TRABAJOS DEL FORO CONTRA LAS CAMPAÑAS DE DESINFORMACIÓN

INICIATIVAS 2024

CAPÍTULO 3

MONETIZACIÓN Y ECONOMÍA DE LA DESINFORMACIÓN: ANÁLISIS DEL MODELO DE NEGOCIO EN LAS OPERACIONES DE DESINFORMACIÓN DIGITAL

Los expertos participantes en los Grupos de Trabajo lo son a título personal y no a título institucional. Por lo tanto, sus opiniones y recomendaciones no representan ni comprometen a las instituciones a las que pertenecen.

El resultado de los trabajos es producto de un ejercicio de reflexión colectivo, si bien, no tiene por qué representar la opinión individual de todos los participantes, quienes no necesariamente comparten todas las conclusiones o propuestas.

ÍNDICE

CAPÍTULO 3 4

MONETIZACIÓN Y ECONOMÍA DE LA DESINFORMACIÓN: ANÁLISIS DEL MODELO DE NEGOCIO EN LAS OPERACIONES DE DESINFORMACIÓN DIGITAL 5

INTRODUCCIÓN 7

TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS INVOLUCRADOS 12

RUSIA 12

CHINA 20

IRÁN 25

VENEZUELA 30

IMPACTO ECONÓMICO DE LAS ACTIVIDADES ANALIZADAS 31

ANÁLISIS DE DOCUMENTOS LEGALES PARA ABORDAR LA AMENAZA 41

CONCLUSIONES Y PROPUESTAS 42

ANEXOS 44

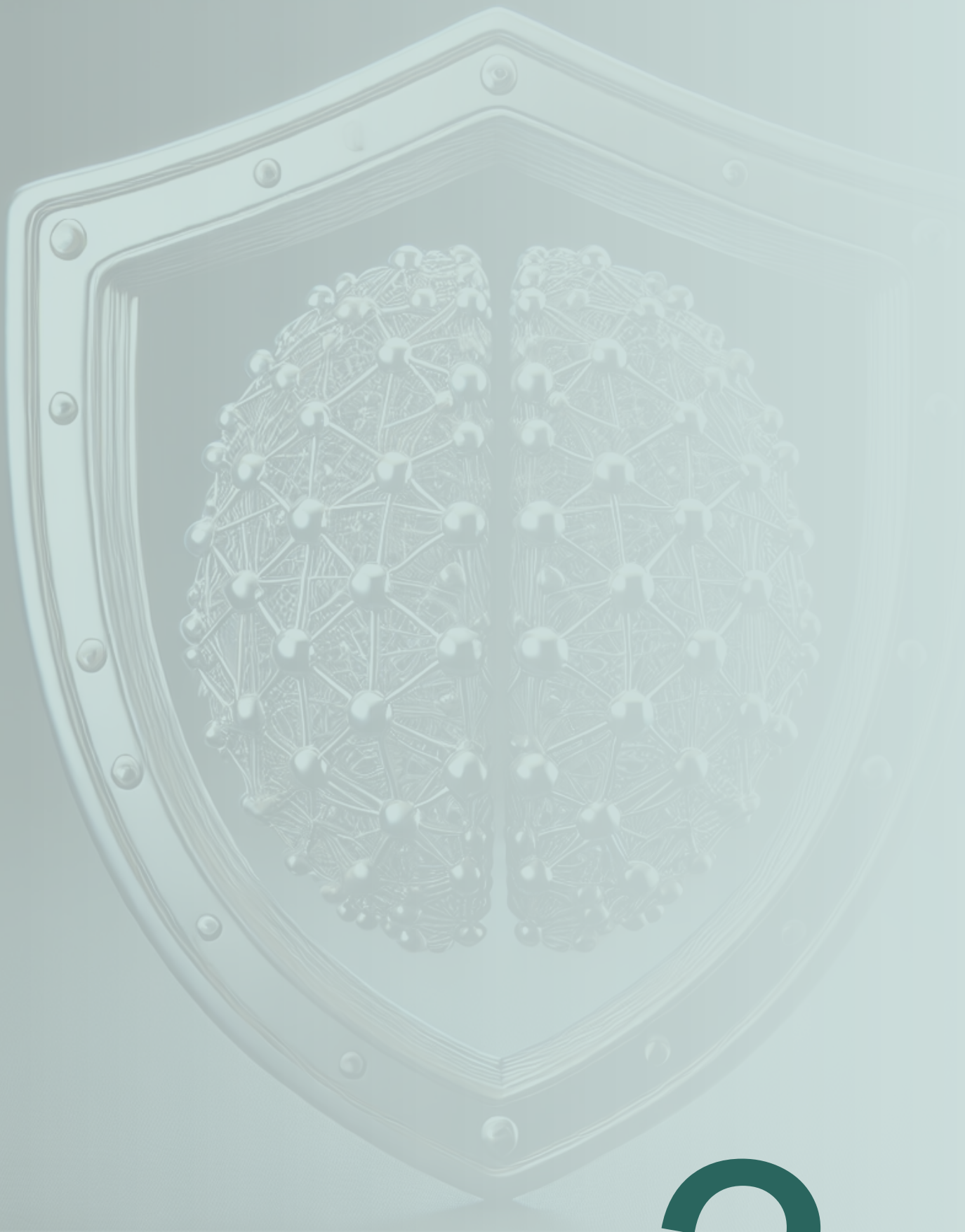
ANEXO I: IDENTIFICACIÓN Y DESCRIPCIÓN DE LAS TTP 45

ANEXO II: RELACIÓN DE COSTE E IMPACTO POR TTP 51

ANEXO III: NIVEL DE ALINEAMIENTO/EFICACIA ESTIMADA DE NORMATIVA NACIONAL Y EUROPEA FRENTE A LA AMENAZA 54

ANEXO IV: CRIPTODIVISAS COMO MÉTODO DE FINANCIACIÓN 62

REFERENCIAS BIBLIOGRÁFICAS 64



CAPÍTULO 3

MONETIZACIÓN Y ECONOMÍA DE LA DESINFORMACIÓN: ANÁLISIS DEL MODELO DE NEGOCIO EN LAS OPERACIONES DE DESINFORMACIÓN DIGITAL

Coordinadores:

Carlos Galán Cordero

Departamento de Seguridad Nacional (DSN)

Autores y colaboradores:

David Arroyo Guardeño

Nicolás de Pedro

Pedro Gómez García

Paula González Nagore

Jesús Manuel Pérez Triana

Nicolás Marchal González

Jania Mier y Teran

Francisco Pérez Bes

Iván Portillo

Jorge Félix Tuñón Navarro

Javier Valencia Martínez de Antoñana

Ministerio de Asuntos Exteriores, Unión Europea y Cooperación

Comisaría General de Información (Cuerpo Nacional de Policía)

INTRODUCCIÓN

Las campañas de desinformación o de manipulación e injerencia extranjera en la información son aquellas actividades hostiles consistentes en patrones de comportamiento desarrollados en el dominio informativo, desplegadas por actores estatales o no estatales extranjeros o sus *proxies*[1], tanto domésticos como no (en adelante, actores de la amenaza), que se llevan a cabo de forma coordinada, intencional y manipulativa, cuya implantación y difusión supone una amenaza para los valores constitucionales, los procesos democráticos, las instituciones democráticamente constituidas y, por ende, para la seguridad nacional (Departamento de Seguridad Nacional (DSN), 2021; Servicio Europeo de Acción Exterior [SEAE], 2023).

