrupción de López Obrador. La web conducía a una página con estética ciberactivista. Pero el análisis del contenido supuestamente escandaloso mostraba que no existían pruebas. Escorcia y otros activistas y periodistas rastrearon los elementos de la página —incluyendo una cartera de bitcoins para recibir donaciones —, y descubrieron que se trataba de una operación política con intención de desacreditar al entonces candidato. Además, Escorcia rastreó varias redes coordinadas de manipulación y las notificó a plataformas como X/Twitter, que tumbó alrededor de un millón de cuentas poco antes de los comicios, sin que los responsables tuviesen tiempo para reconstruirlas. «Las de 2018 fueron las únicas elecciones sin desinformación en la historia reciente de México», que llevaron al poder a López Obrador y su alianza MORENA.

Desde entonces, los problemas son otros. López Obrador cuenta hoy con sus propios ejércitos digitales con los que ataca a sus enemigos en redes, la llamada Red AMLO. «De un grupo de apoyo ciudadano en 2006, la Red AMLO se fue transformando en una red de ataque y de represión, que no necesariamente está bajo las órdenes del presidente. Pero ellos sienten que tienen que defenderlo desde una posición muy fanática. Muchos están financiados con recursos públicos. Es una red que se volvió muy paranoica, muy brutal, muy violenta». De hecho, muchos de los antiguos «Peñabots» son hoy «Morenabots», tras poner sus actividades mercenarias al servicio de un nuevo pagador.

En 2024, México ha sido también el campo de pruebas de otra técnica de desinformación: la difusión de falsos audios creados mediante inteligencia digital, como los que afectaron al ministro de

Exteriores Marcelo Ebrard durante las primarias para suceder a López Obrador, o al senador opositor Martí Batres. En este último caso, Escorcia reconoce que no fue capaz de discernir si se trataba de un audio real o falso, y solo pudo hacerlo porque se hacía referencia a un conocido suyo que nunca estuvo en ese lugar. «El peligro de los *deepfakes* es que, si tú haces un intento con un personaje, el siguiente va a ser mejor porque queda el antecedente. La inteligencia artificial aprende de ejemplos anteriores, y, si tú la entrenas, va a ser más sencillo la próxima vez». Algo que ya estaría empezando a ocurrir: «Aunque no creo que sea tan catastrófico como se dice. Creo que la IA hace lo mismo que cualquier desinformador, solo que más barato, más rápido y más asequible. Ya no tienes que contratar a una agencia para un audio falso, porque lo puedes hacer con una aplicación que te cuesta cien dólares». La democratización de la desinformación, con México, una vez más, como punta de lanza.

CUALQUIER TERRORISTA TIENE SU CIBERGUERRILLA

Dado que crear una cuenta en una red social es por lo general gratuito, cualquier grupo organizado con efectivos suficientes —pagados o voluntarios— puede montar una ciberguerrilla. Esto resulta especialmente relevante en contextos con violencia real, lo que puede suponer un desafío para los actores armados a la hora de promover narrativas que les favorezcan. También cuando la omnipresencia de los usuarios de redes garantiza una pluralidad de voces, incluso en contextos represivos. En México, por ejemplo, numerosos «periodistas ciudadanos» reportan sobre las atrocidades de los narcos amparándose en el anonimato virtual.[1]

«Las redes sociales han ayudado a desmantelar las jerarquías tradicionales de los medios y la información, y, al hacerlo, han dado a luz a un nuevo tipo de individuo hiperempoderado, con conexiones, conectado globalmente y más potente que nunca: un fenómeno único del siglo xxi que denomino *Homo digitalis*», escribe el periodista

británico David Patrikarakos en su libro *Guerra en 140 caracteres*. En ese mismo ensayo, añade:

> El Estado-nación del siglo XX tradicionalmente tenía la primacía en dos áreas, de las cuales se derivaba gran parte de su poder: su casi monopolio en el uso de la fuerza, y su control dominante de los flujos de información. La web 2.0 ha otorgado a la gente dos habilidades cruciales para alterar ese poder: primero, pueden producir contenido de forma activa en plataformas de redes sociales sin casi ninguna barrera de entrada, y, segundo, a través del uso de estos foros pueden crear redes transnacionales. Ambas capacidades les permiten cumplir roles tradicionalmente ocupados por los estados nación y dar forma a eventos alrededor del globo.

Quizá uno de los elementos más significativos de estas prácticas es que, en el mundo de hoy, casi cualquiera puede llevarlas a cabo. Y lo hacen.

Un ejemplo son las organizaciones armadas y terroristas. Tanto Hezbollah[2] como Hamás tienen sofisticados enjambres de cuentas en múltiples plataformas, de manera encubierta en aquellas con reglas contra la propaganda terrorista, como las de Silicon Valley o TikTok, o de forma más abierta en otras como Telegram.[3] Y, cuando las necesitan, las utilizan con eficacia.

Nada más comenzar el atentado coordinado del 7 de octubre en el sur de Israel, Hamás utilizó sus canales oficiales de Telegram para anunciarlo. Poco después, empezaron los vídeos de propaganda, tanto algunos preparados con anterioridad, como atrocidades filmadas por los atacantes durante el ataque, buscando amplificar al máximo el impacto psicológico. En unas pocas horas, el canal de Telegram de las Brigadas de Al-Qassam duplicó su distribución, alcanzando los 337.000 suscriptores —en pocos días, llegaría a los 600.000—. En las primeras 72 horas de la guerra, Hamás, sus grupos asociados y el resto de organizaciones que habían tomado parte en el atentado produjeron más de 6.000 *posts* de Telegram.[4]

Pese al veto de plataformas como X/Twitter, que aseguró haber eliminado «cientos de cuentas afiliadas con Hamás», los contenidos de

esta organización terrorista y su número de seguidores crecieron exponencialmente en la aplicación de mensajería rusa.[5] De ahí, el material saltaba a cientos de cuentas en otras redes —del ecosistema de Hamás, pero no vinculadas oficialmente al grupo—, desde donde las retomaban miles de simpatizantes en todo el mundo que ayudaban a propagarlas.

Diecinueve días después del atentado, ante la presión de Israel y otros países, Telegram prohibió el canal oficial de la organización, pero esta logró mantener activas otras cuentas y continuar sus prácticas. La nueva estrategia de Hamás en las redes había llegado para quedarse.[6]

Los hutíes de Yemen —los rebeldes apoyados por Irán que en octubre de 2023 causaron una conmoción global con sus ataques contra barcos civiles en el mar Rojo— también tienen su propio ecosistema digital compuesto por decenas de cuentas formales e informales en X/Twitter, más una veintena de canales de Telegram y múltiples cuentas en Facebook, Tik-Tok, Instagram, YouTube y en la red social iraní Virasty.[7]

La operación en el mar Rojo, que los hutíes describieron como una respuesta a la guerra de Gaza y cuyo espectacular ataque inicial también fue filmado por los asaltantes, llevó al bloqueo efectivo de esta vía marítima crucial para el comercio internacional y al lanzamiento de una operación de represalia por parte de Estados Unidos y el Reino Unido en enero de 2024. Durante todo este conflicto, los insurgentes yemeníes desplegaron su propia guerra de propaganda y desinformación, plagada de exageraciones y victorias inexistentes.[8] Ansar Allah —el nombre formal de los rebeldes hutíes— se beneficiaba de cierta ambigüedad sobre su estatus legal, dado que el grupo había salido de la lista de organizaciones terroristas extranjeras de Estados Unidos en 2021, antes de volver a ser incluida en 2024. En ese limbo, la mayoría de las plataformas toleraban la existencia de sus cuentas, a diferencia de Hamás.

En el otro extremo del espectro político están los Mojahedin- e Halq (Luchadores del pueblo, o MeK), una organización disidente iraní con un pasado terrorista, y cuya historia y características son fascinantes.[9] Mientras el grueso de sus militantes se encuentra exiliado en Albania, su brazo político, el llamado Consejo Nacional de la Resistencia de Irán, se codea con altos cargos políticos en Estados Unidos y en Europa, a quienes paga enormes sumas de dinero para que asistan a sus multitudinarios eventos, gracias a la generosa financiación de Arabia Saudí.

Los MeK tienen su propia granja de trols en Albania, dedicada a hostigar a quienes defienden posturas distintas a las del CNRI[10] y a promover mensajes pidiendo el derrocamiento de la República Islámica. Las escasas imágenes que han trascendido sobre este lugar, difundidas por el régimen iraní para desacreditar al grupo, muestran a decenas de miembros de ambos sexos —en su mayoría ancianos, dado que casi todos los militantes que quedan en la organización se unieron a ella en los años setenta y ochenta— frente a numerosas filas de computadoras. En el recinto, los hombres trabajan en una mitad de la nave y las mujeres, en la otra. Ellas visten de uniforme color caqui, cubiertas con el velo islámico. En abril de 2021, Facebook eliminó una red de 300 cuentas y páginas vinculada a dicha granja.[11]

Uno de los principales perfiles digitales vinculado a los MeK es el del supuesto activista Heshmat Alavi, que ha escrito artículos de opinión para publicaciones como *Voice of America*, *Forbes*, *Al Arabiya English*, *The Hill* y *The Federalist*, entre otros. Además de estos artículos, esta figura también se dedicaba a atacar públicamente a periodistas, investigadores y políticos que abogasen por una política menos dura desde Washington hacia Irán. Sin embargo, según el testimonio de varios desertores de los MeK, este individuo no existe, sino que su trabajo y el mantenimiento de sus cuentas en redes es obra de un equipo del brazo político del CNRI.[12] Tras esta revelación, varios de los medios de los mencionados anteriormente retiraron los artículos del falso colaborador.[13] Pero, tal y como pude comprobar,

todas sus cuentas en redes seguían activas en el momento de escribir estas líneas.

CÓMO AL QAEDA Y ESTADO ISLÁMICO CAMBIARON LA ESTRATEGIA

Si el terrorismo siempre ha tenido un elemento comunicativo *sine qua non* —¿de qué sirve cometer un atentado o asesinato con el propósito de aterrorizar y presionar a una sociedad si nadie se entera?—, el advenimiento de internet supuso un salto cualitativo en esta estrategia. Según un estudio realizado por investigadores israelíes entre 1998 y 2002, a principios de este siglo las principales organizaciones armadas y terroristas del planeta tenían presencia en internet, como Hamás, Hezbolá, Sendero Luminoso, ETA, el IRA, las FARC, el ELN, Tupac Amaru, el Grupo Islámico Egipcio, el Frente Popular de Liberación de Palestina, la Yihad Islámica de Palestina, los Tigres Tamiles de Sri Lanka, el Ejército Rojo Japonés, el EZLN mexicano, el Movimiento Islámico de Uzbekistán, la secta japonesa Aum Shinrikyo (responsable del atentado con gas sarín en el metro de Tokio en 1995), el Partido de los Trabajadores del Kurdistán (PKK), los extremistas violentos israelíes Kahane Lives o el grupo marxista turco DHKP/C.[14]

Al Qaeda era muy consciente de esta dimensión comunicativa. En julio de 2005, su número dos, Ayman Al Zawahiri, dijo en un discurso: «Estamos en una batalla, y más de la mitad de esta batalla está teniendo lugar en el terreno de los medios de comunicación. Y esta batalla en los medios es una batalla por ganar las mentes y los corazones de los miembros de la Umma [la comunidad global de creyentes del islam]».[15] Entre ese año y 2007, Zawahiri cuadruplicó la producción de vídeos.[16] La guerra de Irak marcó un importante punto de inflexión en este fenómeno: si hasta entonces los comunicados de Al Qaeda habían estado dirigidos mayoritariamente a audiencias musulmanas, a partir de ese momento, sus vídeos y productos comunicativos empezaron a dirigirse al mundo occidental. La

decapitación de rehenes ante las cámaras se convirtió en una ocurrencia regular.

En poco tiempo, la estrategia cognitiva de Al Qaeda pasó a ser vista como un éxito tanto por partidarios como por sus enemigos, que veían con desazón cómo sus mensajes llegaban a todos los rincones del planeta y suponían una fuente de radicalización constante. A finales de 2006, una delegación de los talibanes envió representantes a Irak para estudiar las técnicas de los yihadistas, que no tardaron en poner en práctica en el propio Afganistán.

Desde 2007, los talibanes empezaron a difundir sus propios vídeos propagandísticos, con temáticas como la ceremonia de graduación de una promoción de futuros terroristas suicidas, destinados a intimidar a las audiencias occidentales. También empezaron a dar entrevistas a Al Jazeera, e incluso permitieron que el corresponsal paquistaní de la cadena se empotrase con sus combatientes.[17]

«Se ha hablado mucho sobre la asimetría. La verdadera asimetría en esta campaña es que los talibanes se basan en un 90% en la psicología y un 10% en la fuerza, mientras que nosotros nos basamos un 90% en la fuerza y un 10% en la psicología. En un entorno en el que la percepción es la realidad, las memorias llegan muy lejos y se hacen enemigos muy fácilmente», declaró un comandante británico a su regreso de Afganistán en 2007.[18] En el punto álgido del conflicto, los talibanes llegaron a lanzar operaciones psicológicas, como conseguir los datos personales de soldados de la coalición desplegados en territorio afgano y usarlos para hacer llamadas amenazantes a sus familias.[19]

La siguiente etapa la marcó la explosión de las redes, que los yihadistas transnacionales empezaron a utilizar para operaciones psicológicas y propagandísticas. Los talibanes pasaron de una prohibición total del uso de internet y el control total de las comunicaciones a abrazar las nuevas herramientas.[20] Si en 1998 habían creado su primera web, durante su primera época como gobernantes de Afganistán, y desde 2005 mantenían una página oficial

llamada Al-Emarah —que hoy publica contenido en pastún, árabe, dari, urdu e inglés—, durante su época en el exilio y la guerra de guerrillas, utilizaron los estudios de Al Qaeda en Pakistán para producir vídeos de ataques con explosivos improvisados y de atentados contra vehículos de la coalición y las fuerzas de seguridad afganas.[21] Desde entonces, los yihadistas afganos han demostrado un manejo cada vez más avanzado, hasta el punto de que muchos expertos consideran que el uso eficaz de estas plataformas es una de las claves de su victoria contra la coalición internacional.

Soldados del cibercalifato

También la emergencia de Estado Islámico en Irak y Siria volvió a cambiar las reglas del juego. Esta organización se benefició del reclutamiento de miles de jóvenes que habían crecido con las nuevas tecnologías y con experiencia avanzada en el manejo de las redes, los códigos de internet y las narrativas audiovisuales, y que pusieron su experiencia al servicio de la ideología yihadista. El resultado fue lo que el investigador Javier Lesaca ha denominado «terrorismo transmedia», basado en la combinación de la violencia en el mundo real y su proyección en el virtual, en múltiples formatos que permitieran llegar a múltiples audiencias al mismo tiempo. Una auténtica guerra cognitiva multinivel destinada a seducir a los simpatizantes, convencer al mundo musulmán de la justicia y éxito de su causa, y atraer a los indecisos, al tiempo que se buscaba amenazar a los enemigos e intimidar e influenciar a las masas de civiles.

«Los terroristas de Estado Islámico habían comprendido que gran parte de su posible éxito radicaba en ganar la batalla de las percepciones, en construir una reputación en torno a su marca basada en valores intangibles que las audiencias potenciales percibieran como positivos, familiares y atractivos», escribe Lesaca en su libro *Armas de seducción masiva*, donde añade:

> El análisis científico de la comunicación del califato demuestra que su fórmula no solo consiste en crear, expandir y socializar el terror, sino que busca convertir el terrorismo en un producto de comunicación popular comprensible, seductor, bello e imitable. Un símbolo cultural lo bastante poderoso para canalizar la frustración, el odio, el vacío intelectual y político, e incluso el aburrimiento permanente, que afligen a miles de jóvenes en todo el mundo, y no precisamente a los más ignorantes o incultos.

Estado Islámico levantó la maquinaria de propaganda yihadista más formidable de la historia. No solo sus ejércitos virtuales inundaban las redes sociales de mensajes radicales,[22] sino que sus equipos también creaban y difundían repositorios de contenidos, para que cualquier simpatizante pudiese convertirse en un «soldado del cibercalifato» y contribuir a su esfuerzo en internet.[23] A medida que las plataformas y las autoridades internacionales desmantelaban sus estructuras, los voluntarios de Estado Islámico se convirtieron en expertos en el uso de Telegram, donde apenas existían restricciones, para seguir comunicándose con sus audiencias.[24]

ISIS no solo cuenta con su propia productora audiovisual, Al Furqan, sino que también creó agencias de prensa que publicaban comunicados e informaciones al estilo de una agencia profesional, entre las que destacaba Amaq, que difundía material sobre los atentados que cometía la organización,[25] y que sigue existiendo.

Varias productoras, como Ajnad Media y Asdaa Foundation, distribuían archivos de audio en árabe con los llamados *nashid*: música vocal cantada sin instrumentos y de contenido religioso, utilizada como propaganda. Al Hayat Media Center, la rama de propaganda internacional de ISIS, produce materiales en una docena de idiomas —inglés, francés, alemán, ruso, turco, urdu, kurdo, bosnio, indonesio, bengalí, uigur y chino—, y durante años publicaba revistas en varias de esas lenguas: *Dabiq* (inglés),[26] *Dar al-Islam* (francés), *Istok* (ruso), *Rumiyah* (árabe) y *Konstantiniyye* (turco).[27] Después ha creado otros organismos de comunicación específicos para regiones como la península arábiga (At-Taqwa Media), Uzbekistán (I'lam

Foundation) o Afganistán (Al-Azaim Foundation, que edita la publicación *Voice of Khorasan*).[28]

Estado Islámico también puso en marcha iniciativas como el desarrollo de su propia aplicación en árabe, «El amanecer de las buenas nuevas», que llegó a estar disponible para descarga gratuita en Google Play Store.[29] La *app* tomaba el control de las cuentas de X/Twitter del usuario, lo que permitía a una especie de *community manager* de la organización terrorista utilizarla para repostear los contenidos del grupo. Al combinar un número significativo de estas cuentas, podían amplificarse los contenidos de forma artificial, asegurándose de que estos reposteos estuviesen lo suficientemente espaciados entre unos y otros. Los usuarios podían seguir utilizando sus cuentas de forma normal el resto del tiempo. La combinación de ambas cosas —pausas en la difusión del mismo contenido y el uso orgánico por parte de los propietarios reales— permitían evitar los sistemas de detección automática de X/Twitter y la eliminación de estos enjambres de cuentas.[30]

Estado Islámico también recurrió a otras técnicas clásicas de *astroturfing*. Lanzó una cuenta en árabe llamada @ActiveHashtags, donde cada día publicaba los *hashtags* que le interesaba promover en esa jornada. Así, sus simpatizantes podían difundir los contenidos del grupo etiquetándolos con los *trending topics* del momento, lo que atraía a miles de usuarios y los exponía a su propaganda.[31] Estos *hashtags* no tenían por qué tener relación con el movimiento yihadista. Por ejemplo, el 19 de agosto de 2014, ISIS emitió el primero de una larga serie de vídeos de ejecuciones de prisioneros titulado «Un mensaje a América». Mostraba el degollamiento del periodista estadounidense James Foley a manos de un encapuchado. Para difundirlo, su ejército digital recurrió a los *hashtags* del día, incluyendo el cumpleaños de la cantante Demi Lovato, #22ReasonsWeLoveDemi, garantizando que muchos de los fans de esta estrella pop se encontraran súbitamente con las imágenes de la sangrienta ejecución y multiplicando su impacto social.[32]

Un impacto que puede ser formidable en muchos sentidos. En junio de 2014, las fuerzas de Estado Islámico avanzaban hacia la ciudad iraquí de Mosul, defendida por unos 20.000 soldados regulares iraquíes entrenados y bien equipados. En contraste, los efectivos yihadistas apenas superaban el millar. Pero el ciberejército yihadista llegó a generar 40.000 tuits en un día, en los que se exageraban las capacidades de ISIS y sus conquistas. Los militares iraquíes carecían de datos de inteligencia, pero prácticamente todos tenían un teléfono móvil, y ansiosos por la situación, empezaron a buscar información en las redes. Se encontraron una previsión apocalíptica de la inminente caída de Mosul. Atrapados por el pánico, y ante la llegada de lo que pensaban eran unas fuerzas muy superiores, huyeron a toda prisa, dejando la ciudad indefensa y abandonando equipamiento y vehículos militares por valor de cientos de millones de dólares, de los que inmediatamente se apropiaría el enemigo.[33]

Los talibanes aplicaron una estrategia similar durante su avance sobre Kabul en 2021: exagerando victorias incluso en lugares que todavía no habían conquistado. La presencia de combatientes con teléfonos móviles que podían tomar imágenes de lugares reconocibles les permitía atribuirse esas localidades como «liberadas», propiciando la huida de las fuerzas del Gobierno central y convirtiendo el vídeo o la foto en profecía autocumplida. Sus mensajes enfatizaban su control territorial; su victoria, inevitable. Al mismo tiempo, reforzaban que su ofensiva equivalía a una liberación, negando legitimidad del Gobierno de Ashraf Ghani,[34] presentado como una marioneta de la coalición internacional, que aparecía descrita como una fuerza invasora. Los talibanes, como una fuerza moderada que buscaba un Afganistán soberano, verdaderos guerreros del islam.[35]

Ejércitos de cuentas de simpatizantes y militantes tuiteaban *hashtags* en inglés como #kabulregimecrimes («crímenes del régimen de Kabul») o #westandwithTaliban («estamos con los talibanes»), o en pastún y árabe con leyendas como «Dios nos ayuda y la victoria está cerca».[36]

Tras la caída de la capital afgana en el verano de 2021, la experta del Atlantic Council Evanna Hu escribió un revelador comentario titulado «El secreto del éxito de los talibán: *Psy-Ops*», donde afirmaba:

> En una gran parte de los territorios conquistados por los talibanes hubo pocos o ningún combate, gracias a las operaciones psicológicas estratégicamente organizadas por el grupo contra el ejército afgano y los funcionarios gubernamentales de alto nivel, así como contra la población afgana. Al atacar a los primeros, los talibanes han hecho promesas políticas e inflado el número de tropas que tienen. También han conformado una narrativa de que los aliados del Gobierno afgano, principalmente Estados Unidos, los han abandonado, además de resaltar las malas acciones del Gobierno durante las últimas dos décadas, particularmente la corrupción generalizada. Mientras tanto, a la población el grupo le promete estabilidad y le comunica que sus vidas bajo el Gobierno no son mejores.[37]

Después de su victoria, los talibanes mantuvieron una intensa estrategia comunicativa en redes. Promovieron la proliferación de *youtubers* e *influencers* afganos que mostrasen las maravillas naturales y culturales del país, así como las supuestas bondades de su régimen. Según medios afganos, pagan salarios de hasta 10.000 afganis (unos 190 dólares) a casi un centenar de creadores de contenido. Algunos *youtubers* niegan su afiliación con el grupo o recibir dinero, pero de lo que no hay ninguna duda es de que, en el Afganistán de hoy, no podrían trabajar sin, al menos, su autorización tácita[38]. También están permitiendo la entrada de *influencers* extranjeros, en un intento de suavizar su imagen y legitimar su gobierno,[39] buscando tanto el reconocimiento internacional como la llegada de potenciales inversores.

La propaganda yihadista en internet goza de buena salud gracias a su adaptabilidad,[40] que les ha permitido integrar avances tecnológicos, desde TikTok[41] hasta la IA. Conforme mejoraban los mecanismos de detección automática, por ejemplo, simpatizantes de Estado Islámico empezaron a colocar logotipos de Netflix o Amazon Studios sobre sus

emblemas, para esquivar las restricciones de dichas plataformas.[42] También han empezado a copiar técnicas de otros actores, como Rusia, creando vídeos desde cero en los que integran logos de medios como CNN y Al Jazeera. En 2024, el ISIS se atribuyó el atentado del Crocus City Hall de Moscú con ocho vídeos así, cuando el atentado lo había cometido el ISKP, la rama afgana del grupo, como respuesta a la campaña rusa que insistía en culpar a Ucrania.

«Eran esencialmente *fake news* para desmontar otras *fake news*», le dijo el analista Moustafa Ayad, del Instituto para el Diálogo Estratégico, a la publicación *Wired*.[43] Cuatro días después de ese atentado, ISIS difundió un videoclip de 92 segundos de un programa llamado «News Harvest», cuyo presentador aparecía en ropa de combate diciendo que el ataque no era una operación terrorista, sino «el contexto normal de la guerra en marcha entre Estado Islámico y aquellos países que luchan contra el islam». Lo sorprendente es que ni la imagen ni el reportero eran reales: habían sido generados totalmente por inteligencia artificial. A partir de entonces, el ecosistema yihadista empezó a emitir vídeos de «News Harvest» creados mediante IA con una frecuencia casi semanal, informando sobre sus acciones en todo el mundo.[44]

EL CONTRAATAQUE DE LA NAFO

«Necesitamos un nuevo marco conceptual que tome en cuenta cómo las redes sociales han transformado la forma en la que las guerras se llevan a cabo, se cubren y se consumen», sostiene Patrikarakos, quien destaca «la extraordinaria capacidad de las redes para otorgar a individuos ordinarios, frecuentemente no combatientes, el poder de cambiar el curso del campo de batalla físico y el discurso alrededor de este». Conceden dicho poder gracias a «una forma de alistamiento virtual masivo» en la que «todo el mundo podía ser ahora un actor en la guerra».[45]

El mejor ejemplo de cómo grandes ejércitos de trols pueden movilizarse por una causa, incluso de forma espontánea, sea el surgido a raíz de la invasión rusa de Ucrania: la NAFO, las siglas en inglés de North Atlantic Fellas Organization (Organización de Colegas del Atlántico Norte, en traducción libre), cuya imagen icónica es un perro de la raza japonesa *Shiba Inu* pertrechado con todo tipo de uniformes y armas.

Los miembros de la NAFO, algunos de los cuales se coordinan a través de un servidor de la plataforma Discord, se dedican a trolear a diplomáticos rusos y a cuentas que difunden mensajes prorrusos. A finales de 2022, eran capaces de lanzar más de 5.000 tuits al día.[46] La lógica detrás de esta estrategia, dado que Rusia ha perfeccionado el arte del troleo, es responderle con su propia medicina, volviendo absurdas las interacciones. «En lugar de que los trols y propagandistas [rusos] arrastren a sus oponentes a discusiones fútiles que no llevan a nada, si la conversación en sí es ridícula, va contra sus intereses enzarzarse en ella», explica Keir Giles, un experto sobre Rusia del *think tank* británico Chatham House, en un informe revisado por la CNN. O en palabras de Matt Moores, cofundador de dicho laboratorio de ideas, y que pronunció durante un acto en el Centro de Estudios Estratégicos e Internacionales de Washington: «En el momento en el que alguien le está respondiendo en internet a un perro dibujado, ha perdido».[47]

Le sucedió al diplomático ruso Mijaíl Ulyanov el 18 de junio de 2022, cuando tuiteó: «La narrativa occidental más popular: Rusia lanzó una invasión no provocada de Ucrania. ¿No provocada? El bombardeo de la población civil en el Dombás por el ejército ucraniano empezó en 2014 y continúa hasta ahora». Inmediatamente, la cuenta de análisis militar y miembro de la NAFO @LiveFaustDieJung le respondió: «Tú: "Tenemos que bombardear a todos los civiles de Ucrania porque Ucrania estaba luchando una guerra interna y algunos civiles fueron bombardeados"». Ulyanov, exponiendo accidentalmente las contradicciones de la propaganda

rusa, replicó a su vez: «Tú has pronunciado este sinsentido. No yo». El diplomático no solo recibió una tormenta de respuestas proucranianas, obligándole a desaparecer de las redes durante días, sino que su frase se convirtió en un eslogan memético de la NAFO.[48]

«Solía ser difícil hablar sobre lo que está haciendo Rusia sin que te gritasen los trols, y la gente se sentía sola haciéndolo. La NAFO ha estado usando esas tácticas de forma inversa para darle espacio a la gente donde hablar de forma crítica sobre Rusia, sabiendo que hay una batalla en marcha», explicó el responsable de la cuenta Bad Baltic Takes —uno de los voluntarios de la NAFO en Estonia— en una entrevista con el diario británico *The Times*.[49]

La agrupación ha supuesto un quebradero de cabeza para Rusia. María Zajárova, portavoz del Ministerio de Exteriores: «La NAFO personifica lo que la UE parecía estar combatiendo: el discurso de odio, la intolerancia, todas las formas de xenofobia. Esta es la esencia de la hipocresía de Occidente: "Nos volveremos unos hijos de perra, si sirve para escupir a Rusia"», escribió en su cuenta de X/Twitter.

No es de extrañar que el ecosistema de desinformación ruso los describa como un proyecto de guerra informativa de la CIA, el Pentágono y otros servicios de seguridad occidentales. Anticipándose, muchos de los integrantes de la NAFO ponen como ubicación de sus cuentas de X/Twitter «Langley, Virginia», donde se encuentra la sede de la CIA.[50]

Pero no hay nada secreto u oscuro en su origen: fue fundado en mayo de 2022 por un artista polaco llamado Kamil Dyszewski (Kama) a través de su cuenta @Kama_Kamilia y como parte de una iniciativa de recaudación de fondos para la Legión Georgiana, una unidad militar de voluntarios internacionales en Ucrania. Kama utilizó la imagen de un *Shiba Inu*, un conocido icono de las subculturas de internet desde 2010, cuando el dueño de uno de estos perros le hizo una fotografía a su mascota en la que parecía levantar las cejas en un gesto de sorpresa. La imagen se convirtió en un meme llamado

«Doge», y llegó a motivar la creación de una criptomoneda, el Dogecoin, que ha ido ganando valor con los años.[51]

El caso es que Dyszewski tomó este icono, lo colocó sobre un logotipo modificado de la OTAN y comenzó a vender la imagen resultante, que se convirtió en un éxito. Kama adaptaba el diseño a petición de los clientes, que empezaban a actuar como trols voluntarios en esta operación de influencia improvisada contra Rusia. En pocas semanas, su número era el suficiente para un impacto real. Varios establecieron unas mínimas líneas organizativas y objetivos. Había nacido la NAFO.

«Por sí sola, la forma editada del logo de la OTAN no se habría extendido. Pero, al añadirle con plena conciencia un meme y un espíritu de irreverencia, el movimiento empezó a crecer», señala el investigador en ciberpolítica Callum Harvey, en una publicación del Instituto Australiano de Política Estratégica (ASPI). «Permite a los usuarios que creen el suyo propio. No hay una autoridad central. Miembros del enjambre crean sus propios avatares de los "fellas" (amigos, colegas) de la NAFO, o se los regalan a otros. Los "fellas" trabajan juntos, coordinando respuestas para ahogar los contenidos de desinformación y llamando la atención sobre casos de crímenes de guerra o fallos del ejército ruso».[52]

Pese a su origen orgánico, hay indicios de que durante la guerra de Ucrania muchos mensajes en redes han sido amplificados artificialmente por cuentas vinculadas a los servicios secretos occidentales y ucranianos. Entre sus voluntarios —más bien, miembros honoríficos— hay figuras como el exsecretario británico de Defensa Ben Wallace, la jefa de la diplomacia europea Kaja Kallas, el ministro ucraniano de Defensa Oleksii Reznikov, el congresista estadounidense Adam Kinzinger o el ex primer ministro estonio Toomas Hendrik Ilves. En julio de 2023, la agrupación había crecido tanto, que pudo organizar su primera «Cumbre de la NAFO» en Vilna, a la que asistió el ministro de Exteriores lituano Gabrielius

Landsbergis. Pocos días antes, la OTAN había celebrado su cumbre en esa misma ciudad.

Al tratarse de un colectivo descentralizado sin líderes ni un código deontológico claro, la NAFO ha sido criticada por las posturas maximalistas de muchos miembros. Por ejemplo, analistas militares occidentales nada sospechosos de simpatías prorrusas han sufrido las iras de voluntarios por señalar las dificultades —totalmente reales— del ejército ucraniano en el campo de batalla, acusándoles de difundir propaganda rusa o de hacerle el juego al Kremlin. Es lo que sucede cuando desatas a los trols.

Pero, cuando Patrikarakos habla de que estas capacidades están ahora al alcance de cualquiera, literalmente acierta. Y no solo grupos e individuos vinculados a movimientos políticos, sino también organizaciones criminales.

En Brasil, el Comando Vermelho de Río de Janeiro utiliza las redes sociales para intimidar a organizaciones rivales y a la policía. También para dar publicidad a las acciones en favor de la comunidad, como los intentos de imponer la distancia social durante la pandemia del COVID-19. O para reclutar a nuevos miembros. Sus miembros alardean en redes de su pertenencia, y glorifican a los «caídos en combate» contra las autoridades y otros enemigos.[53]

Los cárteles mexicanos tienen una importante presencia en línea con fines similares. A mediados de la primera década de este siglo comenzaron a colgar vídeos de ejecuciones y otras atrocidades en YouTube, como la paliza y decapitación de un miembro de Los Zetas en 2007, una de las primeras instancias documentadas de este tipo de contenidos.[54] La aparición posterior de Estado Islámico y la difusión de sus ejecuciones forzó a las plataformas digitales a establecer protocolos para eliminar rápidamente las imágenes violentas, lo que también afectó a los cárteles. ISIS respondió desplegando enjambres de cuentas no oficiales para atomizar la expansión de las imágenes, dificultando su detección y eliminación. Y las organizaciones criminales imitaron su estrategia.[55]

Un informe del International Crisis Group de principios de 2024 analiza en profundidad el fenómeno. «La intimidación de grupos rivales y civiles está en el centro del uso de las redes sociales por las empresas criminales. Para este fin, cuelgan imágenes violentas, incluyendo fotos y vídeos de decapitaciones, palizas y torturas». Los contenidos más violentos son publicados en cuentas que saben que van a ser eliminadas muy pronto, pero desde allí, como hemos visto en el caso de Hamás, saltan a otras cuentas o a grupos de difusión en aplicaciones de mensajería encriptadas, como WhatsApp y Telegram, donde los esfuerzos de moderación son mucho más complicados al tratarse de chats secretos. En una segunda vía, los llamados «narcoblogs» propagan este mismo tipo de contenidos.[56]

En Facebook recaban información sobre enemigos y preparan ataques y amenazas. También muestran sus capacidades militares y ensalzan la «narcocultura»: vida de lujo de los traficantes, «narcocorridos» o filantropías a favor de la comunidad. Durante la pandemia, el cártel Jalisco Nueva Generación distribuyó paquetes de comida con su logotipo mientras lo publicitaba.[57] Igualmente, reclutan, con indicaciones a los aspirantes sobre cómo contactar con los enlaces de sus grupos criminales.

Además, los cárteles utilizan las aplicaciones de mensajería para coordinar sus ataques. Según un informe interno de Meta citado en el informe del ICG, los participantes en el atentado contra el jefe de policía de la Ciudad de México en 2020 utilizaron Messenger para informarse unos a otros en tiempo real. Más espectacular fue lo sucedido durante el ya mencionado «Culiacanazo»: el cártel de Sinaloa lanzó mensajes en WhatsApp ofreciendo dinero a cualquiera que se uniese a la ofensiva contra las fuerzas de seguridad. Una vez que lograron la liberación de Ovidio Guzmán, *el Chapito*, usaron esta misma *app* para decretar el fin del ataque.[58] Pero, al mismo tiempo que las redes han servido para empoderar a los criminales, también lo han hecho con la sociedad civil. Ciudadanos anónimos, narcoblogs y

páginas específicas cumplen una función esencial al informar sobre estallidos de violencia, crímenes, etcétera.

El último informe del Instituto de Internet de Oxford sobre prácticas globales de manipulación digital, publicado en 2021, aportó una clave final sobre otra tendencia: el recurso a empresas privadas por parte de todo tipo de actores. Si cuatro años antes, el OII solo había detectado nueve casos en todo el mundo, para entonces la cifra había saltado a 48, alimentada por la notoriedad de Cambridge Analytica.[59] Y, como veremos en el capítulo siguiente, el fenómeno solo acababa de empezar.

5

MERCENARIOS DE LA DESINFORMACIÓN

Llamémosle «Paul», y digamos que es europeo y trabaja para una de las firmas de inteligencia privadas más importantes de su país. Entre sus clientes se encuentran las principales multinacionales que cotizan en bolsa. La empresa de Paul se dedica a recabar información sobre los competidores de quienes la contratan, revisando todos los datos disponibles en fuentes abiertas y reclutando informantes que puedan tener acceso a elementos clave. Pero, a veces, algunos clientes también solicitan otros servicios adicionales.

En una ocasión, les pidieron una campaña digital para desacreditar a una marca rival. Paul y su equipo pasaron meses creando falsos perfiles en redes sociales, hablando sobre cuestiones intrascendentes —fútbol, asuntos culturales, noticias políticas— para, en un momento dado, llevar a cabo una acción coordinada tratando de erosionar el prestigio público del objetivo.[1] Esto ocurrió en 2019. Hoy, la empresa ni siquiera se molestaría en crear aquella red de perfiles falsos: subcontratarían a otra empresa especializada en este tipo de operaciones. Más eficaz y más barato que diseñarlas y ejecutarlas desde cero.

Las posibilidades de manipulación generadas por los nuevos ecosistemas digitales en los que todos nos desenvolvemos han creado una oportunidad de mercado copada por profesionales, que operan en las sombras al servicio de quienes pueden pagarlo. Estas firmas se mueven entre el marketing digital, la consultoría política, las relaciones públicas y la recopilación de información, en ocasiones por medios no lícitos. El fenómeno se añade a los operadores privados de inteligencia, que cubren una necesidad creciente de las grandes

corporaciones que, enfocadas en sectores muy específicos, a menudo no están en condiciones de abarcar con sus propios medios.

En el mundo periodístico existe desde hace años un término para referirse a esta industria: «Desinformación de alquiler» o «desinformación como servicio»,[2] que se complementa con el que suele utilizarse en el propio sector, como «Black PR» o «relaciones públicas negras». Un campo que no deja de crecer: según una investigación de *BuzzFeed News*, las plataformas de Silicon Valley habían detectado entre 2011 y 2020 al menos 27 operaciones de desinformación en redes sociales atribuibles, total o parcialmente, a empresas privadas de este tipo. De ellas, o el 70% del total (19), habían tenido lugar tan solo en el año anterior. La cifra no ha hecho sino aumentar.

Cindy Otis, exanalista de la CIA y autora de un libro sobre detección de desinformación,[3] aseguró a ese mismo medio que las operaciones de información de países como Rusia e Irán habían creado «un manual para que individuos y grupos cuya motivación es financiera se adentren en este espacio». Cuanto más experimentan los Estados en este campo, más aprenden las empresas privadas.[4]

En 2019, la firma de ciberseguridad Recorded Future llevó a cabo un experimento: creó una empresa ficticia y contactó a dos grupos de cibercriminales rusos. Al primero le pidió una campaña positiva para aumentar el atractivo de la empresa, mientras que al segundo le encargó una operación de difamación acusándola de prácticas poco éticas. Los investigadores descubrieron que «lanzar una campaña de desinformación es alarmantemente simple y barato»: el total que abonaron a ambos grupos fue de apenas 6.050 dólares, 1.850 para la campaña positiva y 4.200 para la negativa. «Los servicios de desinformación están disponibles públicamente en los foros criminales *underground* y accesibles a clientes del sector privado, no solo a estados nación. Estos servicios son asequibles y personalizables», concluyó la compañía.[5]

HUNDIR LA REPUTACIÓN

La firma suiza Alp Services estaba especializada en campañas reputacionales negativas. Durante dos décadas llevó a cabo operaciones de inteligencia en Kazajistán, Montenegro, el Congo, Nigeria, Gabón, Mónaco, Angola, Uzbekistán y Arabia Saudí. Su lista de clientes incluía a millonarios franceses, estadounidenses, israelíes, kazajos, rusos y de varios países de Europa oriental. En 2023, se desveló que Alp Services había estado trabajando para los Emiratos Árabes Unidos en una campaña de investigación y descrédito contra cualquier individuo en Europa sospechoso de simpatías o vínculos con los Hermanos Musulmanes, una organización que el monarca emiratí Mohamed Bin Zayed odiaba por encima de todas y a la que veía como su principal enemiga.[6]

Aprovechándose de ello, Alp elaboró listas de centenares de personas y organizaciones en toda Europa (incluida España),[7] con acusaciones a menudo ridículas.[8] El episodio no habría pasado del bochornoso fraude de una firma privada que explotaba la paranoia de su cliente si no fuese porque el contrato también incluía la difamación pública de muchos de estos objetivos, a través de filtraciones a periodistas y medios favorables a las «revelaciones»,[9] caso de la reescritura de entradas en Wikipedia, la manipulación de los resultados de búsqueda en Google y la difusión de contenidos que mezclaban realidad y fantasía en redes sociales, que después eran amplificados por publicaciones reales o políticos de ideas islamófobas.[10] El plan último consistía en mostrar que las víctimas tenían relaciones con los Hermanos Musulmanes, con Qatar, con organizaciones yihadistas o con todos a la vez.[11]

Algunos rumores tuvieron efectos devastadores para los afectados. El empresario Hazim Nada, hijo de un antiguo miembro de la Hermandad Musulmana, carecía de vínculos, pero Alp logró plantar artículos en varias publicaciones de segunda fila y en blogs en los que acusaba a su empresa de logística energética Lord Energy de estar

relacionada con Al Qaeda. Como resultado, una importante base de datos sobre *compliance*, o cumplimiento regulatorio, puso a Lord Energy dentro de la categoría de «riesgo», lo que llevó a clientes importantes a cortar lazos con ella. Nueve días después, la base de datos se retractó públicamente, pero el daño estaba hecho: Credit Suisse, el banco que financiaba las operaciones de Lord Energy, dejó de hacerlo. Cuando Nada se reunió con el director de la entidad financiera, este le explicó que incluso la mera apariencia de posibles vínculos con el terrorismo era un riesgo reputacional inaceptable. Lord Energy acabó quebrando.[12]

Los detalles de toda la campaña sucia se conocieron a principios de 2023. No obstante, un grupo de hackers había conseguido acceder a la información interna de Alp Services años antes, y se la había ofrecido a Nada a cambio de treinta millones de dólares en criptomonedas. Pero el empresario no tenía liquidez ni intención de adquirirla.[13] Los documentos acabaron llegando al diario francés *Mediapart*, que los compartió con el consorcio de reporteros European Investigative Collaborations, y acabaron publicados por media docena de medios en todo el continente.[14]

En España…

También Cenyt, la empresa de inteligencia privada del hoy bien conocido comisario José Manuel Villarejo,[15] ofrecía entre sus servicios «generar desconcierto y/o desconfianza en su círculo más íntimo y operativo, con continuas maniobras de intoxicación informativa» acerca del objetivo designado por el cliente. El caso más conocido es el llamado «Informe King», elaborado a petición de una de las esposas del dictador de Guinea Ecuatorial, Teodoro Obiang, para desacreditar a uno de sus hijos con otra mujer, el ministro de Minas e Hidrocarburos del país, Gabriel Mbega Lima, y asegurar que al autócrata le sucediese su otro hijo, Teodorín Obiang Nguema.

La firma de Villarejo ofrecía «neutralizar y en todo caso penetrar en su equipo de apoyo informativo con el fin de alterar los datos estratégicos que consigan, inutilizando su eficacia y rentabilidad [...] debilitando sus capacidades políticas con opción, incluso de poder facilitar informes negativos al entorno de GM —las iniciales con las que se referían a Gabriel Mbega—». Villarejo proponía crear una «plataforma amiga» en la que lanzar la información negativa para la víctima. Pedía, a cambio, 5,3 millones de euros por la operación, cuyas posibilidades de éxito cifraba en un «85%».[16]

Otras empresas de este cariz operan en España y Latinoamérica. Uno de los ejemplos más conocidos es el de la firma i3Ventures, cuyo nombre saltó a los medios en febrero de 2020 cuando la cadena SER desveló que había sido la herramienta del llamado «Barçagate»: una campaña en redes orquestada por el entonces presidente del Futbol Club Barcelona Josep Maria Bartomeu para atacar a sus críticos y manipular el espacio digital para tratar de asegurarse la reelección en el cargo.[17] Siguiendo órdenes de Bartomeu, el Barça contrató a i3Ventures en 2017 para hacer trabajos de análisis y monitorización del sentimiento en redes acerca del club. Sin embargo, según las revelaciones periodísticas, la empresa también creó perfiles falsos en Facebook y X/Twitter desde los que se alababa la gestión del presidente, al tiempo que atacaba la imagen de otros candidatos al cargo y arremetía contra jugadores antiguos, como Carles Puyol o Pep Guardiola, o contra estrellas en activo como Leo Messi o Gerard Piqué, que habían criticado a Bartomeu.[18] La empresa cobró 990.000 euros.

Unos días después de saltar el escándalo, el ingeniero informático y etnógrafo digital Josep María Ganyet entrevistó a una extrabajadora de i3Ventures identificada como Sonia D., quien le explicó el funcionamiento interno de la empresa. En realidad, Sonia trabajaba para otra empresa llamada Nicestream, con la que comparte sede social y administrador, aunque en la práctica la distinción entre ambas es casi testimonial. Sonia relató que la firma hacía campañas tanto

positivas, para elevar el perfil de un cliente, como negativas, deteriorando la imagen de un objetivo designado. Utilizaban perfiles falsos comprados en Rusia, donde son baratos, y «humanizados» por el equipo de Nicestream, dándoles nombres y avatares verosímiles. Durante algunos meses, les van creando una personalidad a base de postear frecuentemente sobre contenidos inocuos.

Cuando llega un cliente, la empresa decide cuáles de dichos perfiles podrían encajar con los objetivos que les requiere. Si una de estas cuentas es desenmascarada como falsa, se descarta para siempre. Su principal campo de actuación es X/Twitter, porque es la plataforma de mayor impacto político, seguida de Facebook, dado el elevado número de usuarios. «Instagram y LinkedIn no los trabajábamos», le dijo esta exempleada a Ganyet. También le confirmó que la empresa cuenta con una potente herramienta de procesamiento masivo de datos llamada Sentinnel, que, según la web oficial «sigue, analiza e interpreta la actividad social basándose en diferentes técnicas de inteligencia artificial para crear y proteger reputación para marcas, productos, artistas, políticos y ejecutivos». De acuerdo con Sonia, el software es muy eficiente no solo para monitorizar redes, sino también para influir en estados de opinión.[19]

La historia continúa con datos más interesantes: el administrador único de i3Ventures y Nicestream es un empresario uruguayo llamado Carlos Rafael Ibáñez Constantino, también cofundador de otra empresa registrada en Buenos Aires, Illuminati Lab, junto a otro hombre de negocios, Gastón Douek, a quien la prensa argentina apodó como «El Señor de los Trols». Ibáñez y Douek son las dos figuras clave, juntos o por separado, en una red de compañías dedicadas al marketing político y a la gestión reputacional con un componente importante de desinformación y manipulación digital. En su perfil de LinkedIn, Illuminati Lab asegura haber tomado parte en «más de veinte procesos electorales» y en «crisis institucionales y cuestiones de imagen pública» en Argentina, Chile, Colombia, Guatemala, México, Panamá, Paraguay, Brasil, Ecuador y Uruguay. En

una entrevista con el diario argentino *La Nación*, Douek afirmó que la empresa llegó a tener 150.000 cuentas falsas operando en las elecciones de México en 2012.[20]

Douek e Ibáñez también constituyeron en 2009, junto a otros dos socios, otra empresa llamada Emerging Media Consulting de México, que fue contratada por el Gobierno de Enrique Peña Nieto para limpiar la reputación de Petróleos Mexicanos (Pemex).[21] También trabajó para el Gobierno de Rafael Correa en Ecuador hackeando páginas de internet críticas con el entonces presidente ecuatoriano —como una llamada Bananaleaks, que lograron tumbar con éxito—, y atacando a un destacado político opositor[22]. Las diferentes empresas de Ibáñez ayudaron asimismo a blanquear la imagen de la constructora brasileña Odebrecht tras un escándalo internacional de sobornos llamado «caso Lava Jato», logrando que las menciones positivas pasasen de un 1% a un 35% en doce meses.[23] Una trayectoria que demuestra que estas actividades son eficaces para quienes las contratan, y tremendamente lucrativas para quienes las llevan a cabo.

… y en todo el mundo

La industria de los cibermercenarios no se limita a Occidente. Desde hace una década, China estimula la creación de empresas «patrióticas» que ejercen de contratistas para entidades gubernamentales, como el Ministerio de Seguridad Pública —del que depende la policía—, el Ministerio de Seguridad del Estado —el servicio de inteligencia—, o el Ejército de Liberación Popular. La mayoría se dedican al hackeo, pero otras libran guerras cognitivas.

Es el caso de iSoon, una firma con sede en Shanghái que ofrece entre sus servicios «el control y gestión de las conversaciones en X/Twitter» y la posibilidad de detectar y responder a «sentimientos reaccionarios» e «ilegales» a través de cuentas controladas para «manipular la discusión». ¿El precio? 55.600 dólares por paquete.

Dado que X/Twitter está bloqueada en China, cabe entender que se refieren a usuarios chinos que recurren a mecanismos como una red privada virtual (VPN) para evadir las restricciones, o bien a residentes en otros Estados. Es decir, guerra cognitiva en estado puro. Lo conocemos gracias a documentos internos filtrados en la plataforma GitHub en febrero de 2024[24] —posiblemente por un empleado descontento o por un grupo rival que hackeó a iSoon— que ofrecen una ventana detallada, incluidas sus tarifas, planes de negocio y correos electrónicos cruzados con sus clientes en los que se describen algunos de los objetivos atacados.

En Taiwán opera desde hace años una empresa llamada Bravo-Idea, dedicada a reescribir artículos en chino usando un software especializado, para después publicarlo en webs controladas y, finalmente, amplificarlos mediante miles de cuentas en redes. «He desarrollado esto para manipular la opinión pública», explicó el creador de la empresa, el empresario Peng Kuan Chin, al medio de investigación taiwanés *The Reporter*. Entre sus clientes se encuentran grandes empresas, marcas, partidos políticos y candidatos de países asiáticos.[25]

La lista de empresas en todo el planeta es interminable. En Arabia Saudí, Smaat operaba una red de 88.000 cuentas que, entre otras ocupaciones, se dedicaba a denigrar al periodista Jamal Khashoggi, asesinado en el consulado saudí en Estambul. En Egipto, New Waves gestionaba páginas falsas que imitaban medios de comunicación para promover mensajes favorables a los países del Golfo en estados africanos en conflicto como Sudán y Libia.[26] En México, encontramos la empresa de relaciones públicas Sombrero Blanco.[27] En Georgia tenemos una agencia de publicidad llamada Panda. En Puerto Rico, la consultoría de marketing KOI. En Ucrania, otra firma de relaciones públicas llamada Pragmatic, igual que Cat@ Net en Polonia.[28] Aún más conocidas son las actividades del Grupo Archimedes, una empresa israelí que operaba cientos de cuentas en redes para interferir en las elecciones de países como Mali, Senegal, Togo, Níger, Túnez o Nigeria,

así como en Panamá, México y Honduras.[29] En todos estos casos sabemos de su existencia por los informes de plataformas que han tumbado sus redes de cuentas falsas.

El «BOT RUSO» QUE DESVELÓ TODO

A principios de 2022, el libro *Confesiones de un bot ruso* mostró los entresijos de esta industria entonces desconocida. Un antiguo trabajador de una empresa que el texto nunca identifica explica las técnicas para manipular el discurso digital, y por qué son tan eficaces. El autor se hace llamar de forma irónica «Bot Ruso» porque, según sostiene, cada vez que aparecen sospechas de manipulaciones digitales se traen a colación los famosos bots de Rusia, cuando, casi siempre, son obra de individuos como él, al servicio de una entidad comercial.

Entrevisté a Bot Ruso por aquella época, vía correo electrónico, para que me aclarase algunas cuestiones sobre el sector. «En el imaginario popular se ha instalado la idea de chicos inadaptados y encapuchados que se esconden en un garaje con sus portátiles para hacer el mal. Y la realidad es muy distinta. Sí, el perfil general es que se trata de personas jóvenes, pero nada que ver. Se trata de profesionales con formación y conocimientos sobre sociología y marketing digital. Que trabajan en oficinas con espacios diáfanos y mesas divididas en grupos de trabajo y jerarquías. El salario del que tiene una nómina, como fue mi caso, ronda los mil euros al mes. La verdad, para el sacrificio y dedicación que se exige, y teniendo en cuenta lo que se factura, me parece una cifra irrisoria», se quejaba.

Bot Ruso dejó claro que, cuando estaba dentro, no se planteaba dilemas morales: «Yo abandoné mi cargo por cuestiones relacionadas con el estrés y la ansiedad. Nada que ver con la conciencia. No fue hasta tiempo después cuando empecé a hallar casos similares. Y al verlos desde fuera, pensaba: "Joder, qué hijos de puta". Y, a la vez, me daba cuenta de que yo había hecho exactamente lo mismo».

Quise indagar si empresas como aquella de la que había formado parte trabajaban para todo tipo de clientes. Si existían sesgos por afinidad política o ideológica, o si manejaban listas negras de clientes a rechazar. «Es una pregunta interesante. Aquí cada agencia sabrá lo suyo, pero hay un detalle a tener en cuenta: a diferencia de otro tipo de negocios, no es el cliente quien viene a ti, sino que es la agencia quien va al cliente. Para dirigirte a la empresa, necesitas un contacto. Así que dependerá de los contactos que tengas. Definirán, por ejemplo, si puedes trabajar para izquierda y derecha, solo para derecha o solo para izquierda». No le constaban casos de firmas de su sector que hubiesen realizado servicios para gobiernos o agencias de inteligencia.

Le pregunté también si, además de manipular el sentimiento en redes, recurría a la desinformación pura y dura. Su respuesta fue muy ilustrativa, basada en un escenario ficticio: «Pongamos un supuesto: yo tengo un cliente. Llamémosle X. *El Confidencial* publica una nota, firmada por Daniel Iriarte, en la cual se desvela una trama de corrupción de menores en la cual ha estado implicado el señor X. *El Confidencial* anuncia la publicación de más información durante los próximos días. Es posible que esa trama de corrupción de menores sea cierta y que el señor X haya estado implicado. Pero a mí eso me da igual. Mi objetivo y prioridad tiene nombre y apellidos: Daniel Iriarte. Lo primero que haría es una búsqueda de información sobre esa persona. Para ello, se utilizan herramientas OSINT,[30] que permiten crear un documento muy detallado: en este caso, de Daniel Iriarte. Pongamos que en dicho documento se encuentra un dato (irreal): te pillaron en una redada en un prostíbulo cuando tenías veinte años. Existen herramientas de Open Data muy potentes que permiten recolectar la información necesaria sin necesidad de acudir a prácticas ilegales, como es la compra de datos que no están autorizados para ese fin».

¿Y a partir de ese momento? «El siguiente paso es elegir... no sé, ¿te parecen bien cincuenta cuentas *troll*? Estas cuentas se dividirían en veinte cuentas para acosarte (dejarte treinta comentarios negativos

cada vez que publiques un tuit), diez cuentas para influenciar en la conversación (difundir la información polémica sobre Daniel Iriarte) y otras veinte que se moverán entre los principales influenciadores del clúster para instaurar la información polémica sobre Daniel Iriarte». Y *voilà*: se ha completado un proceso de lo que en el mundo anglosajón se denomina «asesinato del personaje», una campaña de descrédito brutal que, inevitablemente, genera antipatía por la víctima y lleva a las audiencias a desconfiar de lo que esta diga, a menudo de forma inconsciente.

Bot Ruso me pintó un panorama deprimente, en el que los ciudadanos tienen escaso margen de defensa ante una industria poderosísima. «Somos fáciles de manipular. Piensa que estas agencias te han investigado antes de ponerse en acción para saber qué es lo que más te duele. De esa forma saben dónde, cómo y cuándo compartir un mensaje efectivo para manipularte. El problema es que las leyes, por lo general, están anticuadas. Y hay muchas cosas que no se contemplan. Está claro que lo que sucede en el mundo digital tiene consecuencias en el real (por eso mismo, se contrata a este tipo de agencias). Así que, bajo mi punto de vista, también deberíamos plantearnos si debe estar prohibido. El primer paso es saber de qué nos defendemos. Este tipo de agencias son muy herméticas y hay mucho desconocimiento». Esperaba que su libro ayudase a descubrir cómo funcionaban estas empresas y a paliar el problema. «Me gustaría decirte que espero que tengan poco futuro, pero es complicado».[31]

«No tenemos la culpa de que al ciudadano no le interese su país»

A juzgar por el ejemplo de Carlos Merlo, es difícil no darle la razón a Bot Ruso. Merlo, empresario mexicano, ha convertido su firma Victory Lab en una máquina de hacer dinero ofreciendo servicios de «periodismo digital personalizado». Otros lo llamarían desinformación, algo que el propio Merlo admite. «Merlo es el más conocido, pero no es el más peligroso», me advirtió el activista contra

la desinformación Alberto Escorcia. Según un artículo de la edición mexicana de BuzzFeed, en México operan «cientos de agencias» similares.

En dicho artículo, Merlo hizo una demostración a los reporteros sobre cómo opera su equipo, convirtiendo el *hashtag* falso #GanaConVictoryLab en *trending topic* mediante técnicas de *astroturfing* en apenas dos horas, hasta posicionarlo como el cuarto más usado en todo México ese día, el 15 de junio de 2018, por encima incluso de los tres goles que Cristiano Ronaldo acababa de marcar en la Copa del Mundo.[32]

Su estrategia era relativamente sencilla: colocar contenidos en Facebook y X/Twitter mediante bots y con *hashtags*, etiquetando a medios y periodistas reales. A menudo lograban que alguno de ellos se hiciese eco de la historia, de modo que seguían impulsándola todo lo posible y mediante los medios a su alcance. En ocasiones, llegaba incluso hasta el noticiero de la noche. Entonces, celebraban una pequeña fiesta.

La clave del éxito de Merlo es que, a diferencia de otros empresarios de la desinformación, no se esconde. Ha ofrecido decenas de entrevistas a medios mexicanos e internacionales, donde explica que el hecho de que los contenidos que difunde sean ciertos o falsos le resulta irrelevante, mientras cumplan su función. «Si el ciudadano leyera y se interesara un poco más en saber, nos cacharía», le dijo a la publicación mexicana *Expansión* en 2017. «Nosotros no tenemos la culpa de que al ciudadano no le interese su país. Mi ética es cumplirle al cliente y a mi gente».[33]

La filosofía de Merlo es que, en lugar de un sitio con un millón de seguidores, prefiere 4.000 páginas diferentes aunque tengan poca audiencia, porque de este modo es más fácil que las audiencias se lo crean. En 2018 aseguraba controlar alrededor de cuatro millones de cuentas en X/Twitter, una gran parte de ellas compradas en Rusia a un precio de 25 centavos cada una, y después «mexicanizadas» para

darles la apariencia de que pertenecen a compatriotas.[34] El mismo *modus operandi* que ya vimos que utilizaba i3Ventures.

ANDRÉS SEPÚLVEDA: CASI UN MITO

Los ejemplos vistos hasta la fecha se limitan a la mera manipulación digital y cognitiva, o a la falsificación del espacio virtual. Pero algunos mercenarios del teclado pueden ir más lejos, hasta cambiar el destino de un país. Y si hay un episodio ilustrativo, es la historia de Andrés Sepúlveda.

Hasta el 6 de mayo de 2014, el nombre de este hacker colombiano era prácticamente desconocido para todo el mundo excepto para un puñado de individuos que contrataban sus servicios. Desde hacía unos meses, también para los oficiales de inteligencia que le seguían la pista. Ese día, Sepúlveda fumaba un cigarrillo en la terraza de su oficina en el norte de Bogotá, cuando vio llegar un convoy de vehículos de la policía. Instantes después, cuarenta agentes del Cuerpo Técnico de Investigación de la Fiscalía de Colombia, armados y vestidos de negro, penetraban en el edificio y le detenían, poniendo fin a la carrera de una de las personas que, de forma silenciosa, más impacto había tenido en la arena electoral de Latinoamérica.

El trabajo de Sepúlveda era operar en el ciberespacio para manipular elecciones. La parte más obvia, similar a la que realizan cientos, quizá miles, de consultorías de comunicación y agencias de relaciones públicas y marketing en todo el mundo, tenía lugar en las redes sociales. De acuerdo con un miembro de su equipo entrevistado por una publicación colombiana pocos días después del arresto, el trabajo tenía dos partes: la «blanca», que consistía en defender al candidato cuyo equipo les había contratado y apoyar sus propuestas, y la «negra», mucho más controvertida: «atacar, desprestigiar y ensuciar» a los rivales, criticando sus acciones o generando memes que los ridiculizaban. En ambos casos se utilizaban centenares de cuentas falsas para promover los mensajes correspondientes. «El trabajo

“blanco” lo puede hacer cualquiera. Pero tienes que tener ciertas habilidades para hacer el trabajo “negro”. Yo me ocupaba de eso».

Según contaría dos años después de su detención en una larga entrevista con la agencia Bloomberg, también realizaban hackeos, robos de información de las campañas rivales y envíos masivos de mensajes falsos a las bases de datos de los partidarios de los candidatos y afiliados a sus partidos, para confundirlos y enfadarlos. «Mi trabajo era hacer acciones de guerra sucia y operaciones psicológicas, propaganda negra, rumores…, en fin, toda la parte oscura de la política que nadie sabe que existe, pero que todos ven», contó a los reporteros desde la cárcel. «Cuando me di cuenta de que las personas creen más a lo que dice internet que a la realidad, descubrí que tenía el poder de hacer creer a la gente casi cualquier cosa».

«Su aporte era entender que los votantes confiaban más en lo que creían que eran manifestaciones espontáneas de personas reales en redes sociales que en los expertos que aparecían en televisión o periódicos», coinciden los autores del artículo. Sepúlveda creó un software propio que le permitía administrar una extensa red de cuentas falsas en X/Twitter, y cambiar rápidamente los nombres, fotos de perfil y biografías. Es decir, flexibilidad para adaptarse a los acontecimientos y reaccionar movilizando a la opinión pública según le interesaba.

Una de sus principales tareas era «hacer la vida difícil para las otras campañas, muy difícil. Desde sabotear sus comunicaciones hasta averiguar qué iban a decir en un discurso diez o quince días después», explicó en otra entrevista en 2018. «Muchas veces, al chequear mi X/Twitter o Facebook, veía a la gente empezando a difundir rumores que yo había estado sembrando». A menudo estaba a sueldo de Juan José Rendón, uno de los operadores políticos más conocidos de América Latina, donde ha trabajado en las campañas de decenas de candidatos de derechas por todo el continente. Venezolano residente en Miami, Rendón es un personaje extravagante: budista devoto y

practicante de artes marciales, suele vestir de negro, con atavíos de estilo oriental. Posee una colección de vehículos de lujo.

Rendón replicó a Bloomberg que Sepúlveda solo había trabajado para él como diseñador de páginas web. Los periodistas pudieron verificar mediante peritos especializados no solo que los correos electrónicos y otros documentos eran auténticos, sino también muchos otros detalles de la historia que el hacker les había contado.

Sepúlveda y sus equipos habían trabajado para manipular elecciones presidenciales en Nicaragua, Panamá, Honduras, El Salvador, Colombia, México, Costa Rica, Guatemala y Venezuela. El hacker, que cobraba en metálico —la mitad por adelantado—, se desplazaba a esos lugares con un pasaporte falso y se alojaba en solitario en un hotel, alejado de la campaña que le había contratado. Rendón le entregaba una hoja con los datos recabados hasta ese momento con los objetivos, los individuos de interés y su información personal. Sepúlveda copiaba esa información en un archivo encriptado y destruía la hoja de papel. Rendón y él se comunicaban a través de teléfonos encriptados que cambiaban cada dos meses, o mediante correos en los que hablaban en clave: por ejemplo, «dar caricias» significaba atacar y «escuchar música», interceptar un teléfono.

Para las operaciones, alquilaba servidores específicos en Rusia y Ucrania, que posteriormente borraba. También alquilaba pisos en Bogotá, donde juntaba a un equipo de entre siete y quince hackers de diferentes países latinoamericanos, en función de su especialización y de lo que requiriese cada trabajo. Por estas operaciones podía cobrar desde 12.000 dólares al mes por la tarifa básica, hasta 20.000 dólares por el paquete *premium*. Todas las acciones se coordinaban con las campañas que les habían contratado, pero a través de múltiples asesores e intermediarios, por lo que es posible, dice, que muchos de los candidatos para los que trabajó no fueran conscientes de su existencia o de lo que hacía.

Una vez rematado el trabajo, destruía la información siguiendo un orden por colores: los archivos «rojos», aquellos que podían llevar a la

cárcel a Sepúlveda y a quienes tuvieran conocimiento de su existencia, eran eliminados el mismo día de las elecciones. Los «amarillos», menos sensibles, se encriptaban y se pasaban al equipo de campaña para que hiciese una revisión final, tras lo cual también se hacían desaparecer. Todo el soporte material utilizado, como discos duros, memorias USB o teléfonos, era destruido físicamente, taladrando agujeros, quemando los circuitos en hornos microondas o reduciéndolo a pedacitos a martillazos.

Entre sus operaciones más destacadas estuvieron las campañas a favor de Porfirio Lobo en Honduras en 2009, Enrique Peña Nieto en México en 2012, Juan Carlos Navarro en Panamá en 2014 y Johnny Arana en Costa Rica ese mismo año. Del mismo modo, actuó contra Daniel Ortega en Nicaragua en 2011, y contra Hugo Chávez y Nicolás Maduro en Venezuela en 2012 y 2013. También llevó a cabo campañas menores a favor o en contra de políticos en países como México.

Su suerte se acabó en 2014. Ese año, su país natal, Colombia, celebraba elecciones presidenciales en las que solo había dos candidatos con posibilidades reales de victoria, ambos de derechas: Juan Manuel Santos, que aspiraba a la reelección, y Óscar Iván Zuluaga. Rendón había aceptado trabajar para Santos, pero en esta ocasión Sepúlveda se negó a colaborar con él. El Gobierno del presidente Santos se encontraba inmerso en una negociación con la guerrilla de las Fuerzas Armadas Revolucionarias de Colombia (FARC), que el hacker veía como una traición al país, así que decidió ponerse al servicio de su adversario, Zuluaga. No solo eso: hackeó los teléfonos y correos electrónicos de un centenar de miembros de las FARC y compiló evidencias con información comprometida, como operaciones de narcotráfico y acciones violentas contra campesinos, y se lo pasó a la campaña de Zuluaga.

Esa fue la gota que colmó el vaso para el Gobierno colombiano. Pocas semanas después, era detenido por la policía. Fue juzgado y condenado por delitos de espionaje, hackeo y empleo de software

malicioso, de los que se declaró culpable. Tras ser sentenciado a diez años de cárcel, fue enviado a una prisión común en Bogotá, donde sorteó tres intentos de asesinato. Las autoridades le trasladaron a un módulo de aislamiento en una cárcel de máxima seguridad en las afueras de la capital colombiana, donde dormía con una manta antibalas y era supervisado cada hora por los funcionarios. Tras cumplir tres quintas partes de su condena, fue puesto en libertad discretamente.

CAMBRIDGE ANALYTICA, EL PRIMER GRAN ESCÁNDALO MUNDIAL

El de Sepúlveda es quizá un caso extremo, pero no es ni mucho menos el único, ni el más célebre. Ese mérito le corresponde a la empresa que dio a conocer al mundo la existencia de este tipo de prácticas, ayudada por el revuelo causado por el referéndum sobre el Brexit y las elecciones estadounidenses de 2016: Cambridge Analytica.

Quizá nunca habríamos sabido nada de esta firma de no haber sido por uno de sus empleados principales, el consultor especializado en datos Chris Wylie. Después de estos dos acontecimientos, este canadiense vegano, gay y de ideología liberal —que, sin embargo, había ayudado a diseñar el sistema utilizado por Cambridge Analytica para favorecer ambos resultados—, se sentía tan culpable que se puso en contacto con el diario *The Guardian* para revelar sus entresijos. Los artículos de la periodista Carole Cadwallard sirvieron para arrojar luz sobre las operaciones de esta empresa, aunque el efecto de su publicación fue limitado.

Cambridge Analytica era una subsidiaria de una matriz bastante exitosa orientada al sector de la defensa, SCL Group, con contratos con el Departamento de Estado de Estados Unidos y otros gobiernos. Uno de sus productos estrella era el Análisis de Audiencia Objetivo, una técnica basada en encuestas en profundidad entre las poblaciones donde se iban a lanzar las operaciones de información. Estaba causando sensación en un mundillo donde, durante años, habían

primado los expertos en marketing, pero en el que faltaba verdadero conocimiento sobre las personas a las que dirigir mensajes.

Uno de los ejecutivos de SCL, Alexander Nix, entró en contacto con el estratega político de Trump, Steve Bannon, quien, a su vez, trajo a su amigo, el multimillonario conservador Robert Mercer. El equipo de SCL, liderado por Wylie, le vendió a Mercer un proyecto que combinaba los análisis de las audiencias con una técnica digital llamada Psicografía, que, según Nix, era capaz de presuponer la personalidad de cada individuo a partir de la recolección de una serie de puntos informativos. Al sumar los datos de cientos de miles de individuos, se podía predecir el cambio social. Es más: planteado de forma inversa, usando esos datos para influir en los comportamientos, era posible orquestarlo. Mercer accedió a financiar la aventura, que se llamaría Cambridge Analytica, y Wylie sería el responsable de crear lo que luego llamaría «la herramienta de guerra psicológica de Steve Bannon».

Podría pensarse que la recolección de datos para la influencia electoral es una técnica legítima de relaciones públicas y comunicación política. De hecho, se utiliza en campañas en todo el mundo. El primer gran problema en este caso vino del modo de recogida, a través de una encuesta fraudulenta de personalidad en Facebook creada por el científico social Aleksandr Kogan. Los participantes autorizaban, sin darse cuenta, a los responsables de la *app* a acceder a la información de todos sus contactos. Unas 270.000 personas participaron, lo cual permitió a la contratista acceder a millones de estadounidenses. En 2015, Cambridge Analytica ensayó su maquinaria durante la campaña del candidato al Congreso Ted Cruz, a quien Mercer quería favorecer.

En los años siguientes, Cambridge Analytica vendió sus servicios en sesenta países, con clientes que abarcaban desde el régimen iraní a la compañía nacional de petróleos de Malasia. Haber sido parte de la victoriosa campaña de Trump le abrió muchas puertas ante otros potenciales clientes, ante los que Nix alardeaba con frases como: «Las

cosas no tienen que ser necesariamente verdad, mientras la gente se las crea».

Pero la deserción de Wylie y la aparición de la información sobre Cambridge Analytica supuso el principio del fin. Mientras Wylie y otros trabajadores arrepentidos, como Brittany Kaiser, eran llamados a declarar ante investigaciones parlamentarias en Estados Unidos y Reino Unido, otro grupo de periodistas se puso a trabajar. Periodistas de Channel 4 se hicieron pasar por clientes potenciales en representación de un gobierno africano y se reunieron varias veces con Nix y otros ejecutivos en diferentes hoteles de Londres.

Nix explicó las técnicas que usaba la empresa, que tenían poco que ver con psicografía y mucho con los viejos trucos sucios del espionaje empresarial, como sobornos o el uso de prostitutas para chantajear a políticos. «Las chicas ucranianas son muy guapas, creo que eso funciona muy bien», dijo en una ocasión. «Le ofrecemos una gran cantidad de dinero al candidato, para financiar su campaña a cambio de tierra, por ejemplo; lo grabamos todo, dejamos a nuestro tío blanco y lo colgamos en internet», explicó en otro momento. Este tipo de sobornos son ilegales tanto en el Reino Unido como en Estados Unidos, las dos jurisdicciones a las que estaba sometida la empresa. El problema para Nix es que todos sus comentarios habían sido registrados por las cámaras ocultas de Channel 4. Esta vez sí, el escándalo llevó a la ruina a la compañía, cuya marca se había vuelto demasiado tóxica.

La debacle de Cambridge Analytica no supuso el final de sus prácticas. Algunos antiguos miembros crearon empresas dedicadas a actividades similares, como Emerdata y Auspex International. Pero el hueco que dejó la empresa británica fue rápidamente aprovechado por otros actores.

El equipo Jorge

En febrero de 2023, un pequeño grupo de supuestos consultores accedía a la oficina de una empresa en un polígono industrial en la localidad israelí de Modi'in, a medio camino entre Jerusalén y Tel Aviv. El despacho carecía de rótulos o cualquier cartel identificativo. Pero el reducido número de personas en todo el mundo que sabía de la existencia de la firma la conocía como «Team Jorge», por el nombre con el que se hacía llamar su jefe. Mientras estrechaba la mano de los recién llegados, Jorge les dijo: «Habéis visto lo que dice en la puerta, ¿no? No dice nada. Esos somos nosotros. No somos nada».[35]

Los «consultores» eran en realidad periodistas de varios medios internacionales,[36] que estaban grabándolo todo con una cámara oculta. Llevaban meses detrás de Jorge, tratando de exponer sus actividades como un representante destacado del mercado global de la desinformación, y habían mantenido varias reuniones online con él sin que hasta ese momento hubiese mostrado su rostro. En esas presentaciones, «Team Jorge» había explicado muchos de los servicios que ofrecía: recopilación de inteligencia sobre un adversario, difusión de información falsa y hackeos. Pero aquel encuentro en persona iba a ser la confirmación definitiva sobre sus capacidades.

La verdadera identidad de Jorge era Tal Hanan, un veterano de la inteligencia militar israelí reconvertido en empresario. Hanan era también el fundador de la empresa de exportación de productos de defensa Demoman International, registrada ante el Ministerio de Defensa de Israel y con presencia en Tel Aviv, Washington y Barcelona.[37] Durante los seis meses anteriores, los periodistas habían fingido trabajar para un candidato presidencial de un país africano necesitado de ciertas prácticas. Hanan les dijo que sus servicios les costarían entre seis y quince millones de dólares.[38]

Entre sus clientes se contaban media docena de servicios secretos. «Dirigimos una clase diferente de servicio de inteligencia», aseguró el israelí, que afirmaba haber intervenido en la manipulación de treinta y tres elecciones presidenciales, incluyendo Indonesia, Nigeria y Bosnia, «veintisiete de ellas con éxito». Aseguraba que no era demasiado

difícil, especialmente con la práctica continuada. La forma más efectiva, dijo, era paralizar la logística en torno al día de las elecciones, que denominaba «Día D». «¿Qué puede pasar? Quizá el sistema se rompe. Quizá el registro de votantes no funciona».[39]

Tal Hanan relató a *Der Spiegel* que solo importaban la imagen del candidato, la movilización de votantes, y el sistema electoral específico y cómo podía ser manipulado. «Cubrimos los tres aspectos», dijo, indicando que a menudo recurrían a métodos como la supresión de votantes —es decir, que la gente no acuda a las urnas—, y el fomento del caos en la campaña del adversario a través de falsas acusaciones.[40] «Tenemos un equipo en Grecia y otro en los Emiratos», añadió, explicando que su gente nunca trabajaba en Israel o Estados Unidos, al menos en operaciones de carácter político, y que descartaba actuar en contra de Vladímir Putin, presumiblemente por el riesgo de represalias. Hanan alardeó de sus capacidades de plantar información falsa en la prensa francesa, que después sería amplificada por redes de bots, y mostró un vídeo de la cadena BFMTV en la que el presentador estrella Rachid M'Barki indicaba que las sanciones contra oligarcas rusos estaban causando un enorme perjuicio a la industria de los yates en Mónaco.[41]

Pero el verdadero tesoro de su empresa era un software propio llamado AIMS, que permitía la creación automatizada de miles de bots para desplegar «mensajes en masa» y «propaganda», que podía ser utilizado en cualquier idioma, y que, según Hanan, había sido utilizado en decenas de procesos electorales. Durante su entrevista con los falsos consultores, aseguró controlar un ejército de más de 30.000 avatares con un historial digital que se remontaba a años atrás. Hizo una pequeña demostración en la que indicó la facilidad con la que podía cambiar la nacionalidad y el género de estos perfiles, así como los nombres para que encajaran con el resto de datos geográficos y raciales. «Este es hispano, ruso…, ¿veis?, asiáticos, musulmanes. Hagamos un candidato juntos», propuso, eligiendo la imagen de una mujer blanca. «Sophia Wilde, me gusta ese nombre. Británica. Ya tiene

email, fecha de nacimiento, todo».[42] Los avatares estaban vinculados a números de teléfono reales verificados mediante SMS, y en algunos casos disponían de tarjetas de crédito, para dotarlos de una capa adicional de credibilidad.[43]

Según reveló la investigación periodística posterior, avatares y perfiles creados con AIMS habían sido utilizados en campañas de manipulación, por lo general relacionadas con disputas comerciales, en una veintena de países, incluyendo Reino Unido, Estados Unidos, Canadá, Alemania, Suiza, México, Senegal, la India y los Emiratos Árabes Unidos. «Team Jorge» alquilaba el software como servicio, pero también se ofrecía a venderlo «por el precio adecuado».[44]

Durante la presentación, Hanan se atribuyó el ciberataque contra la Generalitat de Catalunya durante una consulta independentista informal celebrada el 9 de noviembre de 2014, una operación que había durado tres días y que había logrado interrumpir el funcionamiento de webs creadas por la institución catalana como participa2014.cat, el portal e-justicia, el servicio de emergencias médicas y otras páginas. En el caso de la web sobre la consulta, el sistema utilizado fue el envío de peticiones de información por un volumen 60.000 veces superior al normal. «Los autores querían romper el sistema informático del referéndum», dijeron fuentes del Centro de Seguridad de la Información de Cataluña (CESICAT) al diario *El País*.[45]

Otras técnicas utilizadas implicaban el hackeo de las comunicaciones y los equipos del adversario para plantar información falsa, de lo cual su equipo hizo varias demostraciones a los supuestos clientes. El israelí se vino arriba al relatar que en una ocasión había utilizado un falso perfil en redes llamado Shannon Aiken para comprar juguetes sexuales en Amazon y enviárselos a la casa del político rival de su cliente, de modo que su esposa creyó que le estaba siendo infiel. «Después de eso, la historia se filtró, y el tipo no podía volver a casa. La campaña dio un giro».[46]

La investigación periodística también reveló que «Team Jorge» había colaborado con Cambridge Analytica en al menos una ocasión. Documentos de la firma británica filtrados a *The Guardian* mostraron que en 2015 había enviado un presupuesto de 160.000 dólares por participar en una campaña de ocho semanas en un país latinoamericano no identificado. Dos años después, pidió una cantidad superior por trabajar en Kenia, pero los británicos lo rechazaron con el argumento de que su cliente no estaba dispuesto a pagar «Cuatrocientos o seiscientos mil dólares al mes, y, sustancialmente, más para una respuesta de crisis». No hay constancia de que «Team Jorge» colaborase finalmente con Cambridge Analytica en ninguna de esas dos campañas, pero sí lo hizo con certeza en las elecciones presidenciales de Nigeria en 2015, a favor de la reelección del presidente Goodluck Jonathan. Creó un escándalo artificial en redes que obligó a posponer la votación, pero, en último término, no tuvieron éxito, y el líder opositor Muhammadu Buhari acabó ganando los comicios.[47]

Der Spiegel resumió así la filosofía de «Team Jorge», extensible a la industria de la manipulación digital: «El tiempo pasado escuchando a Hanan y sus asesinos de la verdad puede llevar a darse cuenta de que la verdadera democracia, en su mundo, no es sino una ilusión. Y que consideran las elecciones un juego amañado en cualquier caso, uno en el que aquellos que despliegan más trucos generalmente emergen victoriosos. Es, parecen creer, ingenuo pensar que el campo de juego es justo solo porque la gente va a las urnas de vez en cuando. Y, si ese es el caso, ¿por qué no conducir las cosas a tu favor?».[48]

6

LOS MEMES SON UN ARMA (CARGADA DE FUTURO)

A diferencia de muchos otros lugares de Cuba, la localidad de San Antonio de los Baños, al suroeste de La Habana, es un sitio sin grandes atractivos turísticos. Pero, en muchos sentidos, es un microcosmos de la propia isla: acoge una base de la fuerza aérea, además de la sede de la legendaria Escuela Internacional de Cine y Televisión, y un Museo del Humor famoso en toda Latinoamérica. Es, también, el lugar natal del cantautor Silvio Rodríguez.

El 11 de julio de 2021, San Antonio se despertó con un evento inaudito: una protesta popular contra los apagones y la carestía, que pronto se convirtió en un clamor contra el Gobierno. Retransmitida en directo a través de Facebook por algunos de los asistentes, la inesperada movilización encontró eco en otros puntos de todo el país, alimentada también por el enfado por la mala gestión de la crisis del coronavirus, que había dejado miles de muertos en la isla. Los manifestantes coreaban eslóganes como «¡No tenemos miedo!», «¡Abajo la dictadura!» y «¡Patria y vida!».[1] Pese al carácter pacífico de las protestas, el régimen cubano reaccionó deteniendo a más de dos mil personas, muchas de las cuales fueron llevadas a juicio y sentenciadas a largas penas de cárcel. El Gobierno confirmó la condena a prisión de 297 personas, algunas de hasta veinticinco años.[2]

Las detenciones tuvieron un efecto demoledor en Yosbel,[3] un joven diseñador instalado en La Habana, pero originario de San Antonio que, como gran parte del país, había seguido con esperanza las protestas, y que ahora veía con ansiedad creciente cómo la ola de represión se cebaba con muchos de sus conocidos. «En los vídeos, yo

oía las voces y sabía quiénes eran los que estaban ahí», me dijo tiempo después en un pueblo de la costa española, donde él y su pareja se habían instalado por razones tanto económicas como políticas. Yosbel me contó los abusos cometidos contra sus amigos, que supusieron la última línea roja: «Se nos cayó la venda de los ojos». Como tantos de su generación, eran conscientes de la naturaleza del régimen cubano: no en vano las autoridades se habían pasado el año anterior machacando a los participantes del llamado «Movimiento San Ysidro», que exigía libertad en la creación artística, y a varios de sus miembros, a quienes Yosbel y su novia conocían personalmente. Pero hasta entonces la represión había sido más contenida, focalizada en individuos específicos que, en líneas generales, sabían los riesgos que corrían. Ahora, sin embargo, las represalias eran generalizadas y desproporcionadas. No solo eso: las víctimas eran amigos y parientes. De toda la isla.

Yosbel estaba furioso. La gota que colmó el vaso fue la detención de su amigo Alexander, un actor y artista cuyo único «delito» había sido filmar las protestas: «Eso fue lo que me movió el suelo. Me dije: "voy a liberarme y a hacer algo, al menos por las redes"». El campo de batalla que eligió fueron los memes, un área en la que ya tenía experiencia. Si hasta entonces casi todo lo que hacía era de carácter humorístico, a partir de ese momento sus creaciones se volvieron políticas.

Así era posible expresar algo profundo pero de una forma divertida, que rompiera barreras. «Estoy diciendo "Abajo Fidel", pero de un modo que no asuste tanto a quien lo ve. Relaja la cosa y a la vez está diciendo mucho. Te ganas el apoyo de otra gente porque le haces reír. El humor se filtra mucho mejor y transmite muchísimo. Trasciende más».

Yosbel diseñó un logo para las protestas del 11-J. También creó un número importante de memes que se convirtieron inmediatamente en virales, como el Ojo de Saurón (el villano de *El señor de los anillos*) flotando sobre el obelisco de la plaza de la Revolución de La Habana.

U otro en el que aparecía el presidente Miguel Díaz-Canel bajo el eslogan «Vamos por más», pero enarbolando un remo en la mano, un guiño al fenómeno de emigración masiva que se ha producido en Cuba a consecuencia del deterioro económico.[4]

Del mismo modo, este artista arremetió contra la empresa de telefonía nacional, Etecsa, por sus servicios escandalosamente caros, a la par que muy deficientes. Uno de sus memes mostraba una guillotina con el logo de la empresa a modo de cuchilla. «La "guillotecsa" es un dibujo violento, pero a la vez es gracioso. Dice mucho de una verdad que todavía existe». Otra de sus creaciones icónicas es una animación adaptada de la película de Disney *La Sirenita*, con Díaz-Canel en el papel de la bruja Úrsula secundada por anguilas con gorras de policía, y en el que la villana le roba la voz a Ariel, la protagonista. La frase de Úrsula/Díaz-Canel diciendo «Tu voz es mía», cobra un nuevo significado político, imposible de pasar por alto.

«Tenía la posibilidad de apoyar a mi gente y a mí mismo haciendo esto, de luchar contra cosas que no me cuadran a través de mi poder, que es el humor. El meme funciona igual que las tiras cómicas, que le llegan a la gente, pero que muchas veces tienen una enorme profundidad». Yosbel cita el ejemplo de un personaje humorístico local creado por el caricaturista Eduardo Abela a principios de los años treinta, sin nombre, pero al que los ciudadanos rápidamente bautizaron como «El Bobo». A través de sus comentarios satíricos y ciertas claves en el dibujo —como su vestimenta, o el tamaño de las velas que utilizaba, grandes o pequeñas dependiendo de si la situación era buena o mala», El Bobo de Abela criticaba la dictadura de Gerardo Machado y la censura. Pronto los lectores aprendieron a descifrar estos mensajes, como la aparición de bolas gigantes que perseguían al protagonista si las demás noticias que aparecían en la publicación eran mentiras propagandísticas del régimen.[5] Tras la llegada al poder de otro dictador, Fulgencio Batista, Abela prefirió marchar al extranjero.

Para su desgracia, Yosbel tuvo que seguir el mismo camino. «Durante mucho tiempo no pensé que todo esto me iba a traer problemas. Había riesgos, pero yo no los veía. Estaba tranquilo porque yo no había tirado una piedra, no hice daño a nadie». En junio de 2023, el Gobierno cubano aprobó la Ley de Comunicación Social, que criminaliza toda crítica a funcionarios oficiales, dirigida específicamente a reducir la expresión del malestar en redes. «Te inventan una ley así cuando les da la gana». Un pariente de su novia que trabajaba para la Seguridad del Estado les avisó de que, si Yosbel seguía por ese camino, iba a acabar mal. Los servicios de inteligencia sabían perfectamente quién era y lo que estaba haciendo, lo que terminó por convencer a la joven pareja de la necesidad de marcharse de Cuba. Pero, incluso en estas circunstancias, Yosbel sigue reivindicando la capacidad subversiva de los memes: «El humor te permite defenderte y a la vez burlarte del fuerte». Que el régimen cubano se haya sentido lo suficientemente amenazado por sus creaciones como para vigilar e intimidar a un diseñador gráfico sin grandes conexiones políticas es, probablemente, la mejor demostración de su poder.

¿QUÉ ES UN MEME?

El término «meme» fue acuñado por el científico y divulgador británico Richard Dawkins en su obra *El gen egoísta* (1976) para referirse a las pequeñas piezas de cultura que se propagan entre las personas, tales como melodías, ideas, frases pegadizas, técnicas de elaboración de artefactos o formas de vestir.

Con la llegada de internet, el concepto cobró un significado diferente, pasando a referirse a ciertas imágenes y elementos culturales que circulan en el ciberespacio sin una autoría concreta y de los que sus receptores pueden apropiarse, a menudo introduciendo cambios. Lo explica Jesús Manuel Pérez Triana, analista y director del portal especializado Monitor Disinfo:

> En este nuevo contexto, un meme sería un elemento humorístico, desde un simple gesto a un vídeo, pasando por una frase o imagen, que se presta a ser modificado y replicado. Las características fundamentales de un meme de internet son tener, por un lado, elementos que lo hacen reconocible y, por otro, haber sido alterado, transformado y mezclado. El meme establece por tanto un juego de complicidad con el receptor al hacer referencia a ciertas claves compartidas, mientras se presta a ser modificado en infinitas variaciones. De hecho, muchos memes gráficos existen como plantilla que se presta a ser fácilmente modificada.[6]

Dos ejemplos clásicos serían el póster de reclutamiento estadounidense en el que el Tío Sam nos apunta con el índice bajo la leyenda «*I want you for the US army*» («Te quiero para el ejército de Estados Unidos»), o el de la joven trabajadora con un pañuelo en el pelo que flexiona el brazo enseñando el bíceps mientras dice: «*We can do it!*» («¡Podemos hacerlo!»). En ambos casos se han generado innumerables memes que mantienen las icónicas imágenes, pero añaden una leyenda nueva y diferente.

En la actual sociedad hiperconectada, los memes son un poderosísimo elemento de comunicación. Imágenes con leyendas sencillas que apelan a los instintos primarios de los receptores, y que con frecuencia los comparten de forma acrítica. Una forma extremadamente barata de lanzar un mensaje, más eficaz cuanto más impacto emocional genera a un gran número de personas con afinidades comunes. Según un estudio interno de Instagram citado por la cadena británica BBC, al menos un millón de *posts* en esta red social en los que se mencionaba la palabra «meme» fueron compartidos durante cada día de 2020. Los memes «son un lenguaje en sí mismos, con una capacidad de trascender culturas y construir identidades colectivas entre personas. Estas bromas visuales compartibles también pueden ser poderosas herramientas de autoexpresión, conexión, influencia social e incluso subversión política», señala el artículo.[7] La «memética» empieza a ser una disciplina seria de estudio en universidades de muchos países, como

ejemplifica la creación de la Meme Studies Research Network, lanzada en 2020 por un académico de la Universidad de Edimburgo y abierta a académicos de todo el mundo.

Este carácter subversivo pronto empezó a ser percibido y utilizado por algunas subculturas de internet, y no precisamente las benignas. Grupos por aquel entonces marginales —comunidades misóginas o supremacistas— los promovían para expresar ideas que la mayoría de la sociedad rechazaba, con el pretexto de que este tipo de contenido era «solo humor», y apelando a la libertad de expresión. Detrás se ocultaba un pensamiento estratégico: la ampliación de la denominada «ventana de Overton»,[8] una teoría política según la cual existe un rango de ideas que la sociedad considera aceptable, pero variable, de forma que lo que es tabú en una época determinada acaba siendo considerado razonable en otra.

Los movimientos de extrema derecha en internet han teorizado que el uso de memes para introducir mensajes de odio o de carácter extremista mediante el humor y la ironía suponen una manera de ampliar estos límites, al exponer masivamente a la ciudadanía a ideologías que progresivamente van penetrando en la conciencia colectiva.[9] También es una forma de crear lazos y familiaridad dentro de su propia comunidad, al establecer bromas internas cuyo significado solo es accesible a los iniciados. Estos, a su vez, pueden continuar el proceso editando los memes existentes y creando otros nuevos, lo que contribuye a una implicación progresiva con el movimiento.

Fabricar un meme en medio del anonimato de internet requiere un nivel de compromiso mucho menor que, pongamos, difundir panfletos por la calle o asistir a una reunión de una organización política estigmatizada por sus ideas radicales. De esa manera, se reduce la barrera de la participación. A medida que estos individuos se van integrando en las comunidades extremistas, se les expone a los llamados «memes de impacto», que muestran imágenes de naturaleza violenta explícita, lo que contribuye a ir eliminando las reticencias

psicológicas ante un futuro uso de la violencia. En suma, un proceso de radicalización.

«Los memes han hecho más por el movimiento etnonacionalista que cualquier manifiesto», afirma un informe del Instituto para el Diálogo Estratégico sobre este fenómeno.[10] Su importancia para estos activistas es tal que muchas organizaciones de lucha contra los movimientos de odio, como la Liga Antidifamación o el Southern Poverty Law Center de Estados Unidos, tienen expertos dedicados a monitorizar y estudiar su creación y difusión.[11]

Los radicales de ultraderecha no están solos. Los movimientos yihadistas, y, sobre todo, Estado Islámico, llevan años utilizando los memes para dinamizar sus redes sociales, como mecanismo para galvanizar y atraer a sus seguidores y, en último término, radicalizarlos.[12] Son mensajes con un componente difícil de comprender para los ajenos a la comunidad, como las imágenes de pájaros verdes —que simbolizan a aquellos miembros de ISIS muertos como mártires camino del Paraíso—, o el famoso eslogan «*Keep Calm and Carry On*» («Mantén la calma y sigue con lo tuyo»), lanzado por las autoridades británicas en 1939 como campaña de concienciación cívica durante los bombardeos alemanes, y que este grupo extremista reformuló como «*Keep Calm and Say Baqiya*», un término del *slang* ciberyihadista que hace referencia al regreso de sus contenidos a una plataforma, tras la suspensión anterior de sus cuentas.[13]

En otros casos se produce una reapropiación de iconos culturales globales, como el uso de la imagen de *El rey león* superpuesto a contenidos yihadistas: en los textos religiosos islámicos, el león es un símbolo de valentía, y muchos partidarios de ISIS en redes sociales usan leones como símbolos en sus avatares.[14] O las fotografías de gatitos junto a *hashtags* como #catsofjihad (#gatosdelayihad), #ISISCat o #Mewjahid, un juego de palabras que mezcla la onomatopeya de un maullido con la palabra *muyahid*, o guerrero santo islámico.[15]

El uso agresivo de los memes saltó en seguida de bando. Usuarios de internet de todo el planeta pronto empezaron a utilizar las mismas técnicas para ridiculizar las acciones de los yihadistas y romper su temible aura. Aunque los ciudadanos del mundo árabe fueron pioneros, la primera acción de envergadura global tuvo lugar en Japón en enero de 2015, después de que Estado Islámico lanzase un vídeo en el que el tristemente célebre Jihadi John —el yihadista británico que decapitó o ejecutó delante de una cámara a decenas de personas, incluyendo a otros cinco extranjeros—[16] amenazaba a dos rehenes japoneses arrodillados: el periodista Kenji Goto y el consultor de seguridad Haruna Yukawa.

Las redes sociales niponas se llenaron de imágenes y tuits mofándose del terrorista: sustituyendo su cuchillo por un plátano o comparando su lenguaje corporal con el del Doctor Maligno, el villano de la trilogía cinematográfica *Austin Powers*.[17] Lo mismo sucedió en México,[18] después de que Estado Islámico publicase un vídeo que incluía al país entre la coalición de sesenta estados que podrían «sufrir el mismo destino que Francia» tras los atentados del 13 de noviembre de 2015. O incluso España: tras los atentados de Barcelona, ISIS envió un mensaje en vídeo protagonizado por el yihadista español Abu Lais Al Qurdubi, apodado así porque su ciudad natal era Córdoba. Pero los compatriotas mexicanos y españoles, lejos de amedrentarse,[19] inundaron las redes sociales de mofas y parodias.[20]

En otras latitudes, cuentas como @IsisKaraoke o The Duck-State también lucharon durante años contra la mensajería yihadista mediante canciones y memes. Por ejemplo, sustituyendo, en el último caso, las cabezas de los combatientes por las de patitos de goma, o el círculo de la bandera de Estado Islámico por la forma de un gran pato de juguete.[21]

Y mientras tenían lugar todas estas «guerras meme», algunos las observaban muy de cerca.

POLARIZAR AL ADVERSARIO

Una de las instituciones pioneras a la hora de utilizar los memes como arma fue la mencionada Agencia de Investigación de Internet (IRA), o la granja de trols de San Petersburgo.[22] Esta agencia lanzó en 2014 una operación diseñada por los servicios de inteligencia de la Federación Rusa para modificar comportamientos a través de las redes. Los primeros conejillos de indias fueron los propios ciudadanos rusos. La IRA creó páginas como vshtabe.rf, dedicada a la elaboración de memes humorísticos, a menudo de carácter político, con la intención de promover las fortalezas del Gobierno de Putin y desmovilizar a los descontentos. Entre sus temas favoritos destacaban las prodigiosas capacidades de Putin, el carácter ridículo de la oposición rusa, los dobles estándares de Occidente o la decadencia europea. «Sí, son estúpidos, pero juegan un papel enorme», opina Lyudmila Savchuk, la periodista de San Petersburgo que se infiltró como trabajadora en la granja de trols. «Estos desmotivadores funcionan con las emociones básicas de los rusos menos educados y conectan con ellos».[23]

La estrategia se expandió a todos los países que el Kremlin consideraba su zona de influencia directa, como Ucrania, Georgia o los países bálticos[24]. Y, aunque el impacto exacto es imposible de cuantificar, sus costes extremadamente bajos lo convirtieron, a ojos de las agencias rusas, en una alternativa muy atractiva. De modo que, cuando el Kremlin decidió interferir en las elecciones de Estados Unidos de 2016, los memes fueron uno de los elementos principales de su esfuerzo. Utilizando los algoritmos generados por las propias redes, que muestran páginas de «intereses similares», sus operativos detectaron objetivos potenciales a los que bombardear con desinformación y memes políticos. La estrategia fue gradual: primero utilizando *posts* humorísticos más o menos inocuos, apoyados en una amplia gama de referentes culturales —Pokémon, Bob Esponja, Beyoncé o los Simpson—, con los que ir ganando seguidores.

Una vez establecidas dichas audiencias, los responsables pasaron a mensajes cada vez más políticos, añadiendo sutiles elementos como un

«Dale a "Me gusta" si estás de acuerdo» al final de los textos, para ir clasificando a estos receptores en función de sus preferencias. Por ejemplo, aquellos usuarios que habían demostrado sensibilidades religiosas eran atraídos hacia una página llamada *Army of Jesus* («Ejército de Jesús»), con mensajes como este: «¿Luchando con tu adicción a la masturbación? Ven conmigo y la derrotaremos juntos. Firmado: Jesús». Una vez convertidos en miembros de la página, sus usuarios empezaron a recibir mensajes que identificaban a Hillary Clinton con Satán.

«La IRA demostró su soltura en la cultura estadounidense del troleo», señala un informe de la firma de ciberseguridad Newknowledge, contratada por el Comité de Inteligencia del Senado para analizar la campaña rusa. Nada extraño, teniendo en cuenta que la agencia rusa, como mostró posteriormente la investigación, había enviado de antemano a varias personas a Estados Unidos para estudiar los principales rasgos socioculturales del país, poniendo énfasis en sus elementos más divisorios.

Entre 2015 y 2017, los rusos crearon 81 páginas en Facebook, 3.841 cuentas en X/Twitter, 133 en Instagram y 17 en YouTube. Produjeron casi 10 millones y medio de tuits, 116.000 *posts* de Instagram, 61.500 de Facebook y 1.100 vídeos de YouTube. En conjunto, lograron generar más de 200 millones de interacciones.[25] La mayoría de los contenidos eran de carácter memético o viral, y trataban de explotar algún rasgo identitario común, como el apoyo (o el rechazo) a la libre posesión de armas de fuego, la postura ante la inmigración, las creencias religiosas o la raza. Además de acentuar la polarización, había un objetivo electoral: promover el voto por Donald Trump, dividir a los demócratas y reducir la participación de la comunidad afroamericana, tradicionalmente más proclive a votar demócrata. Buscaron incrementar el desdén por Hillary Clinton de los partidarios del candidato demócrata Bernie Sanders enfatizando el estilo austero del senador de Vermont frente a las presuntas corruptelas de la antigua secretaria de Estado, en un intento de

fomentar la abstinencia electoral. Entre las páginas dirigidas a republicanos, términos como «Hitlery» hacían furor.[26]

Aunque la operación global se orientó sobre todo hacia una de las principales brechas de la sociedad estadounidense: la cuestión racial. De los 3.500 anuncios en las redes entre 2015 y 2017, más de la mitad, unos 1.950, hacían referencias expresas a la raza. Los rusos crearon páginas como *Don't Shoot.US* o *Black Matters* para promover la identidad afroamericana y el victimismo ante la brutalidad y el racismo policial, al tiempo que promovían memes racistas y páginas de contenido abiertamente discriminatorio. La islamofobia también fue debidamente explotada: uno de sus memes mostraba a un individuo disfrazado de cerdo que reparte panfletos comerciales de una carnicería frente a un musulmán devoto, bajo el lema: «El momento en el que te das cuenta de que tienes el mejor trabajo del mundo».[27]

Se ha podido determinar que Rusia está detrás de estos memes porque aparecieron por primera vez en páginas de Facebook creadas por individuos y entidades asociadas a la IRA, en *posts* y anuncios pagados en rublos. Muchos investigadores sospechan que el Kremlin quería dejar un rastro visible para que quedase clara su responsabilidad, a modo de advertencia, o quizá para sembrar dudas sobre la integridad del proceso electoral. La importancia crucial de los memes políticos queda demostrada en el hecho de que muchos siguieron siendo compartidos durante años por miles de estadounidenses que ignoraban su proveniencia. Rusia también continuó reutilizándolos: en octubre de 2019, Facebook canceló una red de la IRA con 50 cuentas de Instagram que publicaban contenido sobre temas políticos y sociales en Estados Unidos con el propósito de influir en las elecciones de 2020, y que rescataba muchos de los viejos temas, imágenes e iconos empleados en años previos.[28]

EL PRIMER CREADOR DE MEMES DE TRUMP

Otra de las personas que estaba tomando buena nota era un individuo llamado Jeff Giesea. Este empresario, antiguo estudiante de la Universidad de Stanford, había trabado contacto con Peter Thiel, quien años después se convertiría en una de las figuras más conocidas —y criticadas— de Silicon Valley por su aplicación de las nuevas tecnologías al negocio de la vigilancia y la seguridad.[29] Giesea compartía la misma mentalidad que Thiel, para quien trabajó en su primer fondo de inversión, antes de crear sus empresas. Si había un tema que preocupaba a Giesea, era la seguridad nacional. A su juicio, en la batalla memética, Estados Unidos iba perdiendo.

En 2016, Giesea escribió un artículo para una publicación interna de la OTAN titulado «Es hora de abrazar la guerra memética», hoy considerado un texto pionero. «Para muchos de nosotros en el mundo de las redes sociales, parece obvio que unas tácticas de comunicación más agresivas y unas acciones de guerra más amplias a través del troleo y los memes son una forma necesaria, barata y fácil de ayudar a destruir el atractivo y la moral de nuestros enemigos comunes. Creo que la guerra memética podría ser efectiva a la hora de contrarrestar los esfuerzos de reclutamiento y propaganda de Daesh y en el conflicto moderno en general, que incluye otro tipo de operaciones distintas a la guerra. El troleo, se puede decir, es el equivalente en las redes sociales de la guerra de guerrillas, y los memes son su munición de propaganda. Daesh está conduciendo una guerra memética. El Kremlin lo hace. Es barata. Las capacidades existen. ¿Por qué no lo estamos intentando?».

En realidad, Giesea no era el primer especialista en el universo OTAN que sugería algo así. En 2006, el oficial del ejército estadounidense Michael B. Prosser había escrito otro artículo para una publicación de la Escuela de Guerra Avanzada de la Universidad del Cuerpo de Marines de Quantico, titulado «Memética. Una industria en crecimiento en las operaciones militares de Estados Unidos». Proponía la creación de «centros de guerra de memes», que operarían en apoyo de las fuerzas convencionales como parte de las unidades de

operaciones psicológicas.[30] Cuatro años después, otro militar estadounidense, el entonces primer teniente Brian J. Hancock, desarrolló un enfoque teórico más completo en su artículo «Guerra memética: el futuro de la guerra», todavía centrado en la «guerra contra el terrorismo». Según Hancock, la guerra memética podía ser muy eficaz contra «ciertas organizaciones, como Al Qaeda, [que] utilizan técnicas de lavado de cerebro» en sus acólitos, y que definía como «sectas meméticas».[31]

Pero Giesea iba más allá, expresando su frustración por la falta de comprensión entre los altos mandos políticos y militares de la OTAN de un fenómeno que ya no era meramente teórico. «Quizá el mayor obstáculo a la guerra memética es la falta de apreciación de las redes sociales como un campo de batalla y el alcance hasta el que la guerra memética ya está teniendo lugar. Tal vez es algo generacional: visto desde fuera, no parece que los encargados de tomar las decisiones militares y de política exterior en la alianza comprendan para nada las redes sociales, y mucho menos como una herramienta y un arma para la defensa común. ¿Cuántos generales están activos en X/Twitter y lo comprenden realmente más allá de las explicaciones de sus hijos o colegas más jóvenes? [...]. Una vez que uno empieza a ver internet a través del prisma de los memes, ve la guerra memética en todas partes: en las campañas políticas, en las narrativas en disputa sobre sucesos de actualidad, en los memes bobos compartidos por amigos en Facebook, y en los vídeos de YouTube [...]. Los *hashtags*, podría decirse, son las coordenadas operativas de la guerra memética». También avisaba de que los Gobiernos de Rusia y China ya estaban recurriendo a estas técnicas.