Dentro del conjunto de elementos que configuran el panorama de actores implicados en las campañas de desinformación orquestadas, sobresale la amalgama de tácticas, técnicas y procedimientos (TTP) cuyo despliegue obedece a criterios de efectividad en la persecución de sus objetivos estratégicos a través de acciones de interferencia en el espacio informacional del estado objetivo, lo que les lleva a combinar, acciones planificadas basadas en la selección adecuada de la audiencia objetivo, con otras de carácter oportunista, sobre los cimientos de metodologías previamente testadas, pero igualmente efectivas.

[1] Los *proxies* o actores interpuestos son entidades, organizaciones o individuos dentro de un Estado que actúan en interés de un actor extranjero. Pueden actuar como supuestos medios de comunicación, empresas de márketing y publicidad, organizaciones políticas, grupos de interés, funcionarios, o incluso figuras públicas e influencers. Aunque pueden estar radicados y operar dentro de su propio país, estos actores diseminan mensajes o propaganda que beneficia a un gobierno o entidad extranjera, en contra de los intereses nacionales. Los *proxies* pueden no estar directamente afiliados con los agentes extranjeros, o incluso encubrir dicha afiliación, pero pueden recibir apoyo en forma de financiación, información, o recursos. La utilización de *proxies* obedece a un interés del actor extranjero en ocultar su identidad o eludir la aplicación del derecho internacional. El término también hace referencia para identificar dominios web utilizados por actores maliciosos como fachadas diseñadas para blanquear su contenido informativo manipulado.

Dentro del conjunto de TTP[2], encontramos las que se basan en el empleo de supuestos expertos, "estrellas invitadas" (Centro Criptológico Nacional [CCN], 2019) o *influencers*, que se caracterizan por gozar de cierta credibilidad entre las audiencias potenciales para, de una forma directa o indirecta, alinearse con los intereses estratégicos y propagandísticos de los actores de la amenaza, por ejemplo, distribuyendo sistemáticamente las narrativas que viene difundiendo la estructura mediática, encubierta y abierta, desplegada por aquellos. En ocasiones, estas narrativas se adaptan al contexto sociopolítico doméstico, donde la propaganda directa no es explícita, sino que se disfraza con aparentes críticas legítimas con distorsiones, aprovechando el sesgo de confirmación de la audiencia objetivo, convirtiéndose estos actores intermedios en armas de influencia maliciosa, sutil y efectiva, para debilitar el apoyo a políticas enfocadas a contrarrestar las acciones hostiles de los actores de la amenaza.

Este acervo de actores se caracterizaría por tratar de aparentar la no vinculación o interés directo con los asuntos de discusión, es decir, proyectar una aparente naturalidad y neutralidad a la hora de abordar temáticas de índole internacional y geopolítico pero que, sin embargo, podrían constituirse en agentes encubiertos con motivación política, ideológica y/o económica y que, incluso, sus mensajes podrían llegar a formar parte de una estrategia coordinada de desinformación que las audiencias desconocieran.

Las vinculaciones o motivaciones económicas podrían subyacer de una serie de indicadores, como el empleo recurrente de plataformas específicas de *crowfunding*, o *wallets* de criptomonedas que propician la financiación encubierta mediante donaciones, algunas de forma opaca, donde algunas destacan por su carácter recurrente o por ser inusualmente elevadas. Frente a esta casuística, los analistas se enfrentarían a dos escenarios: el primero, un conjunto de individuos que divulgarían periódicamente la narrativa alineada con el actor de la amenaza, por el simple hecho de ver incrementados sus beneficios económicos por donaciones de terceros, lo que supondría una forma de cultivar actores propagandistas inconscientes (existen otras denominaciones en la literatura, como "*unwitting agents*"); un segundo, en el que los individuos serían conscientes del origen de los pagos recurrentes, independientemente de la mayor o menor opacidad del emisor.

La instrumentalización maliciosa de los algoritmos de recomendación de contenido de plataformas online supone también un mecanismo para obtener ingresos por publicidad mediante la creación de contenido como parte de una campaña de desinformación microsegmentada donde, necesariamente, intervienen un conglomerado de cuentas que, por un lado pueden coordinarse para potenciar la difusión y, por otro, insertar contenido en comunidades específicas para conducir la opinión a los intereses de los actores de la amenaza o, simplemente, provocar respuestas exacerbadas y polarizantes.

Adicionalmente, existen otras estrategias que ahondan en la monetización de las campañas de desinformación, que incluye el ingreso por publicidad insertada en sitios web creados ad-hoc; el uso de empresas de consultoría o servicios estratégicos apoyados financieramente por actores estatales, empresas privadas u organizaciones o entidades afines que canalizan los fondos hacia operaciones de influencia y/o cibernéticas; venta de productos de *merchandising*, libros u otros productos para, además de generar ingresos, consolidar la identidad del actor; así como estrategias de recopilación y venta de datos personales de usuarios para su posterior distribución a terceros

[2] El presente documento adopta como referencia el marco DISARM para describir y analizar los comportamientos manipulativos de los actores de la amenaza (DISARM, 2019).

con fines lucrativos y poder crear sofisticadas campañas de desinformación segmentadas con las que maximizan su rentabilidad.

A pesar de los esfuerzos para combatir la desinformación, los sitios web de informaciones poco fiables han aumentado su presencia en el ámbito informativo. Los propietarios de estos sitios también operan otros tipos de sitios web, incluyendo páginas de “Entretenimiento”, “Negocios” y “Política”, sin dejar de destacar que, aproximadamente, el 70% de los sitios de informaciones objetivamente falsas publicitan productos y servicios de “Negocios”, y cerca del 40% muestran anuncios de “Entretenimiento”. Todo ello indica que estos tipos de sitios web atraen una variedad de anunciantes que persiguen aprovechar el tráfico generado en estos lugares para mantener el flujo de ingresos hacia estos sitios de desinformación.

Por ejemplo, de cada 2,16 dólares gastados en sitios web de noticias en EE. UU., algo menos de la mitad se destina a sitios web que publican piezas desinformativas. Pese a todo ello, las agencias de publicidad en internet persiguen espacios publicitarios de menor costo, aunque residan en lugares de contenido cuestionable, lo que provoca que los presupuestos publicitarios se desplacen desde lugares de noticias de alta calidad a sitios controvertidos de bajo coste (Papadogiannakis et al., 2023).

Y todo ello es posible porque la producción de información manipulada es extremadamente barata y puede ser muy rentable. La creación y difusión de este tipo de narrativas requiere muy pocos recursos en comparación con noticias legítimas y de calidad. Como es lógico suponer, las piezas informativas objetivamente falsas o manipuladas no necesitan cumplir con los estándares periodísticos de verificación de hechos y precisión. Además, las redes sociales facilitan una rápida y amplia difusión de este tipo de contenidos ya que los algoritmos de estas plataformas tienden a priorizar el contenido que genera más interacción, lo que a menudo incluye narrativas distorsionadas o de posverdad presentadas con un discurso sensacionalista, generando un ciclo en el que este contenido se difunde con enorme rapidez y extensión.

Como se viene incidiendo, los costes de producción de este tipo de contenido son muy bajos, porque no requieren periodistas profesionales ni investigaciones rigurosas, todo ello sin contar con que los creadores de dichas piezas informativas pueden utilizar contenido generado por terceros usuarios, imágenes manipuladas o descontextualizadas y llamativos titulares para atraer la atención de los lectores, lo que posibilita a los actores de la amenaza maximizar sus ganancias con una inversión mínima (Condliffe, 2017).

Sin embargo, tampoco se puede obviar que, entre las factibles estrategias, se encuentra también la creación de supuestos *think tanks* enfocados a cubrir análisis geopolíticos utilizando figuras como los citados “expertos” o “estrellas invitadas”, para simular una mayor garantía de veracidad en la narrativa transmitida, a la vez que ocultan la entidad, organización o agencia que los financia o dificultan su atribución por la excesiva complejidad de la estructura societaria y/o económica que las sufraga.

En 2020, la Universidad de Oxford (Bradshaw et al., 2020) publicó un informe en el que identificaba las cibercapacidades que poseían numerosos países para realizar campañas de desinformación.

En concreto, el documento establece que **Rusia** posee un alto número de recursos humanos dedicados a tales propósitos, contando con equipos permanentes operando a nivel nacional e internacional, y empleando una amplia variedad de herramientas y estrategias sofisticadas para generar y difundir campañas de desinformación, particularmente efectivas en la amplificación

de narrativas antidemocráticas, incluyendo la interferencia en procesos electorales en diversos países.

China, por su parte, también posee una alta capacidad de elementos ciber en tales actividades, asimismo centralizados y operando de manera permanente. Las campañas de desinformación chinas se han centrado en amplificar narrativas favorables al gobierno y en desacreditar a los críticos, tanto a nivel nacional como internacional.

Del mismo modo, **Irán** ha evidenciado poseer una alta capacidad para interferir en el dominio de la información, dirigiendo sus campañas desinformativas tanto a audiencias nacionales como internacionales, utilizando una combinación de cuentas automatizadas y gestionadas por humanos para difundir propaganda progubernamental y atacar a la oposición.

Según el citado informe, **Venezuela** contaría asimismo con una significativa capacidad de generación de campañas de desinformación, a través de equipos tanto permanentes como otros que operan exclusivamente en momentos de crisis. Las campañas de desinformación en Venezuela habrían sido utilizadas para apoyar al gobierno y desacreditar a la oposición, utilizando una estructura militarizada para gestionar grandes cantidades de cuentas en redes sociales.

Todos estos países, gobernados por regímenes dictatoriales, autocráticos o híbridos (Freedom House, 2024; Economist Intelligence Unit, 2023), constituyen retos estratégicos, al disponer de las capacidades necesarias para desplegar acciones de injerencia en el espacio informacional, siendo objeto de estudio y análisis en el presente documento.

Como ejemplo reciente de cómo operan este tipo de campañas, en septiembre de 2024, el Departamento de Justicia de EE. UU., inculpó a un medio controlado estatalmente por Rusia por financiar y planificar la creación y distribución de contenido a diversas audiencias estadounidenses que incluían mensajes encubiertos pro-Kremlin. Este proyecto consistía en financiar y dirigir, de forma opaca, una empresa de creación de contenidos con sede en EE. UU. a través de la cual se publicaban narrativas en diversos canales de redes sociales, incluyendo TikTok, Instagram, X y YouTube, con el objetivo de provocar divisiones internas a la vez que estaban específicamente dirigidos a objetivos declarados púbicamente por el Kremlin (Departamento de Justicia de EE. UU., 2024). Para llevar a cabo esta actividad, se llegó hacer uso de identidades falsas, se financió operaciones a través de una red de entidades pantalla a objeto de aparentar financiación independiente, se reclutaron *YouTubers* a los que se ofrecía ingente cantidad de dinero, o se crearon contenidos videográficos dirigido para lograr un mayor impacto.

Dado este escenario planteado, este documento pretende por un lado, describir como afectan este tipo de campañas y, por otro, abordar una metodología de análisis, basado en el estudio de información recopilada de fuentes abiertas, que permita dotar a los distintos investigadores de organizaciones públicas o privadas, periodistas y a ciudadanos en general, de herramientas e indicadores para identificar las TTP relacionadas con la monetización de las campañas de desinformación y contribuir a exponer la infraestructura económica que respalda estas actividades enfocadas a interferir en los flujos informativos de los estados democráticos.

Pese a que pueden existir actores domésticos, que se valen de este tipo de estrategias para obtener fuentes de financiación, este documento se centrará únicamente en analizar las TTP originariamente empleadas por actores estatales y no estatales extranjeros y sus proxies, así como de otros actores que, sin una atribución directa y manifiesta, se alinean, voluntaria o involuntariamente, con los intereses de aquellos.

Igualmente, se aborda una selección de documentos normativos, tanto europeos como nacionales, a objeto de analizar si las democracias consolidadas cuentan con las capacidades y con suficientes instrumentos legales para afrontar el reto planteado por los actores de la amenaza que utilizan las campañas de desinformación como modelo de negocio, para obtener financiación propia con la que seguir sufragando su estructura digital, además de captar potenciales proxies como fuente de difusión doméstica de propaganda y desinformación alineada con aquellos.

TÁCTICAS, TÉCNICAS Y PROCEDIMIENTOS INVOLUCRADOS

En relación con los mecanismos usados por los agentes de la amenaza, se ha determinado un procedimiento de análisis inicial basado en estipular la superficie de herramientas que, dentro de la metodología DISARM, deben ser tomadas en consideración.

DISARM es un marco maestro para hacer frente a la desinformación a través de análisis y compartición de datos, desarrollado a partir de las mejores prácticas mundiales en materia de ciberseguridad. DISARM se utiliza para ayuda a los analistas a obtener una clara comprensión compartida de los incidentes derivados de las campañas de desinformación y a identificar inmediatamente las acciones defensivas y de mitigación de que se disponen.

Con el propósito de centrar la atención en los objetivos fijados para el presente trabajo, se han considerado exclusivamente aquellas TTP de DISARM (ver listado de TTP en ANEXO I) que, formando parte del grupo de herramientas usadas por los atacantes, poseen claras implicaciones en la determinación del impacto económico de las campañas de desinformación y de su eventual monetización por parte de los actores de la amenaza.

RUSIA

Para analizar las TTP de los mecanismos de monetización que utiliza Rusia, es necesario considerar diversas dimensiones. Partiendo de la tabla de TTP identificadas para el marco de este estudio, para el caso de Rusia podemos abordar el análisis desde diferentes perspectivas:

Dependencia del coste asumible con la necesidad de ofuscación y la capacidad de infraestructura

A partir de las tácticas definidas, el coste económico de cada una de ellas hace referencia a la infraestructura requerida para ejecutar la acción, lo cual incluye el gasto en construcción, implementación, mantenimiento y funcionamiento de dicha infraestructura.

En este sentido, encontramos TTP como la de adquirir o reclutar una red (T0093), desarrollar medios o activos propios (T0095) o apropiarse de fuentes confiables para hacerlas tuyas (T0100) son acciones con altos costes económicos y logísticos. Por otro lado, el coste también puede hacer alusión a la necesidad de ofuscación. Tácticas como la de ocultar a las personas, la actividad operativa o la infraestructura de la operación (T0128, T0129 y T0130) son un ejemplo de TTP que se accionan con el objetivo de evitar que se descubra al actor que hay detrás de dichas operaciones. Armar y costear la infraestructura necesaria para que una red de usuarios (excluyendo el caso de los *bots* y granjas) pueda activarse en redes sociales para mover un mensaje de manera orgánica, requiere de un sistema muy bien coordinado. Además, organizar dichas cuentas para evitar una vinculación directa con un Estado autocrático, sumamos un coste adicional que es el tiempo, que no deja de traducirse también a un factor económico.