Giesea pronto tendría una oportunidad de poner en práctica lo aprendido, pero no contra un adversario exterior. Ese mismo año organizó una guerra memética para la campaña de Donald Trump. Como explicó en una entrevista, veía «el trumpismo como el único camino práctico y moral para salvar a la civilización occidental de sí misma». Así que decidió implicarse, ayudando a establecer una red de

influencers pro-Trump y un enjambre digital de voluntarios para difundir memes y contenidos denominado «MAGA3X».[32] Sus cuentas difundieron miles de memes, caricaturas, artículos de la publicación ultraconservadora *Breitbart News* y vídeos con mensajes que apoyaban a Trump y denigraban a los altos cargos del Partido Demócrata, incluidas teorías de la conspiración como el llamado «Pizzagate».[33]

Aunque MAGA3X se definía en su cuenta de X/Twitter como «un movimiento ciudadano de base que ayudó a que Trump fuese elegido», los voluntarios de Giesea no fueron los únicos partisanos. «Trump ha sido el primer presidente en adoptar plenamente las guerras meme como una estrategia de campaña y gobernanza. Retuiteó memes, amplificó las voces de dedicados guerreros meme, integró en su campaña oficial materiales meméticos que habían sido manufacturados en [el foro de internet copado por la extrema derecha] 4chan, y a menudo se comportó como un "general en las guerras meme"», escribieron los expertos de la Universidad de Harvard Joan Donovan, Emily Dreyfuss y Brian Friedberg en su libro *Meme Wars: The Untold Story of the Online Battles Upending Democracy in America*.[34]

Estas guerras —que en cierto modo habían empezado ya con la elección de Barack Obama en 2009, y la avalancha de contenidos virales que atacaban al primer presidente negro— continuaron durante los cuatro años de la presidencia de Trump. Sus ejércitos siguen activos. Pero, tras la victoria de Joe Biden en noviembre de 2020, ocurrió un suceso que añadió una nueva dimensión: el asalto al Capitolio del 6 de enero de 2021, que horrorizó a Giesea. A partir de ese momento, se convirtió en un crítico acérrimo de Trump y comenzó a apoyar activamente a Biden.

Pero las guerrillas digitales que contribuyó a crear han seguido actuando. Por ejemplo, cuando el FBI llevó a cabo una redada en la residencia de Trump en Mar-a-Lago en agosto de 2022, los grupos generaron una oleada de memes que equiparaban a la agencia de

seguridad con la Gestapo, se burlaban de sus miembros por husmear entre la ropa interior de la esposa del expresidente, Melania, o mostraban a Trump con una ametralladora en la mano bajo el eslogan «Es la hora de la venganza-Trump 2024».[35] En los años siguientes, la presunta senilidad del presidente Joe Biden se convirtió en una cantera inagotable de memes, conformando un estado de opinión negativo sobre sus capacidades cognitivas.

Pronto aparecieron candidatos dispuestos a tomar el testigo de Giesea, como el *podcaster* e *influencer* ultraconservador Brenden Dilley, que creó el llamado «Dilley Meme Team», o dos docenas de personas dedicadas a tiempo completo a crear memes y contenidos contra los demócratas. Se definían como «la máquina de guerra digital de Trump» y se coordinaban en un grupo privado de Telegram en el que compartían ideas y decidían objetivos a los que atacar. El Dilley Meme Team jugó un papel clave al orientar a las bases trumpistas en contra del gobernador de Florida Ron DeSantis, haciendo descarrilar su candidatura presidencial.

LA RESPUESTA DEMÓCRATA

Eso no significa que el Partido Demócrata estuviese de brazos cruzados. Sus estrategas pronto se dieron cuenta de la necesidad de apropiarse de los memes y temas de sus adversarios. Es lo que ocurrió con el meme «Dark Brandon».

El 21 de octubre de 2021, durante una carrera de coches televisada en Talladega, Alabama, muchos asistentes empezaron a corear «*Fuck Joe Biden*» («Que se joda Joe Biden»). La comentarista deportiva Kelli Stavast no lo escuchó bien y anunció que la multitud estaba gritando «*Let's go Brandon*» (que puede traducirse como «Ánimo, Brandon»). En medio de chanzas, la fórmula «*Let's go Brandon*» fue adoptada como una frase en clave en contra de Biden, impresa en camisetas, pegatinas y banderas que se ponían en vehículos o en fachadas de casas.[36] Al mismo tiempo, otros memes promovían el concepto de

Dark MAGA, el supuesto lado oscuro del movimiento «Make America Great Again», que se cobraría su venganza cuando Trump regresase al poder en 2024.

Pero las tornas cambiaron cuando empezaron a aparecer imágenes en las que un Joe Biden de cómic lanzaba rayos por los ojos bajo el lema «*Dark Brandon*». Este meme. que mostraba al presidente como una suerte de poderoso justiciero, tuvo un éxito apabullante entre los partidarios de Biden, y fue rápidamente adoptado por su campaña de reelección.[37]

Aunque los demócratas estaban perdiendo la guerra, y lo sabían. De ahí que contrataran a lo que la publicación *Tech-Crunch* definió como un «Señor de los memes experimentado». En mayo de 2024, el Partido Demócrata anunció que buscaba un perfil para gestionar las «operaciones diarias de interacción con el contenido principal de internet y páginas de memes», por un salario de 85.000 dólares. El trabajo consistía en reclutar a creadores de contenido para la campaña de Joe Biden, en aquel momento de capa caída, y explicar los logros del presidente en un lenguaje que todo el mundo pudiese entender.

La contienda meme continuó incluso después de que Biden anunciase su retirada y de que Kamala Harris fuese designada como la candidata oficial. A medida que las principales figuras del Partido Demócrata empezaron a mostrar su respaldo por la entonces todavía vicepresidenta, las redes se vieron inundadas de imágenes que la atacaban o la apoyaban. Mientras los primeros a menudo eran de índole sexual —por ejemplo, la palabra «Harris» tomada de su logo de campaña, pero donde la H la formaba una mujer arrodillada haciéndole una felación a un hombre—,[38] los segundos la mostraban como una mujer poderosa, vestida de Capitán América o cabalgando un tiburón que perseguía a Donald Trump.

Su equipo también se apropió del símbolo de la palmera, después de que la campaña de Trump hiciese circular un vídeo en el que Harris contaba una anécdota en la que su madre les había dicho: «¿Creéis que os acabáis de caer de un cocotero?». El vídeo tuvo el efecto

contrario al que deseaban: a muchos jóvenes estadounidenses les encantó.[39]

La campaña de Harris acabó contratando a más de 200 trabajadores dedicados exclusivamente a la esfera digital, la mayoría veinteañeros. Algunos indicadores mostraban que la estrategia parecía estar funcionando: según una encuesta del Instituto de Política de la Escuela Kennedy de Harvard de finales de septiembre, más de la mitad de los jóvenes adultos menores de treinta años había visto memes sobre Harris y Trump. Pero, mientras que el 34% de ellos decía que los memes habían modificado positivamente su visión sobre Harris, solo el 13% afirmaba lo mismo sobre Trump. Otro 25% aseguraba tener una peor percepción de este último.

Aunque, como se comprobaría en las urnas, a esas alturas la suerte ya estaba echada.

Y POR SUPUESTO, RUSIA LOS USA EN UCRANIA

La invasión de Ucrania en febrero de 2022 vino acompañada de la habitual ola de caricaturas y contenidos virales con el carácter «nazi» del Gobierno ucraniano, la ausencia de una identidad nacional ucraniana o la sumisión del país a sus amos de la OTAN. Una vez más, la ridiculización y la denigración de la propaganda rusa justificaban el ataque contra su vecino. Pero el Kremlin no esperaba recibir una dosis de su propia medicina.

A diferencia de 2013 y 2014, Ucrania había tenido casi una década para estudiar las técnicas rusas de guerra cognitiva y memética, y las autoridades y los ciudadanos del país sabían lo que tenían que hacer para contrarrestar los mensajes rusos en las redes sociales y plantarles cara. En los días siguientes al inicio de la ofensiva, se crearon docenas de cuentas de X/Twitter[40] que empezaron a difundir memes mofándose de los invasores, ridiculizando sus fiascos y celebrando la resistencia del ejército ucraniano. Este esfuerzo colectivo dejó algunas imágenes icónicas, como un tractor ucraniano arrastrando un tanque

ruso —basado en un vídeo real— o un desfile de helicópteros rusos cargando lavadoras sobre el Kremlin, publicado después de que se viese a numerosos soldados de regreso a Rusia con electrodomésticos robados en las poblaciones ocupadas. «Los rusos saquearon de todo: dinero, ordenadores, hervidores, alfombras, porcelana. Pero fue la lavadora lo que capturó la imaginación colectiva», explicaría poco después Roman, un diseñador de memes que utilizaba este elemento con frecuencia en sus creaciones, a la publicación polaca *OKO.press*.[41]

Incluso la cuenta oficial de Ucrania en inglés @Ukraine, comparte a menudo memes contra Rusia. Apenas unas horas después de la invasión, ya posteaba una ilustración de Adolf Hitler acariciándole la cara a Putin, con la leyenda: «Esto no es un meme, sino nuestra realidad y la tuya ahora mismo».

Ucrania había tenido tiempo para allanar ese camino. En 2015, el Ministerio de Información había creado una web llamada *I-ejército* que ofrecía a cualquier ciudadano la oportunidad de convertirse en voluntario en el ámbito digital. «Cada ucraniano que tenga acceso a internet puede contribuir a esta lucha. Cada mensaje es una bala en la mente del enemigo».[42] La cuenta @Ukraine empezó poco después, como resultado de la iniciativa de un grupo de veinteañeros. Uno de ellos, Yarema Dukh, había sido el jefe de prensa del presidente Petro Poroshenko. Tras descubrir las cuentas oficiales de Canadá en X/Twitter, dedicadas a promover las bellezas naturales del país, pensó que cabía desarrollar una iniciativa similar en Ucrania.[43] Pero, a diferencia de Canadá, Ucrania estaba inmersa en un conflicto armado y político, y los impulsores de la cuenta pronto se vieron inmersos en batallas tuiteras no solo con trols, sino también con las cuentas de las instituciones oficiales de Rusia. En aquellos años, Ucrania aprendió mucho. Cuando las bombas empezaron a caer sobre sus ciudades y los primeros tanques cruzaron la frontera, sus partisanos digitales estaban preparados.

Uno de los vehículos de difusión más populares al inicio de la invasión fue el canal de Telegram «Novynach», dirigido por un joven

llamado Ihor Kharkin y operado por estudiantes universitarios. Hasta entonces, publicaba noticias de actualidad, con la novedad de que, por cada información, incluía un meme relacionado. Cuando la guerra se convirtió en el asunto noticioso, también pasó a ser el tema principal de los memes, que después eran compartidos en otras plataformas.

Los memes ucranianos están todavía dirigidos a tres audiencias diferentes: la doméstica, la rusa y la internacional. A los propios ucranianos, el humor contenido en este formato les ayuda a mantener la cordura en medio del horror y a sostener el espíritu de lucha. Por lo que respecta a los rusos, pretenden desanimarlos, minar su moral con mensajes negrísimos, como la imagen de un soldado partiendo en un tren mientras Putin le dice desde el andén: «Iván, es hora de morir». Por último, mediante la risa, los memes persiguen atraer las simpatías internacionales y mantener el foco en el conflicto a medida que la fatiga informativa va haciendo mella. En ese sentido, los voluntarios NAFO, de quienes ya hablamos en el capítulo cuatro, han sido esenciales.

Probablemente el meme de la invasión que acabará por pasar a la historia es «Saint Javelin»: la imagen de un santo al estilo del cristianismo ortodoxo, que sostiene entre sus manos un arma antitanque Javelin, que tan útil les resultó a las fuerzas ucranianas para cazar tanques rusos y repeler sus embestidas en los primeros días de la guerra. Creada por un antiguo periodista canadiense de origen ucraniano, Christian Borys, «Saint Javelin» ha sido plasmada en la gran fachada de un edificio en Kiev. Borys ha utilizado este y otros diseños, adaptados a las novedades en el conflicto y a las peticiones de los donantes, para vender *merchandising* y recaudar fondos para las tropas.[44]

Rusia, por supuesto, también ha utilizado ampliamente los memes: mostrando al presidente ucraniano Volodímir Zelenski nadando en billetes, por su presunta corrupción, o reaccionando de forma oportunista a los acontecimientos: después de que un misil ucraniano cayese accidentalmente sobre territorio polaco y matase a dos

personas en una granja en noviembre de 2022, se difundió una composición sacada de un cómic en la que un bandido (sobre el que se lee «Ucrania») lanza un jarrón contra el personaje de Tintín (identificado como «Rusia»), pero, accidentalmente, golpea a uno de sus compañeros («Polonia»). No obstante, estas imágenes no han logrado alcanzar la misma penetración.

7

ELECCIONES, LA TRINCHERA PERFECTA

El 13 de enero de 2024, los ciudadanos de Taiwán acudieron a las urnas para elegir si la formación gobernante, el Partido Democrático Progresista (PDP), continuaba en el poder durante otro mandato o era reemplazada por la oposición. La complejidad geopolítica que rodea a este territorio hace que unas elecciones nunca sean solamente eso: en aquellos comicios no se dirimía simplemente qué partido gobernaría la isla durante los siguientes cuatro años, sino también la misma supervivencia de Taiwán como entidad independiente.

En la competición política participaban los taiwaneses, pero también la República Popular de China, que llevaba meses movilizando recursos para influir en los resultados: pocos días antes de la jornada electoral, las autoridades taiwanesas afirmaban haber investigado casi 3.000 intentos de interferencia.

Situada frente a las costas de la China continental, Taiwán ha sido históricamente refugio de forajidos y lugar de asentamiento de colonos e invasores: holandeses y españoles controlaron partes de la que entonces era conocida como Formosa, y los japoneses fueron propietarios formales de la isla entre 1895 y 1945. Durante la Segunda Guerra Mundial, los dos grandes movimientos armados de China, los nacionalistas del Kuomintang (KMT) de Chiang Kai-shek y los comunistas liderados por Mao Tse-tung, dejaron de lado sus enfrentamientos para colaborar contra los ocupantes japoneses. Posteriormente, volvieron a enzarzarse en una sangrienta guerra civil, que concluyó en 1949 con la victoria comunista. Los nacionalistas se refugiaron en Taiwán, y el Kuomintang instauró un régimen dictatorial, que duraría hasta bien entrados los años noventa.

Chiang Kai-shek esperaba que el nuevo gobierno comunista colapsaría rápidamente y que el Kuomintang podría reunificar China bajo su mandato, algo que nunca ocurrió. La historia del conflicto en el estrecho de Taiwán es larga y compleja y excede los objetivos de este libro, pero baste decir que en lo único en lo que tanto el Kuomintang en Taipéi, como el Partido Comunista (PCCh) en Pekín estaban de acuerdo es en que Taiwán y China son el mismo país.

Han pasado muchas décadas, y Taiwán ha evolucionado de forma muy diferente a la autocrática China: se ha convertido en una democracia vibrante, en una potencia económica por derecho propio, y en un lugar con una identidad singular que cada vez tiene menos que ver con la de la República Popular, pese a que compartan idioma y rasgos culturales. Las encuestas muestran que los jóvenes, a diferencia de sus mayores, cada vez se sienten menos chinos y se identifican más como solamente taiwaneses. En ese ambiente ha surgido un nacionalismo taiwanés, cuyo máximo exponente político es el PDP, que llegó al poder por primera vez en 2016.

Según una encuesta del Pew Research Center de 2025, un 67% de los ciudadanos se consideran principalmente taiwaneses, un 28% se declaran tanto chinos como taiwaneses, y solo un 3% se ven chinos. «El objetivo de la República Popular era alterar esta tendencia. Pero, durante dos décadas, esto ha ido cambiando en sentido contrario, e incluso se ha acelerado con las tensiones geopolíticas. Cuanto más intentan los chinos presionar, menos éxito tienen», me dijo David Gardas, analista de Sinopsis, un proyecto del Departamento de Sinología de la Universidad Carolina de Praga.

China aborrece lo que califica como «separatismo». Adopta movimientos agresivos para coaccionar a Taiwán, su Gobierno y su ciudadanía: desde una legislación cada vez más represiva hasta el boicot económico, pasando por la intimidación militar y las campañas de desinformación. Pekín preferiría ver en el poder a un Kuomintang porque, pese a tener una ideología antagónica a la del PCCh, mantiene posiciones más cercanas sobre una reunificación. China lleva años

maniobrando en este sentido. Las elecciones de 2024 representaban el campo de batalla perfecto para inclinar la balanza a su favor.

El día de la jornada electoral, el PDP llevaba ocho años en el poder. La erosión, el malestar y el hastío que suelen acompañar a cualquier gobierno extenso mellaban las perspectivas de su candidato, Lai Ching-te, que aspiraba a suceder a la presidenta Tsai Ing-wen. Al PDP le había surgido un nuevo competidor, el Partido del Pueblo de Taiwán (PPT), que amenazaba con robarle votos entre descontentos o quienes aspiraban a una renovación. Por otra parte, el tradicional Kuomintang (KMT), pese a la reducción de su base electoral, seguía siendo un rival formidable. Aunque muchos taiwaneses sentían que el PDP era su mejor baza para mantener su estilo de vida democrático y no acabar absorbidos por el autoritarismo, como ya había ocurrido en Hong Kong.

China trató de explotar las debilidades de los nacionalistas taiwaneses. Permitió al KMT hacer campaña en territorio chino entre los más de un millón de taiwaneses residentes allí, que representan un 5% de la población de la isla. Pero, sobre todo, utilizó todas las herramientas a su alcance para sugerir que la relación entre China y Taiwán sería mucho mejor con el Kuomintang al mando, dando a entender que se podrían cancelar ciertos aranceles siempre y cuando el PDP no se obcecase en «su posición proindependencia», al tiempo que dejaba siempre presente la amenaza de represalias económicas. Y no solo económicas.

China mantiene contra Taiwán una constante actividad de «zona gris», de hostigamiento militar, aunque sin cruzar cierto umbral. Un ejemplo son los ciberataques, que se multiplicaron por 30 en el último trimestre de 2023 en comparación con el año anterior. Alrededor del período electoral, las incursiones aéreas en la llamada Zona de Identificación de Defensa Aérea se produjeron casi a diario, una técnica que obliga a las fuerzas armadas taiwanesas a hacer despegar cazas que hagan frente a estas penetraciones, lo que supone un importante desperdicio de recursos y un desgaste que, a largo plazo,

podría minar la eficacia y el sentido de alerta de los defensores. En decenas de casos, estas violaciones del espacio aéreo tuvieron lugar en forma de globos, algo que muchos observadores interpretaron como una medida netamente intimidatoria.

«China ha estado llevando a cabo muchas acciones que pueden ser vistas como "guerra cognitiva". Y, en este tipo de guerra, lo que se busca es ganarse a la opinión pública», me explicó Gardas. Según la organización de verificadores taiwanesa Cofacts, en 2023 se produjo un incremento del 40% en la desinformación respecto al año anterior. Desde mostrar las ventajas económicas de acercarse a Pekín —y los inconvenientes de hacer lo contrario— hasta la difusión de información falsa.

«El mensaje de una amenaza militar china inminente fue la idea más prevalente, representando el 25% de todo el contenido [analizado], seguido de cerca por las narrativas que sugerían que Estados Unidos estaban manipulando a Taiwán hacia una precaria confrontación militar [con China]», concluyó una investigación de la organización de verificadores Taiwan AI Labs.

Redes de cuentas en múltiples plataformas, que investigadores australianos han relacionado con las fuerzas de seguridad y el Ministerio de Exteriores chino, hicieron circular la alegación de que Lai y su candidata a la vicepresidencia Hsiao Bikhim habían firmado un acuerdo secreto con Estados Unidos para comprar armas por valor de 65.000 millones de dólares, a cambio de que Washington les ayudase a ganar las elecciones. Otros mensajes afirmaban que la presidenta Tsai había autorizado la creación de biolaboratorios en connivencia con Estados Unidos para desarrollar bioarmas que solo afectasen a la raza asiática.

La organización estadounidense Graphika, que analiza operaciones de influencia online, denunció en diciembre de 2023 la existencia de «un esfuerzo sostenido y coordinado para manipular las conversaciones en internet sobre política taiwanesa antes de las elecciones presidenciales», que habría comenzado en fecha tan

temprana como mayo de 2022. «La operación parece enfocarse en promover al Kuomintang (KMT) y criticar a sus oponentes», se lee en aquel informe. Otros investigadores encontraron granjas de trols chinas en Camboya, Malasia, Hong Kong y la propia China continental.

Las narrativas amplificaban el malestar por la carestía de algunos alimentos, como los huevos. Agitaban el miedo a un futuro reclutamiento forzoso de los jóvenes en caso de guerra. Acusaban a Tsai y Lai de ser «lacayos de los estadounidenses». Afirmaban que el PDP preparaba la venta de la empresa estrella de Taiwán, la firma de semiconductores TSMC, a Estados Unidos. En internet llegó a aparecer un test de paternidad falsificado que «demostraba» que Lai tenía un hijo ilegítimo. Varios altos cargos del PDP, tanto hombres como mujeres, fueron acusados de acoso sexual, y se difundieron fotografías del ministro de Exteriores Joseph Wu manipuladas para incluir a mujeres en ellas junto con el *hashtag* #metoo.

También destaca la multiplicidad de plataformas utilizada: Facebook, X/Twitter, TikTok —una aplicación prohibida en China, pero no en Taiwán, donde una de cada cuatro personas la utiliza—, y por supuesto, YouTube. En el momento culminante de las elecciones, los operativos chinos creaban hasta doscientos canales de vídeo al día, según DoubleThink, una organización taiwanesa creada para contrarrestar tanta desinformación.

Pero lo que verdaderamente marcó esta operación fue la rápida adopción de nuevas tecnologías: «En las elecciones de enero vimos varios métodos emergentes o innovativos. Por ejemplo, *deepfakes* de audio o vídeo. En uno de esos audios, por ejemplo, se modificaron las declaraciones de Lai Chingte para que pareciese que estaba en contra de la identidad nacional taiwanesa», cuenta Gardas. En un vídeo falso detectado por Microsoft en noviembre de 2023, la presidenta Tsai Ing-wen apoyaba a la oposición en lugar de a Lai, y aseguraba que la oposición «representaba a la mayoría taiwanesa». Dicho vídeo está

considerado el primer caso en el que un Estado utilizó la IA para influir en las elecciones de otra nación.

No acabó ahí el uso chino de la IA. Semanas antes de las elecciones, empezó a circular en redes un libro de trescientas páginas titulado *La historia secreta de Tsai Ing-wen*, que recogía rumores y afirmaciones escandalosas sobre la presidenta. Esto desconcertó a los analistas de desinformación, puesto que parecía improbable que un volumen semejante fuese a tener demasiados lectores. No obstante, pronto vieron que el libro servía como guion para cientos de vídeos generados mediante inteligencia artificial a partir del texto. En algunos casos, la IA creó avatares de inexistentes presentadores de noticias que leían fragmentos del libro, que según Tim Niven, de DoubleThink Lab, «podría haber sido él mismo también fruto de la IA generativa». No obstante, la mayoría de estos vídeos apenas acumularon unas pocas visualizaciones, en gran medida debido a su escasa calidad.

Del mismo modo, muchos de los perfiles de las redes descritas cuentan con miles de seguidores, pero la interacción con los contenidos que postean tiende a ser muy baja, lo que apunta a un sistema poco perfeccionado. ¿Funcionan, entonces, este tipo de campañas? Gardas cree que no. «Al contrario, porque cuando uno ve las encuestas a largo plazo y cómo se ve la gente a sí misma, si como chinos o taiwaneses o ambos, la mayoría dicen que se sienten o identifican sólidamente como taiwaneses», señala este especialista.

Ese 13 de enero, Lai Ching-te acabó ganando las elecciones con un 40,05% de los votos, frente al 33,49% obtenido por Hou Yu-ih, el candidato del Kuomintang, y al 26,46% de Ko Wen-je del PPT. Muchos, dentro y fuera de Taiwán, suspiraron aliviados.

Sin embargo, otros expertos señalan que la injerencia china podría haber funcionado. Aunque Lai ganó por una diferencia considerable, los partidos de la oposición mejoraron sus resultados en las legislativas, y el Kuomintang pasó a ser la principal fuerza en el Parlamento. La interferencia habría incrementado tanto la polarización como el escepticismo hacia el PDP y sus políticas. «Los

intentos de interferencia de la RPC en la elección no solo buscaban dañar las perspectivas del DPP y apoyar al Kuomintang y otras fuerzas de oposición vistas como más abiertas a las posturas de Pekín. También estaban dirigidos a sembrar el caos para desacreditar a la democracia taiwanesa y reducir el atractivo de la democracia a nivel global», afirman Mareike Ohlberg y Etienne Soula, dos expertos sobre China, en un estudio publicado por el German Marshall Fund. Otros investigadores como Niven han detectado un cambio en la estrategia china, cada vez menos enfocada hacia la promoción de determinados candidatos y más hacia la erosión del sistema democrático taiwanés en su conjunto.

Paseando por Taipéi uno nunca lo diría, pero Taiwán era, y sigue siendo, una nación bajo constante asedio. En mayo de 2024 tuve la oportunidad de asistir a la toma de posesión del presidente taiwanés Lai Ching-Te en Taipéi. El ambiente era de alegría festiva, pero también de solemnidad. Las actuaciones de titiriteros, acróbatas y bandas de rock se combinaban con exhibiciones marciales, salvas de artillería y cazas sobrevolando el área. «Quiero pedirle a China que deje de intimidar a Taiwán política y militarmente, y que asuma la responsabilidad global de trabajar duro con Taiwán para mantener la paz y la estabilidad en el estrecho de Taiwán y en la región, para asegurar que el mundo no tema que estalle una guerra. También quiero decirle al mundo: Taiwán no va a hacer concesiones en la democracia y la libertad», declaró el ya presidente Lai en su discurso inaugural.

China no ha cejado en sus esfuerzos para desestabilizar al Gobierno y forzar su caída.

EL NUEVO NOMBRE DE MACEDONIA

Suele entenderse la interferencia electoral como cualquier intento de manipular el proceso o la celebración de elecciones libres, secretas e igualitarias. «En un sentido amplio, el término se refiere no solo a la

elección en sí misma, sino también a la integridad de las instituciones legitimadas democráticamente asociadas con ella, como el parlamento electo, sus diputados, y el gobierno legitimado por su electorado», según un documento elaborado por la Fundación Heinrich Böll sobre este concepto.[1]

La interferencia electoral existe desde que empezaron a celebrarse elecciones nacionales en el siglo xviii, e incluso antes, cuando se llevaban a cabo votaciones para elegir a figuras relevantes como los papas e incluso, en algunos casos, a un rey. En época más reciente, fue sonada la polémica por la publicación de la llamada «Carta Zinóviev» en el diario *Daily Mail* en 1924, en la que el entonces director del Komintern de la URSS Grigori Zinóviev pedía una normalización de relaciones con el Reino Unido en caso de una victoria del Partido Laborista. La carta, una falsificación, provocó un vuelco en las elecciones de ese año.[2]

Entre 1946 y 2000, Estados Unidos o su principal adversario ideológico, es decir, primero la URSS y después Rusia, intervinieron en una de cada nueve elecciones de carácter nacional en el mundo: los estadounidenses, en 81 ocasiones, y los soviéticos o rusos en, al menos, 36. Según el historiador Dov Levin, que ha estudiado dichas operaciones, para que un Estado poderoso se decida a interferir en las elecciones de otro país deben darse dos condiciones: «La primera es que la gran potencia vea a los candidatos o partidos en el país objetivo como una amenaza a algunos de sus intereses clave. La otra es que haya un candidato o partido en el país objetivo que esté dispuesto a aceptar esta asistencia, y eso se debe normalmente a que tiene problemas políticos profundos».[3]

Unas elecciones son el campo de batalla perfecto para la guerra cognitiva: con un esfuerzo e inversión relativamente pequeños, se puede modificar el resultado en un acontecimiento de alto impacto de un modo conveniente a los intereses de quien promueve la campaña de injerencia. Sucede, por ejemplo, cuando uno de los candidatos a la presidencia propugna un cambio de orientación en las relaciones

exteriores del país. Si el resultado posible no va a producir grandes variaciones, la interferencia no tiene sentido. Así, durante las elecciones generales de 2024 en el Reino Unido, apenas se registraron injerencias por parte de Rusia, puesto que los dos únicos partidos con opciones reales de gobernar, *tories* y laboristas, coincidían en la necesidad de mantener el apoyo económico y militar a Ucrania. No sucedió así en los comicios en Eslovaquia, Moldavia, Georgia o Rumanía, donde competían tanto candidatos con una orientación prooccidental y europeísta como otros que favorecían un acercamiento a Rusia, la reducción o cancelación de la ayuda a Kiev e, incluso en un caso, la salida de la OTAN.

El referéndum en Macedonia en 2018 ilustra esta situación. Esta diminuta nación balcánica se jugaba, en cierto modo, su futuro: debía decidir si añadía la fórmula «del Norte» al nombre oficial del país, lo que le permitiría poner fin a una disputa de casi tres décadas con la vecina Grecia, que dejaría de bloquear su entrada en la OTAN y la Unión Europea. El Gobierno del primer ministro Zoran Zaev era firmemente partidario de dicha solución, que también apoyaban sus socios occidentales. Rusia, en cambio, se oponía con vehemencia, puesto que supondría un debilitamiento de su capacidad de influencia en la región.[4] Con estos mimbres, ambos jugaron sus cartas en el ámbito cognitivo.

Durante meses, cuarenta nuevas páginas creadas en el extranjero aparecían cada día en Facebook pidiendo a los ciudadanos macedonios que boicotearan el referéndum y quemaran sus papeletas, siguiendo un patrón que muchos expertos identificaron con Rusia. Se promovieron mensajes con desinformación, asegurando que Google eliminaría el idioma macedonio de su lista si la consulta arrojaba un resultado positivo, o utilizando la imagen de una famosa cantante balcánica lastimada tras una paliza, asegurando que las autoridades la habían maltratado durante una protesta, cuando en realidad las lesiones se debían a un episodio previo de violencia doméstica. Para combatirlos, el Congreso de Estados Unidos aprobó en enero de 2017

una partida presupuestaria de ocho millones de dólares para Macedonia.[5] Mientras tanto, Zaev recurrió a firmas de relaciones públicas occidentales para que le ayudasen a difundir las ventajas del «sí».

Periodistas de investigación británicos descubrieron que al menos una empresa con sede en Londres, Gabara Strategies, ofreció sus servicios al Gobierno macedonio, aunque no está claro si aceptó la propuesta. Otra firma británica, Stratagem International, tomó parte en la campaña a favor de la aprobación del cambio de nombre, con financiación parcial del Reino Unido.[6] Los votantes apoyaron el «sí» con un masivo 91,3% frente a un 5,7% del «no». Pero apenas participó un tercio del electorado, muy lejos del 50% requerido para hacer válido el referéndum. Muchos observadores lo interpretaron como una victoria rusa.[7] En último término, el Gobierno de Skopje decidió seguir adelante con el cambio de nombre pese a la falta de cuórum.

DE UCRANIA A TRUMP

En mayo de 2014, Ucrania se disponía a celebrar elecciones generales. El país se encontraba en una encrucijada política: apenas tres meses antes, la revuelta del Maidán había derrocado al presidente Víktor Yanukóvich, cuya huida y posterior destitución en una votación parlamentaria —boicoteada por los miembros de su partido— había desatado el caos social. Pocos días después de la fuga de Yanukóvich, Rusia se había anexionado unilateralmente la península de Crimea, aprovechando un vacío político que ahora los ucranianos esperaban llenar con estos comicios. Concurrían 29 partidos, entre ellos, el de la antigua primera ministra Yulia Timoshenko. Pero el favorito era el magnate Petro Poroshenko.

El 22 de mayo, tres días antes de las elecciones, el grupo de hackers Cyberberkut —conectado con el servicio de inteligencia ruso— penetró en el sistema de votación de la Comisión Electoral Central

ucraniana y manipuló los datos a favor del candidato ultraderechista Dmytro Yarosh, del Sector Derecho. La alteración presentaba a Yarosh como el ganador de las elecciones con un 37% de los votos, frente a un supuesto 29% que habría recibido Poroshenko.[8]

La manipulación fue rápidamente detectada por las autoridades y no logró alterar los resultados.[9] En realidad, Poroshenko había obtenido el 55,46% de los votos, mientras que Yarosh apenas llegó al 4,6%.[10] Pero, al día siguiente, el Canal 1 de la televisión rusa difundió los falsos resultados, anunciando los mismos porcentajes que los hackers habían introducido en el sistema. El objetivo estaba claro: mostrar que Ucrania había elegido a un extremista neonazi como jefe de gobierno, lo cual probaba lo que Moscú llevaba meses diciendo: que la revuelta del Maidán había sido un golpe de Estado nazi. Cuando las autoridades de Kiev «revirtiesen» los porcentajes electorales —anunciando los reales—, se abriría otra oportunidad para la desinformación, que explotaría el caos resultante para sembrar dudas sobre la democracia ucraniana.

Efectivamente, Rusia volvió a la carga apenas dos meses después. El 24 de octubre, dos días antes de las elecciones parlamentarias, dos paneles digitales de anuncios publicitarios situados en lugares céntricos de la capital ucraniana fueron hackeados para que mostrasen anuncios acusando a los políticos ucranianos de crímenes de guerra y de la muerte de civiles en el conflicto en el Dombás, que el propio Moscú había ayudado a orquestar.[11] Los anuncios, de 75 segundos, estaban coordinados con las luces del tráfico, para que apareciesen justo cuando los semáforos se ponían en rojo. Las imágenes eran bastante gráficas, diseñadas para enfadar a las audiencias, con la intención de cambiar su voto.[12]

Rusia estaba ganando experiencia en la interferencia electoral con las operaciones cognitivas. Pronto, ese conocimiento se utilizaría para manipular todo tipo de procesos electorales; a favor del Brexit durante el referéndum en 2016,[13] aunque existe un importante debate sobre si esto tuvo algún efecto real en el resultado.[14] Pero lo que casi nadie

esperaba era que dirigiese ese bagaje contra el país más poderoso del mundo. Muy pocos lo vieron venir, y, cuando lo hicieron, ya era tarde.

El 6 de noviembre de 2016, también dos días antes de las elecciones presidenciales de Estados Unidos, un grupo de especialistas en ciberseguridad y operaciones de influencia —Clint Watts, Andrew Weisburd y J. M. Berger— escribieron un artículo en el que relataban algo llamativo: en los años previos habían percibido cómo cada vez que algún experto publicaba contenido crítico con el régimen de Bashar al-Ásad, hordas organizadas de trols emergían de la nada para atacar al autor en redes y tratar de hundir su reputación. Los tres profesionales habían recopilado una base de datos de más de 7.000 cuentas de este tipo, y ahora veían con alarma cómo habían pasado de defender la dictadura siria a tratar de sembrar la confusión y las divisiones en Estados Unidos ante los inminentes comicios.

A finales de octubre, algunas de esas cuentas, ayudadas por bots, estaban promoviendo una petición a la Casa Blanca: «La eliminación de máquinas de votación propiedad de George Soros en 16 estados». Dichas máquinas no existían, pero la petición consiguió 129.000 firmas. El propósito de la campaña era bastante transparente: sembrar dudas sobre un fraude electoral. «El objetivo de estos esfuerzos podría no ser que Trump salga elegido como presidente sino, más bien, asegurar que el resultado de la elección sea lo más divisivo y negativo posible», especulaban Watts, Weisburd y Berger.[15]

Se ha escrito muchísimo sobre cómo Rusia interfirió en esas elecciones, así que nos limitaremos a reseñarlo de forma muy esquemática. En líneas generales, la operación se desarrolló en tres ámbitos diferentes: el hackeo de comunicaciones internas de funcionarios y agrupaciones políticas, las campañas en redes sociales para polarizar a las audiencias y crear dudas sobre el sistema democrático, y los contactos entre operativos rusos y miembros de la campaña de Donald Trump. De cara a este libro, son los dos primeros los que más nos interesan. Sobre todo, lo relacionado con el aspecto cognitivo.

Dos semanas antes de los comicios, el experto Thomas Rid había publicado otro artículo en la revista *Esquire* titulado «Cómo Rusia llevó a cabo el mayor hackeo electoral en la historia de Estados Unidos». Describía en detalle las acciones que grupos de hackers asociados con diversos servicios de inteligencia rusos habían llevado a cabo contra individuos e instituciones. El otoño anterior, el FBI había contactado con el Comité Nacional Demócrata (DNC) para avisarles de que revisasen sus equipos y sistemas informáticos. Los responsables no lo consideraron una prioridad y hasta mayo del año siguiente no contactaron con una empresa de ciberseguridad para que examinase potenciales vulnerabilidades. Pero en junio se hizo público que dos grupos diferentes de hackers rusos, denominados Cozy Bear y Fancy Bear,[16] habían penetrado las redes del DNC y llevaban bastante tiempo paseándose a voluntad por sus sistemas. También habían accedido a los emails de John Podesta, el jefe de campaña de la candidata demócrata Hillary Clinton, y a las conversaciones privadas del comandante supremo de las fuerzas de la OTAN en Europa, Philip Breedlove. Esta información empezó a ser filtrada en diferentes páginas web, como DC Leaks, que había sido creada en abril, pero había pasado desapercibida hasta julio. Y, finalmente, a la célebre WikiLeaks.[17]

Los hackers cometieron una serie de errores que permitieron a varios especialistas en ciberseguridad atribuir la penetración, con un grado sólido, a Rusia, apenas unas horas después de que se hiciese pública la brecha de los servidores del DNC. Inmediatamente, un supuesto pirata informático desconocido hasta el momento, que se hacía llamar Guccifer 2.0 —un guiño a un famoso hacker rumano, Guccifer—,[18] hizo una declaración pública atribuyéndose la ciberoperación. Más tarde, el fundador de WikiLeaks, Julian Assange, insinuaría en una entrevista que la fuente de los documentos y correos electrónicos filtrados era Seth Rich, un empleado de la DNC que había sido asesinado en Washington D. C.[19] La investigación de la comunidad de inteligencia norteamericana concluyó que ambas

afirmaciones eran una pantalla destinada a encubrir el verdadero origen de las filtraciones: los servicios secretos de Rusia.

La segunda dimensión de esta operación se centró en las redes sociales. Tal y como revelaría la investigación posterior, Yevgueni Prigozhin envió a equipos de personas en viajes exploratorios a Estados Unidos para que se empaparan de la cultura estadounidense y averiguaran cuáles eran los asuntos más polarizados entre la sociedad norteamericana: la inmigración, la raza, la religión o el movimiento Black Lives Matter —creado apenas dos años antes— y su reverso a favor de la acción policial, Blue Lives Matter.[20] Con esta información, la avanzadilla de Prigozhin regresó a Rusia y se puso a trabajar.

Un extrabajador de la IRA entrevistado por la televisión independiente Dozhd en 2018 e identificado como «Maxim», aportó información interesante sobre cómo se ejecutó la operación. Las acciones eran más sofisticadas que las llevadas a cabo para las audiencias internas en Rusia. En lugar de eslóganes sencillos y vacíos insultando a Obama y alabando a Putin, se orquestaban conversaciones emocionales sobre asuntos como impuestos, derechos LGTB o armas de fuego. A los trabajadores se les daban instrucciones para que posteasen en los comentarios de los principales medios estadounidenses, como *The New York Times* o *The Washington Post*, y que soltasen algunas frases incendiarias para «agitar el barco», como azuzar los sentimientos religiosos contra los homosexuales. También se les ordenaba que no hablasen de Rusia o de Putin, sino que buscasen provocar el desorden, atacando constantemente a Hillary Clinton y culpándola de todo lo que iba mal en el país. «El mensaje principal era: "¿no estáis cansados, hermanos estadounidenses, de los Clinton? ¿Cuánto tiempo llevan por aquí?"» A los trols les hacían ver la serie *House of Cards* en inglés. También recibían lecciones para corregir su gramática.[21]

Existe la teoría de que Putin, furioso por la revelación de la que casi con certeza era su riqueza personal en la investigación periodística conocida como «los papeles de Panamá»,[22] y convencido de que era

una maniobra de los servicios de inteligencia estadounidenses, buscó la forma de vengarse. Y encontró el modo de hacerlo interfiriendo en el proceso electoral en contra del Partido Demócrata.

«Querían hacerlo lo más público posible. Querían que su presencia se supiera», señala la periodista rusa Yevguenia Albats, autora de un libro sobre el KGB, en una entrevista con *The New Yorker.*[23] Según Albats, Putin no creía que pudiese alterar los resultados, pero, dada su antipatía hacia Barack Obama y Hillary Clinton, pensó que era buena idea impulsar a Trump. «Fue una decisión táctica, muy emocional. La gente [del Gobierno ruso] estaba muy molesta por los papeles de Panamá», explica el también periodista ruso Andréi Soldatov, experto en los servicios de inteligencia de su país, en un artículo de *The Atlantic*. «Nadie creía en Trump, ni siquiera un poco», indica Soldatov. «Fue una serie de operaciones tácticas. A cada momento, la gente que lo estaba llevando a cabo estaba cada vez más excitada por lo bien que iba, y ese éxito les iba empujando a ir más y más allá».[24]

Según revelarían posteriormente las pesquisas del fiscal especial Robert Mueller, designado por la Administración Trump para investigar la interferencia del Kremlin, operativos rusos adquirieron espacios publicitarios por valor de 100.000 dólares, en los que introdujeron sus mensajes y memes. Unos 126 millones de estadounidenses estuvieron expuestos a estos contenidos durante 2015 y 2016. La IRA llegó a crear un personaje de ficción llamado Jenna Abrams, una supuesta «activista conservadora» muy activa en redes sociales, que llegó a ser citada por la BBC y otros medios. Una parte muy importante de la operación era magnificar la asociación entre Hillary Clinton y el problema con sus emails, y funcionó: una encuesta de Gallup llevada a cabo poco antes de las elecciones mostraba que, cuando se preguntaba a los participantes cuál era la primera palabra que les venía a la mente cuando se les preguntaba por cada candidato, la mayoría, al hablar de Clinton, respondía: «emails».[25] El 8 de noviembre de 2016, finalmente, Donald Trump ganaba por sorpresa la contienda electoral, contradiciendo casi todas las encuestas.

Dada la naturaleza del sistema electoral en los países democráticos, es imposible asegurar que las dos operaciones paralelas, la de Rusia y la de Cambridge Analytica, decidieran la victoria de Trump, en la que sin duda influyeron muchísimos otros factores. Pero, dado que el republicano ganó por una diferencia de apenas 40.000 votos repartidos por los estados clave de Michigan, Wisconsin y Pensilvania, no es descabellado pensar que tuvieron el impacto suficiente para el empujón final. En cualquier caso, solo cabe especular al respecto.

EL APRENDIZAJE DE MACRON

Aquella interferencia se percibió como un éxito en el Kremlin y sus servicios de inteligencia no tardarían en volver a intentarlo. En marzo de 2017, David Grout, un experto en ciberseguridad de la firma FireEye, avisó en una entrevista con la BBC del «interés por parte del grupo de hackers rusos APTO, también conocido como Fancy Bear, en influir en las elecciones francesas». En abril, el equipo de campaña de Emmanuel Macron confirmó que su partido había sido objeto de ciberataques desde principios de año, y que al menos cinco de los colaboradores más cercanos del candidato habían sido hackeados.

El 3 de mayo, unos supuestos emails filtrados en internet parecían indicar que Emmanuel Macron tenía una cuenta bancaria secreta en las Islas Caimán. Esta filtración fue inmediatamente amplificada por unas 7.000 cuentas de X/Twitter, muchas de ellas identificadas como partidarias de Donald Trump, con los *hashtags* #MacronGate y #MacronCache-Cash («#MacronEscondeEfectivo»). La información fue rápidamente investigada por varios medios y desacreditada públicamente como falsa.

Pero el 5 de mayo, justo antes de las 19.00 horas, un gran conjunto de archivos emergió en una página para compartir documentos llamada Pastebin, con el título «EMLEAKS». Poco después, en un foro de política de la página 4chan, alguien colgó un enlace a dichos archivos. Faltaban apenas unas horas para que comenzase la

moratoria informativa en Francia, que prohibía la publicación de información política o electoral hasta el día de las elecciones. Pero en escasos minutos, los *influencers* de ultraderecha Jack Posobiec y William Craddick llamaron la atención sobre este enlace en su cuenta de X/Twitter, con el *hashtag* #MacronLeaks. Según Posobiec, el individuo que había colgado los primeros documentos le había alertado con antelación de que se avecinaba esta nueva tanda. WikiLeaks también avisó de la existencia de los enlaces y, al poco, cuentas afiliadas con el Frente Nacional de Marine Le Pen se lanzaron a darles difusión. En las siguientes tres horas y media, #MacronLeaks se utilizó en 47.000 tuits. A la vez, correos claramente falsificados aparecieron en multitud de rincones de internet.

Según el informe de 2018 elaborado por el Gobierno francés, el patrón que siguieron los MacronLeaks fue el siguiente: «Primero, el contenido es volcado en un panel de discusión política como 4chan. Segundo, se lleva a redes sociales *mainstream* como X/Twitter. Tercero, se difunde a través de comunidades políticas, notablemente la *alt-right* de Estados Unidos y la extrema derecha francesa con cuentas catalizadoras o "gurús" (Craddick, Posobiec), y finalmente el contenido es retuiteado tanto por personas reales como por bots. El uso de bots era obvio, dado que algunas cuentas postearon casi 150 tuits por hora». Sputnik y RT también se lanzaron a dar a conocer estas informaciones.[26]

Pero, a diferencia de lo sucedido en Estados Unidos el año anterior, MacronLeaks fracasó por varios motivos. La campaña de Macron reaccionó rápidamente: el jefe de operaciones digitales, Mounir Mahjoubi, compareció públicamente para presumir de que su equipo había falsificado deliberadamente algunos documentos y los había plantado estratégicamente en sus servidores, anticipando los hackeos.

Al examinar el contenido de los supuestos archivos secretos, muchos usuarios encontraron algunos que eran claramente burdas falsificaciones, con afirmaciones totalmente inverosímiles, lo que obligó a WikiLeaks a marcar distancias públicas con las filtraciones.

«En unas pocas horas, la campaña había logrado con éxito arrojar dudas sobre la validez de la nueva selección de documentos», señala un análisis del Centro de Estudios Estratégicos e Internacionales (CSIS) de Washington sobre este caso.

«Mientras los medios siguieron informando sobre esta historia en los días siguientes, perdieron interés en los mismos documentos y se enfocaron en su lugar en el ataque. Resultaba imposible saber qué documentos eran genuinamente atribuibles a la campaña de Macron en un período tan corto de tiempo"».[27] Además, los responsables del hackeo habían cometido una serie de errores, como sobrestimar el interés de la ciudadanía francesa en una filtración que realmente no contenía ninguna revelación escandalosa, asumiendo que crear confusión bastaría para provocar un vuelco en las tendencias electorales.

Del mismo modo, «el ataque sufrió de torpeza cultural. La mayoría de las cuentas catalizadoras (y bots) estaban en inglés porque las filtraciones fueron difundidas primero por la comunidad *alt-right* estadounidense. Esta no resultaba una forma efectiva de penetrar entre la población francesa, que es conocida por no tener las mejores habilidades lingüísticas», apunta, no sin humor, el informe del Gobierno galo.

Francia se benefició también de las lecciones aprendidas en Estados Unidos. Las autoridades francesas habían puesto en marcha toda una serie de medidas y ciberequipos de profesionales para garantizar la seguridad de los sistemas, habían advertido sobre estos riesgos y concienciado acerca de ellos a los medios y la población en general. También habían instruido a los partidos sobre cómo ser proactivos ante potenciales hackeos. En último término, cuando se produjo la filtración, tanto la campaña de Macron como el Gobierno llevaron a cabo una política de comunicación muy efectiva que permitió darle la vuelta a las narrativas.

El 7 de mayo de 2917, Macron acabó ganando las elecciones con un 66% de los votos.[28]

Los rusos no han sido los únicos en llevar a cabo este tipo de acciones en los últimos años. Según un informe de 2020 del Centro Internacional de Ciberpolítica de Australia, perteneciente al Instituto Australiano de Política Estratégica, durante la década anterior se produjeron al menos 48 intentos de interferir digitalmente en procesos electorales y referéndums en todo el mundo contra 33 estados diferentes: 31 por parte de Rusia, 10 por parte de China, 4 por parte de Irán y 2 por parte de Corea del Norte. En ocasiones, estos intentos ocurrían de forma simultánea. Estos cuatro estados, por ejemplo, desarrollaron actividades de interferencia en las elecciones presidenciales de Estados Unidos en 2020.[29]

El informe revela técnicas desplegadas en esta clase de operaciones. En catorce ocasiones se utilizaron exclusivamente ciberataques, en veintidós se recurrió solamente a operaciones de información, y en doce hubo una combinación de ambos métodos.[30] En un número significativo de casos se recurrió al *phishing* —engaños bien diseñados para que la víctima facilite información esencial, como sus contraseñas y datos personales, o instale malware en sus equipos— para lograr acceso a información de individuos y organizaciones implicadas en las campañas, las elecciones, su infraestructura o su gestión.[31] A veces, como hemos visto anteriormente, la publicación controlada de estas informaciones permitió dar forma a campañas cognitivas mucho más complejas para tratar de influir en la percepción de los votantes.

Habrá quien se pregunte por qué no hay reseñado ningún caso de intento de interferencia por parte de países occidentales en otros estados. Los motivos son varios: primero, porque el informe se enfoca en operaciones de injerencia desarrolladas en el ciberespacio, y lo cierto es que no existen evidencias documentadas de que se haya producido ninguna campaña de este tipo que pueda vincularse directamente a un gobierno. Quizá se debe a que los analistas occidentales tienen su mirada puesta en los países considerados

hostiles o adversarios, y no están mirando donde podrían encontrarlas. O quizá es que, simplemente, por difícil que sea de creer para algunos, realmente Europa, Norteamérica y Australia no participan en este tipo de acciones.[32]

También está el hecho de que hay otras muchas formas de influir en unas elecciones, desde promover o directamente financiar a determinados candidatos y grupos de la sociedad civil hasta imponer sanciones contra otros individuos y organizaciones, o presionar para que las instituciones internacionales actúen en un sentido determinado.[33] Esto abre mucho más el abanico e introduce un interesante debate sobre aspectos como la defensa absoluta de la soberanía nacional frente a la legitimidad de promover a una oposición democrática en un entorno autocrático. Pero eso ya queda fuera del objeto de estudio de este libro.

Sí existen, en cambio, pruebas de que se ha intentado interferir digitalmente en procesos electorales en Latinoamérica mediante operadores privados, aunque de momento no es posible vincular dichas acciones a países como Estados Unidos, porque no existe un rastro contractual o documental que pruebe que su Gobierno tomó parte.

Por ejemplo, en agosto de 2020 Facebook eliminó una red de 55 cuentas y 42 páginas en esta plataforma, más otras 36 cuentas en Instagram, vinculadas a la empresa de comunicaciones y relaciones públicas estadounidense CLS Strategies. Las cuentas enfocaban su actividad en Bolivia, Venezuela y México haciéndose pasar por usuarios locales. De acuerdo con la plataforma, CLS Strategies «violaba su política contra la interferencia extranjera o el comportamiento coordinado inauténtico en beneficio de una entidad extranjera». Según un análisis realizado por el Centro de Ciberpolítica de la Universidad de Stanford,[34] algunas de las cuentas operaban en beneficio del entonces gobierno interino de Jeanine Áñez en Bolivia, que había llegado al poder tras el polémico derrocamiento de Evo Morales, después de que la oposición le acusase de fraude electoral.

CLS Strategies ya había realizado trabajos similares de *lobby* para el Gobierno de Honduras tras el golpe que tumbó al Ejecutivo de Manuel Zelaya en 2009.[35]

En otros casos, la red de CLS Strategies trató de erosionar al Gobierno de Andrés López Obrador en México y al de Nicolás Maduro en Venezuela, aunque el informe de Stanford señalaba que «los activos enfocados en Venezuela apoyaban y promovían a los líderes de oposición venezolanos, pero cambiaron el tono en 2020, reflejando las divisiones entre facciones de la oposición y un alejamiento del presidente opositor Juan Guaidó». CLS Strategies negó firmemente que sus actividades supusiesen un proceso de interferencia extranjera, alegando que sus clientes eran ciudadanos locales de los países donde operaban. «Nuestro anterior trabajo en Latinoamérica, incluida la oposición a regímenes opresivos, no fue realizado en beneficio de entidades extranjeras: el trabajo fue financiado y dirigido por clientes dentro de cada país», declaró un alto cargo de la empresa. «Cualquier caracterización del trabajo de CLS en los tres países en cuestión como "extranjero" es errónea».[36] Sea como fuere, y pese a numerosos intentos de presentar este y otros episodios como ejemplos de campaña de interferencia de Washington,[37] no hay evidencias directas.

Porque, además, estas prácticas no conocen fronteras ideológicas. En julio de 2020, Facebook había eliminado otra red similar de 61 páginas, 35 cuentas y 48 perfiles de Instagram vinculadas a Estraterra, una firma ecuatoriana de relaciones públicas que operaba desde Canadá, fundada por consultores políticos y exfuncionarios del Gobierno de Rafael Correa en Ecuador. La red se dedicaba a promover a candidatos de izquierdas en diversos procesos electorales políticos en gran parte de Latinoamérica: Argentina, Brasil, Bolivia, Chile, Colombia, Uruguay y Venezuela, utilizando también cuentas falsas que simulaban pertenecer a ciudadanos de dichos países.[38]

Los informes sobre redes detectadas y neutralizadas por las plataformas de Silicon Valley en esos años son una mina de

información que demuestra que la utilización de empresas para influir en procesos electorales en el extranjero están a la orden del día: solo en 2019 y 2020, Facebook desactivó operaciones similares llevadas a cabo desde Israel, la India, Egipto, Arabia Saudí o Emiratos Árabes Unidos.[39] También en Túnez, donde la empresa UReputation había interferido en las elecciones no solo de su país, sino en las de Togo, Costa de Marfil y otras siete naciones africanas.[40]

En 2021, Facebook desactivó una red de cuentas de la firma italiana de relaciones públicas Reputation Up por actividades de injerencia política en El Salvador, y otra llamada Leanga Software por hacer lo mismo en Ecuador, tratando de minar la imagen del entonces candidato presidencial Andrés Arauz y difundiendo acusaciones falsas de corrupción. Ambas empresas tenían su sede en Madrid.[41]

Dos años después, Meta (la empresa matriz de Facebook) y X/Twitter actuaron contra las cuentas de la empresa Predictvia, con sede en Miami, que según su página web afirmaba estar «en la primera línea de la lucha contra la información falsa» y combatir «los esfuerzos coordinados para manipular el discurso público». En realidad, el análisis forense realizado por las plataformas descubrió que esta firma dirigía una red de cuentas falsas en Instagram, Facebook y X/Twitter que fingían ser medios de prensa, periodistas o *influencers* de moda y estilo de vida, pero que se habían utilizado para interferir en las elecciones de Honduras y Guatemala. Según Meta, estas cuentas tenían unos 6.700 seguidores en Facebook y 400 en Instagram.[42]

Otra interferencia es a través de donaciones a una campaña. En países como Estados Unidos son ilegales si proceden directamente de un Estado, pero es lo que habrían hecho Emiratos Árabes Unidos y Arabia Saudí en 2016, utilizando como intermediarios a varios hombres de negocios. El californiano de origen árabe Ahmad Khawaja habría canalizado más de 3,5 millones de dólares proporcionados por los emiratíes para ganar acceso e influencia en Washington, primero a la campaña de Hillary Clinton y, en una segunda fase, a la de Donald

Trump. Según Khawaja, los saudíes también participaron en este esquema a favor de Trump. Los intentos de manipulación fueron descritos en detalle en un informe de los servicios de inteligencia estadounidenses en 2022.[43] Ambas actividades fueron descubiertas años después.

Uno de los países que más ha destacado es la Hungría de Viktor Orbán, aunque se limita por lo general al continente europeo. Según las investigaciones del medio húngaro VSquare, su Gobierno no solo envió asesores electorales en apoyo de sus aliados políticos en Eslovaquia y Polonia para los comicios de 2023,[44] sino que gastó millones de euros en anuncios en YouTube en siete países europeos, con el propósito de promover mensajes antiinmigración que favoreciesen a partidos de su órbita política. Los vídeos, que mostraban imágenes dramáticas filmadas en la frontera entre Hungría y Serbia y que afirmaban que «Hungría protege a la UE de la inmigración ilegal», aparecieron en las pantallas de los ciudadanos de dichos países —Eslovaquia, Polonia, República Checa, Austria, Alemania, Italia y Bélgica— durante el verano y principios del otoño de 2023, en mitad de una crisis migratoria en el sur de Eslovaquia. Estaban etiquetados como no políticos, para evitar las restricciones que las plataformas imponen a la publicidad política, lo que, entre otras cosas, permite afinar mucho más a qué público objetivo dirigirlos gracias al *microtargeting*. Las campañas estuvieron a cargo del ministro Antal Rogán, a cargo de todas las cuestiones relacionadas con asuntos propagandísticos en el Gobierno húngaro.[45]

De acuerdo con VSquare, la campaña más intensa tuvo lugar en Eslovaquia, donde se lanzaron entre 1,6 y 1,8 millones de anuncios. Al estar clasificados como no políticos, también evitaron la legislación eslovaca durante las últimas 48 horas antes de la apertura de las urnas. En esa franja, por imperativo legal, las campañas de todas las formaciones políticas tuvieron que poner fin a los contenidos que llevaban meses promoviendo en redes. Pero, al hablar sobre los supuestos peligros de la inmigración, los anuncios húngaros

impulsaron la campaña del partido SMER de Robert Fico, que contenía varias cláusulas antiinmigrantes en su programa. La televisión pública húngara hizo una entrevista a Fico durante esos dos días de moratoria, que después fue distribuida dentro de Eslovaquia por redes sociales.

«No veo otra razón para esto que el interés del Gobierno húngaro en ayudar a traer a colación el tema [de la inmigración]», declaró el exministro eslovaco de Defensa Jaroslav Nad' a la citada publicación. «Si yo quisiera influir en la opinión pública, especialmente un día o dos antes de las elecciones eslovacas, lo haría de ese mismo modo. Hungría, de hecho, jugó un papel muy intenso en que Robert Fico ganase las elecciones».[46]

Los mismos anuncios no lograron que el Partido Ley y Justicia (Pis) fuese reelegido en Polonia, ni sirvieron en Austria, República Checa o Bélgica, pero sí podrían haber influido en las elecciones locales de Alemania e Italia, donde Alternativa para Alemania (AfD) avanzó en los estados de Bavaria y Hessen, y la Lega de Matteo Salvini, un estrecho aliado de Orban, ganó en la región de Trento.

Lo que este episodio pone de manifiesto es que en el universo de la manipulación cognitiva y las operaciones de influencia, los procesos de interferencia electoral pueden adoptar formas muy sutiles.

8

CONSPIRANOICOS Y EXTREMISTAS

Tú también crees en las teorías de la conspiración. Todos lo hacemos. Quizá creas que los atentados del 11-S fueron una operación de falsa bandera de la Administración Bush, porque hay demasiadas cosas que no terminan de encajar.[1] O que los individuos más poderosos del mundo deciden lo que va a suceder en los próximos doce meses durante su reunión anual del club Bilderberg.[2] O que ciertas élites favorecen deliberadamente la inmigración a países occidentales como mano de obra barata o para diluir su identidad.[3] O que el intento de asesinato de Donald Trump en octubre de 2024 fue orquestado por él mismo; o por los «globalistas», George Soros y/o el Estado Profundo.[4] O que en los años ochenta, el Estado español distribuía heroína en los barrios obreros más combativos, especialmente en Euskadi.[5]

Es normal. Estudios recientes muestran que prácticamente todo el mundo cree en al menos una teoría de la conspiración,[6] sobre todo acerca de sucesos o dinámicas de los que no sabe demasiado. La mayoría de nosotros encuentra entretenidas muchas de estas ideas, y resulta divertido especular sobre los motivos, el contexto o el modo en que se ejecutan las conspiraciones. Y, si detrás de todo ello está, presuntamente, un gobierno en la sombra, una sociedad secreta o un malvado servicio de inteligencia, el cóctel resulta irresistible.

Pero además, así es la naturaleza humana: nuestro cerebro tiene dificultades ante la incertidumbre y elabora atajos mentales para explicar eventos complejos, especialmente cuando hay oscuridad sobre muchos aspectos de lo ocurrido. La falta de información es, de hecho, una de las claves principales: he comprobado personalmente que mucha gente cree que el hombre no ha pisado la Luna y asume que las

famosas imágenes de Neil Armstrong y Buzz Aldrin con la bandera estadounidense son un montaje, simplemente porque no sabe que un total de 24 astronautas estadounidenses han tomado parte en expediciones que han llegado hasta allí, que doce han caminado sobre la superficie lunar,[7] que otros tres países —la URSS, China y la India— han llevado a cabo alunizajes exitosos,[8] y que se han recogido 2.415 muestras de rocas lunares que pesan un total de 382 kilogramos y que se encuentran repartidas por museos de todo el mundo, incluida una en el Museo Geominero de Madrid.[9] Si hablamos de personas razonables —y el asunto se aborda con tacto—, la mayoría comprende que la creencia que habían albergado hasta la fecha era falsa. Aunque no siempre ocurre así.

Tampoco ayuda el hecho de que, en ocasiones, las conspiraciones son reales. El incidente del Golfo de Tonkín en 1964, la supuesta agresión de barcos norvietnamitas contra navíos estadounidenses que fue tergiversada por la Casa Blanca para justificar la escalada bélica de Estados Unidos en Vietnam, es un hecho comprobado históricamente.[10] El complot de la firma Volkswagen para instalar legalmente un software que falsificaba los datos sobre las emisiones contaminantes de sus vehículos ocurrió de verdad.[11] Las acciones de las autoridades británicas que, en un intento de no estigmatizar a la comunidad paquistaní y agitar los prejuicios raciales, minimizaron durante años la existencia de bandas de ciudadanos mayoritariamente de dicha nacionalidad dedicadas al abuso sexual de menores, mientras la lista de víctimas seguía creciendo, son una realidad.[12] La lista es interminable.

Los estudios muestran que, a la hora de creer en teorías de la conspiración, no hay grandes diferencias entre género, edad, nivel de educación, orientación política o cuestiones religiosas.[13] En cambio, el entorno sociocultural sí importa. De modo que, en algunos países, la población es más proclive a creer este tipo de narrativas. Pero el factor que destaca como más relevante es uno que, a estas alturas, no debería sorprender: los teóricos de la conspiración tienen una tendencia mayor

a informarse en las redes sociales, en lugar de en los medios tradicionales.[14]

Antes de proseguir, aclaremos algo: una leyenda urbana no es una teoría de la conspiración. Es decir, la idea de que las alcantarillas de Nueva York y otras ciudades albergan caimanes, o la de que Elvis Presley vivió durante muchos más años después de su supuesto fallecimiento y se desplazaba por todo Estados Unidos en secreto, son de una naturaleza diferente, y generalmente más inocua, que las ideas que hemos apuntado al principio de este capítulo. A no ser que añadamos que las autoridades neoyorquinas son muy conscientes del peligro que suponen los reptiles, pero mantienen el silencio para no alarmar a la población. O que Elvis no es sino uno entre cientos de celebridades oficialmente muertas, a quienes las autoridades conceden ese tipo de «retiro» en sus últimos años. Las teorías de la conspiración, como su propio nombre indica, requieren la existencia de algún tipo de complot. Y, por lo tanto, tienen por definición un componente político, que puede llegar a ser notoriamente dañino.

El filósofo Quassim Cassam, profesor de la Universidad de Warwick afirma en su libro *Teorías de la conspiración*[15] que son «primero y sobre todo, formas de propaganda política. Son apuestas políticas cuya función real es promover una agenda política». Pone como ejemplo predominante el negacionismo del Holocausto, cuyo propósito es promover causas antisemitas de extrema derecha. Una de las razones en las que apoya su argumento es que, a menudo, los teóricos de la conspiración sostienen que sus ideas no han sido demostradas todavía. Aunque la falsedad haya sido probada más allá de toda duda razonable, el hecho de que persistan demuestra su carácter eminentemente político. «Las teorías de la conspiración promueven un objetivo político de una forma especial proporcionando explicaciones seductoras ante grandes sucesos que, hablando objetivamente, es improbable que sean ciertas, pero es probable que influyan en la opinión pública en la dirección buscada». Otro ejemplo: la creencia de que muchos tiroteos en escuelas norteamericanas son

montajes u operaciones de falsa bandera para justificar las restricciones al uso y posesión de armamento militar.[16]

Más que una característica biológica o un rasgo de personalidad, la conspiración es una ideología, argumenta el filósofo. Suele existir una correlación directa entre la orientación política de una persona y qué teorías son aquellas en las que cree al tiempo que descarta otras. Por ejemplo, aquellas personas para las que el libre mercado es una parte esencial de su ideología tienden a creer más en las teorías conspirativas sobre el cambio climático, presumiblemente porque no les gustan las regulaciones derivadas.

Cassam enumera las principales características de una teoría de la conspiración: son contrarias a la versión oficial, y tienden a rechazar toda explicación plausible o técnica que no entre en su marco. Cuando algún experto refuta sus razonamientos, pasa automáticamente a ser integrado como parte de la supuesta conspiración. Además, los teóricos recurren a explicaciones científicas de andar por casa, y tienden a ser *amateurs*. Pueden tener mucha formación, pero raramente en el campo específico relacionado con el evento que están tratando de explicar. Por ejemplo, apenas hay verdaderos ingenieros entre los llamados *truthers* de los atentados del 11 de septiembre, muchos de los cuales sostienen que la caída de las Torres Gemelas fue una voladura controlada y no el resultado del impacto de dos aviones secuestrados por terroristas de Al Qaeda.

Estas teorías son también esotéricas y promueven un pensamiento premoderno, al buscar siempre una razón para cosas que a veces no es posible entender o para las que no hay una explicación única o definitiva, o cuya explicación real es otra. Por último, son especulativas, porque, por lo general, no existen evidencias sólidas que las respalden, puesto que si las hubiese, ya no serían una teoría sino un hecho demostrado, como sucede con las conspiraciones apuntadas anteriormente. Cassam admite que porque una teoría sea especulativa, contraria a la versión oficial, esotérica o *amateur* no tiene por qué ser

necesariamente falsa, pero que, cuando se dan todos estos elementos, la probabilidad de que sea cierta es mínima.

Aunque, en realidad, eso tampoco es lo más importante: «En la práctica lo que cuenta no es si una teoría de la conspiración es cierta, sino si es seductora. En ese punto es difícil cuestionar el éxito de muchas teorías de la conspiración. Cuentan historias que la gente quiere oír».

ALEX JONES, EL MAESTRO CONSPIRANOICO

Tomemos el caso del que probablemente es el teórico de la conspiración más famoso del mundo: Alex Jones, empresario y director del programa alternativo *Infowars*, que se emite en radios de todo Estados Unidos al tiempo que su versión televisiva se retransmite a través de su página web,[17] que también aloja decenas de artículos y extractos de sus vídeos. La lista de teorías de la conspiración desplegada por Jones en estos años en su estudio en la ciudad texana de Austin es interminable, desde que el matrimonio gay es una conspiración global «para estimular la ruptura de la familia y deshacerse de Dios» hasta que la actuación de Lady Gaga en la Superbowl fue un ritual satánico,[18] que George Soros está detrás de un supuesto incremento de la potencia de la marihuana, que los Navy SEAL estuvieron detrás de los atentados de Boston de 2013, o que el Gobierno controla el clima.[19]

Empotradas aquí y allá entre esas piezas de contenido, se venden suplementos vitamínicos, complementos de supervivencia o *merchandising* del programa. Su modelo de negocio se basa en el de los televangelistas estadounidenses:[20] un contenido dinámico, entretenido y altamente emocional, en el que se anima a los espectadores a donar dinero o contribuir a la causa común; en este caso, la «lucha por la verdad». Junto a las ventas en su página, Jones organiza «bombas de dinero», telemaratones como los que se llevan a cabo para recaudar fondos para ONG o víctimas de desastres

naturales, pese a que *Infowars* no entra en esas categorías. Según extrabajadores de la plataforma, en estos telemaratones Jones puede recaudar unos 100.000 dólares en un día.[21]

«Los suplementos son populares. Son buenos. Son un mercado en rápido crecimiento. Los uso para financiar la operación. Otros revolucionarios roban bancos y secuestran a gente, ¿ok? Yo no hago eso», se justificaba Jones en una entrevista con *The New York Times* en 2018. No existen datos económicos sólidos sobre su negocio en la actualidad, pero, según documentos que tuvo que presentar durante el juicio por su divorcio en 2014, su patrimonio superaba los cinco millones de dólares. Ante el tribunal, declaró que sus negocios generaban ingresos brutos superiores a los veinte millones anuales.[22] Dos tercios provienen de las ventas en la web de *InfoWars*.

¿Se cree Alex Jones lo que dice? No está claro. En un perfil que le hizo la revista *Rolling Stone* en 2011 se le definía como «el hombre más paranoico de América». Y es cierto que algunas de sus teorías le han causado perjuicios: insistir en que los atentados del 11-S fueron obra de la Administración Bush llevó a más de 70 radios afiliadas a cancelar su programa. Pero también hay evidencias de que Jones no ha dudado en difundir bulos de cuya falsedad era consciente por razones económicas. En 2011, tras el accidente nuclear de Fukushima en Japón, *Infowars* aseguró que la radiación había llegado a las costas de California. El programa envió a dos reporteros a tomar mediciones con un contador Geiger y retransmitir los resultados en directo, pero solo encontraron niveles de radiación normales. De repente, se les ordenó parar, y se les hizo saber que Jones estaba furioso con ellos: sus vídeos estaban afectando a las ventas de complementos de yodo que *Infowars* vendía en la web a modo de protección.[23]

El 14 de diciembre de 2012, a las 09:30 de la mañana, un joven de veinte años con problemas mentales llamado Adam Lanza asesinó a su madre de cuatro disparos en la cabeza en la localidad de Newton, en Connecticut. Inmediatamente después, condujo hasta la escuela primaria de Sandy Hook, situada a apenas unos minutos de allí, y

disparó una ráfaga de ocho tiros contra una de las aulas desde el exterior con un rifle Bushmaster, capaz de lanzar 45 balas por minuto. Luego penetró en el edificio y ametralló a profesores y niños que trataban de buscar protección dentro de varias clases, matando a veinte niños de seis y siete años de edad, y a seis adultos, e hiriendo a otros dos menores. Al terminar, Lanza se suicidó de un disparo. En total, la masacre duró menos de un cuarto de hora. Fue el segundo tiroteo en un centro educativo más mortífero de la historia del país, solo por detrás de la matanza del campus de Virginia Tech en 2007.

Menos de tres horas después, Alex Jones ya estaba hablando en *Infowars* sobre estos hechos, recordando a la audiencia que Connecticut es uno de los estados más restrictivos con las armas de fuego y que todo apuntaba a que el incidente había sido orquestado para imponer aún más limitaciones a nivel gubernamental. Sobre un letrero donde se leía «Parece una falsa bandera», Jones aseguró: «Ya avisé de que vendrían a por nuestras armas, y por arte de magia, está sucediendo. Ya vienen. Ya vienen. Ya vienen».

La histeria de Jones acerca de este episodio no haría otra cosa que crecer en los siguientes días. Cuando Robbie Parker, el padre de una de las niñas asesinadas, dio una rueda de prensa, hizo un extraño gesto ante las cámaras que Jones explotaría durante años para acusarle de ser un actor. Como resultado, la página de Facebook en memoria de la niña, Emilie Parker, se llenó de comentarios de odio, amenazas y burlas.

Poco después Veronique Pozner, la madre de Noah, otro de los niños asesinados, fue entrevistada por el periodista Anderson Cooper de CNN desde el Memorial de Sandy Hook instalado en homenaje a los fallecidos. Jones utilizó una anomalía digital en un vídeo de la entrevista para asegurar que la entrevista era falsa, acusando a Cooper de haberla realizado en estudio con un fondo verde alterado digitalmente para que pareciese el Memorial, y a Pozner, de ser una actriz. Años después se demostraría ante un tribunal que dicha

anomalía no existía en el vídeo original de la entrevista, sino que había sido creada artificialmente por el equipo de edición de *Infowars*.

Las consecuencias de estos ataques fueron devastadoras para las familias. En internet brotaron decenas de páginas sobre «la farsa de Sandy Hook» y eslóganes similares. Durante años, los padres de las víctimas recibieron todo tipo de insultos y amenazas, tanto en línea como de boca de individuos que les reconocían por la calle y les acusaban de haber ganado mucho dinero con el incidente, o de no haber perdido ningún hijo. Tuvieron que lidiar con personas que se presentaban en sus viviendas y les exigían ver a los niños, totalmente convencidas de que seguían vivos. Hasta que, en un momento dado, decidieron que aquello había ido demasiado lejos. Sus abogados iniciaron dos procesos judiciales contra Jones, en Texas y Connecticut, que revelaron datos sorprendentes, como que en 2021 un 24% de los estadounidenses —alrededor de 75 millones de personas, casi una cuarta parte de la población— estaban convencidos de que la matanza de Sandy Hook había sido un montaje.

Jones se ofreció a pagar compensaciones de 120.000 dólares a cada uno de los trece demandantes, que rechazaron la oferta.[24] El comportamiento de Jones durante los juicios fue irreverente y despreciativo, algo que sin duda influyó en el veredicto final: en total, Jones fue condenado a pagar compensaciones a los padres de las víctimas por más de mil millones de dólares, la mayor sentencia por difamación en la historia estadounidense. Sin embargo, el empresario declaró a *Infowars* en bancarrota y realizó una serie de maniobras económicas para presentarse como insolvente, mientras seguía pidiendo dinero a sus seguidores para financiar sus costes legales. Las víctimas no recibieron el dinero nunca, al tiempo que la página seguía retransmitiendo el programa *El show de Alex Jones*.[25] En el momento de escribir estas líneas, el asunto sigue en los tribunales.[26]

Jones aparece mencionado en el texto de Cassam, quien apunta que, aunque podría asumirse que tanto productores como consumidores de las teorías de la conspiración se las creen, no es

necesariamente así. «Merece la pena tener en cuenta que son un gran negocio», dice, apuntando a lo que otro experto ha denominado «empresarios de la conspiración». Pero además, apunta Cassam, existen consumidores que no se las creen pero interactúan con ellas, las discuten y difunden. Son los «agnósticos de las teorías de la conspiración».

EL CRIMEN DE ALCÀSSER

Hay pocas dudas de que las teorías de la conspiración acaban por alterar la forma en la que se percibe el mundo. Veamos, por ejemplo, el caso de la teoría conspirativa más famosa de España: el crimen de Alcàsser. El asesinato de tres adolescentes en esta localidad valenciana en 1997, con sus escabrosos detalles —las menores fueron llevadas a un caserón en el campo, donde fueron violadas y brutalmente torturadas— fue resuelto rápidamente, pero la chapucera redada policial posterior, que permitió la huida y permanente desaparición del sospechoso principal, Antonio Anglés, levantó la sospecha de que había recibido ayuda de las autoridades. Esto, sumado a la posibilidad real de que en el crimen hubiese participado alguna persona más no identificada, llevó a algunos a especular que detrás del crimen había una red organizada de políticos y famosos que abusaba de niños y después los asesinaba, y que todo era filmado para alimentar un mercado de películas *snuff*.

Sorprendentemente, uno de los que alimentó esta teoría fue Fernando García, el padre de Míriam, una de las chicas asesinadas. Ya fuese por razones emocionales, por afán de notoriedad, por dinero o por una mezcla de todo, García se dedicó a pasearse por platós de programas sensacionalistas durante varios años junto al criminólogo Juan Ignacio Blanco, explicando que en realidad Anglés y el otro detenido, Miguel Ricart, no eran sino chivos expiatorios de una trastienda criminal mayor.[27]

La mayoría de los puntos oscuros de este episodio ya han sido aclarados, pero la teoría de la conspiración sobre Alcàsser persiste. Cuando el 15 de septiembre de 2019, el programa *Cuarto Milenio* emitió un programa especial sobre el caso, hizo una encuesta entre el público. Solo el 10% decía creer en la versión oficial, mientras que el 90% afirmaba creer en una «versión alternativa», sin especificar. Pese al sesgo que se le puede atribuir a los espectadores de un programa de este tipo, los resultados son significativos.[28]

QANON, COMO UNA SECTA

Al menos las teorías sobre el crimen de Alcàsser, que sepamos, no han llevado a discusiones en las que se hayan roto familias ni han inducido a acciones violentas, como sí ha ocurrido con otras que han resultado mucho más peligrosas. Es lo que sucede cuando un movimiento entero se estructura alrededor de unas creencias conspirativas pensadas para seducir a franjas enteras de la población, diseñadas según los parámetros de una secta. Estamos hablando, por supuesto, de QAnon.

El 28 de octubre de 2017, un mensaje apareció en un hilo del panel de discusión 4chan: «Extradición de HRC [Hillary Rodham Clinton] ya en marcha efectiva ayer con varios países en caso de huida cruzando la frontera. Pasaporte aprobado para ser marcado efectivo 10/30 @ 12:01am. Se espera que ocurran disturbios masivos organizados en respuesta y otros huyendo de Estados Unidos. Los M's [presumiblemente, los militares] llevarán a cabo la operación mientras se activa NG [la Guardia Nacional]. Prueba: localiza a un miembro NG y pregunta si en servicio activo 10/30 en la mayoría de las grandes ciudades». El mensaje estaba firmado solamente como Q.

Ese mismo día, el mismo usuario posteó varios mensajes más, que hablaban de «HRC detenida, todavía sin cargos» y de que «POTUS [el presidente de Estados Unidos] debe aislarse para prevenir imagen negativa». Lanzaba además preguntas como «¿Por qué Potus se rodea de generales?» o «¿Por qué George Soros donó todo su dinero

recientemente?». También incluía elementos sin un significado obvio, como la palabra *mockingbird* (ruiseñor) o la frase «¿Dónde está Huma? Seguid a Huma».[29]

Los mensajes se convirtieron en una sensación en Internet. La Q fue interpretada como una referencia a una credencial de seguridad nivel Q, de un nivel tan alto que permite el acceso a información de máximo secreto sobre armamento nuclear. Q sería un alto cargo del Gobierno cercano al presidente Donald Trump, con información privilegiada. Alguien recordó que, pocos días antes, Trump había hecho un comentario oblicuo durante una comparecencia pública con varios oficiales militares y sus familiares, en la que había dicho: «Quizá sea la calma antes de la tormenta», mientras hacía un extraño círculo con la mano que podía asemejarse a una letra Q. Al ser preguntado por un reportero sobre a qué tormenta se refería, Trump respondió: «Ya lo veréis». El vídeo fue suficiente evidencia para muchos, que empezaron a creer fervientemente en las profecías de Q, quien predecía una jornada de arrestos masivos de traidores («la Tormenta») y una purga en el Gobierno, las instituciones e incluso en Hollywood.

Los entresijos del movimiento QAnon merecen su propio libro.[30] Pero lo que aquí nos interesa es que, de repente, millones de personas —no solo en Estados Unidos, sino en todo el mundo— empezaron a creer en sus «revelaciones», inaugurando un culto cuasirreligioso.

Las entregas de Q eran a menudo frases o preguntas crípticas, sujetas a interpretación. Envió 4.958 mensajes entre ese día de octubre de 2017 y junio de 2022.[31] En ocasiones lanzaba diez al día, mientras que podía dejar pasar semana y media sin colgar nada. Sus seguidores las esperaban con impaciencia, discutían su significado en foros, investigaban tratando de atar cabos. Surgieron fenómenos como los *Qtubers*, comunicadores que colgaban vídeos en YouTube interpretando los mensajes de Q, y que en varios casos llegaron a vivir de ello (y bastante bien). Muchas de las frases de Q se convirtieron en eslóganes del movimiento, impresas en camisetas y gorras: «Confía en

el plan», «Donde va uno, vamos todos (WWG1WGA)», «Octubre Rojo», «Esto no es un juego», «El Padrino III», «Alicia y el País de las Maravillas», «El futuro prueba el pasado», «El Gran Despertar», «Pánico en D. C.», «De la oscuridad a la luz»…

La comunidad crecía día a día, integrando otras teorías de la conspiración dentro de una explicación global de cuanto iba sucediendo. Una de estas ideas era el «Pizzagate», que propugnaba la existencia de élites —casi siempre integradas por altos cargos del Partido Demócrata o figuras liberales— que abusaban sexualmente de menores, y en cuyas comunicaciones los términos «pizza», «queso», «*hot dog*» o «pasta» eran palabras clave relacionadas con pedofilia y pornografía infantil, utilizadas para hacer pedidos a las mafias que les suministraban a las víctimas.

Esta idea marginal no explotó hasta 2016, cuando hackers rusos filtraron los correos electrónicos de John Podesta y muchos usuarios encontraron referencias a pedidos de pizzas y otros tipos de comida. Algunos hacían referencia a un popular restaurante cercano a la Casa Blanca llamado Ping Pong Comet, lo que acabaría provocando un incidente violento cuando un hombre llamado Edgar Maddison Welch se presentó armado dispuesto a liberar a los niños supuestamente encerrados en el sótano, lo que, por supuesto, era falso. El indecente, por fortuna, se saldó sin heridos y con Welch sentenciado a cuatro años de cárcel. Los conspiranoicos tuvieron que enfrentarse al hecho irrefutable de que en el Ping Pong Comet no se traficaba con niños —de hecho, ni siquiera tenía sótano—, pero la teoría del «Pizzagate» no murió: sus partidarios simplemente concluyeron que esos hechos atroces se producían en otro sitio. La aparición de QAnon un año después vaticinaba una acción justiciera y despiadada, liderada por el presidente Trump, contra estas redes de pedófilos globalistas.

La creencia en QAnon se convirtió en un fenómeno destructivo, que dividió a familias enteras:[32] miles de personas vieron con alarma e impotencia cómo sus parientes iban cayendo en la espiral de un movimiento interactivo que, en muchos sentidos, estaba diseñado

como un juego,[33] y que cubría muchas de las necesidades de sus integrantes, desde el mero entretenimiento con el que llenar las horas vacías hasta el deseo de justicia. Visto desde fuera, el credo era totalmente absurdo, pero para muchos de sus seguidores se convirtió en algo importante, incluso en parte de su identidad.

El movimiento QAnon se extendió fuera y llegó a cobrar especial fuerza en países como Reino Unido o Alemania. También llegó a España. Yo mismo me uní a varios de sus canales en Telegram bajo una identidad falsa —bastaba con escribir «QAnon» y «España» en el buscador de la plataforma y ella misma te los sugería—, y los seguí durante algunas semanas. «Gracias por ayudarme a ver la Luz», decía una usuaria a finales de 2020. «Trump está luchando por todos nosotros y al final saldrá victorioso. Palabra de Q», se leía en otro mensaje. El fraude electoral supuestamente cometido por los demócratas se mezclaba con acusaciones improbables acerca de George Soros, los Clinton, Bill Gates, Joe Biden, artículos de prensa auténticos sobre eventos reales a los que se daba una interpretación bajo el prisma de QAnon, y bastantes memes. Muchos comentarios atacaban a los periodistas que hablaban del movimiento «sin entender nada», o directamente eran acusados de ser parte de la conspiración global. En aquel momento, el canal más importante tenía 6.000 seguidores.

El caso de QAnon muestra cómo las teorías de la conspiración pueden sustituir un sistema de creencias y forjar identidades completamente nuevas. Pero también pueden producir otro efecto: un estado mental que he denominado «solipsismo político», la noción de que no se puede creer en ninguna institución, medio de comunicación e incluso información que no podamos certificar mediante nuestros propios sentidos. Ese nivel de desconfianza es tremendamente destructivo para la cohesión social. Y, por eso, quienes buscan erosionar los cimientos de nuestros sistemas sociopolíticos son promotores activos de estas teorías.

En 2018, el diario ruso *Vedomosti* y la empresa Medialogia realizaron un estudio sobre teorías de la conspiración en Rusia: analizaron 43.000 contenidos periodísticos de televisión, radio y medios impresos y digitales desde el año 2011. Los resultados mostraban que este tipo de narrativas se había multiplicado entre seis y nueve veces, dependiendo del momento. Muchas de las teorías más prominentes son las mismas que en gran parte del planeta: un gobierno secreto dirige el mundo; el virus del VIH es un cuento, igual que la llegada del hombre a la Luna; las vacunas son peligrosas; los reptilianos están entre nosotros; la tierra es plana; los masones controlan el planeta.

Pero otras son específicamente rusas: la existencia de un *lobby* gay cuyo objetivo es destruir los cimientos morales de Rusia. O, rizando el rizo, una red de historiadores conspiran de forma coordinada contra Rusia para falsificar el pasado del país. El estudio mostraba que esta teoría era la más popular y repetida, hasta cuatro veces más que la siguiente: había sido mencionada 15.730 veces en ese bloque de contenidos.[34]

Si a alguien no le sorprendería es a Ilya Yablokov, un profesor de periodismo digital y desinformación en la Universidad de Sheffield, en el Reino Unido, que ha convertido el análisis de la difusión de las teorías de la conspiración en la Rusia postsoviética en su principal campo de estudio.[35] Según Yablokov, la mentalidad conspirativa es una herramienta clave para el régimen de Putin: «Las teorías son una de las pocas maneras de mantener a la sociedad unida y prevenir un cambio de régimen», declaró en una entrevista en 2024.[36]

La promoción de este tipo de mentalidad permite convencer con mayor facilidad al público de los mensajes que el gobierno necesita propagar rápidamente en momentos de crisis. Por ejemplo, tras la muerte del líder opositor Alexei Navalny en una colonia penal de Siberia en febrero de 2024, los medios difundieron la idea de que

probablemente había sido «asesinado por sus amos occidentales, para dar una mala imagen de Putin».

La repetición estratégica y constante de ideas va dando forma a una cosmovisión bipolar en la que las autoridades rusas trabajan para el bien del país, el resto del mundo —especialmente, Occidente— conspira constantemente contra Rusia, y los ciudadanos rusos son divididos entre «patriotas» (si apoyan a Putin) y «traidores» (cualquier tipo de oposición). Aunque uno sea escéptico hacia las bondades del Kremlin, resulta muy difícil resistirse a ese marco mental, como se ha comprobado tras la invasión de Ucrania.[37]

Por esos mismos motivos, Rusia no se limita a difundir los mensajes entre su población, sino que los promueve activamente en todo el mundo.[38] Por un lado, siembra la desconfianza hacia las instituciones internacionales, contribuyendo al objetivo estratégico de erosionar las democracias occidentales y reducir así la amenaza que representan. Por otro, forja unos parámetros cognitivos en las audiencias que facilitan determinados mensajes clave, por inverosímiles que sean. Se logra, por ejemplo, que grandes grupos en todo el mundo consideren más verosímil la rocambolesca idea de que grupos de rebeldes sirios hayan utilizado armas químicas contra su propia población en ataques de falsa bandera —para forzar una respuesta militar occidental— que la infinitamente más simple idea de que el responsable de dichos ataques sea un régimen conocido por su crueldad y desdén hacia sus enemigos, que posee ese armamento químico, y que ya lo ha utilizado en lugares donde la insurgencia se había atrincherado sin que la artillería convencional pudiese hacer nada.[39]

No es de extrañar que un movimiento tan corrosivo como QAnon haya sido objeto de interés de Rusia. Según un estudio interno de X/Twitter realizado en 2020, cuentas asociadas con el ecosistema de desinformación ruso empezaron a promover contenidos de QAnon ya en noviembre de 2017, menos de un mes después de las primeras

entregas de Q,[40] lo que podría haber contribuido a su difusión y crecimiento iniciales.

En 2019, investigadores sobre desinformación ya habían alertado de que cuentas asociadas a la IRA de Prigozhin estaban moviendo un elevado número de tuits con los *hashtags* #QAnon y #WWG1WGA. Al año siguiente, meses antes de las elecciones de 2020, RT y Sputnik incrementaron sus contenidos acerca de QAnon,[41] no tanto para difundir sus ideas como para subrayar la narrativa del colapso estadounidense o la posibilidad inminente de una guerra civil.

Otros países también estaban activos en ese sentido. La consultoría de inteligencia privada The Soufan Group realizó su propio análisis de datos de redes y concluyó que, en 2020, el 44% de los contenidos sobre QAnon en Facebook de origen extranjero habían sido creados por administradores en Rusia, el 42% en China, el 13% en Irán y el 1% en Arabia Saudí. Al principio, la contribución china había sido relativamente menor, pero, a raíz del incremento de las tensiones entre China y Estados Unidos por la expansión de la pandemia del COVID-19, China aumentó las publicaciones de este tipo. En septiembre de 2020 ya había sobrepasado a Rusia como el origen principal de mensajes sobre QAnon creados fuera de Estados Unidos. En 2021, generaba el 58% de dichos contenidos, más del doble que los creados en Rusia.[42]

EL TESTIMONIO DE UN NAZI

Michael German, un agente del FBI que pasó muchos años infiltrado en movimientos supremacistas blancos en Estados Unidos, explica en su libro de 2007 *Thinking Like a Terrorist* («Pensando como un terrorista») que muchas de las teorías de la conspiración sobre poderes en la sombra, como los Illuminati, los protocolos de los sabios de Sión, los relatos misteriosos sobre el club Bilderberg y la Comisión Trilateral, o las menciones al Gobierno de Ocupación Sionista (o ZOG, por sus siglas en inglés), ya estaban presentes en el mundillo

neonazi a finales de los años ochenta y noventa.[43] Hoy, un número sorprendente de estas ideas siguen presentes en muchos ámbitos, aunque el componente antisemita es menos marcado.

Las teorías de la conspiración son esenciales para el extremismo. Es imposible, al menos en un contexto de paz, que alguien pueda hacer suya una causa de odio si no está convencido de algunas ideas más o menos improbables, como que existe una causa superior que justifica sus acciones, que su cultura está en peligro por algún tipo de complot, o que sus adversarios u otra comunidad son menos humanos que los miembros de su grupo. Por eso es importante estudiar el vínculo entre estas teorías y los procesos de radicalización, para entender esa forma de razonar.

«Una de las preguntas que más me hacían a mí al principio, y que yo creo que los periodistas que me lo preguntaban no se creían mi respuesta, era si los ideólogos dentro de este mundillo, los que hacían más conferencias y daban más charlas, como Pedro Varela [la figura nacionalsocialista más conocida de España] y toda esta gente, si de verdad creían en lo que decían o utilizaban el discurso como una herramienta con la que engañar a la gente, aprovecharse de los chavales», dice David Saavedra, un antiguo militante nacionalsocialista que rompió con sus antiguos camaradas. La ruptura le supuso un importante coste personal y emocional, en un proceso que todavía seguía en marcha cuando le entrevisté en marzo de 2025, poco antes de que este libro fuese a imprenta.

«Yo creo que la amplia mayoría de los periodistas compran la segunda opción, pero es que no es así. No es cierto. Al menos yo, todos los que me encontré, el cien por cien, e incluso yo mismo, puedo decir que creemos ciegamente en lo que decimos. Y de hecho, en todo ese constructo, ese sentido común ajeno al que tiene la gente que no está radicalizada, los buenos somos nosotros. Nosotros somos los que estamos luchando contra un mal oculto que desde las sombras intenta cumplir una serie de agendas y de objetivos».

Durante dos décadas, Saavedra fue una de las figuras más destacadas del movimiento nacionalsocialista español. Quizá su nombre no fuera conocido para el público, pero casi todos dentro del mundillo sabían quién era. Ayudó a montar publicaciones, a crear grupúsculos activistas, a apuntalar por dentro el partido Alianza Nacional. Hasta que, de repente, algunas grietas en su forma de razonar hicieron que todo el castillo ideológico sobre el que había construido su vida adulta se viniese abajo.

No ocurrió de la noche a la mañana, sino que fue algo gradual, una mezcla de circunstancias. Sus problemas personales. Su trabajo en el ejército: el contacto con individuos de otras razas y nacionalidades y, sobre todo, con personas fuera de su burbuja ideológica que le ayudaron a ver más allá. Y, finalmente, encontrarse formando parte de un grupo paramilitar que se estaba preparando para ir un paso más allá y recurrir a la acción violenta. Todo le convenció de echarse a un lado. Un camino personal que detalla en el libro *Memorias de un exnazi*, publicado en 2021.[44]

El caso de Saavedra es doblemente interesante, porque es una persona muy reflexiva que ha dedicado mucho tiempo a pensar sobre su experiencia y sus procesos mentales, tanto al filtro que condiciona todos los pensamientos de un miembro de un grupo extremista, como al «desradicalizarse». «El discurso, la ideología, es como una sábana. Y lo que yo llamo "pensamiento burbuja" es todo ese molde psicológico, especialmente emocional, que queda cuando eliminas lo que es político o ideológico. Le pongas la sábana que le pongas por encima, lo va a radicalizar, va a ir a la visión extremista. Un radical, aunque diga que ya no es radical, lo sigue siendo. Es un poco como los alcohólicos, que, aunque lleven veinte años sin beber, siguen diciendo que son alcohólicos. De hecho, yo sé, a día de hoy, que me arrime a la ideología que me arrime, aunque sea la de los derechos humanos, mi mente va a radicalizar ese discurso. Y tú dirás: "¿Cómo vas a radicalizar los derechos humanos?". Pues llamando nazi a cualquiera

que no defienda los derechos humanos como los defiendo yo», me confió.

David da charlas en institutos y centros educativos, buscando ayudar a adolescentes que puedan encontrarse en vías de radicalización. No necesariamente hacia la extrema derecha, porque el proceso, insiste Saavedra, es el mismo para un yihadista o para un miembro de una banda latina, por poner dos ejemplos. Con empatía y orientación, puede reorientar esa inquietud hacia un camino más constructivo. Saavedra también tiene un canal de YouTube en el que expresa sus ideas sobre estas cuestiones.[45] «Yo ahora estoy en generar herramientas que permitan detectar este pensamiento en burbujas mucho antes de que aparezca la ideología, que es cuando es posible volver a canalizar esa forma de pensar. Una vez ya surge la ideología, o el discurso, o la religión, es como que se cierra un candado. La ideología es lo que le da forma a eso que tú ya tienes dentro de tu cabeza, cómo atas tú las piezas, cómo organizas tu visión del mundo, de ti mismo. Pero todo empieza mucho antes. La gente se alarma cuando los chavales en el instituto dicen "Heil Hitler", pero las alarmas saltaron antes: cuando son de blanco o negro, cuando surge la soberbia, cuando desaparece la curiosidad y llega ese "yo ya lo sé todo". Ese tipo de comportamientos son los peligrosos».

A su juicio, «el conspiracionismo se enfoca siempre desde el narcisismo, y verdaderamente fomenta que te conviertas en un narcisista por ese rollo de tener siempre la razón, del ego, del qué tontos son los demás. Entiendo que se haga esa lectura, pero hay que estar abierto a que pueda haber algo más. Y ese algo más es el miedo, es la inseguridad. Muy poca gente está dándose cuenta de cómo todo este auge de la extrema derecha empezó en la pandemia. Es que está clarísimo. La pandemia fue una ventana de radicalización brutal por la inseguridad que produjo en las personas, por el miedo por el qué va a pasar ahora. Yo me acuerdo de la tranquilidad que me generaba ir por la calle y ver simplemente en una ventana un "Todo va a salir bien" con un arcoíris que había hecho un niño pequeño, la gente

aplaudiendo en los balcones. Ahora decimos: "¡Buah, qué tontería!". Pues tenía un valor simbólico muy grande porque te daba ánimos y te ayudaba a ser positivo. Pero es que hubo gente que en esa época entró en una espiral hacia abajo y no ha salido de ahí, que sigue ahí metida».

A Saavedra le condujo al nacionalsocialismo «la curiosidad»: a los catorce años, un día, al pasar por delante del televisor, su padre estaba viendo un documental sobre Hitler. El David adolescente se quedó absolutamente fascinado por las imágenes del mitin de Núremberg. Al preguntar quién era el líder, su padre le respondió: «Un loco». Pero algo no le cuadraba: ¿cómo era posible que un simple loco pudiese movilizar así a las masas? Así fue cómo empezó a interesarse por el nazismo.

«Yo no sé si eres capaz de empatizar con tu yo de catorce o quince años. Yo sí, y me acuerdo cómo me impresionaba todo muchísimo. Y cómo cosas que igual tú decías que para ti eran insignificantes, a mí se me grababan a fuego en la cabeza. De hecho, aún las recuerdo. Entonces, las movidas que recibimos a esas edades, aunque desde la percepción de un adulto no parezcan gran cosa, en estos chicos y chicas pueden ser la diferencia entre el abismo y tener una vida normal. Yo empezaba a sentir cierta atracción [por el nazismo] y a hacer preguntas: "¿y esta gente cómo son, y cómo piensan, y por qué, y por qué, y por qué?". Y lo que me decían era que solo eran gente que quedaba por la noche a emborracharse, y salían en manada a cazar homosexuales y ya está. Eso es todo. Entonces, claro, cuando me encontré por vez primera a nazis de verdad en mi tierra, en Galicia, y era gente normal y corriente, que ni siquiera iba con la cabeza rapada, que eran bastante majos, que sabían mucho, muy leídos... Que sí, que vale, que solo leían libros nazis, pero cuando tienes catorce años no eres capaz de detectar eso, simplemente ves a alguien que tiene un vocabulario muy rico y que sabe mucho de historia, y eso es lo único que ves desde fuera. Si eres historiador, pues te das cuenta inmediatamente y dices: "Cuéntame también la otra parte de la

historia, ¿no?". Pero con catorce o quince años, te choca muchísimo. Ahí es cuando empiezas a establecer que las personas que han sido siempre tu referencia, tus padres, tus profesores, los libros de historia, etcétera, pues igual no son una fuente tan fiable como tú pensabas».

Ahora, ha transformado esa historia adolescente en un estereotipo fácil de entender, con el objetivo de prevenirlo y frenarlo: «Yo explico un proceso de radicalización con solo tres elementos. Está la curiosidad, que termina mutando en el sesgo de confirmación, obviar las cosas que no nos cuadran», y menciona el «efecto Semmelweis», la tendencia de los seres humanos a rechazar todo nuevo conocimiento que contradiga sus creencias ya establecidas. «Lo explico en los colegios con el proceso de enamoramiento. Cuando te enamoras es como que en el momento en que ocurre ese clic, el momento que alguien nos entra por los ojos y cualquier cosa negativa que te digan de esa persona, tu cabeza va a ignorarlo y a decir: "No me interesa esto". El efecto Semmelweis que tuve con el nazismo fue de: "¡Guau, cómo mola esto!". No fue: "¡Guau, qué de acuerdo estoy con esto". Siempre es una emoción. Cuando empecé a investigar, a leer, y me encontraba con referencias al Holocausto, a crímenes, etcétera, mi mente, con lo único con lo que se quedaba era con lo bueno. En los colegios enseño un *collage* de fotos que hice de Hitler dando de comer a ciervos, con perritos, con niños pequeños, fotos de Hitler dándole la mano desde su coche al pueblo, a la gente, a los alemanes, que demuestra que es alguien muy querido. Es como que fui construyendo la imagen de "Hitler bueno". ¿Por qué? Porque coincidía con el "¡Guau, cómo mola esto!". Es así de simple. Luego, a partir de ahí, viene todo lo demás, pero la base es esa».

Posteriormente, entra ya en juego la teoría de la conspiración: «Luego viene el ego, cuando dices la frase de "Ahora lo entiendo todo". La conspiración lo bueno que tiene es que no deja cabos sueltos. Todo encaja a la perfección. Si tú hablas con alguien muy leído, algún científico por ejemplo, ves que con el conocimiento son supercautos y siempre te dicen la frase de "cuanto más leo, más me

doy cuenta de lo ignorante que soy". Un radical es al revés. Un radical, cuanto más lo es, más listo se cree, y por ende, como ve el mundo en blanco y negro, más tontos son los demás, evidentemente. Cuanto más sube él, más baja el resto. Esto, además, es algo que nunca para: siempre eres cada vez más listo y los demás son cada vez más idiotas. Por eso hablamos con desprecio cuando hablamos con la gente que no es como nosotros, como si estuviéramos hablando con niños de cinco años. Y ya, a partir de ahí, es simplemente relacionarte solo con gente que piensa como tú, la cámara de eco, el aislarte cada vez más. Y ya está. Luego ya entra el discurso, el de aquello por lo que luchamos, pero eso es ya en última instancia».

Cuando una persona llega a ese punto, la burbuja condiciona toda su forma de razonar, el modo en el que se procesa la información nueva, adaptándola a ese armazón mental inflexible. Si la realidad no encaja, se adapta la propia realidad, no la forma de verla.

9

DE LAS REDES A LAS CALLES

«¡Quitaos de en medio! ¡Somos el pueblo!». Un hombre grita a escasos centímetros de la cara de los policías. Detrás, una masa enfervorizada de gente avanza, tumbando las vallas de protección y cercando el edificio. Los agentes retroceden sin dar la espalda a los manifestantes, cada vez más arrinconados. «¡Sois unos traidores!», les increpa la masa, que sube las escaleras del Capitolio sin que nada pueda pararla. Algunos trepan por los andamios hasta una de las terrazas superiores. Otros han roto una de las puertas de acceso y penetran en las instalaciones del Congreso. Grupos de personas de ambos sexos recorren los pasillos buscando a los congresistas, que en esos momentos están siendo evacuados por el personal de seguridad. La persona más buscada —y más odiada— es la presidenta de la Cámara de Representantes, Nancy Pelosi. Un hombre canturrea: «¡Nancy! ¡Ya estoy en caaaaasa!», imitando al personaje de Jack Nicholson en la película *El resplandor*. Rompen mobiliario, encuentran documentos abandonados a toda prisa por los políticos, se hacen selfis en sus escaños o subidos a los podios de los oradores.[1]

Son imágenes del asalto al Capitolio de Washington el 6 de enero de 2021, que dejaron al mundo estupefacto. Horas antes, más de 120.000 personas se habían reunido en el National Mall,[2] uno de los principales parques de Washington D. C., en una atmósfera festiva pero también amenazante. Alguien —nunca se ha sabido quién— había construido un falso patíbulo junto a la estatua del general Ulysses S. Grant.[3] Había un ambiente de expectación, que muchos equiparaban con «la Tormenta» que había predicho QAnon. Sobre el podio, Donald Trump animaba sutilmente a la multitud: «¡Nunca os

rindáis! ¡Nunca admitáis una derrota!».[4] En un momento dado, añadió: «Después de esto, vamos a marchar, y yo estaré allí con vosotros».

Antes incluso de que Trump terminase de hablar, unas ocho mil personas se desligaron de la muchedumbre y se dirigieron hacia la sede del Congreso, donde los representantes del Colegio Electoral debían presentar sus votos, que certificarían la victoria electoral de Joe Biden, algo que en circunstancias normales hubiera sido poco más que un trámite burocrático, un ritual necesario pero sin consecuencias. No en esta ocasión.

Al terminar la jornada habían muerto dos manifestantes. Ashli Babbit, una veterana de la Fuerza Aérea de treinta y cinco años y ferviente creyente en QAnon, recibió un disparo de un policía de la unidad de protección del Capitolio que resultó fatal. Rosanne Boyland, de treinta y cuatro años, murió de una sobredosis de anfetaminas. Aparte, el oficial Brian Sicknick, de cuarenta y dos años de edad, sufrió dos infartos cerebrales tras haber sido rociado con un espray de gas pimienta. Falleció al día siguiente. Cuatro policías más, traumatizados por los hechos, se suicidaron durante los meses que siguieron al asalto. Ciento treinta y ocho agentes resultaron heridos, y quince tuvieron que ser hospitalizados. Hubo 52 detenidos ese día, y las autoridades estadounidenses acabaron presentando cargos criminales contra un total de 1.488 personas.

Este episodio fue la encarnación real de la guerra meme por antonomasia. Muchos de los asaltantes del Capitolio llevaban símbolos que hasta entonces habían pertenecido casi exclusivamente al mundo virtual, como la bandera de Kekistán[5] o imágenes de la Rana Pepe.[6] Algunos parches los identificaban como «veteranos de las guerras meme».[7] Todos estaban convencidos de actuar contra un supuesto golpe de Estado perpetrado por el Partido Demócrata, que habría orquestado un gigantesco fraude electoral. Su lema, *Stop the Steal!* («¡Parad el robo!»).

Trump llevaba meses agitando este fantasma, anticipando una posible derrota en los comicios. Como hemos visto en capítulos anteriores, en sus comentarios públicos hablaba de «máquinas trucadas» y «fraude masivo». Sus abogados habían inundado los estados clave de recursos legales, que no habían prosperado. El mismo Departamento de Justicia de Trump validó la integridad del proceso electoral. El fiscal general de Texas había pedido al Tribunal Supremo —donde había una mayoría de jueces conservadores, gracias a los últimos nombramientos realizados por el presidente saliente— que invalidase los votos de Wisconsin, Georgia, Pensilvania y Míchigan, estados bisagra donde había ganado Joe Biden. Pero la corte rechazó el caso.