Siguiendo esta reflexión, resulta necesario definir para cada Estado objeto de este estudio en qué posición se ubican dentro del eje ofuscación - infraestructura, que nos puede ayudar a explicar por qué se decantan por unas TTP u otras.

Figura 1. Agrupación de TTP en función de su necesidad de infraestructura y ofuscación. Siguiendo el esquema planteado, podríamos decir que Rusia sería un actor bastante versátil, moviéndose en cualquiera de los 4 grupos dependiendo de la situación. Existirán ocasiones en las que se permite perder capacidad de ofuscación en aras de ser más efectivo y operativo con sus acciones, no renunciando a realizar acciones de los grupos 1 y 3 mientras desarrolla en segundo plano acciones del grupo 2 y 4.

Asumir que el uso es independiente del coste

A pesar de que hay algunas tácticas más costosas que otras económicamente hablando, Rusia por lo general se caracteriza por utilizar cualquier medio o recurso a su alcance para poder llevar a cabo sus operaciones. Esto se debe a que, en el espectro de operaciones de influencia o desinformación analizadas y atribuidas a Rusia por acción directa o a través de terceros, se han localizado acciones altamente elaboradas con el objetivo de ofuscar la estructura que puede haber detrás de ella, pero también otras acciones menos elaboradas y directas que pueden pasar por utilizar sus propios canales oficiales, o contar con la ayuda de personas que actúan como altavoces, difundiendo sus narrativas estratégicas independientemente de lo expuestos o no que queden dichas personas al difundirlas. Por ejemplo:

1. Una operación elaborada es el caso analizado y publicado por el servicio francés denominado *Portal Kombat* sobre una red de propaganda prorrusa (Servicio de Vigilancia y Protección contra Injerencias Digitales Extranjeras [VIGINUM], 2024a).

2. Como operación a través de sus canales oficiales tendríamos de ejemplo las acciones llevadas a cabo por Rusia tras el inicio de la Guerra de Ucrania en 2022 y el bloqueo europeo de RT y Sputnik, que coordinó sus mensajes y narrativas sobre el conflicto a través de las cuentas oficiales en redes sociales occidentales de las embajadas y consulados en Occidente y Latinoamérica.

3. Como operación a través de portavoces estratégicos, tendríamos el caso del conocido Robert Kennedy Jr., al que se identifica en multitud de medios por su narrativa alineada con intereses de Rusia, desde temas geoestratégicos como la guerra de agresión rusa en Ucrania o la política estadounidense, hasta otras basadas en teorías de la conspiración durante la crisis de la pandemia de la COVID-19 (Kerr, 2023; Sammarco, 2024; Novelo, 2024).

Por todo ello, podríamos decir que en este caso Rusia tiene un plan de acción muy enfocado al largo plazo para mantener sus acciones de influencia, las cuales prepara y ejecuta con un nivel medio o alto de ofuscación y un coste de infraestructura variable, ejecutando en el proceso otras operaciones inmediatas que pueden llevarse a cabo con menor necesidad de ofuscación y que incluso utiliza recursos ya establecidos en su operativa, como *influencers*, canales de difusión y narrativas estratégicas, medios de comunicación o sitios web apropiados[3], etc.. Para ello es imprescindible disponer de recursos económicos para poder llevarlo a cabo, teniendo claro dónde

[3] El pasado octubre, la organización Center for Defense Reforms (2024) publicó un informe en el que exponían razonadamente, siguiendo una metodología de desarrollo propio, bajo los auspicios de la Plataforma OTAN-Ucrania para la Detección Temprana y lucha contra las Amenazas Híbridas, diferentes medios y actores que supuestamente actuaban bajo los intereses del Kremlin o estaban alineados con su estrategia de propaganda y desinformación. Estos actores o "agentes de influencia" se les presume un nivel inherente de confianza dentro de la sociedad, al ser vistas como expertas en seguridad, defensa y relaciones internacionales, lo que les permitiría influir directa e indirectamente en la toma de decisiones. Por otro lado, en relación con los medios, se encuentra Rebelión, cuyo contenido no es original, habría venido utilizando perfiles falsos para publicar sus contenidos (T0009). Un ejemplo de ello lo encontramos con el perfil "María Mercedes Blanco Reyes", la cual ha publicado numerosos artículos en dicho medio (véase https://rebelion.org/autor/maria-mercedes-blanco-reyes/) y en otros con base en estados dictatoriales (véase https://www.5septiembre.cu/author/maria/) o de fuerte polarización social (véase https://www.tercerainformacion.es/opinion/27/10/2024/la-cooperacion-ucraniana-con-los-terroristas-africanos-la-verdad-o-desinformacion/). Estos artículos tienen fácil replicación en otras plataformas gracias a la licencia que permiten su distribución gratuita en otras fuentes siempre que se referencie al autor.

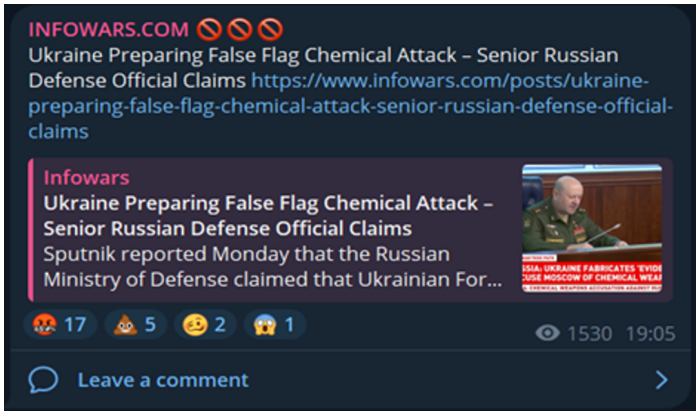
y cuándo poner el esfuerzo económico, sin realmente descartar ninguna de las opciones. Esta estrategia claramente se contrapone a la de otros países incluidos dentro de este estudio, que cuentan con situaciones diferentes a la de Rusia. Podríamos compararlo con el caso de Venezuela, que cuenta con menos recursos económicos y por lo tanto se puede considerar limitado tanto en la variable de infraestructura como en la de ofuscación; o el caso de Irán o China, que cuentan con una necesidad ofuscación mucho más elevada derivada de su operativa y de sus objetivos estratégicos, que buscan moverse en una penumbra que ayude a ocultar sus movimientos e intereses reales.

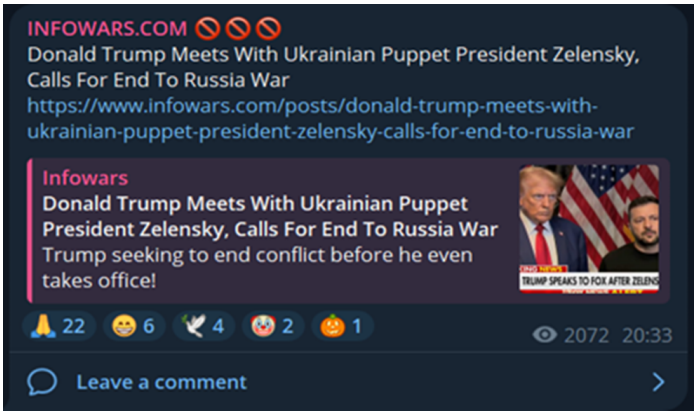
¿Acción directa o a través de terceros?