Reporteros que habían salido a la búsqueda de pruebas de fraude en seis de dichos estados bisagra habían encontrado 475 casos potenciales, entre un total de 25 millones de votos, una cifra que podía considerarse anecdótica.[8] Pero nada había disuadido a Trump, ni a sus seguidores. A pesar de que las instituciones implicadas en el proceso certificaron por activa y por pasiva unas elecciones totalmente limpias,[9] el mensaje de las irregularidades permeó, afectando a votantes de ambos partidos: según una encuesta de YouGov después de los comicios, un 75% de los estadounidenses creía que se había producido algún tipo de fraude, aunque no se ponían de acuerdo en si había influido en los resultados finales. El 81% de los partidarios de Trump pensaba que sí.[10]

No obstante, algunos participantes en el asalto al Capitolio eran conscientes de que no existió fraude, pero buscaban instrumentalizar la creencia para avanzar sus agendas políticas. Milicias como los Proud Boys, por ejemplo, llevaban semanas preparándose para la toma del emblemático edificio.[11] El plan era intimidar al vicepresidente Mike Pence, y que se negase a certificar los resultados, abriendo la puerta a maniobras que permitirían a Trump mantener el poder. La misma mañana del 6 de enero, Trump tuiteó: «Hay estados que quieren corregir sus votos, que ahora sabemos que estuvieron basados

en irregularidades y fraude. Además, el proceso corrupto nunca recibió la aprobación legislativa. Todo lo que Mike Pence tiene que hacer es enviarlos de vuelta a los Estados, Y ASÍ GANAMOS. ¡Hazlo, Mike, este es un momento para un coraje extremo!».

Pero Pence reiteró, como ya había hecho en los días previos, que no podía rechazar unilateralmente los votos del colegio electoral. Cumplió con su deber constitucional y certificó la victoria de Joe Biden. No obstante, el mito del fraude seguiría persistiendo. Una encuesta de enero de 2024 reveló que más de un tercio de los estadounidenses continuaba pensando que Biden no había sido investido de forma legítima.[12]

Para muchos observadores de las subculturas de la derecha estadounidense en redes, el estallido de 2021 no fue ninguna sorpresa. «Una década de guerras meme ha radicalizado a la gente, y un presidente que comprende el poder de las guerras meme pudo enviar un tuit ("Gran protesta en D. C. el 6 de enero. Estad allí. ¡Va a ser salvaje!") que reclutó a miles en una batalla contra la propia democracia», escriben los autores del libro *Guerras Meme*.[13] «Aunque la insurrección falló, el éxito de la guerra online que llevó a la insurrección queda de manifiesto por el simple hecho de que tuviera lugar el 6 de enero. Las guerras meme tratan de llevar la energía de una comunidad online al mundo real».

CUANDO EL BULO PROVOCA SANGRE (Y FACEBOOK CALLA)

La guerra cognitiva, la desinformación y la manipulación, pueden desembocar en efectos sangrientos en la vida real. El temor no es infundado: en México[14] o la India[15] se han producido linchamientos de personas tras la difusión de rumores sobre la presencia de violadores o asesinos de niños. En países como Kenia,[16] Gambia[17] o Arabia Saudí,[18] las acusaciones de brujería suelen tener consecuencias funestas.

Los bulos difundidos por el presentador de radio norteamericano Alex Jones han sido vinculados con al menos media docena de acciones violentas graves. En 2002, un hombre fuertemente armado entró en el recinto de Bohemian Grove, un campamento en California donde varios líderes políticos y empresariales internacionales realizaban un retiro anual, y provocó un incendio. El individuo estaba convencido de que allí tenían lugar sacrificios humanos y abusos de menores, inspirado directamente por los reportes de Jones. En 2011, un joven de veintidós años con problemas mentales completamente obsesionado con *Loose Change* —una película producida por Jones que apunta que los atentados del 11-S fueron obra de la Administración Bush—, abrió fuego contra una multitud en Tucson, Arizona, matando a seis personas e hiriendo a varias más, incluida una congresista.[19] Las diatribas de Jones contra los familiares de las víctimas de Sandy Hook los convirtieron en objeto de amenazas de muerte y hostigamiento por parte de sus seguidores. Y, como hemos visto en el capítulo anterior, en 2016, un hombre llamado Edgar Maddison Welch, seguidor de *Infowars*, irrumpió armado en la pizzería Comet Ping Pong totalmente convencido de que en su sótano se traficaba con niños, tal y como afirmaba la teoría de la conspiración del «Pizzagate».[20]

En otras ocasiones, estos mensajes de odio han sido promovidos activamente por actores malignos interesados en provocar esta violencia, llegando incluso al genocidio. Veamos algunos ejemplos.

En Myanmar existe una minoría étnica musulmana, los rohinyá, cuya presencia en la región se remonta al siglo xv. La mayoría, sin embargo, se asentó en lo que entonces era conocido como Birmania en los siglos xix y xx, cuando el país estaba bajo el dominio colonial británico. Por este motivo, la mayoría de los birmanos considera a los rohinyá como extranjeros —en los años ochenta incluso se les privó de la ciudadanía—, lo que ha llevado a oleadas cíclicas de violencia contra ellos. En ese discurso de odio destacan figuras como el monje Ashin Wirathu, líder del llamado Movimiento 969, a quien la revista

Time denominó «el rostro budista del terror».[21] Como reacción a la voladura de los Budas de Bamiyán por los talibanes en Afganistán en el año 2001, Wirathu alentó a sus seguidores a destruir mezquitas y atacar a musulmanes. Encarcelado en 2003 por incitar a los disturbios, salió a la calle en 2010 como parte de la apertura democrática que empezaba a experimentar el país, justo a tiempo para lo que estaba por venir.[22]

En mayo de 2012, tres hombres rohinyás violaron y asesinaron a una joven budista en una pequeña localidad del estado de Rakhine, donde los musulmanes eran mayoría y los budistas apenas suponían un 4% de la población. Como respuesta, se desataron pogromos y enfrentamientos entre ambas comunidades, que fueron creciendo en intensidad hasta desembocar en ataques coordinados contra múltiples localidades rohinyá, en los que participaron las fuerzas armadas.[23]

Desde entonces, las agresiones y matanzas contra los rohinyá no han dejado de crecer en intensidad, provocando un éxodo de más de un millón de personas hacia los países vecinos, especialmente Bangladesh. Cuando algunos militantes de esta etnia trataron de organizarse como insurgencia armada,[24] el Tatmadaw —el ejército birmano— reaccionó con asesinatos extrajudiciales en masa, quema de aldeas —a menudo, con sus habitantes dentro— violaciones grupales, y ametrallamientos y acuchillamientos de quienes intentaban escapar.[25]

Mientras esto sucedía, los discursos de odio que preparaban a la población para las masacres proliferaban en internet, especialmente en Facebook. Durante años, el Tatmadaw operó cientos de páginas y grupos, aparentemente sobre temas como entretenimiento, belleza y estilos de vida, desde los que lanzaba mensajes de odio que justificaban las matanzas de los rohinyá. Meta, en parte debido a la falta de recursos y personal que pudiese examinar los contenidos en idioma birmano, permitió que estos discursos proliferasen.[26] En marzo de 2018, la misión de investigación de la ONU señaló directamente el papel de Facebook en el genocidio.[27] Medio año después, la compañía eliminó la red de cuentas del Tatmadaw[28] y lanzó una investigación,

que concluyó que Meta no había «hecho lo suficiente para ayudar a prevenir que [la] plataforma fuese usada para fomentar la división e incitar a la violencia en el mundo real».[29]

En 2022, Amnistía Internacional emitió un informe en el que afirmaba que «los sistemas de Facebook promovieron la violencia contra los rohinyá» y que la empresa debía ofrecer reparaciones a las víctimas. Pero ¿por qué esa insistencia en señalar la responsabilidad de la red social? El autor del informe, el abogado e investigador Patrick de Brún, lo explicaba así en una entrevista con el diario francés *Le Monde*: «Facebook ha desempeñado un papel central en el aumento del clima de odio desde 2012. Para muchas personas en el país, la red social era el único servicio de internet accesible, y Facebook amplificaba enormemente los mensajes violentos. Ciertas personas buscaban deshumanizar a los rohinyá, lo que en consecuencia allanó el camino para la limpieza étnica y las violaciones masivas que siguieron. Al elegir qué publicaciones mostrar en el *feed* de cada usuario, [el algoritmo de Facebook] resalta el contenido que genera muchas reacciones, ya sean positivas o negativas, que es de lo que se trata el contenido que incita al odio. Facebook ha dado a estas publicaciones una audiencia sin precedentes en Myanmar».[30]

Algo similar sucedió en 2018 en Sri Lanka, cuando grupos de extremistas budistas lanzaron pogromos contra centros y negocios musulmanes, provocando otro baño de sangre igualmente acompañado de mensajes masivos de odio en las redes sociales: «Matad a todos los musulmanes, no dejéis escapar ni a una cría de estos perros», o «Golpeadlos tan fuerte como podáis».[31] Los ataques fueron precedidos de historias falsas que acusaban a la minoría musulmana de intoxicar a la población budista con sustancias esterilizantes, o de que un individuo asesinado en una disputa de tráfico había sido, *en realidad*, víctima de un complot musulmán.[32]

Cuando empezaron las agresiones, vídeos de mezquitas ardiendo acompañados de mensajes que incitaban a imitar los incendios empezaron a circular en Facebook, Whatsapp y otras plataformas, lo

que llevó al Gobierno esrilanqués a bloquearlas en todo el país. De nuevo, Meta reaccionó tarde y mal, a pesar de las exigencias del Ejecutivo de Colombo.[33] Cuando bloqueó la página del líder extremista Amit Weerasinghe, ya había reunido 150.000 seguidores en su página de Facebook, a quienes llevaba semanas azuzando contra las comunidades musulmanas, lo que motivó su detención.[34]

Sorprendentemente —o no, dado el modelo de negocio y la falta de rendición de cuentas de Meta—[35], el mismo esquema volvió a repetirse dos años más tarde en Etiopía. Tras el estallido de la guerra civil entre el Gobierno etíope y el Frente de Liberación Popular de Tigray (TPLF), los discursos de odio por ambos bandos incitando a la violencia contra comunidades específicas se dispararon,[36] especialmente entre los etíopes de la diáspora, dado que el porcentaje de conectividad dentro del país es muy bajo. Una vez más, Facebook jugó un papel clave en su difusión.[37] Tras abandonar Meta, la exempleada Frances Haugen hizo pública una gran cantidad de documentos sobre las prácticas ilícitas de la empresa que prueban que «en lugares como Etiopía, [Facebook] está literalmente agitando la violencia étnica».[38] La respuesta de la compañía, una vez más, fue lenta e insuficiente,[39] a remolque de las denuncias de periodistas e investigadores, y más como reacción ante la mala prensa que ante una preocupación genuina por las atrocidades en sí.

Las redes sociales son vehículos perfectos para promover ideas que inciten a la acción violenta. Especialmente si al otro lado, recibiéndolas, hay alguien dispuesto a empuñar las armas.

AMAGOS DE GOLPES DE ESTADO

El 7 de diciembre de 2022, tres mil policías se desplegaron por casi todo el territorio de Alemania con un objetivo: impedir un golpe de Estado. Los agentes registraron más de 130 viviendas y detuvieron a 25 personas, una lista que se ampliaría en los días siguientes. Los detenidos pertenecían al llamado movimiento Reichsbürger, o «los

ciudadanos del Reich», que no reconoce la legitimidad del Estado alemán y que cuenta con varias decenas de miles de seguidores en todo el país.[40]

Esta pequeña facción, de acuerdo con las autoridades alemanas, había decidido convertir sus aspiraciones en realidad. Los presuntos conspiradores llevaban tiempo haciendo prácticas de tiro, habían adquirido teléfonos por satélite por si se producía un bloqueo de las comunicaciones convencionales y habían acumulado grandes sumas de dinero. El grupo contaba con un ala militar, entre cuyos miembros había oficiales del Ejército y de la Policía, incluyendo un soldado en activo de los comandos especiales, o KSK.[41]

El plan, según la Fiscalía alemana, implicaba el asalto armado del Bundestag (el Parlamento alemán), la toma de diputados como rehenes, la disrupción de las redes eléctricas y, finalmente, el derrocamiento del Gobierno. Después pondrían al frente del país a su líder, el aristócrata Heinrich XIII, príncipe Reuss de Greiz y cabecilla de la operación.[42] El fiscal general, Peter Frank, añadía que la organización buscaba «eliminar el orden existente en Alemania usando la violencia y medios militares». Tenían buenas conexiones. Una de las investigadas era la exdiputada de Alternativa para Alemania Birgit Malsack-Winkemann, que habría sido nombrada «ministra de Justicia».

El complot era sorprendentemente similar a otro destapado a finales de 2021 por las autoridades francesas. Una red de unas 300 personas lideradas por Rémy Daillet, una conocida figura del movimiento antivacunas en Francia, planeaba asaltar el Palacio del Elíseo y derrocar al Gobierno en un golpe de mano que denominaban «Operación Azur».[43] Entre los conspiradores había miembros del ejército retirados y en activo —en algunos casos, oficiales—, que habían formado a otros en técnicas paramilitares. Varios habían empezado a fabricar explosivos y a almacenar armas.

La policía también incautó listas de objetivos a atacar, que incluían sedes institucionales, centros de vacunación y torres 5G. Daillet y

otras trece personas fueron imputadas. El plan golpista era simple: convocar una manifestación gigantesca frente al Elíseo y tratar de abrirse paso hasta el interior del recinto. Cuando, inevitablemente, las fuerzas de seguridad recurrieran a la violencia contra los manifestantes, los equipos entrenados por Daillet responderían abriendo fuego y forzando el asalto a la sede del Gobierno francés. El plan fue descubierto de forma fortuita cuando las autoridades investigaban a Daillet y a su grupo por el secuestro forzoso de una niña al cuidado de su abuela, a petición de la madre de la pequeña, a quien se le había retirado la custodia legal.

Lo más inquietante es que ninguno de estos dos episodios eran aislados. ¿Qué estaba pasando?

En enero de 2023, las autoridades alemanas y francesas llevaron a juicio a varios miembros del movimiento Reichsbürger por «fundar una organización terrorista nacional, preparar un acto de alta traición y un acto grave de violencia con peligro para el Estado». Incluía el secuestro del ministro de Salud alemán, Karl Lauterbach, en el primer caso. En el segundo, conspirar para apuñalar al presidente francés, Emmanuel Macron, durante una visita al nordeste del país en 2018.

Lo asombroso es que ni los primeros son miembros de la red de Heinrich XIII ni los segundos de Daillet: se trata de grupúsculos diferentes. He podido encontrar ejemplos similares en Austria, donde otro grupo del llamado movimiento Staatenbund (equivalente al Reichsbürger alemán) había tratado de incitar a miembros del ejército a cometer un golpe de Estado en 2017.[44] Y en Australia, donde en 2021 se detuvo a un hombre de Perth que había fingido ser un agente de policía para tratar de formar un cuerpo paralelo de oficiales con el propósito de «derrocar al Gobierno» y arrestar a parlamentarios «traidores».[45]

En resumen: tenemos, al menos, media docena de ejemplos en los que organizaciones de corte mesiánico y ultraconservador, con un pie fuera de la realidad, conspiran para destruir violentamente el orden constitucional en sus países, que se suman a episodios como el ya

mencionado asalto al Capitolio de Estados Unidos o la toma del Congreso brasileño.

«La extrema derecha grupuscular de nuestros días, con la consolidación de internet y el aumento exponencial de la actividad ultra en redes sociales, ha provocado un solapamiento de perfiles, referencias, modos de acción, etcétera», me explica Arsenio Cuenca, investigador de movimientos ultraderechistas afincado en París. «Los individuos que componen esta nebulosa guardan cierto parecido con la ultraderecha terrorista de antaño. En el caso de Francia, el ejemplo más claro es la OAS».

Cuenca se refiere a la llamada Organización del Ejército Secreto, un grupo terrorista compuesto por militares galos de alto rango, activo durante la guerra de Argelia y la época inmediatamente posterior, que trató repetidamente de asesinar al general Charles de Gaulle por su «traición» al negociar la independencia del territorio norteafricano. «Gran parte de los grupos de extrema derecha desarticulados en Francia a día de hoy están compuestos igualmente por miembros de las fuerzas del orden (Ejército, Gendarmería, Policía...). Al mismo tiempo, otro grupo terrorista ultra desarticulado en 2021, que tenía como objetivo atentar contra musulmanes o el líder de LFI, Jean-Luc Mélenchon, llevaba el mismo nombre».

¿A qué se debe que este tipo de conspiraciones tuviesen lugar tan cercanas en el tiempo unas de otras, en lugares diferentes? El contexto digital ha favorecido un pensamiento conspiranoico, que ha penetrado con fuerza entre quienes se ven a sí mismos como «librepensadores» y «contra las corrientes dominantes de la corrección política», como a menudo sucede en círculos ultraderechistas. No es casual que en países como Alemania se produjera un solapamiento entre las redes antivacunas, los *Querdenker* o negacionistas del COVID-19, el fenómeno QAnon y aquellos que rechazan la autoridad del Estado y sus imposiciones. Y, cuando los movimientos anticiencia se fusionan con aquellos que no solo rechazan la democracia, sino que están

dispuestos a utilizar la violencia para imponer sus ideas, el cóctel resultante es explosivo.

«Mientras las autoridades y los políticos alemanes poseen una comprensión profunda de algunas de las variantes del extremismo de ultraderecha, así como del extremismo islámico, todavía se tiene que salvar la brecha del concepto de terrorismo conspiratorio», señala el analista Thomas O. Falk en un artículo en la revista *Foreign Policy.*[46] Ya se están dando pasos en ese sentido: en 2019, el FBI consideró por primera vez las teorías de la conspiración como amenazas terroristas domésticas potenciales. Especialmente, QAnon.[47]

El crecimiento de la amenaza es meteórico. En 2018, la Oficina Federal para la Protección de la Constitución cifraba el número de miembros del movimiento Reichsbürger —que no deja de ser un término paraguas para individuos que no reconocen la legitimidad del moderno estado alemán— en 15.600. En 2023, eran 23.000, de los cuales, según estimaban los servicios de inteligencia alemanes, 2.100 estaban dispuestos a utilizar la violencia. Este movimiento estaba considerado como inofensivo —se negaban a pagar impuestos y emitir sus propios pasaportes—, hasta que en 2016 un militante se resistió a un arresto y disparó contra la policía, matando a un agente e hiriendo a cuatro.

«Las detenciones en Alemania arrojaron luz sobre el creciente movimiento antidemocrático en el país, ejemplificado en el momento en el que manifestantes motivados por el escepticismo hacia el COVID-19, por conspiraciones y por un sentimiento antigubernamental asaltaron el Reichstag. Aunque fueron rápidamente repelidos, el simbolismo no pasó desapercibido para aquellos que entienden la historia de los movimientos antidemocráticos», señala un informe de 2022 de la consultora de inteligencia privada The Soufan Group, especializada en terrorismo y extremismo violento.[48] El «aceleracionismo» es una corriente política que busca generar caos para acelerar el colapso del sistema actual y permitir el nacimiento de

uno nuevo, una corriente que tiene presencia tanto en la extrema izquierda y el ecologismo radical como en la extrema derecha.[49]

Algo similar sucede en Francia, en un contexto si cabe más inestable. «Existe una importante voluntad contestataria que puede derivar en una violencia alienante. Lo vimos con el movimiento de los Chalecos Amarillos[50] o con las agresiones que ha sufrido el presidente Emmanuel Macron», indica Cuenca. «Del mismo modo, en Francia hay un problema de aprovisionamiento de armas, así como un número mucho más reducido de extremistas violentos dispuestos a pasar a la acción, en comparación con otros países europeos como Alemania».

Estados Unidos, debido a la facilidad de acceso a las armas y al enorme número de milicias organizadas, es el país donde los expertos consideran más probable un estallido violento. En 2020, el FBI consiguió abortar los planes de un grupo de milicianos que se preparaban para secuestrar y asesinar a la gobernadora del estado de Míchigan, Gretchen Whitmer, por las restricciones impuestas en espacios públicos durante la pandemia del coronavirus.[51] El lema del grupo era: «¡Liberen Míchigan!».

España tampoco está exenta de este tipo de riesgos, como muestra el caso de Manuel Murillo, el vigilante de seguridad que en 2018 fantaseó con matar al presidente Pedro Sánchez con un rifle de francotirador y que en 2022 fue condenado a siete años y medio de cárcel.[52] Murillo comparte rasgos con los individuos y grupos descritos en este capítulo, como su formación en seguridad, su ideología ultraconservadora y su tendencia a la fabulación violenta.

Sin embargo, a veces las operaciones siguen el camino contrario: se orquestan acciones físicas en el mundo real, con el propósito de amplificarlas en el universo virtual. ¿Qué ocurre cuando son las masas las manipuladas de forma deliberada por las acciones en el mundo real de un actor experimentado?

10

DESESTABILIZACIÓN *LOW COST*

La noticia saltó a los medios de comunicación de todo el mundo a finales de octubre de 2023: en París, viviendas de judíos estaban siendo marcadas con estrellas de David, igual que en la Alemania nazi. Periodistas y comentaristas se lanzaron sobre el tema: ¿podía acaso haber una prueba más clara de la explosión del antisemitismo en la Europa contemporánea?

La historia pronto dio un giro inesperado. Unos vecinos habían grabado con un teléfono móvil a algunas de las personas que habían realizado las pintadas, lo que permitió a la policía identificarlas y detenerlas.[1] Tras interrogarlas y examinar sus comunicaciones, emergió una imagen completamente diferente: los responsables eran dos parejas de inmigrantes moldavos, algunos, en situación irregular en el país, que seguían órdenes de un compatriota llamado Anatoli Prizenko, un empresario y político conocido por sus simpatías prorrusas y sospechoso de ser un operativo de su inteligencia.[2] A las parejas, además, les acompañaba al menos un fotógrafo cuya tarea era subir inmediatamente las imágenes a internet a través de una red de falsos medios de comunicación, conocida por los servicios de inteligencia europeos y denominada RRN (acrónimo de Reliable Recent News, o «Noticias recientes confiables»). Una red creada por Rusia, que imitaba a medios de referencia de toda Europa como *Le Monde*, *The Guardian*, *ANSA* o *Der Spiegel* para difundir narrativas falsas favorables al Kremlin, especialmente acerca de Ucrania, y que los investigadores sobre desinformación conocen como «Doppelgänger».[3] La existencia de esta red, de hecho, había sido denunciada públicamente por el Gobierno francés en junio de ese

mismo año como «un nuevo ejemplo de la estrategia híbrida que Rusia está implementando para minar las condiciones para un debate democrático pacífico y, por lo tanto, minar nuestras instituciones democráticas».

En el caso de las estrellas de David, el Servicio de Vigilancia y Protección contra las Injerencias Numéricas Extranjeras (Viginium) de Francia pudo constatar que las imágenes de las pintadas aparecieron en Doppelgänger antes de convertirse en virales y saltar a los medios de comunicación convencionales. Doppelgänger también publicó múltiples artículos que enfatizaban el auge del antisemitismo en Francia desde los atentados de Hamás del 7 de octubre de 2023, y que acusaban a las autoridades francesas de no hacer nada para proteger a sus ciudadanos. Según fuentes de la investigación citadas por *Le Monde*, el *modus operandi* —usando a individuos externos y mal pagados— es típico de los servicios de inteligencia rusos, muy afectados por la oleada de expulsiones de sus diplomáticos —en muchos casos, espías que operaban bajo tal cobertura— de gran parte de Europa a raíz de la invasión de Ucrania.

El episodio de las viviendas judías es otro ejemplo de desestabilización contra democracias europeas a un coste ridículo, aprovechando un contexto geopolítico de crispación. Operaciones que van desde radicalizar las protestas propalestinas en el Reino Unido, hasta una campaña de boicot lanzada desde Azerbaiyán contra los Juegos Olímpicos de París de 2024 como represalia por el apoyo del gobierno de Emmanuel Macron a Armenia a propósito del conflicto de Nagorno Karabaj. Las armas: redes sociales y tecnologías informativas, pero también otras más prosaicas como pintadas, *flash mobs*… e incluso una plaga de chinches.

Es probable que en algún momento te hayas tropezado con alguna información sobre la omnipresencia de las chinches en París en los meses anteriores a la celebración de las Olimpiadas.[4] La historia apareció en numerosos medios internacionales, acompañada de imágenes de insectos encontrados en trenes, sofás o butacas de cine.

Había una parte de verdad, aunque no tanta como para justificar la alarma pública. Los servicios de inteligencia franceses albergaban fuertes sospechas de que Rusia alimentó artificialmente la histeria en redes, recurriendo a la mencionada Doppelgänger.[5] Las sospechas se dispararon tras la aparición de un falso artículo en el diario *La Montagne* que, además de promover la psicosis, añadía un mensaje prorruso: «Resulta que, debido a las sanciones, un componente importante de los pesticidas ya no llega a Francia desde Rusia. Lo reemplazaron por otro, pero ha resultado ineficaz y los insectos se lo comen», decía una de las cuentas de X/Twitter que reproducía el supuesto artículo, acompañándolo de una captura de pantalla de la falsificación.

Otro falso artículo, supuestamente del diario *Libération* —que inmediatamente refutó su autenticidad—, afirmaba: «Los parasitólogos opinan que la epidemia de chinches en París está ligada al influjo de refugiados ucranianos en la capital».[6] Esta pieza fue compartida en Telegram por una cuenta asociada a la versión en francés de RT, el canal estatal ruso en múltiples idiomas. El diario *Le Figaro* también fue objeto de una falsificación similar: «Los rusos no están en el origen de esta psicosis, pero han surfeado la ola de forma eficaz. Era una ocasión muy bonita para desestabilizar a Francia, aliada de Ucrania y país organizador de los próximos Juegos Olímpicos», señalaba a finales de octubre de ese año la cadena privada gala *BFM TV*.[7]

«Tenemos Estados autoritarios que, además de identificar vulnerabilidades (políticas, sociales, económicas y de otro tipo) en las sociedades objetivo, y explotarlas en campañas manipulativas y de injerencia, son también oportunistas: aprovechan cuestiones que acaban de surgir y las explotan para sus propios fines. Lo que hacen al difundir estos mensajes es tensionar esas sociedades y tratar de agrietar todo lo posible», me explica Rubén Arcos, profesor de la Universidad Rey Juan Carlos, donde dirige un curso de especialista en amenazas híbridas. «Por el motivo que sea, por temas relacionados

con el cambio climático, ha habido una mayor presencia de chinches en Francia antes de los Juegos Olímpicos. Pues los rusos se dicen: vamos a tratar de aprovechar esto para hacerle daño a lo que ellos, en su lenguaje, denominan un "estado inamistoso"».

El propio presidente ruso, Vladímir Putin, se permitió ironizar, comentando en un vídeo la ampliación de las restricciones de las exportaciones a Rusia: «Bueno, cuanta menos basura, menos posibilidades de que las mayores ciudades europeas nos exporten sus chinches». Al mismo tiempo, el ecosistema de medios rusos se burlaba de la situación con memes.

Otro incidente detectado por las autoridades francesas en esas mismas fechas tenía que ver con vídeos y contenidos llamando al boicot de los Juegos Olímpicos, incluyendo un vídeo que mezclaba imágenes de atletas galos con otras de violencia policial y que alcanzó más de cinco millones de visualizaciones en X/Twitter. Esta campaña buscaba el impacto en el mundo real a través de la manipulación en redes mediante *hashtags* como #BoycottParis2024 o #NoParis2024. Viginium pudo constatar la aparición de más de 1600 publicaciones de este tipo los días 26 y 27 de julio, originadas en un total de 91 cuentas, «lo que sugiere una amplificación artificial». De estas, «una parte importante presenta al menos un vínculo con Azerbaiyán». El episodio fue interpretado como una reacción de Bakú a unas declaraciones del presidente Macron a principios de ese mes, en las que había exigido que se protegiesen los derechos de los armenios de Nagorno Karabaj.

Los Juegos Olímpicos fueron un objetivo para media docena de países. Viginium detectó 43 acciones entre abril de 2023 y septiembre de 2024. Cuentas asociadas al ecosistema de desinformación ruso en Telegram, X y Facebook, por ejemplo, difundieron un falso vídeo de los Lobos Grises, una organización ultranacionalista turca, lanzando amenazas a los atletas israelíes, y otro en el que un supuesto miembro de Hamás prometía atentar contra Francia y las competiciones deportivas. También promovieron fotos de supuestos grafitis que

establecían una relación directa entre los Juegos de Múnich de 1972, cuando el secuestro de once atletas israelíes por un comando palestino se saldó con la muerte de todos ellos, y las Olimpiadas de París, así como falsos comunicados que imitaban los logotipos de la CIA y de la DGSE —el servicio de inteligencia exterior de Francia— alertando de atentados inminentes contra estos eventos.[8]

El aparato de guerra informativa de Irán, por su parte, hizo públicas las identidades de atletas de Israel, a quienes acusó de crímenes de guerra, y promovió imágenes generadas mediante IA que mostraban a deportistas israelíes atacando físicamente a civiles palestinos, en algunos casos utilizando un logotipo falso de Amnistía Internacional.

China difundió de forma masiva y artificial vídeos que comparaban el Sena con el Ganges, por su supuesto nivel de suciedad, criticaban la ceremonia de inauguración y despreciaban las Olimpiadas parisinas frente a las de Pekín en 2008. China también utilizó la guerra en Gaza para promover mensajes contra Israel.

Por último, cuentas que se autoidentificaban como nacionalistas indios o individuos pro Trump y pro Israel difundieron de forma coordinada falsos vídeos de disturbios e incendios de vehículos y edificios de París, que pertenecían a un estallido social en Nanterre en el verano de 2023, para generar la idea de que la capital gala se había convertido en un infierno. Del mismo modo, emergieron cuentas, en inglés y español, que relataban casos de violencia, con el objetivo de presentar París como una ciudad extremadamente insegura debido a sus comunidades de inmigrantes, generalmente acompañados de vídeos de incidentes violentos que en realidad no tenían nada que ver con lo que mostraban.[9] La desestabilización *low-cost* en su máxima expresión.

QUEMAR EL CORÁN

El caso más espectacular quizá sea la quema de coranes en Escandinavia a lo largo de ese año, que provocó una cadena de consecuencias e incidentes violentos.

A finales de enero de 2023, Rasmus Paludan, un activista ultraderechista sueco-danés, conocido por sus ideas extremistas hacia el islam y por acciones anteriores contra el Corán, se presentó frente a la embajada de Turquía en Estocolmo para realizar una quema del libro sagrado de los musulmanes. La reacción inmediata del Gobierno turco fue bloquear la entrada de Suecia en la OTAN, que en aquella época estaba en pleno proceso de negociación, y para la que se requería la autorización de todos los países miembros de la alianza. Pronto se supo que la idea no había partido del propio Paludan, sino de otro individuo conocido en los círculos ultraderechistas suecos: el periodista Chang Frick y antiguo colaborador de la cadena rusa RT, quien había pagado la tasa administrativa de 320 coronas (unos 43 euros) requerida para la autorización de la protesta. Frick, además, había corrido con todos los gastos del viaje de Paludan a Estocolmo. Al ser preguntado por los medios suecos, dejó claro que uno de sus objetivos había sido obstruir el acceso de su país a la OTAN: «Si yo, pagando 320 coronas en una tasa administrativa a la policía, he saboteado la solicitud, es que probablemente ya pendía de un hilo desde el principio», declaró.

Cuatro meses después, cuando las aguas empezaban a volver a su cauce, otro activista, el refugiado iraquí de confesión cristiana Salwan Momika, también prendió fuego en varias ocasiones al Corán, calificándolo de «la fuente de todo mal». La ira en el ámbito musulmán fue incontenible: se produjeron protestas violentas en Irán, Irak y Líbano, una turba asaltó la embajada de Suecia en Bagdad, y varios diplomáticos suecos fueron agredidos en países árabes. Irak expulsó al embajador sueco, prohibió todos los negocios con el país y canceló los permisos de trabajo de los empleados de la empresa de telecomunicaciones Ericsson. Las fuerzas de seguridad de Alemania detuvieron a dos inmigrantes de veinticuatro y veintiocho años que se

preparaban para cometer atentados contra Suecia, que durante mucho tiempo siguió temiendo una represalia violenta por parte de organizaciones o individuos de filiación yihadista.

La situación ponía a Suecia ante un dilema imposible: recortar la sacrosanta libertad de expresión de la que tanto se precia la nación o permitir que extremistas descontrolados siguiesen perjudicando gravemente sus intereses internacionales.[10] Mientras tanto, Salwan Momika se hacía de oro monetizando en TikTok sus provocaciones públicas, en las que insultaba al islam y al profeta Mahoma.

La sorpresa llegó cuando se descubrió que Momika había liderado una milicia vinculada a Irán en su país de origen, la llamada «Brigada del Espíritu de Dios Jesús Hijo de María», formada por cristianos asirios reclutados para luchar contra Estado Islámico e integrada en las Fuerzas de Movilización Popular creadas por los servicios de inteligencia iraníes en Irak. Nada de esto probaba de forma definitiva que los Gobiernos de Rusia o Irán estuviesen detrás de estas acciones. Pero ambos las habían explotado a conciencia, difundiendo masivamente artículos e historias, tanto en redes como en medios en árabe y en otros idiomas de países musulmanes, en las que se afirmaba que este tipo de actos cuentan con el firme respaldo del Gobierno sueco. La Agencia para la Defensa Psicológica de Suecia, un organismo activo durante la Guerra Fría y recuperado a raíz de la invasión de Ucrania en 2022, detectó esa explosión súbita de contenidos: «Repiten narrativas de que Suecia apoya la quema del Corán y de que es un país islamófobo y hostil contra el islam. No nos sorprende mucho, porque Rusia está usando narrativas que hacen que Suecia quede mal y dificulten su entrada en la OTAN», declaró Mikael Östlund, portavoz de la agencia. La institución también percibió, en paralelo, un intento de promover el sentimiento antimusulmán en medios de extrema derecha, para aumentar las tensiones.

La agencia lanzó acusaciones similares hacia Irán, cuyos máximos líderes se implicaron. El ayatolá supremo Alí Jameneí acusó a Suecia de «prepararse para hacerle la guerra al mundo musulmán». Algunos

expertos creen que el régimen de Teherán presionaba así a Estocolmo para forzar el intercambio de uno de sus principales funcionarios, Hamid Nouri —condenado a cadena perpetua en Suecia por su papel en una cadena de ejecuciones de miles de presos en cárceles iraníes—, por el doctor Ahmad Reza Jalali, un ciudadano sueco-iraní detenido injustamente en 2016. En agosto, alrededor de 15.000 residentes en Suecia recibieron mensajes de texto en sueco en sus teléfonos móviles en los que se incitaba a vengarse de las personas que estaban execrando el Corán. Un año después, las autoridades suecas acusaron al Cuerpo de Guardia de la Revolución Islámica de Irán de haber hackeado una de las principales compañías de telecomunicación del país para enviar dichos SMS.

Momika, por cierto, acabaría siendo asesinado por autores desconocidos en su domicilio en enero de 2025, mientras hacía una retransmisión en vivo en TikTok.[11]

Elisabeth Braw, analista del Instituto Americano de Empresa y una de las expertas que más estudió en profundidad este caso, señaló en un artículo para *The Wall Street Journal* que «la campaña es tan inteligente precisamente porque es casi imposible preparar una defensa. Los diplomáticos suecos no llegarán muy lejos vagando por Irán e Irak intentando convencer a los manifestantes de que les han engañado con desinformación, o pidiéndoles a los *tiktokers* locales que no compartan contenido inexacto. Cualquier país cuyo gobierno pueda hacer enfadar a un régimen de este tipo es vulnerable a estas campañas».[12]

Irán, de hecho, es uno de los actores que más recurre a estrategias híbridas. En octubre de 2023, la Policía Metropolitana de Londres alertó de sus esfuerzos para radicalizar y cooptar las protestas propalestinas convocadas en la capital británica.[13] Denunciaron que, si bien las manifestaciones habían sido convocadas por individuos y colectivos legítimos, Irán estaba tratando de incrementar las tensiones no solo con desinformación en redes, sino también enviando operativos a las movilizaciones. Además, las autoridades descubrieron

que Irán no era el único actor que estaba explotando las tensiones derivadas de la guerra de Gaza: los contenidos de los *influencers* propalestinos estaban siendo amplificados de forma artificial por ejércitos de cuentas falsas, que el Gobierno del Reino Unido sospechaba que eran obra de Rusia y China.[14]

El aumento de estas campañas responde a su poder para polarizar a la población y a la facilidad que ofrecen las nuevas tecnologías para movilizar a una masa crítica de gente suficiente para llevar a cabo acciones en el mundo real y amplificarlas hasta el infinito en el virtual.

ODIO AL INMIGRANTE

El 29 de julio de 2024, un joven de diecisiete años irrumpió en un recinto escolar de la ciudad británica de Southport donde se celebraba una fiesta temática sobre la cantante Taylor Swift y comenzó a apuñalar indiscriminadamente a los asistentes. Tres niñas murieron —Bebe King, de seis años; Elsie Dot Stancombe, de siete; y Alice Dasilva Aguiar, de nueve— y varias personas resultaron heridas. Pocos minutos después de que se conociese la noticia, la cuenta de X/Twitter de Europe Invasion difundía la idea de que el sospechoso era «presuntamente un inmigrante musulmán».[15] Conocidos *influencers* de extrema derecha como Tommy Robinson y Andrew Tate también culpaban a un «inmigrante» llamado «Ali al-Shakati».[16]

La primera mención a dicho nombre surgió en la cuenta de X/Twitter de Bernadette Spofforth, una empresaria de cincuenta y cinco años residente en la localidad de Chester: «Ali Al-Shakati era el sospechoso. Era un solicitante de asilo que llegó al Reino Unido por barco el año pasado y estaba en una lista de vigilancia del MI6». Luego añadió: «Si esto es cierto, están a punto de abrirse todos los infiernos». En entrevistas posteriores, Spofforth mostraría arrepentimiento por el papel que jugó en los sucesos, asegurando que no se había inventado el nombre, sino que simplemente lo había

copiado y pegado de otras publicaciones. No se ha encontrado ningún rastro digital que confirme sus afirmaciones.[17]

Al día siguiente, una vigilia convocada por los familiares y vecinos de las víctimas fue cooptada por miembros de la comunidad ultraderechista británica, incluidos antiguos miembros de la Liga Inglesa de Defensa (EDL, por sus siglas en inglés) cofundada por Robinson. Desde allí, empezaron a marchar hacia una importante mezquita y centro islámico de la ciudad. Antes de que acabase la jornada, los manifestantes habían quemado una furgoneta policial y causado importantes destrozos.[18]

La violencia alcanzó tal grado que un juez ordenó que se hiciese pública la identidad del asesino, algo que hasta ese momento las autoridades habían evitado, al tratarse de un menor. Su nombre era Alex Muganwa Rudakubana, un británico hijo de dos refugiados ruandeses, y de confesión cristiana. Pero ya era tarde: para entonces, «Ali al-Shakati» había sido mencionado más de 30.000 veces por unas 18.000 cuentas, era *trending topic* en Reino Unido, y X/Twitter lo sugería en su sección lateral «Qué está pasando».[19]

Durante más de una semana, los disturbios se extendieron a una veintena de localidades, incluyendo Manchester, Liverpool, Cardiff, Newcastle, Blackburn, Tamworth, Hartlepool, Leeds, Nottingham, Middlesbrough, Aldershot, Sunderland y Belfast. En Rotherham, un grupo de manifestantes intentó incendiar un hotel en el que se alojaban familias refugiadas. Usuarios anónimos, en algunos casos extranjeros, crearon cuentas en plataformas como TikTok para amplificar y promover sus provocaciones, convocar concentraciones y difundir mensajes de ultraderecha.[20] En Telegram, un conocido neonazi finlandés llamado Charles-Emmanuel Mikko Rasanen, alias *Mr. AG*.[21], contribuyó a crear el grupo «Southport Wake Up» para coordinar las movilizaciones, y difundió activamente manuales para provocar incendios intencionados.[22]

Uno de los puntos más oscuros de este episodio fue el papel jugado por Rusia: apenas un par de minutos después de que Spofforth lanzase

el nombre de Ali al-Shakati, una página web de corte conspirativo, Channel3 Now, que muchos expertos vinculan a una operación rusa de desinformación, lo repitió en una de sus publicaciones.[23] Después, miles de cuentas del ecosistema ruso de redes lo amplificaron, y medios estatales rusos como RT mencionaron ese mismo nombre en sus reportes[24]. Esas mismas cuentas interactuaron en los canales creados para coordinar las protestas, en muchos casos haciéndose pasar por ciudadanos británicos, apoyando y difundiendo las convocatorias. En un plano internacional, Radio Genoa, una popular cuenta antiinmigración cuyo operador recibe apoyo de Rusia,[25] daba una versión apocalíptica y distorsionada de lo que estaba sucediendo en suelo británico. Análisis realizados posteriormente demostraron tanto la participación activa de medios rusos a la hora de culpar a musulmanes como la amplificación y promoción de las protestas por usuarios rusos en canales de Telegram y otras redes, una campaña que el exdirector del MI6 (el servicio de inteligencia exterior británico), sir Richard Dearlove, calificó de acciones de «guerra gris» contra el Reino Unido.[26] La lógica rusa estaba clara: buscaba mantener viva la violencia en Gran Bretaña como parte de su estrategia para desestabilizar las democracias occidentales.[27]

Cuando las aguas volvieron a su cauce, más de un millar de personas habían sido detenidas por la policía británica, y la mitad afrontaba cargos criminales[28]. Los disturbios habían mostrado la relativa facilidad con la que las divisiones internas, la polarización y las tensiones derivadas de la inmigración podían ser explotadas tanto por actores domésticos como por adversarios extranjeros para empeorar la situación y avanzar sus agendas. Pronto surgirían nuevas oportunidades.

Mientras el Reino Unido ardía, algunos individuos en España seguían muy de cerca la situación. El 4 de agosto, cuando los disturbios en Gran Bretaña se encontraban en su punto álgido, el portal HerQles, de ideología ultraderechista, publicaba el siguiente mensaje: «El Núcleo Nacional español llama a los españoles y

europeos a filas con este vídeo tras el levantamiento del Reino Unido: "Toda Europa está en pie de guerra, no te quedes sentado. Lucha, recupera tu nación. Es la hora"». Canales rusos de Telegram como «Espíritu Templario», que amplificaban los sucesos británicos, reproducían ese *post* llamando a recrear los disturbios en España. HerQles también envió a personas a Gran Bretaña para filmar los disturbios y recoger material con el que alimentar sus contenidos contra la inmigración. Por esas mismas fechas Daniel Esteve, líder de la organización Desokupa, decía en su canal de YouTube: «En Inglaterra creo ya que… el ser de luz de "Jovenlandia" no sé si es marroquí o argelino… Van ya tres criaturas muertas apuñaladas y ayer ya empezaron a haber los primeros disturbios. Eso es lo que tiene que pasar, lo he dicho muchas veces: dais una, damos dos, dais tres, damos cuatro. Ese es el único mensaje que entienden estos animales».

Pocos días después, el 18 de agosto, un niño de once años llamado Mateo era apuñalado en el municipio toledano de Mocejón tras una discusión durante un partido de fútbol. Apenas unas horas tras el suceso, «El Puntual 24 horas», un canal de Telegram camuflado como un medio de comunicación, pero que difunde contenidos racistas, posteaba este titular: «Un magrebí ASESINA a un niño de diez años cuando jugaba al fútbol con sus amigos». *Influencers* ultraconservadores, como Alberto Caliu, lanzaban mensajes similares: «El asesino del niño de Mocejón es un moro. Políticos culpables», tuiteó.[29] También añadió: «Según me comentan, sobre el lunes 5 de agosto llegaron a Mocejón unos cincuenta africanos en autobús y los alojaron en el Hotel Pattaya. En Mocejón se vivía tranquilo hasta entonces, ahora ya vemos lo que sucede». Caliu pidió «señalar y ubicar todos los hoteles que alojen a inmigrantes ilegales», porque «son cómplices».[30] Al día siguiente Esteve, HerQles y el canal del eurodiputado Alvise Pérez, entre otros, se hacían eco de la afirmación de que el asesino era un inmigrante.[31]

El incidente había puesto de manifiesto la existencia de decenas, quizá cientos de cuentas en redes, sobre todo en X/Twitter, dedicadas a

publicar comentarios sensacionalistas sobre sucesos con un elemento en común: los villanos de la historia siempre son inmigrantes. Cada vez que se produce un incidente violento, se apresuran a culpar a un miembro de estas minorías.

El mismo día del crimen de Mocejón, la cuenta «El Puntual» publicaba: «Un grupo de 8 magrebíes con nacionalidad francesa VIOLAN de forma VIOLENTA a una británica de dieciocho años. Ha pasado en Magaluf (Mallorca)». La realidad es que los individuos presuntamente responsables de la agresión sexual, acaecida en agosto de 2023, por la que fueron juzgados al año siguiente, eran siete turistas franceses y un suizo, sin que hubiera nada que indicase un origen magrebí. Un ejemplo del tipo de contenido que componía la casi totalidad de este canal —ya inexistente— con decenas de miles de seguidores: incidentes violentos protagonizados por magrebíes o bandas latinas, inmigrantes africanos culpables de la expansión de la viruela del mono, o mensajes equiparando homosexualidad y pedofilia.[32]

El 7 de agosto, el *influencer* ultraderechista Vito Quiles difundía un vídeo en su cuenta de X/Twitter con la siguiente leyenda: «#ÚLTIMAHORA | Tres menas apuñalan a un niño de catorce años en el barrio de Delicias (Zaragoza) para robarle y después se dan a la fuga. Una ambulancia se ha desplazado hasta la zona para socorrer al menor».[33] Las imágenes, filmadas desde la ventana de un edificio, mostraban a dos patrullas desplegadas en una esquina en la que acababa de suceder algo indeterminado, al tiempo que una ambulancia llega al lugar. El periodista Alejandro Requeijo, del diario *El Confidencial*, se puso en contacto con la Policía de Zaragoza y pudo confirmar que el supuesto apuñalamiento no había tenido lugar, y que las imágenes correspondían a algún otro incidente[34]. A pesar de ello, en marzo de 2025 Quiles no se había dignado a borrar el tuit falso.

Lo mismo había ocurrido con una serie de asesinatos con arma blanca ocurridos en la Comunidad Valenciana el mes anterior. Decenas

de usuarios de las redes difundieron el bulo de que las muertes eran decapitaciones llevadas a cabo por un argelino. Algunas cuentas, como «Ordenado… ¿y qué?»[35] o «Alt Right España»,[36] u otras más modestas como «Hugo de Payns»,[37] publicaron un vídeo de la supuesta detención del asesino, acompañado de una leyenda idéntica: «La policía anuncia la detención del autor del asesinato por decapitación de un hombre de cuarenta años este martes en #Valencia. El magrebí fue detenido tras ser reconocido en el paso de Neptuno de la ciudad, cerca de la playa de la Malvarrosa». De nuevo, el presunto responsable era un hombre de treinta y un años nacido en Barcelona. No solo eso: meses después, esas mismas imágenes volvían a ser utilizadas por otras cuentas para asegurar que «el marroquí que decapitó a un hombre de cuarenta años en Valencia» había sido «puesto en libertad a los pocos días».[38]

Este suceso aportó una clave interesante: el hecho de que el mismo mensaje, palabra por palabra, fuese reproducido de forma exacta el mismo día por múltiples cuentas, lo cual apunta a una probable coordinación entre sus autores. Para analistas y expertos es evidente que, al menos en algunos casos, se trata de campañas coordinadas —que a veces incluso recurren a bots— para alcanzar la máxima difusión posible.

El responsable del apuñalamiento de Mocejón fue detenido en menos de 48 horas y, una vez más, resultó ser un joven llamado Juan, residente en Madrid y con familia en el pueblo. En España no se reprodujeron los disturbios que esperaban muchos de quienes promovieron el bulo sobre el origen extranjero del asesino. Pero siguen ahí: enjambres de cuentas europeas y españolas, que cada día contribuyen a echar gasolina al conflicto social, esperando que, en algún momento, prenda la chispa que lo incendie todo.

11

CAMPO DE BATALLA: ESTADOS UNIDOS

Las elecciones presidenciales en Estados Unidos han sido hasta ahora las más importantes del planeta. Lo que haga el país con el mayor PIB global —y el mayor presupuesto y despliegue militar en el mundo— acaba afectando inevitablemente al resto de la humanidad. Y, aunque no faltan quienes creen que en política exterior no hay muchas diferencias entre administraciones republicanas y demócratas, esto es cada vez menos cierto. Quién sea el ocupante de la Casa Blanca cambia radicalmente el enfoque estadounidense hacia Europa, Rusia, Oriente Medio, el hemisferio sur americano, África y, probablemente, incluso China. Por eso, no es de extrañar que un número asombroso de potencias, grandes y pequeñas, traten de influir en los resultados de esos comicios. En 2020, la lista de países cuyos esfuerzos de interferencia fueron detectados por la inteligencia de Estados Unidos incluía, no solo a los que cabría esperar, como Rusia o China, sino también a Irán, Corea del Norte, Arabia Saudí y Cuba.[1]

Cuatro años después, en las elecciones de 2024, este fenómeno era aún más acusado. En agosto de ese año, la campaña de Donald Trump anunció el presunto hackeo de algunos de sus equipos, del que investigadores en ciberseguridad culparon al grupo iraní denominado Mint Sandstorm, vinculado al Pasdarán o Guardia Islámica Revolucionaria. Este grupo también habría intentado penetrar en las campañas de Joe Biden hasta su retirada, y en la de Kamala Harris después, aunque no trascendió que hubieran tenido éxito.

Sí lo hicieron en el caso de la campaña republicana. Días después de la brecha informática, varios medios de comunicación empezaron a recibir documentos de una fuente que se identificaba solo como

«Robert», incluyendo una potencial bomba informativa: un informe de 271 páginas que detallaba las potenciales vulnerabilidades de J. D. Vance como candidato a la vicepresidencia, elaborado antes de que fuese elegido para el puesto.

Sin embargo, la respuesta de los periodistas, escarmentados por las manipulaciones ocurridas durante los comicios de 2016, fue mucho más cauta que en ocasiones anteriores. *The New York Times* y *The Washington Post* optaron por no publicar nada,[2] mientras que *Politico* publicó un artículo explicando los elementos que rodeaban la filtración y el contenido general de los documentos, pero no sus detalles.[3] La operación de influencia, en resumen, resultó un fiasco. Pero estaba lejos de ser la única.

El 8 de agosto, el Centro de Análisis de Amenazas de Microsoft advertía que Irán se había unido a la competición por interferir en el proceso: «En las últimas semanas, grupos relacionados con el Gobierno iraní […] han sentado las bases para campañas de influencia sobre temas de actualidad relacionados con las elecciones y han comenzado a activar estas campañas en un aparente intento de generar controversia o influir en los votantes, especialmente en los estados clave», aseguraba la firma en una nota informativa.[4] Irán tenía poderosos motivos para inclinar las urnas en contra de Trump. Durante su presidencia, se retiró unilateralmente del acuerdo nuclear, eliminó al comandante de la Guardia Islámica Revolucionaria Qassem Soleimani y trasladó la embajada a Jerusalén, entre otras decisiones.

Se daba la paradoja de que Irán y Rusia, cuya alianza global era cada vez más estrecha, estaban favoreciendo a candidatos opuestos.[5] A finales de julio, la Oficina del Director Nacional de Inteligencia había publicado un informe donde indicaba: «La preferencia de Irán es esencialmente un reflejo de su deseo de no empeorar las tensiones con Estados Unidos, e Irán se opone al candidato que los líderes iraníes perciben que incrementaría dichas tensiones». En otra estimación publicada unos días antes, la ODNI ya había declarado «no haber observado un cambio en las preferencias de Rusia en la carrera

presidencial respecto a pasadas elecciones, dado el papel que Estados Unidos desempeña respecto a Ucrania y a políticas más amplias hacia Rusia». Aunque por razones políticas no se mencionaba a qué candidato se refería en cada caso, la conclusión era evidente. En una llamada aclaratoria a varios medios estadounidenses, un funcionario de inteligencia señaló que «el Kremlin dirigirá sus esfuerzos propagandísticos a apoyar a Donald Trump frente a la vicepresidenta Kamala Harris», mientras que «Irán probablemente seguirá intentando denigrar a Trump».[6]

Rusia llevaba muchos meses tratando de favorecer a Trump. Los medios estatales rusos dirigidos a audiencias extranjeras alababan públicamente al republicano como «candidato de la paz», al tiempo que presentaban a los demócratas como elitistas y corruptos al servicio de las corporaciones. El ecosistema ruso en redes sociales difundió miles de mensajes y cientos de vídeos —incluyendo falsificaciones de baja calidad hechas con inteligencia artificial— exagerando los supuestos problemas cognitivos de Biden, criticando su gestión y, sobre todo, el apoyo a Ucrania. La sustitución de Biden por Kamala Harris parecía haber dejado momentáneamente a los propagandistas rusos un poco fuera de juego. En un primer momento, lo tildaron de «golpe palaciego», o una operación del Estado profundo con Harris como impostora.

CHINA APOYA A TRUMP

La interferencia china fue más sutil. En primavera, investigadores de desinformación estadounidenses, australianos y europeos señalaron que «las principales estructuras chinas de influencia en redes sociales estaban reorientando sus contenidos».[7] Una red de cuentas falsas en múltiples plataformas, conocida como Spamouflage, cuestionaba la integridad del proceso estadounidense y amplificaba las disfunciones del país,[8] como los problemas causados por el fentanilo o las bajas masivas por las armas de fuego. El objetivo: erosionar la confianza en

las instituciones democráticas y ahondar en las divisiones sociales, sin mostrar preferencia por ninguno de los candidatos presidenciales, que eran atacados y denigrados por igual. También explotaban sucesos como la crisis política en la frontera de Texas, sugiriendo que el país estaba a punto de entrar en una guerra civil.[9]

Pero, en abril, la situación había cambiado. Un informe del Instituto para el Diálogo Estratégico (ISD) constató que estas estructuras chinas orientadas al público estadounidense habían virado hacia narrativas favorables a la derecha. «Cuentas vinculadas a Spamouflage que fingen, de manera convincente, ser partidarios de Donald Trump y el movimiento MAGA [...] construyendo audiencias pro-Trump reales».[10]

Ayudadas de la IA, habían empezado a publicar textos en contra de Joe Biden y a favor de Trump. «Nunca había visto nada en esta línea antes», declaró Elise Thomas, una de las autoras del informe, a *The New York Times*. Según esta investigadora, era la primera vez que encontraban cuentas chinas fingiendo ser estadounidenses pro-Trump de una forma realista y logrando una interacción genuina con usuarios reales, un resultado que anteriormente les había sido esquivo[11]. Las redes online de China, hasta entonces torpes y de escaso alcance, empezaban a tener un impacto real.

Pero ¿qué interés podría tener China en poner en la Casa Blanca al candidato que había iniciado las guerras comerciales con Pekín y que había denominado la pandemia del COVID-19 como «el virus de China»? Algunas claves las dio Agathe Demarais, la analista jefa de la unidad de Inteligencia Económica de la publicación británica *The Economist*, en un artículo en la revista *Foreign Policy* titulado «Por qué China espera que gane Trump».[12]

> Dada la retórica incendiaria de Trump sobre Pekín —incluida su promesa de escalar las guerras comerciales entre Estados Unidos y China— es fácil creer que los líderes chinos preferirían al presidente en el cargo Joe Biden sobre Trump, que probablemente será el candidato del Partido Republicano. Pero esta idea es probablemente miope, y eclipsa el panorama completo [...] Desde la perspectiva

de la confrontación a largo plazo entre Pekín y Occidente, el regreso de Trump a la Casa Blanca podría perfectamente acabar beneficiando a China, al menos en el campo económico.

Sus ideas se resumían en cinco puntos:

1. La elección de Trump probablemente incrementaría las divisiones entre Estados Unidos y Europa, ayudando a prevenir la creación de un bloque transatlántico orientado a contener a China.
2. Trump podría revertir las sanciones a Rusia, eliminando el riesgo de que se impusiesen sanciones secundarias contra Pekín por su apoyo a Moscú.
3. La arbitrariedad de la Administración Trump a la hora de imponer sanciones sin previo aviso ayudaría a los esfuerzos chinos para establecer mecanismos financieros alternativos.
4. También incrementaría la dominación china para hacerse con los recursos minerales críticos de países emergentes.
5. Y China, que pugna por la hegemonía de las tecnologías verdes, podría beneficiarse de las restricciones a las exportaciones de una administración que claramente favorece las energías fósiles.

Así lo escribía Demarais:

Una segunda presidencia de Trump no ayudaría a convencer a las economías subdesarrolladas —que Trump una vez denigró colectivamente como «países de mierda»— de que se aliasen con Washington para el suministro de materiales críticos no procesados. Muchos estados ricos en minerales temerían que las promesas de Trump tuvieran escaso valor» [...]. Además, el desdén de Trump por las economías en desarrollo, las probables restricciones a la inmigración, y la retórica incendiaria sobre el islam no ayudarán a romper el hielo con los líderes africanos, del sudeste asiático o sudamericanos. China se alegraría y continuaría promoviendo sus intereses en las economías emergentes, mostrándose como el adulto en la sala, un socio confiable que no mezcla política y negocios [...]. Hay, por supuesto, otras áreas a considerar además de las económicas. Pero la reciente declaración de Trump de que no está muy dispuesto a defender Taiwán

> —otro asunto crucial para China— también alegrará a Pekín. Visto desde China, una victoria de Trump en noviembre podría aparecer como una oportunidad tentadora para beneficiarse del caos, las divisiones y el impacto al prestigio estadounidense que esto desataría.[13]

Meses después, Bloomberg publicó una larga entrevista con Donald Trump en la que expresaba muchos de estos mismos puntos: atacaba a la UE por su «trato violento» hacia Estados Unidos en materia de comercio, aseguraba que no iba a prohibir la red social china TikTok, avanzó que autorizaría nuevas prospecciones petroleras, y se mostró abierto a levantar las sanciones contra Rusia.[14].

¿Y Taiwán? Preguntado si lo defendería en caso de una invasión china, respondió directamente: «No», sin ocultar además su desprecio. «Taiwán se llevó nuestro negocio de chips. Quiero decir, ¿cómo somos así de estúpidos? Se llevaron todo nuestro negocio de chips. Son inmensamente ricos [...] Taiwán está a 9.500 millas. Está a 68 millas de China».[15]

La mencionada red Spamouflage comenzó una década antes de las elecciones de 2024 posteando contenido inocuo y apolítico hasta lograr cierto número de seguidores, momento en el que sus cuentas lanzaron mensajes sobre Hong Kong, Xinjiang, el Tíbet o la alta competencia del Partido Comunista Chino a la hora de gobernar el gigante asiático.[16] A partir de 2020, criticó la respuesta estadounidense al COVID-19, su política exterior o las tensiones raciales. Aun así, según la inteligencia de Estados Unidos, se abstuvo de intervenir en los comicios que ganó Joe Biden.[17] Pero dos años después, la situación era radicalmente distinta.

En abril de 2023, el Departamento de Justicia estadounidense imputó a 34 oficiales de inteligencia, miembros del llamado «Grupo Especial de Trabajo 912 del Ministerio de Seguridad Pública de China», bajo los cargos de «crear y usar un grupo de cuentas bajo nombres falsos en plataformas estadounidenses de redes sociales para diseminar y amplificar mensajes como parte de un amplio esfuerzo para influir y dar forma a las percepciones públicas sobre el gobierno

de la RPC, el PCC y sus líderes, en Estados Unidos y alrededor del mundo». Periodistas e investigadores en redes pudieron conectar los nombres de los espías chinos imputados con los responsables de Spamouflage (por lo que se cree que esta es lo mismo que el llamado Grupo 912).[18]

A partir de entonces, la intensidad de su operación aumentó. En junio de 2024, Google informó de la disrupción de más de 10.000 instancias de actividad de Spamouflage durante el primer trimestre del año.[19] Como sucede casi siempre en este ámbito, es imposible determinar el impacto en el voto de los ciudadanos, aunque el coste de las campañas es muy reducido. Así que China siguió intentándolo.

Ingentes cantidades de cuentas que se hacían pasar por estadounidenses partidarios de Trump promovían teorías de la conspiración, atacaban a Biden y ahondaban en cuanto dividía al país.[20] También amplificaban los contenidos creados por Rusia, caso de vídeos con «pruebas» de fraudes en las votaciones: destrucción de urnas, máquinas de votación que funcionaban mal, uso de identidades de fallecidos a favor de Kamala Harris... La fuente que lo había revelado sería, supuestamente, el director del FBI Christopher Wray, cuya voz había sido copiada mediante IA. Los vídeos imitaban el formato informativo de las cadenas CBS y MSNBC, cuyos logotipos aparecían sobre las imágenes. Los vídeos habían sido detectados en el ecosistema de desinformación ruso, antes de saltar al de China.

Los esfuerzos de China se centraban, sin embargo, en que ciertos congresistas con posturas contrarias a los intereses de Pekín perdieran su escaño. El caso más evidente fue Barry Moore, el representante republicano por Alabama, a causa de su apoyo a la imposición de sanciones contra ciertos funcionarios chinos. Las redes vinculadas a China vertieron todo tipo de insultos antisemitas contra él —algo un poco sorprendente, puesto que Moore no es judío—, y le acusaron de haber ganado su escaño gracias al «maldito consorcio judío». Según un funcionario de inteligencia citado por *The Washington Post*, China

se inmiscuyó en docenas de votaciones de altos cargos electos por debajo del presidente durante 2024.[21]

Y no solo China

Las maniobras de Cuba se han dirigido tradicionalmente al estado de Florida, el principal destino de la diáspora reciente, donde reside la mayor parte de la minoría cubano-estadounidense y, por lo tanto, epicentro de la oposición a una normalización de relaciones con el régimen de La Habana. Según la ODNI, Cuba ya trató de interferir en las elecciones de mitad de mandato en 2022,[22] y se esperaba que lo intentase de nuevo en 2024. «Puedo decir que el Gobierno cubano está llevando a cabo operaciones de influencia localizadas enfocadas de forma mucho más estrecha en oponerse a los candidatos antirrégimen en Estados Unidos», declaró un funcionario de la ODNI al *Miami Herald* a finales de julio.[23]

El caso de Israel fue más complejo. Organizaciones abiertamente proisraelíes, como el Comité de Asuntos Públicos America-Israel (AIPAC), donaron decenas de millones de dólares a las campañas primarias de al menos dos candidatos demócratas para impedir la reelección de representantes que se habían mostrado críticos con la actuación en Gaza, como Jamaal Bowman y Cori Bush. Ambos fueron derrotados por sus adversarios, George Latimer y Wesley Bell.[24]

Además, a principios de junio, una investigación periodística internacional desveló una masiva campaña orientada a congresistas afroamericanos y jóvenes progresistas estadounidenses y canadienses.[25] Según el diario de izquierdas israelí *Haaretz*, la campaña, organizada por el Ministerio de Asuntos de la Diáspora y llevada a cabo por una firma privada llamada STOIC, lanzó cientos de páginas y cuentas falsas para promover contenidos proisraelíes, antipalestinos y antimusulmanes, así como para difundir desinformación sobre antisemitismo en los campus universitarios de Estados Unidos.[26]

Al menos 128 miembros del Congreso fueron el objetivo de unos seiscientos perfiles falsos que trataron de influir en sus decisiones como si pertenecieran a su electorado.[27] Dado que el apoyo a Israel en Gaza era uno de los más divisivos en los comicios, algunos comentaristas consideraron el incidente como un intento de influencia electoral por un actor extranjero, pese a que la ODNI se mostró ambigua al respecto.[28] El primer ministro israelí, Benjamin Netanyahu, no ocultó sus simpatías por Trump.

Entre los gobiernos europeos, la Hungría de Víktor Orbán también destacó por sus movimientos a favor de Trump. El comentarista Nahal Toosi describía los crecientes lazos entre los conservadores estadounidenses y el Gobierno húngaro en un artículo titulado «La Hungría de Orbán ha elegido bando en las elecciones en América»,[29] en *Politico Magazine*:

> El punto de vista general en la mayoría de las capitales, Washington incluida, ha sido desde hace mucho que es mejor permanecer neutral en las competiciones políticas de otras naciones. Después de todo, en último término tienes que relacionarte con el que gane. Pero, a medida que la polarización política en América se agudiza, más líderes extranjeros podrían decidir que la mejor forma de proteger los intereses de su país, o los suyos propios, es cortejar a un solo partido estadounidense.

«Aunque no se sabe de ninguna donación directa de Hungría a los círculos republicanos, los *think tanks* financiados por el Gobierno húngaro han copatrocinado eventos y establecido contactos con el entorno de Trump. Y no sabemos cuánto dinero ni cómo se gastó», me dijo Szabolcs Panyi, editor jefe de la publicación VSquare, un portal centroeuropeo de periodismo de investigación, cuando le pregunté por este tema. «Los lobistas de Orbán apuntan principalmente a la Heritage Foundation, encargada de examinar la futura Administración Trump y de redactar su agenda (el Proyecto 2025[30]), así como a la Conferencia Política de Acción Conservadora y, lo más importante, a J. D. Vance. Sin embargo, esto se parece más a una infiltración en un

partido que a una intromisión en la campaña. Mientras tanto, hay informes de que algunos de los asesores de imagen y estrategas de campaña de Orbán también están involucrados en la campaña de Trump, aunque es difícil corroborarlo», añadía este experto.

EL MÁRTIR HA SOBREVIVIDO

El 13 de julio de 2024, Donald Trump sobrevivió a un intento de asesinato durante un mítin electoral en Butler, en el estado clave de Pensilvania. Un joven de veinte años llamado Thomas Matthew Crooks abrió fuego contra el presidente desde un tejado, rozando a Trump en la oreja y matando a un miembro del público situado detrás del candidato. Inmediatamente, los tiradores del servicio de protección del expresidente abatieron a Crooks. En esos momentos de caos, Trump se incorporó en pie con la oreja ensangrentada y gritó: «¡Luchad! ¡Luchad! ¡Luchad!», mientras el Servicio Secreto lo sacaba de allí, dando lugar a una de las imágenes más icónicas de toda la carrera presidencial de ese año.

Al día siguiente, el magnate sudafricano Elon Musk —propietario de Tesla, Starlink, Space-X y X/Twitter (que renombró inmediatamente como X tras su adquisición en 2022)— mostró públicamente por primera vez su apoyo a la candidatura de Trump: «Respaldo plenamente a Trump para presidente y le deseo una rápida recuperación», tuiteó, en el primero de una serie de mensajes sobre el tema. «El mártir ha sobrevivido», escribió después. Y más tarde: «La última vez que América tuvo un candidato así de duro fue Theodore Roosevelt». A partir de ahí, hizo de la victoria de Trump su propia causa y la convirtió en su objetivo fundamental.

Para la campaña de Trump, que alguien como Musk se implicase a su favor suponía un espaldarazo considerable. El magnate sudafricano tuvo acceso casi directo al candidato, con el que hablaba varias veces por semana. A principios de octubre, Musk compareció en el mitin que Trump volvió a dar en Butler, donde le dijo al público: «Esta es

una elección que hay que ganar. [Los demócratas] buscan acabar con vuestra libertad de expresión, buscan acabar con vuestro derecho a llevar armas, buscan acabar con vuestro derecho a votar, en la práctica».[31] Musk pidió a los asistentes que agarrasen a todos sus conocidos, y a quienes no lo fuesen, y les arrastrasen a que se registrasen para votar: «Si no lo hacen, estas serán las últimas elecciones. Esa es mi predicción».

Musk parecía estar convencido de lo que decía. En una entrevista con Tucker Carlson, el empresario preguntó, medio en broma: «¿Cómo de larga crees que será mi sentencia de cárcel [si Trump pierde]?». Según un artículo de *The New York Times* basado en diecisiete fuentes cercanas a Musk y sus operaciones, este se refería de forma «obsesiva, casi maníaca, acerca de lo que está en juego en estas elecciones y la necesidad de que Trump gane».[32] Para él, se trataba de una encrucijada existencial, y actuaba en modo crisis, igual que cuando una de sus empresas se enfrenta a un problema catastrófico: trabajando hasta altas horas de la noche, microgestionando múltiples iniciativas, encerrado en un cuartel general en Pittsburgh, la capital de Pensilvania, decidiendo junto a un equipo de abogados y expertos qué nuevas iniciativas se podían adoptar para asegurar la victoria del republicano.

Musk se puso como objetivo conseguir que 800.000 personas adicionales votasen por Trump en los estados bisagra que podían decidir el resultado. Creó un «Supercomité de Acción Política» —una institución existente que permite canalizar apoyos y fondos hacia un candidato— al que bautizó como America PAC, aparte de financiar el trabajo de otros comités similares.

Para generar rápidamente una base de datos de presumibles partidarios, Musk ofreció 47 dólares a cualquier persona en los estados de Pensilvania, Georgia, Nevada, Arizona, Míchigan, Wisconsin y Carolina del Norte que consiguiera que otro votante registrado firmase una petición «en apoyo de la Constitución», específicamente a la Primera y Segunda Enmiendas, las que garantizan

la libertad de expresión y el derecho a llevar armas. La cifra 47 es simbólica: si Trump ganaba, se convertiría en el 47º presidente de los Estados Unidos. La idea era conseguir los datos personales de esas personas para después bombardearles con propaganda política, con la esperanza de persuadirles. Una práctica más o menos estándar de todas las campañas, con o sin ofertas económicas de por medio.

Algunos comentaristas criticaron que ofrecer una compensación monetaria suponía una distorsión de los datos, puesto que incentivaba el registro de ciudadanos —por ejemplo, estudiantes u otros perfiles de individuos escasos de fondos— que quizá no albergaban la más mínima intención de votar por Trump, pero que respondían a una oferta de dinero fácil.[33] Musk redobló sus esfuerzos: en Pensilvania subió la cantidad hasta cien dólares, en exclusiva para los votantes de ese estado crucial. Poco después anunció que sortearía un millón de dólares al día para uno de los firmantes de la petición. Algunos demócratas cuestionaron la legitimidad de la iniciativa, pero la mayoría de los expertos legales consideró que todavía no había cruzado ninguna línea legal.[34]

La adquisición de X/Twitter por parte de Musk fue una inversión económica ruinosa que había afectado a la cotización de otras de sus empresas, como Tesla. Pero, desde el punto de vista táctico, le había dado al magnate una poderosísima plataforma que puso, sin disimulo, al servicio de Trump. Aparte de cambiar el nombre a «X», desmanteló muchos mecanismos de verificación que mitigaban la proliferación de desinformación y mensajes de odio. Restableció las cuentas de figuras prominentes previamente expulsadas por haber difundido contenidos de odio, racistas, misóginos o similares. El propio Musk publicó bulos gigantescos contra Harris y a favor de Trump. Uno de los más destacados, que los demócratas estaban acelerando la concesión de la ciudadanía a solicitantes de asilo para que pudieran votar en los estados bisagra. O imágenes generadas mediante IA de Harris vestida como un comisario del Partido Comunista Chino. El equipo de verificadores de la cadena *CBS* analizó los tuits recientes de Musk y

comprobó que un asombroso 55% contenían afirmaciones falsas o erróneas, o amplificaban *posts* que lo hacían.[35] Dado que la cuenta de Musk era seguida por más de 200 millones de personas, dichas publicaciones tenían un alcance masivo, y se traducían en consecuencias en la vida real. Por ejemplo, funcionarios electorales denunciaron recibir aluviones de mensajes intimidatorios y amenazas de muerte cada vez que el empresario difundía un tuit sobre el presunto fraude que se avecinaba.

Más oscura fue la intervención de otros comités, como Future Coalition PAC, cuyo único financiador era una organización política sin ánimo de lucro llamada Building America's Future («Construyendo el Futuro de América»), que a su vez recibía fondos de otro grupo llamado Citizens for Sanity («Ciudadanos por la Cordura»), al que Musk financió con decenas de millones de dólares. Building America's Future —que se habría beneficiado de más de cien millones en contribuciones directas de Musk — financiaba a su vez otro comité, Duty to America PAC (que podría traducirse como «Nuestro deber con América»).

Según una investigación de la publicación *404media*, tanto Future Coalition como Duty to America llevaron a cabo campañas personalizadas en redes sociales promoviendo diferentes ideas en función del perfil del objetivo, una técnica denominada *microtargeting*. Los registros públicos de la plataforma Snapchat — una de las más transparentes respecto al origen y fondos de sus anunciantes—, revelaron que Future Coalition envió mensajes diametralmente opuestos a los votantes musulmanes en Míchigan y a los votantes judíos en Pensilvania: mientras los primeros recibían un anuncio que aparentaba ser de la campaña de Harris, en el que alardeaba del apoyo de la candidata a Israel, en el segundo se aseguraba que «la embustera Kamala Harris apoya a Palestina, no a nuestro aliado Israel».[36]

Duty to America recurrió a prácticas similares: a los votantes afroamericanos les hacía llegar el mensaje de que Harris quería

prohibir los cigarrillos mentolados. Suena raro, pero no es baladí: las encuestas muestran que el 81 % de los fumadores de esta minoría prefieren este tipo de cigarrillos.

En palabras del citado artículo en *The New York Times*, «el hombre más rico del mundo se ha implicado en las elecciones estadounidenses de una forma sin paralelo en la historia moderna».

Las consecuencias no tardarían en llegar.

12

LO QUE VIENE

2024 fue un «superaño electoral». Alrededor de la mitad de la población del mundo tuvo la oportunidad de acudir a las urnas para participar en procesos electorales en 72 países de todo el mundo.[1] Al comenzar el año, en los principales centros de decisión e influencia global flotaba una preocupación: que la explosión de los *deepfakes*, la generación mediante inteligencia artificial de imágenes y sonidos falsos difícilmente distinguibles de los auténticos, turboalimentasen los procesos de desinformación e interferencia electoral, que ya se habían convertido en una constante en cada elección relevante a nivel global.[2]

En los dos años anteriores, la IA generativa había dado un salto de gigante, permitiendo la creación de vídeos, fotografías y audios de una calidad inédita hasta entonces, lo que representaba un enorme desafío para la ciudadanía: si ya no era posible distinguir entre lo real y lo falso, ¿cómo garantizar la integridad del proceso democrático?

Había, de hecho, un precedente sólido: en 2023, tres días antes de las elecciones en Eslovaquia, apareció en Facebook un audio en el que se escuchaba cómo el candidato del partido liberal Eslovaquia Progresista, Michal Simecka, proponía duplicar el precio de la cerveza si ganaba. Al día siguiente emergió otro audio de una supuesta conversación entre él y una periodista en la que discutían cómo amañar los comicios comprando votos entre la minoría gitana. Ambos eran falsos, creados mediante IA. Pero que aparecieran durante la moratoria de 48 horas antes de la jornada electoral, que obliga a medios de comunicación y políticos a guardar silencio, complicó cualquier desmentido. Es imposible saber cuánto impacto tuvieron. El

30 de septiembre, Eslovaquia Progresista perdió las elecciones frente al otro gran partido del país, el SMER de Robert Fico.[3]

El primer *deepfake* viral tuvo como objeto a Barack Obama: un vídeo experimental creado en 2017 por la Universidad de Washington que, tomando como base un discurso real televisado del expresidente, modificaba sus gestos faciales e imitaba su voz de forma sintética, haciéndole decir algo completamente diferente.[4] Pero fueron una serie de vídeos de Tom Cruise en TikTok en 2021, hechos a partir de las acciones de un imitador cuyo rostro era alterado digitalmente para que pareciese idéntico al del actor,[5] los que hicieron saltar la alarma. Semejantes avances tecnológicos auguraban una nueva era de la falsedad.

En marzo de 2022, pocos días después del inicio de la invasión rusa de Ucrania, un falso vídeo del presidente Volodímir Zelenski llamando a sus compatriotas a deponer las armas apareció en internet y fue visto cientos de miles de veces.[6] El discurso resultaba poco verosímil: hasta ese momento, Zelenski había mostrado una enorme determinación contra la invasión. El ejército ucraniano hacía retroceder a las tropas rusas en múltiples frentes. La rendición no tenía sentido.

Veamos ahora un caso completamente diferente. En 2020 apareció un vídeo en el que la portavoz de la Cámara de Representantes de Estados Unidos, Nancy Pelosi, hablaba arrastrando las palabras: parecía borracha. Las imágenes eran reales, tomadas de una intervención de Pelosi en una conferencia, pero la velocidad había sido alterada para crear la impresión de ebriedad. Hany Farid, experto en exámenes forenses digitales de la Universidad californiana de Berkeley, calculó que la imagen había sido ralentizada un 75%. «Esto no es alguien usando la última tecnología. Cualquiera puede hacerlo», declaró Farid a Associated Press. Una manipulación extremadamente sencilla, al alcance de cualquier persona en su casa con el programa de edición más simple del mercado. Un *cheap fake*, una falsificación barata. El vídeo se volvió viral, porque apelaba a la audiencia

adecuada y jugaba con sus sesgos. Apareció en un momento de máxima tensión entre Pelosi y Trump, después de que esta hubiese cuestionado públicamente la cordura del entonces presidente. La mayoría de las plataformas consideraban que no violaba su política y se negaron a retirarlo cuando la oficina de Pelosi lo requirió.[7]

A medida que avanzan las capacidades de creación de imágenes falsas, también lo hacen las herramientas de detección. Pero, en la guerra cognitiva, los aspectos esenciales tienen que ver con la psicología de los receptores. El veterano oficial de operaciones de información británico Steve Tatham explica los elementos necesarios para diseñar una acción de este tipo. La primera es preguntarse: ¿quién es la audiencia? La respuesta condicionará lo demás, porque la siguiente pregunta es: ¿en qué circunstancias esa audiencia modificaría su comportamiento? Puede parecer obvio, pero Tatham explica que, durante años, los cuerpos expedicionarios en Irak y Afganistán de Estados Unidos, Reino Unido y otros países de la OTAN han gastado fortunas en empresas de relaciones públicas expertas en el mensaje y en cómo hacérselo llegar a las poblaciones, sin plantearse si ese mensaje era el adecuado en ese lugar y para ese grupo de gente.[8]

El análisis de la audiencia sirve para integrar los elementos culturales correspondientes a las peculiaridades locales. Por ejemplo, el principio de autoridad: nos fiamos de la información que nos proporciona una persona a la que respetamos. La cadena RT siempre presenta a sus invitados como un «reputado profesor» o «prestigioso experto», aunque el individuo sea un cantamañanas. A veces, esa figura de «autoridad» puede resultar sorprendente: un estudio saudí sobre desradicalización de jóvenes yihadistas encontró que las figuras más eficaces en ese sentido no eran clérigos famosos o eruditos doctos en los textos islámicos, sino los futbolistas árabes con más proyección y éxito internacional. El mismo proceso ocurre con los *influencers*. Muchos regímenes autoritarios han descubierto los beneficios de recurrir a estas figuras para campañas de influencia o blanquear sus expedientes sobre derechos humanos.[9]

Seguimos con el principio de escasez, conocido en el marketing digital por esas ofertas o descuentos de los que podemos beneficiarnos, pero que «duran» unas pocas horas. Hay que comprar rápido. Que algo sea supuestamente escaso nos hace considerarlo más valioso. Lo mismo sucede con el conocimiento. Es el famoso «esto no lo verás en los medios». Al acceder a un grupo exclusivo que maneja información no accesible al gran público —quienes conocen la verdad sobre la pandemia, el plan secreto de la OTAN detrás de la guerra de Ucrania, o lo que quiere decir QAnon— nos convertimos en portadores de esa «verdad revelada» a la que otorgamos un valor excepcional. Un valor que hace que bajemos la guardia hacia su veracidad y plausibilidad. Este mecanismo es utilizado por muchas sectas para arrastrar a sus seguidores.

A finales de 2024 me sucedió algo curioso: encontré un vídeo en Instagram con imágenes de un fabuloso balneario natural en algún lugar de España por un precio ridículamente bajo, cuyos detalles supuestamente estaban en la descripción. Allí no aparecían, pero una leyenda te invitaba a unirte a cierto canal de Telegram con información sobre esta y otras ofertas. Al hacerlo, tu admisión tenía que ser autorizada por los administradores del canal, lo cual tardaba algunos días. Cuando finalmente fui aceptado y pude acceder al contenido, encontré un canal de noticias, la mayoría financieras, policiales y judiciales y meramente factuales, pero que a cada rato introducía sutilmente algunas narrativas islamófobas, antiinmigración y antiprogresistas. Una operación de algún grupo de extrema derecha, diseñada a partir del principio de escasez.

El diseño de la guerra cognitiva podría continuar con los 11 principios de Joseph Goebbels, el ministro de propaganda del nazismo, conocido por su frase «Una mentira repetida cien veces se convierte en una verdad». Aunque no existe un registro histórico que demuestre que Goebbels los recogiera en un único documento, la lista de sus principios ha sido recopilada por historiadores y especialistas:

1. Principio de simplificación y del enemigo único. Reducir los problemas a una dicotomía entre el bien y el mal, identificando un enemigo claro al que se culpa de todo. Facilita la movilización del público al ofrecer una narrativa sencilla.

2. Principio del método de contagio. Agrupar a los adversarios en una sola categoría, presentándolos como una amenaza común. Cualquier oposición queda deslegitimada al asociarse con otros enemigos impopulares.

3. Principio de la transposición. Atribuir al oponente los errores o acciones negativas propias. Desvía la atención de los propios fallos y se pone al adversario a la defensiva.

4. Principio de la exageración y desfiguración. Distorsionar la realidad y amplificar incidentes menores para hacer que parezcan amenazas graves. Genera miedo y refuerza la percepción de peligro constante.

5. Principio de la vulgarización. Utilizar un lenguaje simple y accesible para llegar a la mayor cantidad de personas. La propaganda debe ser comprensible incluso para los menos informados.

6. Principio de orquestación. Repetir los mensajes clave una y otra vez a través de distintos medios hasta que sean aceptados como verdad. La constancia en la repetición refuerza la credibilidad del mensaje.

7. Principio de renovación. Introducir continuamente nuevos argumentos o perspectivas para mantener la atención del público. Evita que los opositores tengan tiempo para responder eficazmente.

8. Principio de la verosimilitud. Presentar información sesgada o incompleta, combinando verdades parciales con mentiras para hacer que la propaganda parezca más creíble.

9. Principio de la silenciación. Evitar que las voces disidentes tengan espacio en la discusión pública, ya sea censurándolas directamente o restándoles visibilidad en los medios.

10. Principio de la transfusión. Apoyarse en creencias, prejuicios y tradiciones preexistentes para que el mensaje propagandístico tenga mayor aceptación y arraigue con facilidad en la población.

11. Principio de la unanimidad. Crear la ilusión de que la mayoría de la sociedad apoya la idea promovida, de modo que quienes piensan diferente se sientan aislados y eviten expresar su desacuerdo.

Al estudiar las campañas de influencia y manipulación contemporáneas, resulta sorprendente hasta qué punto se recurre a Goebbels. Tomemos un caso concreto: cuando en febrero de 2025 se presentó DeepSeek —la IA china— empezó a circular en redes y aplicaciones de mensajería un meme con tres cabezas de dragón, dos amenazantes y una tercera de carácter ridículo, dibujada con los ojos torcidos y con la lengua fuera. Las dos primeras cabezas representaban a Estados Unidos y China. La tercera, a la Unión Europea. Debajo de ellas aparecían algunos de los logros tecnológicos de cada uno: el dragón estadounidense tenía a OpenAI, Grok y Meta. El chino, a DeepSeek. Y el europeo… a los nuevos tapones de botella que se mantienen pegados al recipiente para evitar la generación innecesaria de plástico.

Un meme divertido. Pero lo que no resultaba evidente es que formaba parte de una campaña amplia para generar animosidad

contra la Unión Europea, recurriendo a muchos de los recursos apuntados arriba. Analicémoslo.

Presenta una figura negativa clara, la UE (principio de simplificación y enemigo único), buscando desacreditar a los *eurócratas* detrás de esa iniciativa ridícula (principio del método de contagio), y obviando la existencia de empresas tecnológicas en la Unión Europea presentándola como incapaz de producir nada excepto tonterías (principio de exageración y desfiguración).

Transmite este concepto a través de memes comprensibles para todo el mundo (principio de vulgarización) y con múltiples diseños diferentes (principio de orquestación). El meme vehicula una idea real —el problema del relativo atraso tecnológico y la falta de competitividad de la UE frente a los dos gigantes económicos— presentándola como una exageración gigantesca, como si la UE solo fuese capaz de fabricar tapones de plástico (principio de la verosimilitud). Al usar el formato meme, impide la reacción de posibles críticos, porque ¿cómo se responde a un meme? (principio de la silenciación).

Además, se apoya en un prejuicio asentado hacia la burocracia, ineficiencia y preocupación por parte de la UE por cuestiones que muchos ciudadanos consideran secundarias o irrelevantes (principio de la transfusión). Por último, al distribuirse a través de aplicaciones de mensajería y ser compartido por miles de personas, y siendo un chiste humorístico, se crea la ilusión de que todo el mundo opina igual (principio de unanimidad).

Tras este meme, aparentemente simple, hay nueve de los once principios de Goebbels.

LA CAÍDA DE LOS MEDIOS DE COMUNICACIÓN TRADICIONALES

Las elecciones del 6 de noviembre de 2024 se cerraron con una victoria incontestable de Donald Trump, quien había logrado una

suerte de hegemonía cognitiva sobre gran parte de la sociedad estadounidense. Por ejemplo, de los diez *streamers* más escuchados durante esa noche electoral, nueve eran abiertamente trumpistas.[10]

La cadena tradicional más seguida fue Fox News, que duplicó en audiencia a la siguiente, NBC News, y a enorme distancia de las demás como ABC, MSNBC o CBS. Fue la eclosión de una tendencia generalizada: estos formatos alternativos llevaban años creciendo sin parar ante el retroceso de unos medios tradicionales, por lo general hostiles a Trump, pero que prácticamente han caído en la irrelevancia fuera de las burbujas liberales de las principales ciudades del país.

A modo de ejemplo: el pódcast de Joe Rogan superaba los catorce millones y medio de oyentes por episodio,[11] 28 veces más que la audiencia de CNN. Solo el 8% de los adultos estadounidenses tiene a *The New York Times* como una de sus principales fuentes de información, cifra que cae al 3% en el caso de *The Washington Post*.[12]

Trump entendió esta dinámica y apeló a las audiencias de aquellos medios alternativos que más consumían sus compatriotas. En lugar de conceder una entrevista al programa *60 minutos* de la *CBS*, rompiendo un precedente de décadas, se paseó por los estudios de *podcasters* y *youtubers* de orientación conservadora, superestrellas entre sus fans, como Logan Paul, Theo Von, Lex Fridman o Andrew Schulz. En total, Trump realizó diecisiete horas de entrevistas con estos comunicadores.[13] Su aparición era siempre recibida con un interés inusitado: los episodios fueron número uno en visualizaciones. En conjunto, sus nueve intervenciones lograron más de cien millones de visualizaciones.[14]

Un sondeo del Pew Research Center de finales de octubre hacía una clasificación de los diez medios principales por los que se informaban los estadounidenses, que encabezaba Fox News, medio de cabecera para el 13% de los encuestados. Sin embargo, el 32 % mencionaba «otras fuentes», categoría que incluía YouTube, Facebook, pódcasts o publicaciones «marginales».[15] Casi el 40% de los jóvenes decía informarse por *influencers*.[16]

Entre los votantes registrados que leían periódicos o seguían las cadenas nacionales de televisión, la preferencia por Joe Biden era del 70% y el 55%, mientras que quienes seguían a Fox News y se informaban por redes sociales, se decantaban abrumadoramente por Trump.[17]

La victoria del republicano tuvo consecuencias inmediatas. Elon Musk empezó a dedicar esfuerzos y recursos a interferir electoralmente en Reino Unido, Alemania y Francia.[18] Pronto, Mark Zuckerberg, creador de Meta, anunció que la plataforma dejaría de colaborar con las organizaciones de verificadores con las que venía trabajando hasta la fecha, asegurando que tenían «demasiados sesgos políticos». Un guiño claro hacia los seguidores de un presidente que había lanzado públicamente más de 30.500 falsedades durante su primer mandato,[19] y al que la comprobación y desmentido de ese tipo de bulos le molestaba. «Las elecciones recientes parecen un punto de inflexión cultural hacia la priorización de la libertad de expresión de nuevo. Así que vamos a volver a nuestras raíces y enfocarnos en reducir errores, simplificar nuestras políticas, y restablecer la libre expresión en nuestras plataformas», declaró Zuckerberg a Fox News.[20] Otros grandes magnates estadounidenses, como el propietario de Amazon y *The Washington Post*, Jeff Bezos, o los directores ejecutivos de Google y Apple, Sundar Pichai y Tim Cook, hicieron claros esfuerzos para acercarse también a Trump.[21]

A finales de diciembre el Global Engagement Center, la institución encargada de analizar la desinformación extranjera y combatirla, echó el cierre ante la imposibilidad de aprobar la extensión presupuestaria necesaria para mantenerse en un Congreso dominado por los republicanos, que llevaban tiempo acusando a la institución de ser un órgano de vigilancia y censura contra los estadounidenses.[22] Dos meses después, el Gobierno de Trump desmanteló varios equipos de trabajo contra la desinformación y las operaciones de injerencia extranjeras dentro del FBI y la CISA, la agencia de ciberseguridad encargada de la protección de las infraestructuras.[23] El país quedaba

así en una posición mucho más vulnerable ante operaciones de manipulación e interferencia por parte de sus adversarios.

La decadencia de los medios tradicionales no es exclusiva de Estados Unidos. Según el informe «Digital News Report» del Instituto Reuters de la Universidad de Oxford, que analiza la situación de 47 países, el interés por la información ha caído en todos excepto Finlandia.[24] En España, solo el 33. % de los ciudadanos confía en las noticias, frente a un 40. % que desconfía y un 37% que evita exponerse a ellas.[25] Ni un solo medio es ampliamente percibido como fiable por la población, y solo algunos medios (la Cadena SER, RTVE y cabeceras regionales o locales) llegan o superan ligeramente el 50% en cuanto a confianza. Los resultados se dan indistintamente de la ideología política de los encuestados. Y, aunque el informe no establece una comparativa entre este tipo de medios y las redes sociales, es evidente que su uso como fuente de información no deja de crecer.[26]

Sin desmerecer el excelente trabajo que en ocasiones hacen algunos de estos nuevos profesionales, carecen de las salvaguardas que se imponen los medios convencionales serios: códigos deontológicos, estándares de verificación, organizaciones editoriales cuyo trabajo colectivo sirve para prevenir posibles errores individuales. Las plataformas de mensajería no comprueban si la información que circula en un chat colectivo o el enlace que alguien ha compartido es verídico o un simple rumor infundado, cuando no un bulo malintencionado. Y las redes sociales están desmantelando las ya insuficientes herramientas y equipos que lo hacían. Lo cual nos deja en manos de los manipuladores profesionales.

LA CONMOCIÓN RUMANA

Antes de que terminase 2024 tuvo lugar otro suceso disruptor. El 24 de noviembre, Rumanía se dirigía a las urnas para elegir al sucesor del presidente Klaus Iohannis, a quien la legislación electoral impedía

continuar en el cargo tras cumplir dos mandatos. Al acabar la jornada, el sexto país más grande de la Unión Europea descubría con estupor que el candidato más votado había sido alguien que, hasta hacía pocas semanas, era un completo desconocido para la mayoría de los rumanos: el ultraderechista Calin Georgescu.

Ninguna candidatura había alcanzado la mayoría absoluta, por lo que había que ir a una segunda vuelta, prevista para el siguiente 8 de diciembre, donde el país decidiría entre Georgescu, que había obtenido un 22,9% de los votos, y Elena Lasconi, del partido Unión Salvar Rumanía, la siguiente opción más votada, con un 19,1%.[27] Esa noche, las búsquedas del nombre de Georgescu en la versión rumana de Google se dispararon.

El candidato representaba una novedad en un panorama político marcado por el desencanto con la gestión de Iohannis, las promesas electorales incumplidas y una serie de problemas económicos derivados de la creciente inflación y la subida del precio de los alimentos y la vivienda.[28] Georgescu culpaba a la Unión Europea y a la OTAN, a las que también responsabilizaba de la guerra en Ucrania. Prometía cortar todo apoyo a Kiev y mantener excelentes relaciones con Rusia, cambiando radicalmente la orientación de la política exterior de las últimas décadas.

En sus vídeos en redes sociales, donde se le ve montando a caballo al estilo tradicional o practicando artes marciales —fue judoka en su juventud—, parecía un personaje fresco, interesado por la salud material y espiritual de Rumanía, por los problemas de sus compatriotas y su bienestar. Suficiente, al parecer, para que en el último tramo decidieran respaldarle.

Casado y con tres hijos, Georgescu es un experto en desarrollo sostenible y ha tenido varios cargos medianamente importantes en la Administración rumana y en la ONU relacionados con cuestiones medioambientales. Pero una búsqueda de información más profunda ofrece otros detalles oscuros. Es admirador de Corneliu Codreanu, el fundador de la Guardia de Hierro rumana, una organización fascista y

antisemita conocida por sus atrocidades, y del mariscal Ion Antonescu, el principal responsable del Holocausto en Rumanía. Georgescu es también antivacunas, escéptico del cambio climático, está en contra de los derechos LGTBIQ+ y difunde teorías de la conspiración, como que el hombre no ha llegado a la Luna, que los alimentos contienen nanotecnología o que una vez conoció a un «no humano» en la ONU.

¿Cómo era posible que un candidato presidencial que un mes antes apenas arrastraba una intención de voto de menos del 1% se hubiese convertido súbitamente en el favorito?

A principios de diciembre, el presidente Ioannis convocó una reunión del Consejo Supremo de Defensa Nacional para abordar esta cuestión, en la que se tomó la decisión de desclasificar los hallazgos de los servicios de inteligencia del país. El día 4 se hicieron públicos los documentos, que resultaron ser una auténtica bomba política. Ese mismo día, la Fiscalía y el Tribunal Superior de Casación y Justicia anunciaron la apertura de un caso contra Georgescu por «posibles violaciones de la legislación electoral y la comisión de otros delitos conexos».

Enjambres de cuentas en redes sociales vinculadas con Rusia llevaban tiempo promoviendo la candidatura de Georgescu. Viginium, la agencia estatal francesa de defensa contra operaciones de desinformación, había detectado cómo las páginas web de la red Pravda y los canales de Telegram asociados a esa operación, que los analistas franceses denominan «Portal Kombat»,[29] promovían activamente a Georgescu, de quien aseguraban que iba a prohibir el tránsito de grano a Ucrania para favorecer a los agricultores europeos, y cortar toda ayuda militar a Kiev, presentándole como un verdadero nacionalista opuesto a que su país fuese partícipe en guerras ajenas.

Dichos medios publicaban los mismos artículos en más de una docena de idiomas de la UE, probablemente para despertar simpatías hacia Georgescu entre los lectores prorrusos en esos países.[30] En el mismo sentido, investigadores rumanos con acceso al software especializado Osavul, utilizado por numerosos gobiernos e

instituciones para detectar campañas en internet,[31] vieron cómo cuentas del ecosistema ruso en X/Twitter amplificaban el perfil del candidato. Portal Kombat y esta red aprovechaban su pasado en la ONU para presentarle como alguien que conocía el sistema por dentro y que ahora se rebelaba contra su corrupción, denunciando las tramas de «pedofilia» entre las élites. «El Pizzagate es real», le atribuía Pravda, frase que el candidato no había dicho.[32]

La lista de injerencias continuaba: páginas de Facebook para promocionar el turismo y la cultura de múltiples ciudades rumanas de pequeño tamaño habían logrado reunir un número significativo de seguidores, y poco antes de la jornada electoral empezaron a difundir contenidos de apoyo a Georgescu. Redes de bots creadas en 2016 hicieron lo mismo.[33] Otras 24 cuentas falsas de Facebook creadas por la Alianza para la Unión de los Rumanos, un partido ultraderechista, también apoyaron a Georgescu además de a su propio candidato, al tiempo que atacaban a Iohannis por «dictador», y a Lasconi por globalista y «sirvienta de las élites». Sumaban en conjunto 935.000 usuarios.[34]

Uno de los documentos hablaba incluso de una «campaña de crecimiento de popularidad coordinada, ampliada a dos semanas de la fecha del escrutinio», y explicaba la evolución de los sondeos: si hasta el 5 de noviembre la intención de voto hacia Georgescu había sido inferior al 1%, esta había saltado al 6,2% en el período del 15 al 20 de noviembre, y a un 10,6% entre el 20 y el 21 de noviembre, antes de que se produjese el incremento súbito final.

También aportaba claves que explicaban el aumento, como una red de 25.000 cuentas en TikTok asociadas con el candidato, algunas creadas hacía mucho —hasta en 2016— y dedicadas a otras temáticas, pero después puestas al servicio de Georgescu. También mencionaba un canal de Telegram llamado «Propagator» desde el que se habían coordinado las acciones de los voluntarios pro-Georgescu para difundir sus mensajes de forma masiva evitando las restricciones de Tik-Tok y maximizando el impacto del algoritmo.

Georgescu, según el informe, había declarado a la Autoridad Electoral Rumana que carecía de presupuesto para dicha campaña. Pero el documento establecía que una cuenta llamada «bogpr» había realizado donaciones vía TikTok de más de un millón de euros a las cuentas mencionadas, más pagos por valor de 381.000 dólares durante el último mes antes de las elecciones a uno de los usuarios más implicados. La cuenta pertenecía a un programador rumano de treinta y seis años de edad residente en Sudáfrica llamado Bogdan Peschir,[35] cuyos ingresos no podían justificar cantidades semejantes. ¿De dónde había salido el dinero?

En total, según otro documento, se habían contabilizado más de 85.000 ciberataques por un «actor cibernético estatal con abundantes recursos», pero no identificado por ningún nombre.[36] Datos y contraseñas gubernamentales emergieron poco después en foros de cibercriminales en Rusia.

La noche siguiente a la publicación de estos informes, Georgescu mantuvo un encuentro clandestino con un grupo de hombres en un rancho de caballos a las afueras de Bucarest, propiedad de su amigo el empresario Mohamed Jbara.[37] Pronto, esa reunión cobraría una enorme relevancia. Mientras tanto, las informaciones de los servicios de inteligencia tuvieron un peso esencial en el debate que entonces estaba teniendo lugar en el seno del Tribunal Constitucional de Rumanía. El día 6, la corte decretó la anulación de la primera vuelta de las elecciones, al considerar que se había vulnerado el artículo 146(f) de la Constitución, que subrayaba la necesidad de garantizar la corrección y legalidad del proceso electoral. Era la primera vez en la historia que una democracia anulaba unas elecciones por un presunto caso de interferencia rusa.

Georgescu trató de movilizar a sus seguidores, aunque solo reunió a unos pocos centenares de personas. Mientras tanto, Portal Kombat lo presentó como un mártir, repitiendo sus alegaciones de sufrir un golpe de Estado.[38] La propaganda rusa explotó los sucesos durante

meses para sostener que Occidente solo apoyaba la democracia cuando le gustaban los resultados electorales.

En los días siguientes, miles de rumanos salieron a las calles, algunos a apoyar a Georgescu y otros, apoyando la decisión del Tribunal Constitucional. El 8 de diciembre, el día que el país debía volver a las urnas, la policía interceptó varios coches en diferentes puntos de la región de Bucarest y detuvo a una veintena de personas. En los vehículos se encontraron dos pistolas, varios cuchillos y espadas, bates de béisbol, cascos, equipos de protección tácticos, material pirotécnico, un dron profesional y efectivo por valor de 20.000 euros. Los hombres, aparentemente, se dirigían a la capital para causar disturbios. Según la acusación policial, el dinero era para «incitar a algunos individuos a cometer crímenes durante reuniones públicas no autorizadas y recompensarlo».[39] El líder del grupo era un viejo conocido de las autoridades y amigo de Georgescu, un mercenario llamado Horatiu Potra. La persona con la que el candidato se había reunido en el rancho días antes.

Potra es un personaje de película. Calvo, musculoso, en buen estado físico pese a estar bien entrado en la cincuentena, este antiguo estudiante de ingeniería reconvertido en mercenario es una de las figuras clave en toda esta trama. Veterano de la Legión Extranjera Francesa —un servicio de cinco años por el que le había sido concedida la ciudadanía gala—, Potra llevaba desde 1997 realizando trabajos militares privados en Oriente Medio y África. Había sido miembro del equipo de seguridad del emir de Qatar y del presidente de la República Centroafricana, Ange-Félix Patassé, hasta que fue expulsado del poder en 2004.

Potra se «especializó» en el continente africano: Sierra Leona, Chad, Burkina Faso, Costa de Marfil. Después trabajó para un millonario australiano de origen rumano llamado Frank Timis, proporcionando seguridad a las minas de oro. Había sido herido ocho veces y tomado como prisionero en otras dos ocasiones. Tenía acciones en una empresa que vendía diamantes en los mercados de

Amberes y Tel Aviv, y poseía propiedades inmobiliarias en el sur de Francia y en la propia Rumanía.[40] En África, se hacía llamar «Teniente Henry».

Pocos años antes había creado su propia compañía de mercenarios, RALF (el acrónimo de «Rumanos que sirvieron en la Legión Extranjera Francesa»), y desde 2022 desarrollaba sus actividades en la República Democrática del Congo, proporcionando seguridad al Gobierno congoleño contra la insurgencia del M23, apoyada por Ruanda. Potra, de hecho, acababa de regresar de allí pocos días antes. Aunque algunas informaciones periodísticas le vinculan con el Grupo Wagner, no hay nada que indique una relación directa con la empresa paramilitar creada por Yevgueni Prigozhin. La confusión parece venir de las similitudes en el tipo de actividades de ambas compañías —además de cierto parecido físico entre ambos individuos—, y de los contactos de ambos con el Kremlin.

Según la publicación alemana *Taz*, Potra habría recibido pagos de Moscú para entrenar a los guardaespaldas de Faustin-Archange Touadéra, el presidente de la República Centroafricana y uno de los principales aliados de Rusia en África.[41] Tras su arresto, la investigación demostró que también era un visitante frecuente de la embajada rusa en Bucarest, y que había evidencias fotográficas de que había viajado a Moscú. Potra fue puesto en libertad con cargos poco después, no sin que antes las autoridades registrasen su casa, donde encontraron más de dos millones de euros en efectivo, en diferentes divisas, cuyo origen y propósito se negó a explicar.

Mientras tanto, investigadores y analistas seguían encontrando información sobre el modo en el que se había logrado que la presencia pública de Georgescu se disparase en redes. Resultó que TikTok usaba uno de los algoritmos más manipulables. El 9 de diciembre, periodistas del medio rumano Recorder realizaron un experimento, creando un falso candidato electoral que prometía dos kilos de oro a cada ciudadano de Rumanía si salía elegido. Añadiendo unas pocas líneas de código, el vídeo alcanzó un millón de visualizaciones en

apenas una hora.[42] Una investigación de la ONG internacional Global Witness también descubrió que, a esas alturas, TikTok recomendaba el contenido pro Georgescu entre 4,6 y 14 veces más que el de su rival Lasconi.[43]

DFRLab examinó el canal de Telegram «Propagator» y descubrió que había distribuido más de 1.800 materiales de campaña y otros contenidos, especialmente vídeos y memes, animando a los miembros del grupo y sus voluntarios a que los compartiesen en TikTok y otras plataformas pero con «creatividad», añadiendo sus propios mensajes y leyendas. De esta manera, el algoritmo de TikTok, por ejemplo, no solo no penalizaba el contenido como coordinado, sino que lo identificaba como potencialmente viral e incrementaba automáticamente su visibilidad. Estos vídeos, además, no estaban clasificados como políticos, por lo que su distribución era mucho mayor que la de los otros candidatos, e incluso habían circulado durante la jornada electoral, lo que es ilegal según la legislación rumana. Propagator también compartió tutoriales sobre herramientas de edición para crear vídeos en redes sociales, como CapCut y Filmora, cuyo formato es favorecido por las plataformas con más visualizaciones. Para el día de la votación, la cuenta de TikTok había acumulado más de 540.000 seguidores.[44]

Propagator había sido creada en junio de 2024 y llegó a tener casi 8.000 miembros. Pero solo era el epicentro de una comunidad mucho mayor. El 20 de julio anunció a sus suscriptores que habían creado 41 grupos diferentes, uno por cada región administrativa de Rumanía, y les animó a unirse a la suya. Eso les permitía tener una estructura organizada a nivel local, y movilizarla llegado el momento. «El canal Propagator intentaba alimentar un sentido de comunidad. Sus operadores frecuentemente se dirigían a sus seguidores como "Queridos" y creaban la impresión de que esos partidarios eran parte de algo significativo y con sentido», escribe Victoria Olari, autora del informe de DFRLab. En un momento dado, Georgescu envió un vídeo

titulado «Mensaje para los miembros», lo que sugería algún tipo de coordinación directa entre el candidato y los responsables del canal.