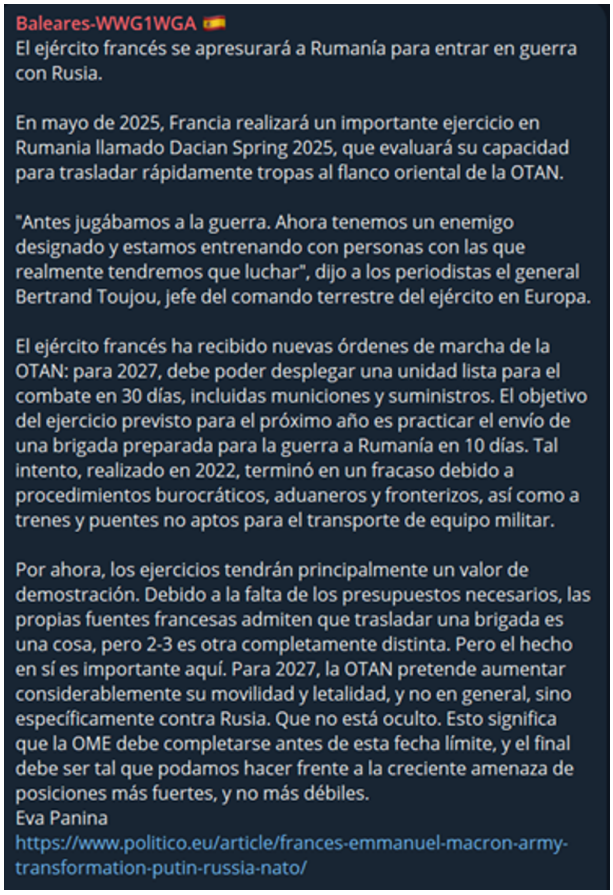
Dentro de las 55 TTP identificadas para el estudio, se han evaluado si Rusia, de acuerdo a las acciones pasadas identificadas bajo su autoría en investigaciones ya publicadas como las ya mencionadas y otras como RNN (VIGINUM, 2023) y Matriochka (VIGINUM, 2024b), la investigación Roller Coaster del medio ucraniano Texty.org.ua entre otras, arrojan otra dimensión a tener en cuenta a la hora de analizar los mecanismos de financiación: si la táctica seleccionada no sólo puede ser llevada a cabo por medios propios o a través de terceros, sino si Rusia prefiere hacerlo a través de otros actores incluso aunque pudiera hacerlo ella misma. En este sentido, casi todas las TTP seleccionadas pueden ser llevadas a cabo directamente por Rusia, si bien algunas de ellas quizás no se realicen directamente a través de ellos. Algunas de las TTP identificadas que Rusia suele realizar a través de terceros son:

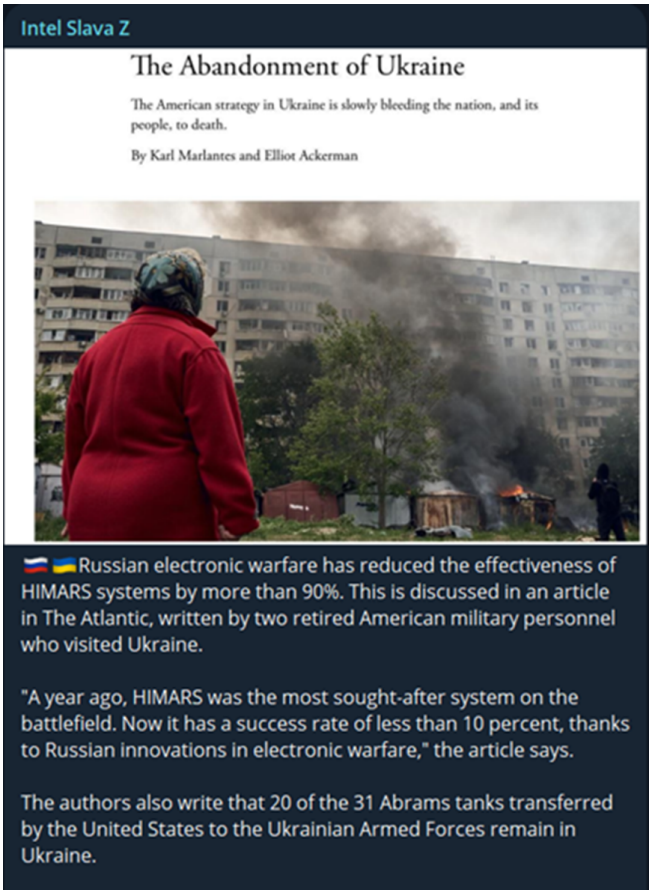
- Aprovechar narrativas basadas en teorías de conspiración (T0022). Por ejemplo, pieza informativa publicada en 2023 por la agencia estatal rusa Sputnik (Sputnik, 2023).

- Usar aplicaciones de chat (T0043)









Ejemplos de mensajes publicados en canales de Telegram no oficiales de Rusia con narrativas prorrusas (https://t.me/InfowarsChat/188036, https://t.me/infowarslive/39160, https://t.me/BalearesWWG1WGA/39155, https://t.me/intelslava/67942)

- Crear *Clickbait* (T0016)

Vídeo difundido basado en titular de clickbait (AFP, 2023) sobre una supuesta propaganda anti-LGTBI en EEUU. El análisis se produjo después de que el vídeo fuera difundido desde la cuenta oficial de Elon Musk y otros perfiles en Twitter. El mismo vídeo es reportado por medios húngaros (Zubor, 2023) y por haber sido difundido a través de VK y por grupos húngaros como "La Legión de San Esteban", que ha sido vinculado (Solymos y Panyi, 2023) con los servicios de inteligencia rusos y la red de desinformación NewsFront (Global Engagement Center [GEC], 2020a).

Del análisis realizado de cara a establecer o definir cuáles son los mecanismos de financiación de la desinformación, la realidad es que tanto para Rusia como para cualquier otro actor que quiera generar acciones de desinformación o campañas de influencia el primer proceso de toma de decisiones está en definir si la acción la lleva a cabo uno mismo o a través de terceros.

Esta decisión es crucial, ya que al realizar las acciones por sí mismo, Rusia controla todos los aspectos del proceso, lo que facilita la obtención de financiamiento. En cambio, si la acción es llevada a través de terceros, se añade la complejidad de encontrar la manera de hacer llegar la financiación al actor que va a desarrollar o formar parte de la campaña.

Teniendo en cuenta esta situación, queda claro que aquellas acciones que Rusia pueda llevar a cabo por sí misma, a través de sus activos como puedan ser medios de comunicación gestionados a través de empresas controladas en última instancia por el gobierno, sus propios canales oficiales, etc. Por contra, si se quiere generar contenido a través de otros medios de comunicación, influencers u otros canales con acción y repercusión en medios digitales, hay que buscar otra forma de hacerlo. Y para ello, la forma más sencilla es utilizar los medios que ponen al alcance las propias plataformas digitales.

¿Cómo financia Rusia las acciones llevadas a cabo a través de terceros?