Por su parte, el servicio de inteligencia rumano (SRI) había recopilado en un anexo público a sus informes los nombres de muchos de los *influencers* que habían participado en la campaña de promoción —más de un centenar, con un total de 8 millones de seguidores en conjunto—, forzándoles a posicionarse públicamente. Uno de ellos, llamado Alex Stremitanu, con más de 50.000 seguidores, publicó un vídeo admitiendo que había sido «estúpido» por tomar parte en esa campaña, que le había sido descrita como un esfuerzo por movilizar a la gente a que votase. Se le había instruido para poner ciertos *hashtags*, como «elecciones presidenciales 2024», que luego atraían a bots a la sección de comentarios donde ponían enlaces a contenidos pro Georgescu.

Las pesquisas habían revelado que a muchos se les había pagado hasta 1.000 euros por distribuir un video creado por la empresa FA Agency, creada en Sudáfrica. Otros habían sido financiados a través de una plataforma llamada FameUp, dedicada a la monetización de las actividades de promoción en redes sociales.[45] El Ministerio del Interior rumano explicó que «parte del texto de apertura» de las piezas de muchos *influencers* era *idéntica* a la usada meses antes en las elecciones de Moldavia a favor del candidato prorruso Alexandr Stoianoglo. Pero, a diferencia de Stremitanu, otros *influencers* de la lista del SRI negaron haber sido pagados, y aseguraron haberlo hecho por convicción propia.

La anulación de las elecciones había creado un debate tanto dentro como fuera de Rumanía sobre los desafíos de las democracias a la hora de defenderse ante estos procesos de manipulación electoral en la esfera digital. Mientras no faltaban voces que aplaudían, otros lo veían como un peligroso antecedente antidemocrático. «La decisión de anular las elecciones presidenciales parece haber estado motivada por la insatisfacción provocada por la victoria del candidato "equivocado" en la primera vuelta más que por un compromiso genuino de

preservar la integridad electoral», escribió el profesor ucraniano Anton Shekhovtsov, director del Centro para la Integridad Democrática de Viena, autor de un libro sobre las relaciones entre el Kremlin y los movimientos europeos de extrema derecha y nada sospechoso de simpatías prorrusas. «Aunque la preocupación por la intromisión rusa, que se ha convertido en una característica permanente de todos los procesos electorales occidentales, no es infundada ni debe desestimarse, las pruebas presentadas eran insuficientes para justificar una medida tan radical como la anulación de las elecciones», sostenía Shekhovtsov.[46] Y lo cierto es que nadie había obligado a los rumanos a votar a Georgescu a punta de pistola. El escándalo, de hecho, solo sirvió para reforzar su candidatura. A mediados de enero de 2025 volvía a liderar las encuestas, con un 38% en intención de voto.

Pero el 26 de febrero Georgescu fue detenido durante una redada llevada a cabo en 47 localizaciones diferentes, incluida otra vez la vivienda de Horatiu Portra. Los fiscales encontraron un pequeño arsenal de armas de fuego, munición de asalto y, en casa de Potra, efectivo por valor de otros 900.000 euros en una caja fuerte oculta bajo un suelo de tarima. La fiscalía tenía conocimiento de ciertas conversaciones y grabaciones presuntamente incriminatorias, incluida una entre Georgescu y Marian Motocu, el dirigente de una organización fascista vigilada por las autoridades por su presunto carácter extremista. Georgescu había dicho: «Si las cosas van bien, empezaré en enero. Hay un plan, una estrategia que solo yo conozco. Cuando llegue el momento, como te dije hace un año, las cosas no se han alineado por muchas razones, entonces tendrás tu lugar en esta acción».[47] En la redada fueron detenidas 27 personas. A Georgescu se le acusó de intento de alteración del orden constitucional, creación de una organización de naturaleza fascista, racista o xenófoba, y declaraciones falsas sobre bienes y fuentes de financiación de campañas electorales. También se le imputaron delitos como «promover, en público, el culto a personas culpables de crímenes de

genocidio contra la humanidad», o «iniciar o establecer una organización de carácter antisemita».[48]

«LA DEBILIDAD DE LA CIVILIZACIÓN OCCIDENTAL ES LA EMPATÍA»

El 20 de enero de 2025, Donald Trump volvió a tomar posesión del cargo en el Despacho Oval. Una de sus primeras acciones fue firmar un decreto presidencial revirtiendo la prohibición de TikTok aprobada por el Congreso, tal vez pensando en las ventajas de poder poner esta plataforma a su servicio (como ya había ocurrido con X/Twitter) si, como se esperaba, era finalmente adquirida por un estadounidense. Para febrero, Trump había logrado la aprobación en el cargo de un militante antivacunas como secretario de Salud, a una agente de influencia de Rusia y otras dictaduras como directora nacional de Inteligencia, a un simpatizante de QAnon al frente del FBI y a un teórico de la conspiración como el número dos de este último.

Por aquellas fechas volví a darme un paseo por los canales de QAnon en español, y lo que vi me chocó bastante: si en 2021 los contenidos eran una colección de teorías de la conspiración detrás de otra, ahora todos versaban sobre Donald Trump, Elon Musk, Javier Milei, criptomonedas y el argumentario de Rusia acerca de Ucrania. La fusión entre estos universos era total.

La Administración Trump encamina a Estados Unidos a un cambio de rumbo de consecuencias profundas, no solo para el propio país, sino para todo el mundo. Por primera vez, muchos observadores consideran que existe una posibilidad real de que el país acabe convertido en una autocracia, y la manipulación cognitiva habrá tenido mucho que ver. La correlación entre mentira y autoritarismo está bien demostrada, como ya estableció Hannah Arendt en *Los orígenes del totalitarismo*, donde escribió: «El sujeto ideal del régimen totalitario no es el nazi convencido ni el comunista convencido, sino la gente para la que la distinción entre hecho y ficción ya no tiene sentido».

Hoy existe una batalla contra el conocimiento científico en muchos sectores de la sociedad, y los movimientos anticiencia ganan terreno. En 2017, un 10% de los estadounidenses creían que los *chemtrails* eran una realidad.[49] Dos años después, la cifra había subido al 40 %,[50] y, aunque no existen datos actualizados, a juzgar por la creciente presencia de esta teoría de la conspiración en plataformas y medios alternativos, nada hace pensar que el porcentaje haya descendido. Este escepticismo hacia la ciencia se concentra sobre todo en determinados sectores políticos y lugares. Según una encuesta de la firma de demoscopia sobre cuestiones de salud KFF, en enero de 2025 un 40% de votantes republicanos estaba convencido de que la vacuna del COVID-19 había matado a más gente que el propio virus.[51]

Señalando la llegada de un nuevo *Zeitgeist* o «espíritu de los tiempos», Estados Unidos ha experimentado un cambio de paradigma cultural donde imperan reglas diferentes. Preceptos morales de larga data, como la idea de que el racismo es algo malo o de que el grande no debe abusar del pequeño, están siendo abolidas, sustituidas por una nueva moralidad en la que el fuerte (y el rico) tiene derecho a todo aquello que esté en condiciones de adquirir con dinero o por la fuerza, mientras que el pobre o débil es avasallado, sometido, arrinconado y desechado. «La debilidad fundamental de la civilización occidental es la empatía», le dijo Elon Musk a Joe Rogan a finales de febrero de 2025.[52]

Lo que está emergiendo es una nueva era, una suerte de neomedievo donde un pequeño grupo de señores tecnofeudales y oligarcas casi omnipotentes toman decisiones que nos afectan a todos y el poder se apoya en nuevos cultos seudorreligiosos, en algunos casos totalmente irracionales, como QAnon. Ese cambio de mentalidad supone la victoria absoluta de una guerra cognitiva que algunos actores se han pasado años alimentando. Probablemente, otros países tomarán también ese mismo sendero muy pronto.

Las experiencias de Estados Unidos y Rumanía prueban que ciertas técnicas de manipulación funcionan, especialmente si son desplegadas

a lo largo del tiempo. Y lo que funciona tiende a ser imitado.

Lo que hemos visto es solo el principio.

AGRADECIMIENTOS

Suele decirse que un libro es siempre resultado del esfuerzo de muchas personas. Este no iba a ser una excepción, así que quiero dar las gracias aquí a todos ellos sin cuya ayuda *Guerras cognitivas* sería un libro mucho peor, o no existiría. En primer lugar, a Álvaro Palau y Arpa Editorial, por haber creído en mí antes que en el proyecto, y por haber visto su potencial desde el primer minuto. A David Remartínez, por todo el trabajo de edición, especialmente esas jornadas sin dormir sin las cuales el libro no habría llegado a tiempo a la imprenta. Y, naturalmente, a todos los que han accedido a ser entrevistados, algunos de ellos hace ya bastante tiempo, cuando no podían saber que iban a acabar en estas páginas porque la idea de «guerras cognitivas» no existía todavía.

También al diario *El Confidencial*, por permitirme ir publicando a lo largo de estos años muchas de las investigaciones y reportajes que luego han tenido cabida en este libro. A mis padres, sin cuyo ejemplo y apoyo siempre incondicional yo no sería quien soy hoy. A mis amigos de verdad, a quienes no necesito decir por qué (cada uno de ellos lo sabe), y especialmente a Ángel, por la inspiración durante todos estos años. A Carlos, Simona y los peques, por todo el amor y los buenos momentos. A Amanda y Gabriel, por esa buhardilla sevillana en la que escribí tres capítulos del libro. A Grettel, por prácticamente todo, pero en este caso por haber sabido encarrilarme en la redacción del libro cada vez que me salía del camino y haberse ocupado de todo cuando yo estaba en un estado alterado de conciencia mientras le daba a la tecla. Y por supuesto, a Isla, la luz de mi vida, sin la cual mi existencia ya no tendría sentido. Verte crecer es lo mejor que me ha pasado nunca.

Si tienes algo que contarme sobre el mundo de las guerras cognitivas, escríbeme a contacto@danieliriarte.es

Más información:
www.guerrascognitivas.com

NOTAS

1. ¿QUÉ ES LA GUERRA COGNITIVA?

1. Faivre, A., «Burkina: ce que dit le blocage du convoi militaire français à Kaya'», *Le Point*, noviembre de 2021.
2. Marchant de Abreu, C., «Social media users falsely claim that French soldiers are arming terrorists in Mali», octubre de 2022.
3. «Interactive: Mali speaks», Al Jazeera, enero de 2013.
4. Estas prácticas llevaron a la experta Candace Rodeaux a definir a Wagner no como mercenarios, un término que siempre fue problemático por los vínculos claros que existían entre esta organización y la inteligencia militar rusa, sino como un «cártel paramilitar». Véase el documental *Shadow Men: Inside Wagner, Russia's Secret War Company*, *Wall Street Journal*, 9 de junio de 2023.
5. Freudenthal, E.; Gebauer, M.; Huon, P.; Nsaibia, H.; Poop, M.; Sandberg, B.; Van der Weide, Y., «People Collected Severed Arms, Legs and Heads - France's War in West Africa», *Der Spiegel*, junio de 2021.
6. Burke, J., «France says Russian mercenaries staged 'French atrocity' in Mali'», abril de 2022.
7. «More-troll Kombat», informe de la firma Graphika y del Instituto de Internet de la Universidad de Stanford, diciembre de 2020.
8. Las autoridades de Níger se negaron a revelar si los autores de los disparos habían sido las tropas francesas o miembros de la gendarmería nacional nigerina que viajaba en apoyo del convoy.
9. La descripción de la escena se basa en la reconstrucción del incidente incluida en este reportaje, a partir de lo que varios testigos contaron a diversos medios y lo que publicaron en redes sociales: «The war on Téra», Rob Lemkin y Femi Nylander, Africa Is a Country, 14 de diciembre de 2021.
10. González, M., «Europa retira sus últimas tropas del Sahel y deja el campo libre a Rusia», *El País*, 28 de marzo de 2024.
11. «France to reduce troops in West and Central Africa to 600, say sources», *France 24*, 17 de junio de 2024.
12. El Centro Superior de Información de la Defensa (CESID), antecesor del actual Centro Nacional de Inteligencia (CNI), había sido creado apenas dos años antes en sustitución del Servicio Central de Documentación (SECED) de la época franquista, del que venían Lejarza y sus compañeros.

13. Lejarza, M.; Rueda, F., *Yo confieso. 45 años de espía*, Roca Editorial, 2019.
14. Pacepa, I. M.; Rychlack, R.J, *Disinformation*, WND Books, 2013.
15. «Descubriendo El Bruc y la historia del famoso tambor», *Crónica Global, El Español*, 9 de septiembre de 2020.
16. Tatham, S., *Information Operations*, Howgate Publishing Limited, 2024.
17. «Operation Silkman: What was the last solely British military campaign?», *Force News*, 28 de junio de 2021.
18. Bing, C.; Schectman, J., «Pentagon ran secret anti-vax campaign to undermine China during pandemic», Reuters, 14 de junio de 2024.
19. *Ibid*.
20. *Ibid*.
21. «Information Manipulation: A Challenge for Our Democracies», CAPS - Ministerio para Europa y Asuntos Extranjeros y IRSEM - Ministerio de las Fuerzas Armadas de Francia, agosto de 2018.
22. Krieg, A., *Subversion: The Strategic Weaponization of Narratives*, Georgetown University Press, 2023.
23. «People Hacking: The Psychology of Social Engineering», charla del hacker ético Harl en el evento Access All Areas III, 7 de marzo de 1997.
24. Du Cluzel, F., «Cognitive Warfare», Innovation Hub de la OTAN, junio-noviembre de 2020.
25. Luberisse, J., *Cognitive Warfare in the Age of Unpeace: Strategies, Defenses, and the New Battlefield of the Mind*, Ed. Fortis Novum Mundum, noviembre de 2023.

2. ESTADOS, EJÉRCITOS VIRTUALES Y PLATAFORMAS

1. El poder blando puede definirse como la capacidad de un estado «para persuadir a otros países evitando el uso de la fuerza o la coerción, valiéndose de medios más sutiles, como su cultura, su modelo social o sus valores políticos». Véase «¿Qué es el poder blando?», Rodrigo Castellanos, *El Orden Mundial*, 18 de agosto de 2020.
2. Nye, J. S., «Today, It's a Question of Whose Story Wins'», *Los Angeles Times*, 28 de julio de 2004.
3. «El Regimiento de Operaciones de Información del Ejército echa a andar», *InfoDefensa.com*, 23 de julio de 2019.
4. Tatham, S., *Information Operations*, Howgate Publishing Limited, 2024.
5. *Ibid*.
6. «Rolling Stone's military psy-ops expose: 5 takeaways», *The Week*, 8 de enero de 2015.
7. Hastings, M., «Another Runaway General: Army Deploys Psy-Ops on U.S. Senators», *Rolling Stone*, 24 de febrero de 2011.

8. Véase por ejemplo «Informe: La UE es "cómplice"de la venta de migrantes como esclavos por 12 dólares", RT en Español, 31 de enero de 2025.
9. Este artículo de RT Deutsch, por ejemplo, contiene la siguiente frase: «Por encima de todo esto se alza la gigantesca Torre de Babel de la euroburocracia. Su grupo voraz de funcionarios igualmente inútiles devora fortunas enteras e inunda Europa con decenas de millones de inmigrantes, convirtiendo su "jardín floreciente" en un enorme vertedero de basura». «Europa – von Macron und Scholz zurück zu de Gaulle und Adenauer», Wladimir Moschegow, RT Deutsch, 22 de febrero de 2025. Encontrar ambos ejemplos en alemán y español mientras redactaba este texto, el 4 de marzo de 2015, apenas me llevó unos minutos, porque solo tuve que poner en el buscador de ambas páginas las palabras «migrantes» y «Unión Europea»: en ambos casos, era el primer resultado que aparecía.
10. Una comparativa interesante sobre las diferentes versiones de RT se encuentra en el volumen «RT in Europe and beyond - The Wannabe Elite of the Anti-Elites», un informe de 2022 del Centro para la Integridad Democrática de Viena, al que contribuyo con un capítulo sobre RT en Español.
11. Bradshaw, S.; Howard, P. N., «Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation», informe del Instituto de Internet de Oxfor (OII), julio de 2017.
12. *Ibid*.
13. Bradshaw, S.; Howard, P. N., «The Global Disinformation Order: 2019 Global Inventory of Organized Social Media Manipulation», informe del Instituto de Internet de Oxfor (OII), 4 de septiembre de 2019.
14. Bradshaw, S.; Howard, P. N., «Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation», informe del Instituto de Internet de Oxford (OII), 13 de enero de 2021.
15. El artículo, en ruso, se titula «Comisarios de Internet» y está firmado por Anna Polyanskaya, Andrei Krivov e Ivan Lomko. Aparece mencionado (sin dar ninguna referencia) en «Invasion of the troll armies: from Russian Trump supporters to Turkish state stooges», Leo Benedictus, *The Guardian*, 6 de noviembre de 2016.
16. Jedrzejewska, K., «Hasbara: Public Diplomacy with Israeli Characteristics», *Torun International Studies*, n.º 1 (13), 2020.
17. Tatham, S., *Information Operations*, Howgate Publishing Limited, 2024.
18. Liphshiz, C., «Israel Recruits 'Army of Bloggers' to Combat anti-Zionist Web Sites», *Haaretz*, 19 de enero de 2009.
19. Kuperboim, R., «Thought-police is here», *Ynet*, 7 de octubre de 2009.
20. Stern, G.; Hoffman, S., «Government to use citizens as army in social media war», *The Jerusalem Post*, 14 de agosto de 2013.

21. Shabi, R.; Kiss, H., «Wikipedia editing courses launched by Zionist groups», *The Guardian*, 18 de agosto de 2010.
22. Cohen, M., «Both Sides Fight Israeli-Palestinian Conflict on the Internet», *Haaretz*, 7 de enero de 2009.
23. «Online tool helps social media accounts amplify pro-Israel messages», *DFR Lab*, 11 de junio de 2024.
24. Tatham, S., *Information Operations*, Howgate Publishing Limited, 2024.
25. «Investigation into Russian military units engaged in psychological operations (PSYOP) and hacking attacks», *Molfar*, 2024.
26. Dixon, R., «Meet Margarita Simonyan, queen of Russia's covert information wars», 11 de septiembre de 2024.
27. «Question That: RT's Military Mission» *DFRLab*, Medium, 8 de enero de 2018.
28. «The Kremlin's weapons of deception: 7 things you need to know about RT and Sputnik», *EUvsDisinfo*, 4 de marzo de 2022.
29. *Ibid*.
30. Michel, C., «It turns out Russia isn't the only country turning Facebook and Twitter against us», *The Washington Post*, 23 de agosto de 2018.
31. Lima, C., «Facebook removes hundreds of accounts tied to Iran, Russia», *Politico*, 21 de agosto de 2018.
32. «The information space around Iran», Graham Brookie e Iain Robertson, DFRLab, 9 de enero de 2020.
33. Brooking, E. T.; Kianpour, S., «Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century», informe del Atlantic Council, 2020.
34. Pérez Colomé, J., «Facebook elimina páginas iraníes de desinformación que operaban en España», *El País*, 31 de enero de 2019.
35. Tatham, S., *Information Operations*, Howgate Publishing Limited, 2024.
36. Fielding, N.; Cobain, I., «Revealed: US spy operation that manipulates social media», *The Guardian*, 17 de marzo de 2011.
37. «Unheard Voice - Evaluating five years of pro-Western convert influence operations», informe de *Graphika* y el Observatorio de Internet de Stanford, 2020.
38. Nix, N., «Facebook, Twitter dismantle a U.S. influence campaign about Ukraine», *The Washington Post*, 24 de agosto de 2022.
39. Nakashima, E., «Pentagon opens sweeping review of clandestine psychological operations», *The Washington Post*, 19 de septiembre de 2022.
40. Schectman, J.; Bing, C., «Exclusive: Trump launched CIA covert influence operation against China», Reuters, 14 de marzo de 2024.
41. Conversación del autor con un analista de la UE experto en desinformación china, 2020.

42. Barragán, C.; Andrés, E., «Retrato de los Wolf Warriors, la agresiva diplomacia china que aterriza en Europa», *El Confidencial*, 24 de abril de 2020.
43. Colville, A.; Bandurski, D., «Total War for Global Minds», *China Media Project*, 7 de enero de 2025.
44. Wuthnow, J., «China's New Info Warriors: The Information Support Force Emerges», *War On The Rocks*, 24 de junio de 2024.
45. Hanso, T., «China's New Information Support Force - Military Lessons Fron Ukraine», informe del Centro Internacional para la Defensa y Seguridad (ICDS) de Estonia, diciembre de 2024.
46. Bristow, M., «China's internet "spin doctors"», *BBC News*, 16 de diciembre de 2008.
47. Wong, T., «China: The patriotic "ziganwu" bloggers who attack the West», *BBC News*, 21 de octubre de 2021.
48. Tatham, S., *Information Operations*, Howgate Publishing Limited, 2024.
49. MacAskill, E., «British army creates team of Facebook warriors», *The Guardian*, 31 de enero de 2015.
50. Owen, G., «Ministers accused of a cover up as it is revealed shadowy army unit DID spy on British critics of Covid lockdown policies», *The Daily Mail*, 25 de noviembre de 2023.
51. Silverman, J., «France Is Flooding Africa With Fake News», *The New Republic*, 28 de diciembre de 2020.
52. «Removing Coordinated Inauthentic Behavior from France and Russia», Nathaniel Gleicher, Head of Security Policy, y David Agranovich, en la página oficial de Meta, 15 de diciembre de 2020.
53. «More-Troll Kombat - French and Russian Influence Operations Go Head to Head Targeting Audiences in Africa», informe de *Graphika* y el Observatorio de Internet de Stanford, diciembre de 2020.
54. Scott, M.; Braun, E., «France feuds with Facebook over disinformation claims», 17 de diciembre de 2020.
55. «Twitter Says Troll Accounts Linked to Russia Were Actually Venezuelan, Revises Data», *The Moscow Times*, 21 de febrero de 2019.
56. «La Infosfera Marroquí: lobos disfrazados de corderos», Monitor Disinfo, 2024.
57. Carrión, F., «Fuera periodistas; bienvenidos influencers españoles: la estrategia de Marruecos para blanquear la ocupación de Dajla», *El Independiente*, 8 de febrero de 2025.
58. Bigas Formatjé, N., «La invisibilidad en redes: el efecto "shadow ban"», Universitat Oberta de Catalunya, 25 de enero de 2024.
59. Fowler, G. A., «Shadowbanning is real: Here's how you end up muted by social media», *The Washington Post*, 27 de diciembre de 2022.

60. «Meta's Broken Promises - Systemic Censorship of Palestine Content on Instagram and Facebook», informe de Human Rights Watch, 2023.
61. Rodríguez, O., «Qué hay detrás de las restricciones y supresiones de contenido sobre Palestina en Instagram y Facebook», *Eldiario.es*, 15 de octubre de 2024.
62. «Analysis of Twitter algorithm code reveals social medium down-ranks tweets about Ukraine», *The New Voice of Ukraine*, 2 de abril de 2023.
63. Wakabayashi, D., «YouTube Sets New Policies to Curb Extremist Videos», *The New York Times*, 18 de junio de 2017.
64. Tufekci, Z., «YouTube, the Great Radicalizar», *The New York Times*, 10 de marzo de 2018.
65. Fang, L., «Twitter Aided the Pentagon in Its Covert Online Propaganda Campaign», *The Intercept*, 20 de diciembre de 2022.
66. Mozur, P., «How Telegram Became a Playground for Criminals, Extremists and Terrorists», *The New York Times*, 7 de septiembre de 2024.
67. Suosalo, I., «The Kremlin Has Entered the Chat», *Wired*, 27 de abril de 2023.
68. «Durov in Detention: The End of Tech Titan Immunity?», Andrei Soldavot e Irina Borogan, 27 de agosto de 2024.
69. Antoniuk, D., «Telegram says it will share phone numbers and IP addresses of "bad actors" to authorities», *The Record*, 23 de septiembre de 2024.
70. Este extremo me fue confirmada por agentes de la Comisaría General de Información de la Policía Nacional española a finales de 2024. Véase también «Telegram ya ha entregado datos de usuarios españoles a la Policía: la caza ya ha comenzado», *El Economista*, 4 de octubre de 2024.
71. Trofimov, Y., «Russia's Military Fears for Its Secrets After Telegram Founder's Arrest», *The Wall Street Journal*, 29 de agosto de 2024.
72. Melkozerova, V., «"Russians do everything vía Telegram". Pavel Durov's arrest upends Kremlin military comms», *Politico*, 26 de agosto de 2024.
73. «Iranian Messaging Platforms Unveil Advertising Services and Capabilities for Upcoming Elections», Ministry of ICT, Irán, 9 de julio de 2024.
74. *TikTok, l'ombre chinoise*, documental de Elsa Guiol, emitido *por* France TV el 3 de diciembre de 2023.
75. Méndez, M. Á., «El jefe tecnológico que dimitió del Pentágono porque cree que se acerca otro Pearl Harbour», *El Confidencial*, 18 de diciembre de 2021.
76. Lutkevich, B., «TikTok bans explained: Everything you need to know», *TechTarget*, 18 de febrero de 2025.
77. Gerken, T.; McMahon, L., y Rahman-Jones, I., «What does Trump's executive order mean for TikTok and who might buy it?», *BBC News*, 22 de enero de 2025.

3. ¿PARA QUÉ SIRVE UN TROL?

1. Aro, J., «My Year as a Pro-Russia Troll Magnet: International Shaming Campaign and an SMS from Dead Father», *Yle*, 9 de noviembre de 2015.
2. «NATO's information expert Jessikka Aro turned out to be a convicted drug dealer», *MV-Lehti*, 24 de febrero de 2016.
3. «Inside Russia's Notorious 'Internet Research Agency' Troll Farm», *Spyscape*, 11 de abril de 2022, actualizado en septiembre de 2024.
4. Pomerantsev, P., *This Is Not Propaganda: Adventures in the War Against Reality*, Ed. PublicAffairs, 2019.
5. *Ibid*.
6. Volchek, D., «Inside The "Propaganda Kitchen" - A Former Russian "Troll Factory" Employee Speaks Out», *RFE/RL*, 29 de enero de 2021.
7. *Ibid*.
8. Pomerantsev, P., *This Is Not Propaganda: Adventures in the War Against Reality*, Ed. PublicAffairs, 2019.
9. Sobre la injerencia rusa en los comicios estadounidenses de 2016 hablaremos más en detalle en el capítulo 6.
10. Lee, D., «The tactics of a Russian troll farm», *BBC News*, 16 de febrero de 2018.
11. Nakashima, *E.,* «U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms», *The Washington Post*, 27 de febrero de 2019.
12. «Inside Russia's Notorious "Internet Research Agency" Troll Farm», *Spyscape*, 11 de abril de 2022, actualizado en septiembre de 2024.
13. Ward, C.; Polglase, K.; Shukla, S.; Mezzofiore, G. y Lister T., «Russian election meddling is back – via Ghana and Nigeria – and in your feeds», *CNN*, 11 de abril de 2020.
14. «"Troll factory" spreading Russian pro-war lies online, says UK *», Agencias, The Guardian*, 1 de mayo de 2022.
15. Fiedler, T.; Scott, M., «Putin ally admits interfering in US elections», *Politico*, 7 de noviembre de 2022.
16. Krever, M.; Chernova, A., «Wagner chief admits to founding Russian troll farm sanctioned for meddling in US elections», *CNN*, 14 de febrero de 2023.
17. «Prigozhin-controlled Russian media group shuts after mutiny», Reuters, 2 de julio de 2023.
18. Nechepurenko, I., «Internet Trolls Propelled Prigozhin's Rise. Now Some Celebrate His Fall», *The New York Times*, 26 de julio de 2023.
19. Volz, D., «Prigozhin Is Dead, but His Troll Farms Are Alive and Peddling Disinformation», 28 de marzo de 2024.
20. «Coordinated Inauthentic Behavior Explained *»*, Nathaniel Gleicher, 6 de diciembre de 2018, página oficial de Meta.

21. Cuenta oficial de Twitter de la Embajada Rusa en Madrid, @Embajada-RusaES, 28 de octubre de 2020.
22. Cuenta personal de Twitter, @Danieliriarteo, 29 de octubre de 2020.
23. Ayala, C. L., «El big data del Gobierno: Los detalles del informe por el estallido social que entregó a la Fiscalía», *La Tercera*, 21 de diciembre de 2019.
24. «Mon Laferte, Claudio Bravo y K-Pop: El informe Big Data que entregó Blumel a la Fiscalía *»*, Cooperativa Chile, 22 de diciembre de 2019.
25. Jakes, L., «As Protests in South America Surged, So Did Russian Trolls on Twitter, U.S. Finds», *The New York Times*, 20 de enero de 2020.
26. «¿Qué es el Grupo de Lima?», *La Nación*, 24 de marzo de 2021.
27. Tras la invasión rusa de Ucrania, YouTube eliminó de un plumazo todo el contenido relacionado con *RT* y otros medios rusos, incluidos los vídeos de «Ahí Les Va».
28. Cuenta personal de Twitter, @Danieliriarteo, 29 de octubre de 2020.
29. «Handbuch Für Medienguerillas», Generación Identitaria, 2016.
30. Davey, J.; Ebner, J., «The Fringe Insurgency: Connectivity, Convergence and Mainstreaming of the Extreme Right», Institute for Strategic Dialogue, 2017.
31. Stegemann, P.; Musyal, S., Kulozik, S. D.; Wandt, L.; Pohl, M.; Gensing, P., «Wahlkampf im Netz: AfD-Funktionär an Troll-Attacken beteiligt *»*, *Tagesschau*, 1 de marzo de 2018.
32. Citado en *La vida secreta de los extremistas: Cómo me infiltré en los lugares más oscuros de internet*, Julia Ebner, Ed. Planeta, 2020.
33. Bradshaw, S.; Howard, P. N., «Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation», informe del Instituto de Internet de Oxfor (OII), julio de 2017.
34. La historia de Maria Ressa y su lucha contra el acoso digital está contada en profundidad en un capítulo del libro *This Is Not Propaganda. Adventures in the War Against Reality,* Ed. PublicAffairs, 2019, del perio-dista británico de origen ucraniano Peter Pomerantsev. Véase también *«Trolls and triumph: a digital battle in the Philippines»*, *BBC News*, 7 de diciembre de 2016.
35. «RSF unveils 20/2020 list of press freedom's digital predators», Reporteros Sin Fronteras, marzo de 2020.
36. Foroudi, L., «In Algeria, 'electronic flies' threaten a protest movement», *Coda Story*, 10 de diciembre de 2019.
37. Shearlaw, M., «Turkish journalists face abuse and threats online as trolls step up attacks», *The Guardian*, 1 de noviembre de 2016.
38. Albayraj, A.; Parkinson, J., «Turkey's Government Forms 6,000-Member Social Media Team», *The Wall Street Journal*, 16 de septiembre de 2013.
39. «Analysis of June 2020 Twitter takedowns linked to China, Russia and Turkey», Observatorio de Internet de Stanford, 11 de junio de 2020.

40. Shearlaw, M., «Turkish journalists face abuse and threats online as trolls step up attacks», *The Guardian*, 1 de noviembre de 2016.
41. Sozeri, E. K., «Mapping Turkey's Twitter-troll lynch mobs», *Daily Dot*, 29 de febrero de 2020.
42. «Disclosing networks of state-linked information operations we've removed *»,* blog oficial de Twitter, 12 de junio de 2020.
43. «La claria: una de las cien especies más dañinas del mundo», 14ymedio, 18 de noviembre de 2014.
44. «#DeZurdaTeam: ciberclarias cubanas buscan atraer jóvenes a sus filas», *YucaByte*, 4 de enero de 2022.
45. «¿Cómo detectar a una ciberclaria?», *ADN Cuba*, 12 de febrero de 2020.
46. González, O., «"Ciberclarias", un ejército que invade las redes sociales con cuentas falsas», *Cubanet*, 21 de mayo de 2019.
47. «De Zurda Team: rostros jóvenes para el cardumen de Ciberclarias», YucaByte, 3 de enero de 2022.
48. «Decreto Ley 35: las nuevas regulaciones en Cuba para condenar a los que hablen mal del gobierno en redes sociales», Lioman Lima, *BBC Mundo*, 19 de agosto 2021; véase también «Estado cubano recrudece ola represiva contra periodistas independientes en el marco de la entrada en vigencia de la Ley de Comunicación Social», Artículo 19 México, 7 de octubre de 2024.
49. Lima, L., «Wasp Network: qué fue la Red Avispa, el anillo de espionaje de Cuba en EE.UU. que recupera la polémica película de Netflix», *BBC Mundo*, 17 de julio de 2020.
50. «#DeZurdaTeam: ciberclarias cubanas buscan atraer jóvenes a sus filas», *YucaByte*, 4 de enero de 2022.
51. Montaner, C. A., «Cómo se organizó la protesta del 11 de julio en Cuba», *El Independiente*, 19 de diciembre de 2021.

4. GUERRILLAS DIGITALES

1. «Citizen journalists in Mexico monitor border safety via Twitter», Nicole Martinelli, International Journalists Network, 30 de octubre 2018.
2. Monnier, A., «Hezbollah's Use of Social Media: Communication Strategy and Impact on Public Opinion *», La Revue*, 12 de febrero de 2024.
3. Thompson, S. A.; Isaac, M., «Hamas Is Barred From Social Media. Its Messages Are Still Spreading *», The New York Times,* 18 de octubre de 2023.
4. «Distortion by design: How social media platforms shaped our initial understanding of the Israel-Hamas conflict'» Emerson T. Brooking, Layla Mashkoor y Jacqueline Malaret.

5. O'Sullivan, D.; Fung, B., «Hamas' social media following has skyrocketed since its attack. America is powerless to stop it», CNN, 17 de octubre de 2023.
6. Cortellessa, E., «The Oct. 7 Massacre Revealed a New Hamas Social Media Strategy», 31 de octubre de 2023.
7. «The Houthi (Ansar Allah) Digital Ecosystem», informe del Instituto para el Diálogo Estratégico (ISD), 28 de mayo de 2024.
8. Observaciones personales del autor mediante la monitorización de canales de Telegram que reproducían propaganda hutí durante el invierno de 2023-2024.
9. Por desgracia, en este libro carezco de espacio para abordar en profundidad el perfil de los MeK, que incluye un historial de atentados, una alianza con Saddam Hussein durante la guerra Irán-Irak y la progresiva conversión en una secta dirigida por un matrimonio. Pero en 2019 escribí un largo artículo sobre esta organización, para el que entrevisté tanto al historiador estadounidense de origen iraní Ervand Abrahamian, autor de un libro sobre el grupo, como al principal apoyo de esta organización en España: el ex eurodiputado y político de Vox Alejo Vidal-Quadras. Véase «Una secta militar confinada en Albania: quiénes son los iraníes que financiaron a Vox», Daniel Iriarte, *El Confidencial*, 15 de enero de 2019.
10. «Faking the online debate on Iran», *Al Jazeera, Listening Post*, 16 de septiembre de 2018.
11. «March 2021 Coordinated Inauthentic Behavior Report», página oficial de Meta, 6 de abril de 2021.
12. Hussain, M., «An Iranian activist wrote dozens of articles for right-wing outlets. But is he a real person?», *The Intercept*, 9 de junio de 2019.
13. Rezaian, J., «Why does the U.S. need trolls to make its Iran case?», *The Washington Post*, 11 de junio de 2019.
14. El estudio aparece citado en el libro *Inside Terrorism*, de Bruce Hoffman, Ed. Columbia University Press, 2006.
15. Citado en *Armas de seducción masiva: La factoría audiovisual del Estado Islámico para fascinar a la generación millennial*, Javier Lesaca, Ed. Península, 2017.
16. Tatham, S., *Information Operations*, Ed. Howgate Publishing Ltd., 2024.
17. *Ibid*.
18. *Ibid*.
19. *Ibid*.
20. Mehran, W., «The Evolution in the Taliban's Media Strategy», Programa sobre Extremismo de la Universidad George Washington, 18 de agosto de 2022.
21. Amiri, S., «Why the Taliban Love Social Media», *The Walrus*, 24 de abril de 2024.
22. Koerner, B. I., «Why ISIS Is Winning the Social Media War», *Wired*, marzo de 2016.
23. Shaheen, J., «Network of Terror: How Daesh Uses Adaptive Social Networks to Spread its Message», informe del Centro de Comunicaciones Estratégicas de la OTAN

(NATO Stratcom COE), noviembre de 2015.
24. Bloom, M.; Tiflati, H.; Horgan, J., «Navigating ISIS's Preferred Platform: Telegram», *Terrorism and Political Violence*, Volumen 31, 2019.
25. Callimachi, R., «A News Agency With Scoops Directly From ISIS, and a Veneer of Objectivity», *The New York Times*, 14 de enero de 2016.
26. Iriarte, D., «Esta es la revista oficial del Estado Islámico… y es increíblemente profesional», *El Confidencial*, 13 de septiembre de 2014.
27. «The Matrix of Islamic State's Propaganda: Magazines», capítulo del libro *ISIS Propaganda*. Stephane J. Baele, Katharine A. Boyd y Travis Coan, Ed. Oxford University Press, 2020.
28. Webber, L., «Voice of Khorasan Magazine and the Internationalization of Islamic State's Anti-Taliban Propaganda *»*, *Terrorism Monitor*, Volumen 20, Fundación Jamestown, 6 de mayo de 2022.
29. «ISIS official app available at Google Play», *itvNews*, 17 de junio de 2014. Un día después de la publicación de este artículo, la *app* dejó de estar disponible en dicho repositorio.
30. Berger, J. M., «How ISIS games Twitter», *The Atlantic*, 16 de junio de 2014.
31. *Ibid*.
32. Lesaca, J., *Armas de seducción masiva: La factoría audiovisual del Estado Islámico para fascinar a la generación millennial*, Ed. Península, 2017.
33. Tatham, S., *Information Operations*, Ed. Howgate Publishing Ltd., 2024.
34. «Decoding Social Media's Role in the Resurgence of the Taliban: A Literature Review», Nassir Ul Haq Wani, Universidad de Kardan, Sistema de Investigación de Información de Cachemira, 20 de julio de 2023.
35. «Decoding Social Media's Role in Taliban 2.0 and its Implications for Afghan Youth *»*, Muhammad Akkram, Asim Nasar y Shama Perveen, julio de 2024, East-West Center.
36. Atiq, S., «The Taliban embrace social media: "We too want to change perceptions"», *BBC News*, 6 de septiembre de 2021.
37. El comentario es parte del informe «Experts react: The Taliban has taken Kabul. Now what?», *Atlantic Council*, 15 de agosto de 2021.
38. Amiri, S., «Why the Taliban Love Social Media», *The Walrus*, 24 de abril de 2024.
39. Nasri, S., «Vloggers revel in Afghan access as our women's rights are erased», *Newsworthy*, 21 de noviembre de 2024.
40. «Mapping the Jihadist Information Ecosystem. Towards the Next Generation of Disruption Capability *»*, Ali Fisher, Nico Prucha y Emily Winterbotham, informe del Royal United Services Institute for Defence and Security Studies (RUSI), 2019.
41. «CaliphateTok: TikTok continues to host Islamic State propaganda», Moustafa Ayad, informe del Instituto para el Diálogo Estratégico (ISD), 13 de junio de 2023.

42. Gilbert, D., «ISIS Created Fake CNN and Al Jazeera Broadcasts», *Wired*, 18 de junio 2024.
43. *Ibid*.
44. Verma, P., «These ISIS news anchors are AI fakes. Their propaganda is real», *The Washington Post*, 17 de mayo de 2024.
45. Patrikarakos, D., *War in 140 Characters: How Social Media Is Reshaping Conflict in the Twenty-First Century*, Ed. Basic Books, 2017.
46. Wynne, M., «Meet NAFO: The Virtual Army Disarming Russian Disinformation», *The National Interest*, 19 de octubre de 2022.
47. Dougherty, J., «The pro-Ukraine internet 'fellas' using Shiba Inu memes to fight Russian propaganda», *CNN*, 11 de julio de 2023.
48. Gault, M., «Shitposting Shiba Inu Accounts Chased a Russian Diplomat Offline», *VICE*, 12 de julio de 2022.
49. Moody, O., «Nafo, not Nato, take the fight to Russia's internet trolls», *The Times*, 17 de julio de 2023.
50. *Ibid*.
51. Fernández, Y., «Qué es el Dogecoin, cómo funciona y por qué se ha hecho tan popular», *Xataka*, 22 de abril de 2022.
52. Harvey, C., «Seizing the memes of advantage in the Ukraine war and beyond», *The Strategist*, Instituto Australiano de Política Estratégica (ASPI), 15 de noviembre de 2022.
53. Almeida, L., «Friend of the Locals, Enemy of the State: The Social Media Presence of Comando Vermelho», *Global Network on Extremism & Technology*, 17 de junio de 2024.
54. «Web video shows Mexico man's beheading *»*, *NBC News*, 1 de abril de 2007.
55. «Fear, Lies and Lucre: How Criminal Groups Weaponise Social Media in Mexico», informe del International Crisis Group, 31 de enero de 2024.
56. *Ibid*.
57. Ferri, P., «El narco mexicano aprovecha el virus para exhibir su poder ante las cámaras», *El País*, 17 de abril de 2020.
58. «Fear, Lies and Lucre: How Criminal Groups Weaponise Social Media in Mexico», informe del International Crisis Group, 31 de enero de 2024.
59. Bradshaw, S.; Bailey, H; Howard, P. N., «Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation», informe del Instituto de Internet de Oxford, 13 de enero de 2021.

5. MERCENARIOS DE LA DESINFORMACIÓN

1. Entrevista personal con «Paul».

2. Thomas, E.; Reyes, K. D., «Commercial Disinformation», Institute for Strategic Dialogue, 14 de junio de 2023.
3. El libro se titula T*rue or False: A CIA Analyst's Guide to Spotting Fake News*, Ed. Feiwel & Friends, 2020.
4. Silverman, C.; Lytvynenko, J.; Kung, W., «Disinformation For Hire: How A Brand New Breed Of PR Firms Is Selling Lies Online», *BuzzFeed News*, 7 de enero de 2020.
5. «The Price of Influence: Disinformation in the Private Sector», Insikt Group, Recorded Future, 2019.
6. Kirkpatrick, D., «The Dirty Secrets of a Smear Campaign», *The New Yorker*, 27 de marzo de 2023.
7. Ramírez, B. P., «Más de 160 españoles son víctimas del espionaje de Emiratos en busca de extremistas islámicos», 7 de julio de 2023.
8. Fayol, C.; Philippin, Y.; Rouget, A.; Harari, A., «Emiratos compró a detectives suizos los nombres de 1.000 europeos señalados sin pruebas como islamistas radicales», *InfoLibre*, 7 de julio de 2023.
9. En España, estos contenidos fueron publicados por *OK Diario*. Véase «Emiratos Árabes usó a *OKdiario* en su campaña contra los Hermanos Musulmanes», Begoña P. Ramírez, *InfoLibre*, 10 de julio de 2023.
10. Fayol, C.; Harari, A.; Philippin, Y.; Rouget, A.; Colart, L., «Emiratos usó en Bruselas a eurodiputados de la extrema derecha para su guerra de influencias contra Catar», *InfoLibre*, 9 de julio de 2023.
11. «Une entreprise genevoise au coeur d'une vaste opération d'influence des Emirats arabes units», *RTS*, 7 de julio de 2023.
12. Kirkpatrick, D., «The Dirty Secrets of a Smear Campaign», *The New Yorker*, 27 de marzo de 2023.
13. *Ibid*.
14. «Une entreprise genevoise au coeur d'une vaste opération d'influence des Emirats arabes units», *RTS*, 7 de julio de 2023.
15. Para los lectores no familiarizados con este personaje, diremos que José Manuel Villarejo es un comisario condenado por corrupción y actividades ilegales, que durante décadas hizo trabajos sucios para grandes empresas españolas —y probablemente también para el Estado—, al tiempo que se enriquecía de forma escandalosa y en gran medida ilícita. Para entender hasta qué punto este individuo ha tenido importancia en la historia reciente de España, recomendamos los dos podcasts del periodista Álvaro de Cozar: «V, las cloacas del estado» y «El país de los demonios».
16. Irujo, J. M., «El comisario Villarejo ofrecía a sus clientes "maniobras de intoxicación informativa"», *El País*, 18 de abril de 2019.

17. Cabezas, F., «La guerra de los "trolls" acorrala a Bartomeu en su "Barçagate"», *El Mundo*, 17 de febrero de 2020.
18. Tapounet, R., «Una trama de cuentas difamatorias en redes sociales agita al Barça», *El Periódico de Catalunya*, 17 de febrero de 2020.
19. Ganyet, J. M., «Una conversación con Sonia D., extrabajadora de 13Ventures», *Vía Empresa*, 19 de febrero de 2020.
20. Cabezas, F., «La guerra de los "trolls" acorrala a Bartomeu en su "Barçagate"», *El Mundo*, 17 de febrero de 2020.
21. «Gobierno de Peña pagó a "mercenario digital" para limpiar reputación de Pemex», *Aristedui Noticias*, 1 de agosto de 2023.
22. Tronchoni, N., «Carlos Ibánez, de "hackear" para Correa en Ecuador a ayudar a Bartomeu», *El País*, 21 de febrero de 2020.
23. Fernández, L.; Revetria J., «El consultor uruguayo Ibáñez, del Barçagate a mejorar la imagen de Odebrecht», *Cazadores de Fake News*, 31 de julio de 2023.
24. Shepherd, Ch.; Cadell, C.; Nakashima, E.; Menn, J.; Schaffer, A., «Leaked files from Chinese firm show vast international hacking effort», *The Washington Post*, 22 de febrero de 2024.
25. Silverman, C.; Lytvynenko, J.; Kung W., «Disinformation For Hire: How A Brand New Breed Of PR Firms Is Selling Lies Online», *BuzzFeed News*, 7 de enero de 2020.
26. Grossman, S.; Ramali, K., «Outsourcing Disinformation», *Lawfare*, 13 de diciembre de 2020.
27. Vavra, S., «Facebook is observing a 'steady growth' in disinformation-for-hire services», *Cyberscoop*, 11 de mayo de 2021.
28. Silverman, C.; Lytvynenko, J.; Kung, W., «Disinformation For Hire: How A Brand New Breed Of PR Firms Is Selling Lies Online», *BuzzFeed News*, 7 de enero de 2020.
29. Cueto, J. C., «Cómo operaba Archimedes Group, la compañía israelí vetada por Facebook y acusada de interferir en las elecciones de México, Panamá y Honduras», *BBC Mundo*, 23 de mayo de 2019.
30. El acrónimo de Open Source Intelligence, o inteligencia de fuentes abiertas, esto es, la recopilación y procesamiento de toda la información no clasificada y por tanto disponible en abierto (internet, fuentes escritas, informes, etcétera).
31. Entrevista personal con Bot Ruso, febrero de 2022.
32. Broderick, R.; Arredondo, I., «Conoce al rey de las fake news en México», *Buzzfeed México*, 28 de junio de 2018.
33. Gabriela Chávez, «El negocio detrás de las noticias falsas», *Expansión México*, 3 de noviembre de 2017.
34. «Lo que se sabe, y lo que no, del "Rey de las *fake news*" en México», *Xataka México*, 2 de julio de 2018.

35. Kirchgaessner, S., «How undercover reporters caught “Team Jorge” disinformation operatives on camera», *The Guardian*, 15 de febrero de 2023.
36. Los falsos consultores eran los reporteros de investigación israelíes Gur Megiddo y Omer Benjakob, de *TheMarker* y *Haarezt*, y el francés Fréderic Métézeau, de Radio France International. En la investigación general sobre Team Jorge, llevada a cabo bajo el paraguas del consorcio Forbidden Stories, participaron también *The Guardian*, *Le Monde*, *Der Spiegel*, *Die Zeit*, *ZDF*, *Der Standard*, *Die Tages-Anzeiger* y *El País*, entre otros medios.
37. Gil, J.; Irujo, J. M., «Un empresario israelí se atribuye el ciberataque a la Generalitat en la consulta del 9-N de 2014», *El País*, 15 de febrero de 2023.
38. Kirchgaessner, S.; Ganguly, M.; Pegg, D.; Cadwalladr, C.; Burke, J., «Revealed: the hacking and disinformation team meddling in elections», *The Guardian*, 15 de febrero de 2023.
39. Buschek, Ch.; Christoph, M.; Diehl, J.; Höfner, R.; Hoffmann, H.; Hoppenstedt, M.; Lehberger, R.; Müller, A.-K.; Obermaier, F.; Obermayer, B.; Rosenbach, M.; Schulz, T.; Wiedmann-Schmidt, W., «How a Covert Firm Spreads Lies and Chaos Around the World», *Der Spiegel,* 20 de febrero de 2023.
40. *Ibid*.
41. Aquella afirmación, al parecer, no estaba en la escaleta del informativo de *BFMTV* aquel día. Ante estas revelaciones, la cadena inició una investigación y M’Barki fue inmediatamente suspendido. Véase «French broadcaster BFMTV suspends presenter amid disinformation scandal», Manisha Ganguly y David Conn, *The Guardian*, 15 de febrero de 2023.
42. «Revealed: the hacking and disinformation team meddling in elections», *The Guardian*, 15 de febrero de 2023.
43. «’Aims’: the software for hire that can control 30,000 fake online profiles», 15 de febrero de 2023.
44. Ganguly, M., «Revealed: the hacking and disinformation team meddling in elections», *The Guardian*, 15 de febrero de 2023.
45. «Un empresario israelí se atribuye el ciberataque a la Generalitat en la consulta del 9-N de 2014», *El País*, 15 de febrero de 2023.
46. Andrzejewski, C., «“Team Jorge”: In the heart of a global disinformation machine», *Forbidden Stories*, 15 de febrero de 2023.
47. Kirchgaessner, S.; Cadwalladr, C.; Lewis, P.; Burke, J., «Dark arts of politics: how “Team Jorge” and Cambridge Analytica meddled in Nigerian election», 16 de febrero de 2023.
48. «How a Covert Firm Spreads Lies and Chaos Around the World», *Der Spiegel*, 20 de febrero de 2024.

6. LOS MEMES SON UN ARMA (CARGADA DE FUTURO)

1. «Patria y vida» era el título de una canción lanzada unos meses antes por los cantantes cubanos Yotuel, Gente de Zona y Descemer Bueno (auténticas estrellas, no solo entre el público cubano a ambos lados del Estrecho de la Florida, sino entre las audiencias latinoamericanas), que arremetía contra muchos de los elementos identitarios del régimen cubano construidos alrededor de la épica revolucionaria, como el eslogan «Patria o muerte, venceremos».
2. «Cuba confirma que 297 manifestantes del 11 de julio han sido condenados a prisión», *BBC Mundo*, 17 de marzo de 2022. Muchos de los detenidos fueron posteriormente liberados y sus sentencias conmutadas o reducidas, pero aún así, 13 personas vieron confirmadas sus sentencias a entre 4 y 15 años de cárcel por supuestos delitos de «sedición, desacato, difusión de propaganda enemiga y sabotaje». Véase «Organización de derechos humanos condena sentencias de hasta 15 años de prisión contra manifestantes en Cuba», Ivonne Valdés, CNN en español, 2 de mayo de 2024.
3. Yosbel no se llama así. Por razones obvias, no puedo desvelar su identidad real.
4. Según una investigación del economista y demógrafo independiente cubano Juan Carlos Albizu-Campos, en torno a un 18 % de la población de Cuba abandonó el país en 2022 y 2023. Véase «La población cubana cayó un 18 % entre 2022 y 2023, según un estudio independiente», Agencia EFE, 8 de julio de 2024.
5. «"Liborio", "El Bobo" y "El Loquito", exponentes del Humor gráfico cubano», *Cubarte*, 27 de octubre de 2016.
6. Pérez Triana, J. M., «Memes y guerra memética», *Monitor Disinfo*, 22 de enero de 2024.
7. Brown, H., «The surprising power of internet memes», *BBC*, 29 de septiembre de 2022.
8. Lissardy, G., «La "ventana de Overton", el modelo que explica cómo ideas políticas consideradas tabú en una época se vuelven aceptables en otra», *BBC Mundo*, 3 de agosto de 2023.
9. «Memes & The Extreme Rigth-Wing», informe del Institute for Strategic Dialogue, 2022.
10. *Ibid*.
11. Azar, T., «Propaganda of the digital age: How memes are weaponized to spread disinformation», *USA Today*, 2 de septiembre 2022.
12. Este fenómeno es analizado más en detalle en el siguiente capítulo, «La burbuja extremista».
13. Bereznak, A., «ISIS Twitter memes, and what they mean», *Yahoo News*, 11 de diciembre de 2015.
14. *Ibid*.