Para este estudio, se seleccionó una muestra de actores con presuntas conexiones prorrusas, incluyendo perfiles de redes sociales y sitios web, de acuerdo con lo señalado en las siguientes investigaciones de terceros:

- Roller Coaster (Gadzynska et al., 2024).
- RNN (VIGINUM, 2023).
- Portal Kombat (VIGINUM, 2024a).
- Matriochka (VIGINUM, 2024b).

De la muestra de usuarios seleccionada, se han localizado los portales web y redes sociales que utilizan para difusión de contenido y, en ellos, los sistemas de financiación que ponen a disposición de terceros para que den su apoyo al proyecto que están desarrollando. Los que se han localizado, de mayor a menor presencia, son:

- **Plataformas de micromecenazgo mediante pagos puntuales o suscripción:** en este apartado encontraríamos sitios web como go-fund-me, ko-fi, BuyMeACoffee, GiveSendGo, SendATip, Patreon o Anedot. En el caso de suscripciones, encontramos SuscribeStar.

- **Suscripciones en redes sociales:** a pesar de que el seguimiento de los donantes es muy complicado, varios de los actores analizados muestran disponer de canales de streaming en Twitch, YouTube o Kick a través de los cuales reciben suscripciones mensuales y suscripciones dadas a durante el streaming. En este sentido, también incluimos la plataforma de miembros de la red social X (anteriormente Twitter).

- **Tiendas de *merchandising*:** predominan principalmente tiendas propias de *merchandising* en las páginas web para la compra de productos promocionales como gorras, camisetas, sudaderas, libros, material de papelería, etc. En este caso también se ha visto el uso de sitios web *eCommerce* como Shopify, BigCommerce, WooCommerce, Magento de Adobe Commerce, Wix eCommerce, Squarespace, PrestaShop, Shift4Shop, Weebly, Volusion o Ecwid. No obstante, éstos últimos se usan en menor medida, probablemente debido al coste de mantenimiento de estos.

- **Plataformas de pago P2P y apartado "donaciones" ("*donate*") en la página web:** en este caso nos encontramos diferentes escenarios, porque hay varios actores que utilizan plataformas más extendidas como Paypal, pero hay otras que se usan de manera más residual, sobre todo en ciertos países como EE. UU. en los que se ha localizado también enlaces a GabPay. En cambio, encontramos que casi cualquier actor que disponga de una página web propia cuenta con un apartado propio de "donaciones" a través del cual se puede dar dinero al proyecto.

- **Wallets de criptomonedas y *crypto exchanges*:** en un volumen similar a las tiendas de *merchandising* y secciones de donaciones en web, a veces incluso

dentro del propio apartado de donaciones, encontramos referencias a *wallets* de las principales criptomonedas (Bitcoin, Ethereum, Solana, Cardano, Monero, USDT, Matic o USDCC entre otras). En cambio, no se han detectado actores que compartan cuentas en *crypto exchanges* como Binance o Coinbase, probablemente porque la identificación del donante y del receptor es necesaria en este tipo de plataformas. En ANEXO IV se amplía información sobre el uso de criptoactivos como fuente de financiación.

- **Plataformas de *crowdfunding*:** de manera residual se ha detectado alguna campaña en plataformas como Kickstarter o mediante *crowfundings* propios anidados en sus páginas web, donde piden donaciones directamente.

Del análisis de todos estos modelos de financiación que se han localizado, se han extraído una serie de variables que permitan evaluar el coste o complejidad de realizar la financiación a través de estos medios:

- **¿Utilizar el medio de financiación conlleva algún coste?** Frente a esta pregunta pueden identificarse tres situaciones:
    - El sistema es gratuito para el receptor de la financiación, como lo podrían ser las criptomonedas, las plataformas de pago P2P o los medios propios en función de la pasarela de pagos utilizada.
    - El sistema conlleva algún coste o fee por transacción recibida, caso de algunas plataformas de suscripción, *eCommerce*, o micromecenazgo.
    - El sistema conlleva también algún coste de mantenimiento de algunas plataformas de *eCommerce*, plataformas de Streaming.
- **¿El medio de financiación implica una identificación del receptor de la transacción?** En este caso, encontramos que la gran mayoría sí requieren que el actor que recibe el dinero se identifique con un DNI o número de identificación empresarial, de cara al pago de los impuestos correspondientes como parte del proceso que llevan a cabo estas plataformas como parte de su acuerdo de servicio de KYC (*Know Your Customer*). El único medio que se escapa a esta situación serían las *wallets* de criptomonedas, ya que depende de la *wallet* que se utilice y si el dinero se trata de convertirse a divisa FIAT, en cuyo caso sí sería necesario.
- **¿Es necesario que el donante se identifique?** En este caso nos encontramos con que en su mayoría no requieren una identificación del donante más allá de la identificación a través del método de pago en todo caso, siendo una situación para la que existen recursos con los que poder evitarlo. En este caso únicamente excluiríamos de manera puntual las plataformas de pago P2P o los *exchanges* de criptomonedas, que sí que requieren una identificación completa del usuario, ya sea emisor o receptor de la transacción.

Teniendo en cuenta estas variables, queda claro que para un país como Rusia es vital que sus actores terceros utilicen plataformas que permitan financiación a través de métodos que supongan

el menor coste posible, y a través de los cuáles se pueda ofuscar la identidad del o los donantes que transfieren el dinero. Esto haría que, a la hora de definir los mecanismos de financiación más utilizados por Rusia de cara a dar soporte económico a terceros en sus campañas de desinformación e influencia, nos quedaríamos con:

1. **Medios de financiación autogestionados**, como tiendas online de *merchandising* o pasarelas de donaciones en sus propias páginas web, siendo el único coste el hosting de la web y la pasarela de pagos.

2. ***Wallets* de criptomonedas**, suponen por un lado el mecanismo más seguro para ofuscar las transacciones, incluso más que los autogestionados. Por contra, conllevan el riesgo de transformar a posteriori las criptodivisas a dinero FIAT para poder utilizarlo.

3. **Plataformas de micromecenazgo**, que pueden hasta ser gratuitas para el receptor, teniendo el único coste de una pequeña comisión por cada transacción recibida.

4. **Plataformas de streaming** que, si bien pueden ser de entre los seleccionados los que más complicado pueden presentar el eludir la identificación mediante el método de pago, la falta de transparencia sobre los listados de suscriptores, miembros y donaciones recibidas en *stream* por parte de las plataformas mencionadas hace que sea sencillo lanzar donaciones periódicas a través de estos métodos.

Con ello, desde un punto de vista financiero, a priori, no sería viable para Rusia el uso de plataformas *eCommerce*, cuyo uso es muy residual debido al coste de mantenimiento, las plataformas P2P por la necesidad de identificación de los participantes en la transacción, y las plataformas de *crowdfunding* porque, si bien se ha detectado alguna, son muy residuales y en la mayoría de las ocasiones son gestionadas a través de plataformas de micromecenazgo.