15. Cornell, M., «Feral memes», *The New Inquiry*, 8 de noviembre de 2016.
16. Las estimaciones sobre el número de asesinatos de Jihadi John ante una cámara varían desde las 19, hasta las 29 víctimas. El motivo es que existe un vídeo en el que el terrorista participa en la ejecución de cierto número de soldados sirios, cuya cifra exacta es imposible de determinar por las imágenes, pero que va desde un mínimo de 12 asesinados hasta, más probablemente, los 22 muertos. Goto y Yukawa fueron también decapitados por este yihadista en un vídeo posterior.
17. «Japanese Twitter Users Mock ISIS With Internet Meme», *NBC News*, 22 de enero de 2015.
18. Basavilvazo, G., «Amenazas' de ISIS a México provocan ola de memes en Twitter», *Excelsior*, 25 de noviembre de 2015.
19. Piñón, M., «Lo que dice de nosotros que (esta vez) respondamos al terror con humor», *Vanity Fair*, 25 de agosto de 2017.
20. Describir estos memes y chistes sería demasiado largo y se perdería gran parte de su componente humorístico, pero muchos de los mejores aparecen recopilados en estos dos artículos: «Humor contra el terror: Twitter se ríe de "El Cordobés"», *Eldiario.es*, 24 de agosto de 2017, y «Los memes televisivos de El Cordobés, el hijo yihadista de La Tomasa», *Eldiario.es*, 25 de agosto de 2017.
21. Butter, S., «The Internet's battle to defeat ISIS - one meme at a time», *The Standard*, 1 de diciembre de 2015.
22. Para más información sobre la I. R. A., véase el capítulo «¿Para qué sirve un troll?».
23. Maynes, Ch., «A guide to Russian "demotivator" memes», *Public Radio International*, 11 de marzo de 2018.
24. Iriarte, D., «¿Qué es el Proyecto Lakhta? Putin, sus 'trolls' y la rabieta que cambió el mundo», *El Confidencial*, 27 de noviembre de 2019.
25. Estos datos fueron recogidos en la extensísima investigación del Senado de EE. UU. sobre el proceso de interferencia rusa en las elecciones de 2016, que abarca cinco volúmenes. Para hacer esta información más accesible, en 2019, el entonces candidato presidencial demócrata Michael Bennet editó un libro gratuito titulado *Dividing America How Russia Hacked Social Media and Democracy*, del que han sido extraídos tanto las cifras como los ejemplos de memes de esta sección.
26. Iriarte, D., «¿Crees que la propaganda rusa no es eficaz? Deberías ver estos "memes"», *El Confidencial*, 2 de enero de 2020.
27. *Ibid*.
28. Francois, C.; Nimmo, B.; C. Eib, S., «The IRA CopyPasta campaign», informe de la firma *Graphika*, 21 de octubre de 2019.
29. Por ejemplo, la principal empresa fundada por Thiel es Palantir Technologies, dedicada a la recolección masiva y análisis de datos (*big data*) en beneficio de los servicios de inteligencia y seguridad de Estados Unidos.

30. Prosser, M. B., «Memetics - A Growth Industry in US Military Operations», Marine Corps University of Quantico, School of Advanced Warfighting, 2006.
31. «Memetic Warfare: The Future of War», First Lieutenant Brian J. Hancock, Military Intelligence Professional Bulletin, abril-junio de 2010.
32. Bernstein, J., «This Man Helped Build The Trump Meme Army - Now He Wants To Reform It», *BuzzFeed News*, 30 de diciembre de 2016.
33. El llamado Pizzagate es una teoría de la conspiración que anticipó los cimientos de la secta digital QAnon. En esencia, proclamaba que algunos de los correos electrónicos de miembros del Partido Demócrata en los que aparecía la palabra «pizza» en realidad eran una referencia en clave a prácticas pedófilas.
34. Donovan, J., Dreyfuss E. y Friedberg B, *Meme Wars: The Untold Story of the Online Battles Upending Democracy in America*, Ed. Bloomsbury Publishing, septiembre de 2022.
35. Azar, T., «Propaganda of the digital age», *USA Today*, 2 de septiembre de 2022.
36. Montenegro, J. L., «¿Cuál es el significado del meme "Dark Brandon" y por qué el equipo de campaña de Biden lo ha hecho suyo?», *The Independent* en español, 13 de febrero de 2024.
37. Romano, A., «The "Dark Brandon" meme and why the Biden campaign has embraced it — explained», *Vox*, 1 de mayo de 2023.
38. Salas, J., «Los fieles de Trump resucitan bulos sexistas y racistas contra Kamala Harris: "Ascendió usando la cama"», *El País*, 23 de julio de 2024.
39. Planas Bou, C., «Del cocotero a la presidencia: Kamala Harris se convierte en meme para seducir a la Generación Z y vencer a Trump», *El Periódico*, 23 de julio de 2024.
40. Algunos de los ejemplos más destacados son las cuentas Ukrainian Memes (@Ukraine_Memes), Ukrainian Memes Forces (@uamemesforces), o Ukrainian Memes for Anti Putin Teens (@ukrainianmilit1), por nombrar solo unas pocas.
41. Opryszek, S., «The art of making memes. How Ukraine is successfully disarming Russia… with mockery», *OKO.press*, 4 diciembre de 2022.
42. Cuppens, T., «The weaponisation of memes», Jason Institute for Peace and Security Studies, 26 de marzo de 2023.
43. Kinstler, L., «Meet the Millennials Who Started Ukraine's Twitter War With Russia», *Fortune*, 28 de julio de 2017.
44. Opryshchenko, A., «Memes about the War Are What Helps the Whole Country to Hold On and Defeat Russia in the Information War», *Zaborona*, 21 de diciembre de 2022.

7. ELECCIONES, LA TRINCHERA PERFECTA

1. Böll, H., «The Global Story of Election Interference», *Stiftung*, 21 de enero de 2022.

2. Todavía hoy se desconoce quiénes fueron los responsables de la «Carta Zinoviev», pero algunos estudios historiográficos apuntan a círculos de «rusos blancos» anticomunistas exiliados en Berlín o en los países bálticos como los autores más probables.
3. Kirby, J., «Why countries interfere in elections», *Vox*, 2 de noviembre de 2020.
4. Pagovski, Z., Marshall Fund G., «Explaining the Referendum in Macedonia and the Future Scenarios», septiembre de 2018.
5. Santora, M., «In the Balkans, Russia and the West Fight a Disinformation-Age Battle», *The New York Times*, 16 de septiembre de 2018.
6. Purkins J., «Russian Warriors and British PR Firms: Macedonia's Information War», *Bureau of Investigative journalism*, 28 de septiembre de 2018.
7. Tisdall, S., «Result of Macedonia's referendum is another victory for Russia», *The Guardian*, 1 de octubre de 2018.
8. Clayton, M., «Ukraine election narrowly avoided 'wanton destruction' from hackers», *Christian Science Monitor*, 18 de junio de 2014.
9. «Russian government-connected hacktivist group CyberBerkut breaches Ukraine's Election Commission», base de datos de la Alianza para la Seguridad de las Democracias del German Marshall Fund.
10. «Presidential elections in Ukraine 2014», web de Ukraine Elections, consultada el 3 de marzo de 2025.
11. Existe abundante documentación que demuestra el papel que los servicios de inteligencia rusos y el propio Kremlin jugó a la hora de instrumentalizar el malestar de gran parte de la población del este de Ucrania para convertirlo en un conflicto armado tremendamente desestabilizador. Las evidencias más irrefutables se encuentran entre los documentos personales del asesor de Putin Vladislav Surkov, filtrados en 2016. Véase «The Surkov Leaks: The Inner Workings of Russia's Hybrid Warfare in Ukraine», Alya Shandra y Robert Sheely, informe del Royal United Services Institute for Defence and Security Studies (RUSI), 2019.
12. Tatham, S., *Information Operations*, Ed. Howgate Publishing Limited, 2024.
13. Field, M.; Wright, M., «Russian trolls sent thousands of pro-Leave messages on day of Brexit referendum, Twitter data reveals», *The Telegraph*, 17 de octubre de 2018.
14. «Russian Twitter trolls meddled in the Brexit vote. Did they swing it?», *The Economist*, 23 de noviembre de 2017.
15. Weisburd, A.; Watts, C.; Berger, J. M., «Trolling for Trump: How Russia is trying to destroy our democracy», *War On The Rocks*, 6 de noviembre de 2016.
16. En el ámbito de la ciberseguridad la atribución es a menudo muy difícil, por lo que los especialistas suelen fijarse en lo que se denomina TTPs (Tácticas, Técnicas y Procedimientos) de los diferentes actores para identificarlos. Cuando algún grupo o actor aparece una y otra vez, se le denomina Amenaza Persistente Avanzada (APT) y

se le asigna un código. Pero como esto es difícil de memorizar y no es muy sexy para el gran público, en el mundillo suele recurrirse a apodos más creativos, como en este caso.

17. Rid, T., «How Russia Pulled Off the Biggest Election Hack in U.S. History», *Esquire*, 20 de octubre de 2016.
18. Bremer, J., «Super-hacker "Guccifer" held and named as Marcel Lazar Lehel», *The Week*, 23 de enero de 2014.
19. El caso Seth Rich es uno de los puntos más desagradables de toda esta trama. Este joven de 27 años, especialista en datos, fue asesinado a tiros en la capital estadounidense durante la madrugada del 10 de julio de 2016. La policía concluyó que el crimen era un intento de robo que se había torcido. Sin embargo, varios políticos, comentaristas medios ultraconservadores, como Newt Gingrich, Kim Dotcom y *Fox News*, hicieron circular sin pruebas la teoría de que Rich era la fuente de la filtración de Wikileaks, e incluso que Hillary Clinton estaba detrás de su muerte. Véase «Un asesinato, convertido en un gran bulo conspirativo en Washington», Cristina F. Pereda, *El País*, 25 de mayo de 2017; «Gingrich Spreads Conspiracy Theory», Eugene Kiely, *FactCheck.org*, 22 de mayo de 2017.
20. *Agentes del Caos*, documental de Alex Gibney, 2020.
21. «Kremlin Troll Tells All About Influencing U.S. Elections», *The Moscow Times*, 16 de octubre de 2017.
22. Es la única explicación plausible para las vastas posesiones del violonchelista Sergei Roldugin, amigo de la infancia de Putin y que sobre el papel sería uno de los hombres más ricos del mundo. Todos los que han investigado el asunto creen que Roldugin es el principal testaferro del presidente ruso. Véase *Los papeles de Panamá: El club mundial de los evasores de impuestos*, de Frederik Obermaier y Bastian Obermayer, Ed. Península, 2016.
23. Osnos, E.; Remnick, D.; Yaffa Y., «Trump, Putin and the New Cold War», *The New Yorker*, 24 de febrero de 2017.
24. Ioffe, J., «What Putin Really Wants», *The Atlantic*, enero/febrero de 2018.
25. *Agentes del Caos*, documental de Alex Gibney, 2020.
26. «Information Manipulation: A Challenge for Our Democracies», CAPS - Ministerio para Europa y Asuntos Extranjeros y IRSEM - Ministerio de las Fuerzas Armadas de Francia, agosto de 2018.
27. Toucas, B., «The Macron Leaks: The Defeat of Informational Warfare», informe del CSIS, 30 de mayo de 2017.
28. Jeangène Vilmer, J.-B., «The "#Macron leaks" operation: a post-mortem», informe del Atlantic Council, 20 de junio de 2019.
29. O'Connor, S., «Cyber-enabled foreign interference in elections and referendums», Centro Internacional de Ciber Política, Instituto Australiano de Política Estratégica,

2020.

30. *Ibid*.
31. Biddle, S., «Here's the email Russian hackers used to try to break into state voting systems», *The Intercept*, 2 de junio de 2018.
32. El historiador David Shimer ha investigado en profundidad las operaciones de injerencia de EE. UU. y otros países, y afirma que «la CIA se ha ido alejando de la práctica de la interferencia electoral encubierta». Véase «"Rigged" details long history of Russian and U.S. electoral interference», Mike Cummings, Yale Daily News, 20 de agosto 2020. Aún así, el exdirector de la CIA Leon Panetta le dijo a Shimer que la agencia ya no altera votaciones o difunde desinformación, pero que influye sobre medios extranjeros para «cambiar actitudes dentro de un país», ocasionalmente «adquiriendo medios en un país o región que pueden usarse para transmitir mensajes» o tratando de «influenciar a aquellos que poseen elementos de los medios para que cooperen, colaboren con uno en hacer llegar ese mensaje». Existe constancia de que Estados Unidos intentó amañar sin éxito los resultados de las elecciones en Afganistán en 2009, y se preparó para hacerlo en las de Irak en 2005 pero abortó el plan ante la resistencia encontrada en el Congreso. Véase «Russia Isn't the Only One Meddling in Elections. We Do It, Too», Scott Shane, *The New York Times*, 17 de febrero de 2018; «Does the US Still Interfere in Foreign Elections?», Jack Goldsmith, Project Syndicate, 28 de octubre de 2020.
33. El caso de Juan Guaidó en Venezuela sería el ejemplo paradigmático de esta clase de acciones.
34. «A US PR Firm Steps Into Contested Elections», Observatorio de Internet de Stanford, 04 de septiembre de 2020.
35. Fang, L., «Interim Bolivian government taps the same lobby firm hired to sell the coup in Honduras», *The Intercept*, 26 de enero de 2020.
36. Timberg, C.; Dwoskin, E., «Washington firm ran fake Facebook accounts in Venezuela, Bolivia and Mexico, report finds», *The Washington Post*, 4 de septiembre de 2020.
37. Alonso Falcón, R.,«Cibermensajes envenenados desde Washington: Campañas en red para Bolivia, Venezuela y México», *Cubadebate*, 9 de septiembre de 2020.
38. «Facebook suspendió cuentas inauténticas que influyeron en diferentes elecciones de Latinoamérica», *DFRLab*, 22 de julio de 2020.
39. Timberg, C.; Dwoskin, E., «Washington firm ran fake Facebook accounts in Venezuela, Bolivia and Mexico, report finds», *The Washington Post*, 4 de septiembre de 2020.
40. Carvin, A., «Operation Carthage: How a Tunisian company conducted influence operations in African presidential elections», *DFRLab*, 5 de junio de 2020.

41. Del Castillo, C., «Facebook elimina cientos de cuentas falsas operadas desde España para intoxicar las elecciones de Ecuador y El Salvador», *Eldiario.es*, 6 de abril de 2021.
42. Siddiqui, Z.; Bing, C.,«Latin American election influence operation linked to Miami marketing firm», Reuters, 3 de mayo de 2023.
43. Hudson, J., «U. S. intelligence report says key gulf ally meddled in American politics», *The Washington Post*, 12 de noviembre de 2022.
44. Panyi, S., «Goulash: Orbán's campaign operatives in foreign elections», *VSquare*, 11 de enero de 2024.
45. Panyi, S., «How Orbán flooded Central Europe with millions of online ads during election season», *VSquare,* 29 de febrero de 2024.
46. *Ibid*.

8. CONSPIRANOICOS Y EXTREMISTAS

1. «Ataques de falsa bandera y profecías: el 11-S según las teorías de la conspiración», *VerificaRTVE*, *RTVE.es*, 11 de septiembre de 2021.
2. Fernández, M., «Grupo Bilderberg: cómo funciona el club secreto de la elite mundial que alimenta teorías conspirativas», *Infobae*, 13 de enero de 2025.
3. Pérez, E., «"Nos están sustituyendo": el lema del Gran Reemplazo, la teoría anti-inmigración que ha vuelto a incendiar Europa», *El Español*, 28 de julio de 2023.
4. Gilbert, D., «Conspiraciones sobre el atentado contra Trump hay para todos los gustos», *Wired*, 14 de julio de 2024.
5. Lenore, V., «Heroína como arma de estado: así se desmonta el mito más absurdo de la izquierda», *El Confidencial*, 13 de diciembre de 2015.
6. Delbert, C., «Most of Us Believe in at Least One Conspiracy Theory, Scientists Say», *Popular Mechanics*, 18 de julio de 2023.
7. Zelazko, A., «How Many People Have Been to the Moon», Encyclopedia Britannica. Consultado el 22 de febrero de 2025.
8. «Moon Exploration», página web oficial de la NASA. Consultado el 22 de febrero de 2025.
9. González, C., «El pedazo de roca lunar que está en un museo de Madrid», *ABC*, 19 de septiembre de 2019.
10. Giménez Chueca, I., «El incidente del golfo de Tonkín, prólogo de la guerra de Vietnam», *La Vanguardia*, 2 de agosto de 2024.
11. Villaécija, R., «Un profesor de Universidad y una ONG destaparon el escándalo de Volkswagen», *El Mundo*, 22 de septiembre de 2015.
12. Ashworth-Hayes, S.; Peters Ch., «How the grooming gang scandals was covered up», *The Telegraph*, 4 de enero de 2025.

13. «No simple answer for why people believe in conspiracy theories, says new study», American Psychological Association, *PHYS.org*, 26 de junio de 2023.
14. Bowler, J., «We All Believe in Conspiracies a Little, But Here's When It Gets Out of Control», *Science Alert*, 16 de febrero de 2021.
15. Cassam escribe este concepto con las iniciales en mayúscula, para diferenciarlas de las teorías sobre conspiraciones históricas reales, algo que entraría dentro del trabajo normal de un historiador. El ejemplo que este filósofo utiliza es el de la llamada «Conspiración de la Pólvora» liderada por Guy Fawkes, en la que un grupo de católicos ingleses intentó hacer volar por los aires al rey Jacobo I en 1605. En castellano el término «teoría de la conspiración» es más específico, por lo que aunque he respetado las citas literales de Cassam, en el resto de menciones utilizo las minúsculas.
16. McCarthy, B., «"False flag" conspiracy theories inundate social media after Iowa shooting», *AFP Fact Check*, 8 de enero de 2024; Richards Z., «House GOP candidate shares post claiming Buffalo, Uvalde shootings were false flag operations», *NBC News*, 8 de junio de 2022.
17. https://www.infowars.com/
18. Veit Medick, V., «The Information Warrior», *Der Spiegel*, 28 de febrero de 2017.
19. Warzel, Ch., «Alex Jones Just Can't Help Himself», *Buzzfeed News*, 4 de mayo de 2017.
20. *Ibid*.
21. *Ibid*.
22. Williamson, E.; Steel, E., «Conspiracy theories Made Alex Jones Very Rich. They May Bring Him Down», *The New York Times*, 7 de septiembre de 2018.
23. Testimonio de un extrabajador de *Infowars* en el documental *La verdad contra Alex Jones*, de Dan Reed (2024).
24. Van Wagtendonk, A., «Lawsuits against Alex Jones are a new strategy in curbing conspiracy theories», *The Grid*, 21 de abril de 2022.
25. El asunto sufrió un giro inesperado cuando la revista satírica *The Onion*, aprovechando la declaración de bancarrota de *Infowars*, compró el sitio durante una subasta pública por una cantidad irrisoria. En último término, un juez bloqueó la adquisición, al considerar que esta venta iba en detrimento de los acreedores de Jones, empezando por las propias familias de las víctimas de Sandy Hook. Collins D., «Judge rejects sale of Alex Jones' Infowars to The Onion in dispute over bankruptcy auction», *Associated Press*, 11 de diciembre de 2024.
26. Knauth, D., «Judge blocks Sandy Hook families' settlement in Alex Jones' bankruptcy», Reuters, 25 de febrero de 2025.
27. Los múltiples artículos del periodista Carlos Prieto sobre el crimen de Alcasser y su repercusión mediática y social, revivida a raíz de la aparición del documental *El caso*

Alcasser en Netflix en 2019, son una mina de información sobre todo lo sucedido. A modo de introducción, recomiendo «Una teoría sobre el crimen de las niñas de Alcàsser que no va a gustar a casi nadie», *El Confidencial*, 20 de junio de 2019, y «Un millón de euros por las cintas del crimen de Alcàsser (que nadie va a cobrar nunca)», *El Confidencial*, 21 de febrero de 2020.

28. *Cuarto Milenio*, 15 de septiembre de 2019.
29. Coaston, J., «QAnon, the scarily popular pro-Trump conspiracy theory, explained», *Vox*, 21 de agosto de 2020.
30. Una buena introducción es la serie documental de seis episodios *Q: En el ojo del huracán*, de Cullen Hoback (2021).
31. «Q drop», glosario de la Liga Antidifamación (ADL).
32. «The QAnon Conspiracy: Destroying Families, Dividing Communities, Undermining Democracy», informe del Network Contagion Research Institute, 15 de diciembre de 2020.
33. Berkowitz, R., «A Game Designer's Analysis Of QAnon», *Medium*, 30 de septiembre de 2020.
34. «Everyone Against Russia: Conspiracy Theories On The Rise In Russian Media», *EUvsDisinfo*, 22 de mayo de 2018.
35. Véase *Fortress Russia Conspiracy theories in Post-Soviet Russia*, Ilya Yablokov, Ed. Polity Press, Cambridge, 2018.
36. «How conspiracy theories help to maintain Vladimir Putin's grip on power in Russia», *The Conversation*, 14 de marzo de 2024.
37. Snegovaya, M., «The reluctant consensus: War and Russia's public opinion», informe del Atlantic Council, 17 de diciembre de 2024.
38. Audureau, W., «Why conspiracy theorists and the Kremlin echo each other's disinformation», *Le Monde*, 2 de marzo de 2023.
39. El periodista británico Brian Whitaker, excorresponsal de *The Guardian* en Oriente Medio, se pasó muchos años luchando contra las teorías de la conspiración sobre el uso de armamento químico en Siria, intensamente promovidas por Rusia y sus aliados, y desmontándolas una a una. Su trabajo está recogido en el libro *Denying the obvious: Chemical weapons and the information war over Syria*, B. Whitaker, 2021. La caída del régimen de Bashar Al Assad en diciembre de 2024 demostró que muchos de los supuestos testigos que habían aparecido en las televisiones sirias y rusas denunciando la culpabilidad de los rebeldes y supuestos montajes lo habían hecho bajo coacciones y amenazas de tortura y muerte. Véase «Syrian medics say were coerced into false chemical attack testimony», *AFP*, 23 de diciembre de 2024; «Syrian gas attack witnesses coerced into false testimony face new threats at home», Neil Hauer, *CBC*, 21 de febrero de 2025.

40. Menn, J., «QAnon received earlier boost from Russian accounts on Twitter, archives show», Reuters, 2 de noviembre de 2020.
41. Menn, J., «Russian-backed organizations amplifying QAnon conspiracy theories, researchers say», Reuters, 25 de agosto de 2020.
42. «Quantifying The Q Conspiracy: A Data-Driven Approach to Understand the Threat Posed by QAnon», informe de The Soufan Center, un laboratorio de ideas perteneciente a la consultoría de inteligencia The Soufan Group, abril de 2021.
43. German, M., *Thinking Like a Terrorist: Insights from a Former FBI Undercover Agent,* Ed. Potomac Books Inc., 2007.
44. Saavedra, D., *Memorias de un exnazi: Veinte años en la extrema derecha española*, Ed. B, Colección Sine Qua Non, 2021.
45. https://www.youtube.com/@DavidSaavedra

9. DE LAS REDES A LAS CALLES

1. «A Reporter's Footage from Inside the Capitol Siege», *The New Yorker*, 17 de enero de 2021.
2. Arkin, W. M., «Exclusive: Classified Documents Reveal the Number of January 6 Protestors», *Newsweek*, 23 de diciembre de 2021.
3. Edmonson, C., «"So the Traitors Know the Stakes": The Meaning of the Jan. 6 Gallows», *The New York Times*, 16 de junio de 2022.
4. Tan, S.; Shin, Y.; Rindler D., «How one of America's ugliest days unraveled inside and outside the Capitol», *The Washington Post*, 9 de enero de 2021.
5. La República de Kekistan es un país imaginario creado por los usuarios de 4chan como parodia de las políticas identitarias, cuyos planteamientos lleva al extremo, y que en ese sentido ha acabado siendo abrazado por la extrema derecha de EE. UU. y otros países. Su bandera es una copia de la de la Wehrmacht (el ejército alemán) durante las eras imperial y nazi), pero sustituyendo el color rojo por el verde de la Rana Pepe, y con un círculo con la palabra KEK en el centro.
6. La Rana Pepe es un icono contracultural nacido como personaje de cómic en 2005, muy utilizado en foros de internet, y del que una década después se apropiaron los movimientos de extrema derecha estadounidenses, fusionándolo con otros elementos como el cabello amarillo de Donald Trump. Véase «How Pepe the Frog Became a Nazi Trump Supporter and Alt-Right Symbol», Olivia Nuzzi, The Daily Beast, 26 de mayo de 2016.
7. Donovan, J.; Dreyfuss, E.; Friedberg B., *Meme Wars: The Untold Story of the Online Battles Upending Democracy in America*, Ed. Bloomsbury Publishing, 2022.
8. «Exhaustive fact check finds little evidence of voter fraud, but 2020's "Big Lie" lives on», *PBS*, 17 de diciembre de 2021.

9. «It's Official: The Election Was Secure», Brennan Center for Justice, 11 de diciembre de 2020.
10. Jaimungal, C., «Three-quarters of voters think fraud occurred during the election», *YouGov*, 12 de noviembre de 2020.
11. El documental de Michael Premo *Homegrown: Fanáticos en el Capitolio* (2024) sigue a varios miembros de los Proud Boys durante meses, desde antes de las elecciones de noviembre de 2020. Premo pudo filmar muchas de las conversaciones entre ellos, en las que planifican premeditadamente la operación, y hacen lo posible para movilizar a los manifestantes en Washington DC para que se sumen al asalto. El FBI también recaudó un número abrumador de evidencias en ese sentido, como conversaciones en los chats de muchos de los participantes en la toma del Congreso.
12. Pengelly, M., «More than a third of US adults say Biden's 2020 victory was not legitimate», *The Guardian*, 2 de enero de 2024.
13. Donovan, J.; Dreyfuss, E.; Friedberg B., *Meme Wars: The Untold Story of the Online Battles Upending Democracy in America*, Ed. Bloomsbury Publishing, 2022.
14. McDonnell, P. J.; Sánchez, C., «When fake news kills: Lynchings in Mexico are linked to viral child-kidnap rumors», *Los Angeles Times*, 21 de septiembre de 2018.
15. «India "WhatsApp child abduction rumour": Five more lynched», *BBC News*, 2 de julio de 2018.
16. «Queman vivas a 15 mujeres en Kenia acusadas de brujería», *Colpisa*/*AFP*, 22 de mayo de 2008.
17. Popoviciu, A., «Thousands of Gambians Were Accused of Witchcraft and Tortured. Can Their Country Make Them Whole?», *New Lines Magazine*, 18 de agosto de 2023.
18. «Arabia Saudí ejecuta a un hombre por brujería», *EFE*, 19 de junio de 2012.
19. Zaitchik, A., «Meet Alex Jones», *Rolling Stone*, 2 de marzo de 2011.
20. Yuhas, A., «"Pizzagate" gunman pleads guilty as conspiracy theorist apologizes over case», *The Guardian*, 25 de marzo de 2017.
21. «El monje budista que divide a Birmania», *BBC Mundo*, 28 de junio de 2013.
22. González Francisco, L. A., «Argumentario religioso para difundir el terror: El caso del monje Wirathu, "el Bin Laden birmano"», Observatorio Internacional de Estudios sobre Terrorismo, 11 de abril de 2024.
23. *Ibid*.
24. Villadiego, L., «El apartheid que creó una nueva insurgencia musulmana en el sudeste asiático», *El Confidencial*, 5 de enero de 2017.
25. «Report of the independent international fact-finding mission on Myanmar», Consejo de Derechos Humanos de Naciones Unidas, 10-28 de septiembre de 2018.
26. Mozur, P., «A Genocide Incited on Facebook, With Posts From Myanmar's Military», *The New York Times*, 15 de octubre de 2018.

27. Miles, T., «U. N. investigators cite Facebook role in Myanmar crisis», Reuters, 12 de marzo de 2018.
28. «Removing Myanmar Military Officials From Facebook», Comunicado de prensa en la página oficial de Meta, 28 de agosto de 2018.
29. Warofka, A., «An Independent Assessment of the Human Rights Impact of Facebook in Myanmar», Comunicado de prensa en la página oficial de Meta, 05 de noviembre de 2018.
30. Six, N., «Rohingya massacre: "Facebook played a central role in the rise of the climate of hate"», *Le Monde*, 29 de septiembre de 2022.
31. Safi, M., «Sri Lanka accuses Facebook over hate speech after deadly riots», *The Guardian*, 14 de marzo de 2018.
32. Taub, A., «Where Countries Are Tinderboxes and Facebook Is a Match», *The New York Times*, 21 de abril de 2018.
33. Morris, D. Z., «Facebook Accused of Ignoring Government Warnings Before Mob Violence in Sri Lanka», *Fortune*, 22 de abril de 2018.
34. Safi, M., «Sri Lanka accuses Facebook over hate speech after deadly riots», *The Guardian*, 14 de marzo de 2018.
35. Scheck, J.; Purnell, N.; Horwitz J., «Facebook Employees Flag Drug Cartels and Human Traffickers. The Company's Response Is Weak, Documents Show», *The Wall Street Journal*, 16 de septiembre de 2021.
36. Knight, T.; Alexion B., «Influential Ethiopian social media accounts stoke violence along ethnic lines», *DFR Lab*, 17 de diciembre de 2021.
37. Mackintosh, E., «Facebook knew it was being used to incite violence in Ethiopia. It did little to stop the spread, documents show», *CNN*, 25 de octubre de 2021.
38. Mwai, P., «Ethiopia's Tigray conflict: What are Facebook and Twitter doing about hate speech?», *BBC News*, 23 de noviembre de 2021.
39. Crystal, C., «Facebook, Telegram, and the Ongoing Struggle Against Online Hate Speech», Carnegie Endowment for International Peace, 7 de septiembre de 2023.
40. «Detenidos 25 presuntos ultraderechistas en Alemania por planear un golpe de Estado», *EFE*, 7 de diciembre de 2022.
41. Risco, I., «Quiénes son los 'Reichsbürger' que quieren tomar el poder con las armas en Alemania», *El Confidencial*, 10 de diciembre de 2022.
42. Castellanos, S., «Heinrich XIII, el polémico príncipe alemán detenido por un intento de golpe de Estado en el país», *El Confidencial*, 7 de diciembre de 2022.
43. Rivas Pacheco, G., «Desmontando la Operación Azur: un complot surrealista para dar un golpe de Estado en Francia», *El Confidencial*, 20 de noviembre de 2021.
44. «Jail terms Austrian far-right group trying to incite coup», *Deutsche Welle*, 25 de enero de 2019.

45. Bourke, K., «Perth man charged over video of fake Australian Federal Police Commissioner seeking government overthrow», *ABC News Australia*, 2 de agosto de 2021.
46. Falk, T. O., «Why Germany Is Struggling to Address the Reichsbürger Threat *», Foreign Policy*, 19 de diciembre de 2022.
47. Wilson, J., «Conspiracy theories like QAnon could fuel "extremist" violence, FBI says», *The Guardian*, 1 de agosto de 2019.
48. «IntelBrief: Arrests in Germany Target Far-Right and Anti-Government Extremists», *The Soufan Group*, 8 de diciembre de 2022.
49. «Qué es el aceleracionismo, la teoría en la que creen los nacionalistas blancos de EE. UU. que conspiran para atacar su red eléctrica», *BBC Mundo*, 15 de marzo de 2021.
50. Cereceda, R.; Chatreau J., «Rebelión de los chalecos amarillos: ¿Quiénes son y qué quieren?», *Euronews*, 3 de diciembre de 2018.
51. Reilly, L.; Sgueglia, K., «Three militia members sentenced in plot to kidnap Michigan Democratic Gov. Whitmer», *CNN*, 15 de diciembre de 2022.
52. Gabilondo, P., «Siete años y medio de cárcel para el "francotirador" que planeó asesinar a Sánchez», *El Confidencial*, 12 de abril de 2022.

10. DESESTABILIZACIÓN *LOW COST*

1. «Estrellas de David en muros de París: Francia denuncia un intento de desestabilización rusa», Radio France Internationale, 14 de noviembre de 2023.
2. Val, E., «Conexión rusa en el caso de las estrellas de David de París», *La Vanguardia*, 10 de noviembre de 2023.
3. «What is the Doppelganger operation? List of resources», *EU Disinfo Lab*, 30 de octubre de 2024.
4. Villaécija, R., «Alarma en París por la "invasión" de chinches en espacios públicos», *El Mundo*, 4 de octubre de 2023.
5. «Punaises de lit: la France affirme que la psychose a été "amplifiée" par "des comptes liés au Kremlin"», *Agencias*, *BFM TV*, 1 de marzo de 2024.
6. Glouthière, F., «Non, "Libération" n'a pas imputé l'invasion de punaises de lit à l'arrivée des réfugiés ukrainiens», *Libération*, 4 de octubre de 2023.
7. Poincaré, N., «Punaises de lit: la Russie soupçonnée d'avoir eu un rôle sur la psychose en France», *BFM TV*, 23 de octubre de 2023.
8. «Summary of the Information Threat to the Paris 2024 Olympic and Paralympic Games», informe público, Viginium, Ministerio General de la Defensa y de la Seguridad Nacional de Francia, septiembre de 2024.
9. *Ibid*.

10. Gelis Pons, O., «En Suecia ya arde un corán casi a diario y su Gobierno no sabe cómo impedirlo», *El Confidencial*, 4 de agosto de 2023.
11. «Asesinado a tiros mientras retransmitía en TikTok un iraquí que quemó copias del Corán en Suecia», *Agencias*, *El País*, 30 de enero de 2025.
12. Braw, E., «A Curious Quran Burning in Sweden», *The Wall Street Journal*, 7 de septiembre de 2023.
13. Hamilton, F.; Parker, Ch.; Dathan M., «Iran is hijacking pro-Palestinian protests, police warn», *The Times*, 27 de octubre de 2023.
14. Turner, C.; Lisbona, N., «Russia and China 'manipulating UK public opinion by promoting pro-Palestinian influencers», *The Telegraph*, 18 de mayo de 2024.
15. Quinn, B., «Cómo la extrema derecha ha incendiado con bulos xenófobos las protestas por el apuñalamiento que mató a tres niñas en Inglaterra», *Eldiario.es*, 1 de agosto de 2024.
16. Mason, P., «The mob vs Starmer», *The New European*, 4 de agosto de 2024.
17. Dixon, H.; Eastham, J., «Woman who posted fake name of Southport attacker says it "destroyed" her», *The Telegraph*, 10 de agosto de 2024.
18. Mulla, I., «UK: Anti-Muslim mob attacks Southport mosque after misinformation campaign», *Middle East Eye*, 30 de julio de 2024.
19. «From rumours to riots: How online misinformation fuelled violence in the aftermath of the Southport attack», informe del Instituto para el Diálogo Estratégico, 31 de julio de 2024.
20. Wickham, A.; Stone, J.; Zuidijk, D.; Thornber, E., «Suspected Foreign Accounst Aid UK Extremists to Incite Riots», *Bloomberg*, 7 de agosto de 2024.
21. «Mr.AG: The Mixed Race Finnish Neo-Nazi Behind the UK's Race Riots», *Red Flare*, 18 de agosto de 2024.
22. Thomas, E., «BBC confronts neo-Nazi who gave UK rioters arson tips», *BBC News*, 2 de octubre de 2024.
23. Shirreff, L., «The obscure Russian-linked 'news' outlet fuelling violence on Britain's streets», *The Telegraph*, 3 de agosto de 2024.
24. Planas Bou, C., «Cómo la desinformación racista de la extrema derecha ha incendiado las calles del Reino Unido», *El Periódico*, 5 de agosto de 2024.
25. Rogers, F.; Scherre, L., «Who is behind the Italian propaganda platform publishing misleading anti-migrant videos?», *Neue Zürcher Zeitung*, 15 de diciembre de 2023.
26. Penna, D., «Russian fake news about Southport attack is 'grey warfare', says former MI6 head», *The Telegraph*, 1 de agosto de 2024.
27. Morley-Davies, J., «How Did Foreign Actors Exploit the Recent Riots in the UK?», Royal United Services Institute, 28 de agosto de 2024.
28. Thornber, E., «UK Riot Arrests Pass 1,000 as Anti-Immigrant Disorder Subsidies», *Bloomberg*, 14 de agosto de 2024.

29. «Varios difusores de bulos racistas cierran sus cuentas de redes sociales tras el anuncio de la investigación de la Fiscalía», *Eldiario.es*, 21 de agosto de 2024.
30. Infantes Capdevila, G., «La campaña de odio que relaciona el crimen de Mocejón con migrantes: actores, antecedentes y consecuencias», *Newtral*, 22 de agosto de 2024.
31. Requeijo, A.; Iriarte, D., «De Reino Unido a Mocejón: estos son los perfiles que agitan en España la ola xenófoba», *El Confidencial*, 21 de agosto de 2024.
32. *Ibid*.
33. Cuenta personal de Vito Quiles en X, 7 de agosto de 2024.
34. Requeijo A., Iriarte, D., «De Reino Unido a Mocejón: estos son los perfiles que agitan en España la ola xenófoba», *El Confidencial*, 21 de agosto de 2024.
35. Cuenta de X @SoyDeDerechas, 3 de agosto de 2024.
36. Cuenta de X @AltRightEspan, 3 de agosto de 2024.
37. Cuenta de X @IgdePablo, 3 de agosto de 2024.
38. Cuenta de X @anubi77787292, 26 de febrero de 2025.

11. CAMPO DE BATALLA: ESTADOS UNIDOS

1. Vavra, S., «List of 2020 election meddlers includes Cuba, Saudi Arabia and North Korea, US intelligence official says», *Cyberscoop*, 20 de agosto de 2020.
2. David, B., «News outlets were leaked insider material from the Trump campaign. They chose not to print it», *Associated Press*, 13 de agosto de 2024.
3. Isenstadt, A., «We received internal Trump documents from "Robert." Then the campaign confirmed it was hacked», *Politico*, 8 de octubre de 2024.
4. Watts, C., «Iran Targeting 2024 US Election», Microsoft Threat Analysis Center, 8 de agosto de 2024.
5. Gazis, O., «Iran trying to undercut Trump campaign and Russia doing opposite, U.S. officials indicate», *CBS News*, 30 de julio de 2024.
6. Collier, K., «U.S. intelligence official: Russia and Iran likely seeking to influence election outcome», *CBS News*, 30 de julio de 2024.
7. Lesser, M.; Ben-Am, A.; Fulde-Hardy, M.; Nazari, S.; Malcomb, P. J., «Much Ado About 'Somethings': China-Linked Influence Operation Endures Despite Takedowns», informe de la Fundación para la Defensa de las Democracias, 27 de marzo de 2024.
8. Menn, J.; Schaffer, A.; Nix, N.; Morse, C. E., «Chinese propaganda accounts found by Meta still flourish on X», *The Washington Post*, 16 de febrero de 2024.
9. Burnett, E., «Chinese media seizes on US tensions to float false "civil war" theories», *CNN*, 8 de febrero de 2024.
10. Thomas, E., «Pro-CCP Spamouflage campaign experiments with new tactics targeting the US», informe del Instituto para el Diálogo Estratégico (ISD), 1 de abril de 2024.

11. Hsu, T., «China's Advancing Efforts to Influence the U.S. Election Raise Alarms», *The New York Times*, 7 de abril de 2024.
12. Demarais A., «Why China Is Rooting for Trump», *Foreign Policy*, 7 de febrero de 2024.
13. *Ibid*.
14. Nancy Cook, N.; Joshua Green, J.; Parker, M., «Trump on What He'd Do With Taxes, Tariffs, Jerome Powell and More», *Bloomberg*, 16 de julio de 2024.
15. «The Donald Trump Interview Transcript», *Bloomberg Businessweek*, 16 de julio de 2024.
16. Nimmo, B.; Eib, C. S.; Tamora, L., «Cross-Platform Spam Network Targeted Hong Kong Protests», informe de *Graphika*, 25 de septiembre de 2019.
17. «Foreign Threats to the 2020 US Elections», *Intelligence Community Assessment*, 10 de marzo de 2021, desclasificado el 15 de marzo de 2021.
18. Rawnsley, A., «Chinese Intel Officers Interfered in U.S. Election», *Rolling Stone*, 29 de agosto de 2023.
19. Butler, Z., «Google disrupted over 10,000 instances of DRAGONBRIDGE activity in Q1 2024», Threat Analysis Group, Google, 26 de junio de 2024.
20. Hsu, T., «China's Advancing Efforts to Influence the U.S. Election Raise Alarms», *The New York Times*, 2 de abril de 2024.
21. Merrill, J. B.; Schaffer, A.; Nix N., «A firehose of antisemitic disinformation from China is pointing to two Republican legislators», *The Washington Post*, 10 de octubre de 2024.
22. «Foreign Threats to the 2022 US Elections», *Intelligence Community Assessment*, 23 de diciembre de 2022, desclasificado en diciembre de 2023.
23. Wilner M., «U.S. intelligence official says Cuban attempt to influence local races is underway», 29 de julio de 2024.
24. Broadwater, L., «AIPAC Demonstrates Its Clout With Defeat of a Second "Squad" Member», *The New York Times*, 7 de agosto de 2024.
25. Frenkel, S., «Israel Secretly Targets U.S. Lawmakers With Influence Campaign on Gaza War», *The New York Time*s, 6 de junio de 2024.
26. Benjakob, O., «Israel Secretly Targeted American Lawmakers With Gaza War Influence Campaign», *Haaretz*, 5 de junio de 2024.
27. Gedeon, J.; Miller, M., «Israel targeted more than 120 US lawmakers in disinformation campaign», *Politico*, 6 de mayo de 2024.
28. Cameron, D., «US Leaders Dodge Questions About Israel's Influence Campaign», *Wired*, 11 de junio de 2024.
29. Toosi, N., «Hungary's Orbán Has Taken Sides in America's Election. Maybe Other Leaders Should, Too», *Politico*, 8 de julio de 2024.

30. El llamado Proyecto 2025 es una controvertida hoja de ruta elaborada por la Fundación Heritage para remodelar el aparato estatal siguiendo patrones ultraconservadores, que causó tal rechazo en grandes sectores de la sociedad estadounidense que Trump intentó distanciarse públicamente de ella, pese a los múltiples vínculos entre su campaña y los artífices del proyecto. Véase Barro Argemino, «Proyecto 2025 - Estados Cristianos de América: así avanza el conservadurismo religioso en EE.UU.», *El Confidencial*, 23 de junio de 2024.
31. «Elon Musk falsely claims Democrats will eliminate elections in US during Donald Trump rally in Butler», *The Independent*, 6 de octubre de 2024.
32. Schleifer, T.; Haberman, M.; Mac, R.; Swan, J., «Musk Is Going All In to Elect Trump», *The New York Times*, 11 de octubre de 2024.
33. Murphy, T., «Elon Musk Is Offering People Cash To Identify Trump Voters. What Could Go Wrong?», *Mother Jones,* 8 de octubre de 2024.
34. Schleiffer, T., «Musk's $1 Million Offer Raises New Legal Questions», *The New York Times*, 20 de octubre de 2024.
35. Ingram, J.; May, M., «The X factor: How Trump ally Elon Musk is using social media to prime voter mistrust ahead of 2024 election», *CBS News*, 21 de octubre de 2024.
36. Koebler, J., «This Is Exactly How an Elon Musk-Funded PAC Is Microtargeting Muslims and Jews With Opposing Messages», *404 Media*, 18 de octubre de 2024.

12. LO QUE VIENE

1. «A "super year" for elections *»*, Programa de Desarrollo de Naciones Unidas.
2. Chhabria, P., «The big election year: how to protect democracy in the era of AI», Foro Económico Mundial, 29 de enero de 2024.
3. Meaker, M., «Deefakes en elecciones de Eslovaquia reafirman que IA es un peligro para la democracia», *Wired*, 3 de octubre de 2023
4. «El falso Barack Obama creado con inteligencia artificial capaz de hablar como si fuera el original», *BBC Mundo*, 17 de julio de 2017.
5. Díaz, J., «Un Tom Cruise digital indistinguible del real se hace viral en TikTok», *El Confidencial,* 26 de febrero de 2021.
6. Holroyd, M., Olorunselu F., «Deepfake Zelenskyy surrender video is the "first intentionally used" in Ukraine war», Euronews, 16 de marzo de 2023.
7. Lerman, R., «Video of Pelosi brings renewed attention to "cheapfakes''», *Associated Press*, 10 de febrero de 2020.
8. Tatham, S., «Information Operations», *Howgate Publishing Limited*, 2024.
9. Iriarte, D., «¿Quieres sembrar desinformación estatal? Moscú te marca el camino: pon un influencer en tu vida *»*, Daniel Iriarte, *El Confidencial*, 29 de octubre de 2022.

10. Murko, D., «U.S. election results in livestreaming — over 9 million Peak Viewers, new records for top streamers and platforms», *StreamChart*, 6 de noviembre de 2024.
11. Carman, A., «Spotify Reveals Joe Rogan's Podcast Numbers», *Bloomberg*, 21 de marzo de 2024.
12. Estos datos los aportó Martin Barron, el legendario exdirector del diario The Washington Post, en una entrevista con El País en octubre de 2024. Véase Lafuente J., «Martin Baron: "Una presidencia de Trump pondría en jaque a la democracia de Estados Unidos"», *El País*, 26 de octubre de 2024.
13. Nicolaou, A., «The podcast bros who helped put Trump back in the White House», *Financial Times*, 24 de enero de 2025.
14. Alba, D.; Yin, L.; Love, J.; Carman, A.; Bengani, P.; Dottle, R.; Mejía, E., «How 9 Popular YouTubers Helped Trump Win a Second Term», *Bloomberg*, 22 de enero de 2025.
15. St. Aubin, Ch., «Americans' top sources of political news ahead of the 2024 election», Pew Research Center, 31 de octubre de 2024.
16. Casi el 40% de los jóvenes estadounidenses se informan a través de "influencers", según un estudio», *Diario El Universal*, 20 de noviembre de 2024.
17. Waldman, S., «An Overlooked — and Increasingly Important — Clue to How People Vote *», Politico*, 9 de noviembre de 2024.
18. Henley, J., «How Elon Musk has meddled in European affairs», *The Guardian*, 11 de enero de 2025.
19. Kessler, G.; Rizzo, S.; Kelly, M., «Trump's false or misleading claims total 30,573 over 4 years», *The Washington Post*, 24 de enero de 2021.
20. Croucher, S., «Why Has Mark Zuckerberg Copied Elon Musk?*»*,*Newsweek*, 9 de enero de 2025.
21. Swenson, A., «Trump, a populist president, is flanked by tech billionaires at his inauguratio*n», Associated Press*, 21 de enero de 2025.
22. «US agency focused on foreign disinformation shuts down», *AFP*, 24 de diciembre de 2024.
23. Myers, S. L.; Barnes, J. E.; Frenkel, S., «Trump Dismantles Government Fight Against Foreign Influence Operations», *The New York Times*, 20 de febrero de 2025.
24. *Digital News Report 2024*, Instituto Reuters, Universidad de Oxford, 17 de junio de 2024.
25. «El interés por las noticias en España se ha desplomado en la última década», *CTXT,* 19 de junio de 2024.
26. *Digital News Report 2024*, Instituto Reuters, Universidad de Oxford, capítulo «España».
27. «El prorruso Georgescu y la centroderechista Lasconi pasan a la segunda vuelta de las presidenciales de Rumanía», *RTVE.es*, 24 de noviembre de 2024.

28. Sánchez Costa, R., «Hartazgo con la guerra de Ucrania y furor en las redes sociales: los expertos explican el auge del candidato prorruso en Rumanía *»*, *El País*, 28 de noviembre de 2024.
29. Véase «Portal Kombat - A structured and coordinated pro-Russian propaganda network, informe de Viginium», febrero de 2024.
30. Ciobanu R., «Călin Georgescu este prezentat după decizia CCR drept martir, pe o rețea de site-uri răspândite în toată lumea și create la Moscova, a descoperit o agenție a statului francez *», HotNews.ro*, 9 de diciembre de 2024.
31. Entre sus clientes se encuentran la OTAN, la Comisión Europea y algunos ministerios e instituciones del Reino Unido, Estonia, Suecia, Ucrania y Canadá.
32. Rosca, M., «EXCLUSIV Operațiunea Georgescu pe X, Telegram și Facebook. Urcat în algoritmi de conturi rusești cu sute de mii de urmăritori: "În promovarea lui au fost implicate rețele specializate în destabilizarea democrațiilor"*»,* 29 de noviembre de 2024.
33. «En Rumanía, el candidato de extrema derecha Calin Georgescu ha sido detenido. La fiscalía lo acusa de financiación oculta de Moscú», *El Grand Continent*, 26 de febrero de 2025.
34. «Ads, Influence, and Democracy: Meta's Role in Romania's 2024 Presidential Election *»*, informe de *CheckFirst*, 9 de diciembre de 2024.
35. «Documento del CSAT SRI I *»* escrito el 28 de noviembre 2024 y desclasificado el 4 de diciembre de ese año, disponible en la página web de la Presidencia de Rumanía.
36. «Documento del CSAT SRI II *»*, escrito el 2 de diciembre 2024 y desclasificado el 4 de diciembre de ese año, disponible en la página web de la Presidencia de Rumanía.
37. Dunai, M.; Ivanova, P.; Schipani A., «The Wagner-style mercenaries plotting unrest in Romania *»*, *Financial Times,* 11 de diciembre de 2024.
38. Ciobanu, R., «Călin Georgescu este prezentat după decizia CCR drept martir, pe o rețea de site-uri răspândite în toată lumea și create la Moscova, a descoperit o agenție a statului francez», *HotNews.ro*, 9 de diciembre de 2024.
39. «The Wagner-style mercenaries plotting unrest in Romania», *Financial Times*, 11 de diciembre de 2024.
40. Matei, D., «SURSE Horațiu Potra și mercenari apropiați de Călin Georgescu, audiați de poliție / În mașina lui Potra s-a găsit un pistol și mai multe arme albe / Unii dintre șoferi au fost găsiți pozitiv la amfetamină», *G4Media*, 8 de diciembre de 2024.
41. Stefanescu, C., «Romania, DRC: Who is mercenary leader Horatiu Potra?», *Deutsche Welle*, 13 de febrero de 2025.
42. Popa, L., «1 milion de vizualizari intr-o ora pentru un candidat care promite 2 kg de aur fiecarui roman. Cum poate fi pacalit TikTok: "Vreau sa nationalizez Romania"*»*, *Aktual24*, 9 de diciembre de 2024.

43. «What happend on TikTok around the annulled Romanian presidential election? An investigation and poll», informe de *Global Witness*, 17 de diciembre de 2024.
44. Olari, V., «Rise of unknown Romanian presidential candidate preceded by Telegram and TikTok engagement spikes *»*, *DFRLab*, 12 de diciembre de 2024.
45. «Documento del CSAT SRI I *»*, escrito el 28 de noviembre 2024 y desclasificado el 4 de diciembre de ese año, disponible en la página web de la Presidencia de Rumanía.
46. Shekhovtsov, A., «¿Por qué se anularon las elecciones rumanas y a quién ha beneficiado realmente?», *El Español*, 19 de diciembre de 2024.
47. «En Rumanía, el candidato de extrema derecha Calin Georgescu ha sido detenido. La fiscalía lo acusa de financiación oculta de Moscú», *El Grand Continent,* 26 de febrero de 2025.
48. Higgins, A., «Romania Opens Criminal Case Against Ultranationalist Politician *»*, *The New York Times*, 27 de febrero de 2025.
49. Tingley, D.; Wagner, G., «Solar geoengineering and the chemtrails conspiracy on social media *»*, *Nature*, 31 de octubre de 2017.
50. Haunss, M.; Wiegand, K.; Wiegand, M., «Science and Environmental Communication on YouTube: Climate Change and Climate Engineering *», Frontiers in Communication*, 2019.
51. Kearney, A.; Sparks, G.; Hamel, L.; Montalvo III, J.; Valdes, I.; Kirzinger, A., «KFF Tracking Poll on Health Information and Trust: January 2025», *KFF*, 28 de enero de 2025.
52. Wolf Zachary, B., «Elon Musk wants to save Western civilization from empathy», *CNN*, 5 de marzo de 2025.