CHINA

La desinformación: el gran músculo de Pekín en la nueva Guerra Fría

El *Concepto Estratégico de Madrid* —aprobado en junio de 2022, durante la cumbre de la OTAN en la capital de España— oficializa, de alguna manera, un nuevo mapamundi geopolítico marcado por el enfrentamiento de bloques, casi como una versión actualizada de la Guerra Fría. De una parte, los países integrantes de la Alianza Atlántica —junto a sus socios—, y, de otra, China y Rusia —y sus aliados—. Este nuevo paradigma ya había sido percibido en Europa antes de la celebración de la cumbre, especialmente a raíz de la invasión de Rusia a Ucrania del mes de febrero (Hernández, 2022). Puede decirse que aquel momento supuso el inicio de un cambio apreciable en la imagen pública de ciertos países, como mostró el *Barómetro* del Real Instituto Elcano pocos días antes de que se reunieran los mandatarios de la Alianza, y en donde se señalaba que Rusia no solo había empeorado su imagen entre los españoles, sino que ya se percibía como la principal amenaza para la seguridad europea; todo ello al tiempo que se reforzaba el sentimiento de pertenencia a la alianza militar (González Enríquez y José Martínez, 2022).

Efectivamente, la cumbre de Madrid supuso una revitalización de la OTAN que, en algunos aspectos, incluso ha superado las expectativas de los expertos. Ejemplo de ello son los trabajos de

los analistas Arteaga y Simón (2022), comparando los resultados de la cumbre con las previsiones de diciembre de 2021, concluyendo que el *Concepto Estratégico de Madrid* ha asentado una relación entre Europa y Norteamérica mucho más estrecha, que «atrae nuevos miembros, como los neutrales Suecia y Finlandia», y con la que las «regiones de interés estratégico» —término que reemplazada al de «flanco»— se han ampliado a Oriente Medio, el Norte de África y el Sahel. También mencionan como signos de fortalecimiento el hecho de que todos los miembros se comprometieran a incrementar -al menos- en un 2% de su PIB el gasto en defensa, al tiempo que se fijaba el objetivo de hacer de la OTAN la organización internacional que lidere la adaptación a los nuevos retos sobre seguridad. Finalmente, los citados expertos recalcan la apuesta por adaptar la operatividad de la organización a «todos los dominios (tierra, mar, aire, espacio y ciberespacio), en sus formas convencionales y no convencionales (guerra híbrida)», así como el establecimiento de un fondo común para financiar el desarrollo de tecnología en materia de defensa (Arteaga y Simón, 2022), revitalizando y flexibilizando su operatividad para hacer frente a nuevos desafíos tales como el terrorismo, las migraciones o la desinformación (Priego, 2022), esta última una amenaza clara para la seguridad y estabilidad de los aliados que emana de Rusia, sin olvidar un riesgo estratégico y sistémico *a largo plazo*: China (Arteaga y Simón, 2021).

Parece claro, por tanto, que el reposicionamiento de la OTAN (Hao, 2022) frente a China es la muestra más palpable de la entrada en una *nueva Guerra Fría* cuyos principales actores —Estados Unidos, China, Rusia y la Unión Europea— configuran un escenario complejo (Aguirre, 2022). En él, las tecnologías digitales desempeñan un papel fundamental puesto que constituyen uno de los principales recursos de las actuales amenazas híbridas. Según diversos informes europeos (Parlamento Europeo, 2021), estas tecnologías facilitan la creación de grandes volúmenes de información que se difunde a gran velocidad y que pueden ser utilizados como un arma de guerra, incrementando la influencia de los estados a través del denominado "*soft power*" o "poder blando" (Repnikova, 2022). Así, y en línea con lo señalado por el nuevo *Concepto Estratégico* de la OTAN, la combinación de "poder blando" y "poder duro", en forma de "amenazas híbridas", se erige en un componente geoestratégico clave, especialmente utilizado por China para expandir su influencia (Luna, 2022), mediante campañas en las que suelen combinar la propaganda (De la Cal, 2022c) y la desinformación (Milosevich-Juaristi, 2020).

Las narrativas y las campañas de desinformación de China

En el caso del gigante asiático, el Partido Comunista de China (PCCh) es la organización que, desde hace décadas, gestiona el discurso político dentro de las fronteras del país, mediante un férreo control sobre los medios de comunicación —tanto convencionales (Belinchón, 2022) como digitales (T0002)—, esforzándose igualmente por gestionar la imagen exterior del país, concentrando su atención, en un primer momento, en las comunidades de habla china fuera de sus fronteras y en los corresponsales extranjeros destinados en su país.

Pese a la imagen que puede tenerse de China, como el paradigma de un país *aislacionista* (M. Martín, 2021), en la última década el PCCh ha intensificado sus esfuerzos (International Republican Institute [IRI], 2022) para dar forma a los contenidos y las narrativas de los medios de todo el mundo (Dubow et al., 2022) y en diferentes idiomas (Cook, 2020), defendiendo un orden mundial ajustado a la visión de sus intereses. Este discurso enarbola la idea de un nuevo consenso internacional, en el que la República Popular sea uno de los actores principales en la

gobernanza de un nuevo *mundo multipolar* (Delage, 2019), idea implícita en su cultura milenaria[4], en la que el país es representado como *centro del mundo* y del *origen de la civilización* (Hernández y García, 2021). Los diplomáticos y los medios de comunicación oficiales de China abogan de manera sistemática por lo que denominan "mundo multipolar",[5] concepto con el que China persigue aumentar su influencia internacional, aplicando la estrategia (Brime, 2021) del "divide y vencerás" (T0079 / T0077).

Bajo la dirección de Xi Jinping, el PCCh ha adoptado un enfoque más agresivo e integral en su objetivo de extender la influencia china, en muchas ocasiones, a través de estrategias dirigidas, según Cook (2020), a "socavar las normas internacionales y las características fundamentales de la gobernabilidad democrática, incluida la transparencia, el estado de derecho y la competencia justa" (T0127 / T0066).

China dedica una gran cantidad de recursos para fortalecer su *poder blando*, y en el que tanto los medios estatales como sus alianzas internacionales desempeñan un rol esencial para la difusión de una imagen positiva de su régimen, especialmente revelador en aquellos territorios del país en donde ciertas minorías étnicas vienen sistemáticamente sufriendo graves problemas de ataque a los derechos humanos (De la Cal, 2022b). Gracias a tal despliegue, los tentáculos del aparato mediático chino no han dejado de extenderse por todo el mundo en la última década. Entre los medios más influyentes del ecosistema comunicativo de Pekín, caben destacar seis (Cook, 2020): las televisiones *China Global Television Network (CGTN)* y *China Central Television (CCTV)*, los diarios *China Daily* y *People's Daily*, la emisora *China Radio International (CRI)*, y las agencias *Xinhua* y *China News Service (CNS).* A todo ello hay que sumarle el aumento del poder del PCCh sobre medios de comunicación de todo el mundo, logrado a través de una compleja red (Rathbone y Sevastopulo, 2022) de colaboraciones, alianzas, influencias (Corera, 2020; Global Influence Operations Report, 2022; Nimmo, 2022; Reuters, 2022) y adquisiciones, que tienen como base de operaciones su propio ecosistema comunicativo. Con dicha red, Pekín difunde su narrativa usando la propia línea editorial de los medios extranjeros, lo que hace más difícil identificar el origen de la información propagandística, al tiempo que incrementa su eficacia persuasiva.

---

[4] Los ciudadanos chinos llaman a su país «*Zhongguo*», que significa algo así como «Estado» o «pueblo del centro» y, más tarde, «nación del centro». El origen de esta expresión puede ser geográfico, aunque su uso cambió a medida que el país se expandía, para hacer referencia a una cultura central propia, diferenciada y superior. Otro concepto esencial en el pensamiento chino es el de «*Tianxia*» o «todo bajo el cielo», con el que se alude a la identidad milenaria e imperial del país como cultura civilizatoria y cuya legitimidad emanaba desde el cielo al emperador. Estos principios han pervivido durante siglos en la cultura china, la cual se ha mostrado abierta con aquellos pueblos que asimilasen sus recursos culturales y, así, alcanzasen un nivel de civilización superior.

[5] Por ejemplo: Zhang Meifang [@CGMeifangZhang]. (2022, 28 de octubre). #Latest *After Putin's remarks on China-Russia relations on Thursday, Chinese observers said the close interactions between the two countries in the future will drive the world toward a more just, effective and multipolar global order*. View: https://pbs.twimg.com/media/FgLNJvNXgAMKDi6?format=jpg&name=small [Imagen adjunta] [Post]. X. https://twitter.com/CGMeifangZhang/status/1586055594288422912

El valor estratégico del ecosistema digital para las campañas de desinformación chinas

En los últimos años, el ecosistema digital se ha consolidado como el principal espacio a través del cual Pekín difunde la información, campo de juego en el que la *Academia del Pensamiento* promueve las ideas de Jinping (Abril, 2022).

En la esfera interna, el PCCh controla la información que circula por el ciberespacio chino mediante la iniciativa «Proyecto Escudo Dorado», que comenzó a funcionar en los primeros años del siglo XXI. Bajo este programa, también conocido como la «Gran Muralla Digital China» o el «gran cortafuegos chino», Pekín mantiene un control férreo sobre la información que llega a los ordenadores de la población dentro de sus fronteras, de forma que cualquier dato que pueda ser contrario al régimen, se detecta y neutraliza con rapidez; manteniendo la eficacia (Wu y Lam, 2017) a través de las constantes actualizaciones del sistema (T0047).

Como señalamos, el poder del PCCh en este sentido es absoluto, sin que escape a su control ningún discurso mínimamente disidente[6]. Un ejemplo reciente (Hernández, 2022) lo encontramos en la censura que está sufriendo cualquier tipo de protesta (Radio Televisión Española [RTVE], 2022) relacionada con las políticas de Cero-Covid (De la Cal, 2022d; Abril y Bonet Bailén, 2022), entre ellas, las que se sirven de hojas en blanco como símbolo (Pollard y Goh, 2022), haciendo que portar un lienzo en blanco a modo de pancarta está prohibido y donde cualquier tipo de manifestación intelectual que no recoja exactamente lo que dicta el régimen (Araújo, 2022), no tiene cabida (T0123).

Respecto de los actores empresariales, hay que señalar que las empresas tecnológicas que operan en China son, exclusivamente, nacionales. Frente a Google, Amazon, WhatsApp o Twitter, en China se usa Baidu, Alibaba, Tencent, Weibo o WeChat (Yam, 2022). Estos gigantes tecnológicos vienen esforzándose por desarrollar algoritmos cada vez más sofisticados, capaces de responder a las exigencias de censura y vigilancia del régimen, como así señaló recientemente una evaluación del Consejo Nacional de Inteligencia de los Estados Unidos (National Intelligence Council [NIC], 2020). Así, siempre bajo las directrices del PCCh, estas organizaciones lideran la digitalización[7] de la información nacional al tiempo que, muchas de ellas, se expanden en el mercado internacional (Cook, 2020, p. 17). Ante esta situación, los ciudadanos chinos críticos con Jinping han tenido que buscar otras formas de escapar de la censura, tales como el empleo de AirDrop (Cheung, 2022) o la recurrir al uso de pasaportes falsos cuando no les queda más solución que salir del país (De la Cal, 2022a).

A nivel externo, sin embargo, Pekín recurre a las plataformas occidentales (T0059).

---

[6] Uno de los focos de control se refleja a través del funcionamiento de sus instituciones. A modo de ejemplo, puede leerse sobre el funcionamiento del Congreso en Ling (2022a, 2022b, 2022c).

[7] Por ejemplo: Lin, L. [@lizalinwsj]. (2022, 6 de diciembre). *1/ In China, most apps have changed their home page to black and white since Nov 30, the day of Jiang Zemin's death. The only thing remaining in color? Photos of Xi Jinping and the Politburo:* https://pbs.twimg.com/media/FjR2wU3acAA1_cu?format=png&name=900x900 [Imagen adjunta] [Hilo]. X. https://x.com/lizalinwsj/status/1600034448170713088

Como es sabido, el ecosistema digital es la principal fuente de información para el sector más joven de una población globalizada. Los jóvenes no suelen estar familiarizados con los medios impresos y, por lo general, no consumen los informativos de la televisión tradicional, optando por seguir la actualidad a través de plataformas digitales mediante una autoselección de información, incluso cuando su calidad sea más que cuestionable.

Además de ello, el crecimiento en el uso de las redes sociales se ve favorecido en todo el mundo por factores tales como la dificultad de atribución de responsabilidades o el amplio abanico de canales por los que se puede difundir información, verdadera o falsa (Bartolomé, 2021). Por estos motivos, la comunicación estratégica de Pekín ha hecho de la esfera digital uno de sus principales soportes, haciendo que el entramado mediático chino sea amplificado a través de las numerosas cuentas que cada medio tiene en Twitter, Facebook, YouTube o Instagram en el extranjero; mientras que, en China, su *Gran Muralla Digital*, mantiene el bloqueo sobre tales plataformas (Cook, 2020).

En los últimos años, Pekín ha dado un giro importante a su comunicación estratégica, no dudando en emplear un tono agresivo[8,9] con el que orquestar campañas de desinformación (Graham, 2022) contra los que considera sus enemigos (Cook, 2020). Por ejemplo, Taiwán -en 2018- y Hong Kong -en 2019-[10], fueron los objetivos de las primeras campañas de desinformación chinas, aunque fue en el entorno de la pandemia del COVID-19 (The Associated Press, 2020) cuando se produjo el cambio de modelo, al recurrir a la desinformación de una forma generalizada (Milosevich-Juaristi, 2020), viéndose obligado el PCCh a cambiar de táctica debido al degaste por la gestión de la crisis sanitaria. En ese momento, no recurrió a su estrategia tradicional de negar el acceso de la información[11], sino que adoptó un tonó más agresivo y, al estilo ruso, recurrió (Chan y Thornton, 2022) a «canales oficiales para propagar teorías conspirativas y luego divulgarlas por los medios de comunicación que dependen de la financiación estatal y a través de las redes sociales» (T0073, T0002).

---

[8] Por ejemplo: Air-Moving Device [@AirMovingDevice]. (2022, 28 de noviembre). *Thread: Search for Beijing/Shanghai/other cities in Chinese on Twitter and you'll mostly see ads for escorts/porn/gambling, drowning out legitimate search results. Data analysis in this thread suggests that there has been a *significant* uptick in these spam tweets. https://pbs.twimg.com/media/FinEPCBXEAAc7sZ?format=png&name=large* [Imagen adjunta] [Hilo]. https://twitter.com/AirMovingDevice/status/1597034969293271040

[9] Menn (2022) describe como China estaría ocultando noticias sobre las protestas.

[10] El 24 de noviembre de 2018 tuvieron lugar los comicios para elegir a los representantes de ámbito local en Taiwán. El Partido Demócrata Progresista (DPP, por sus siglas en inglés), que gobernaba la isla, fue derrotado frente a la formación pro-sínica Kuomintang (KMT). Durante la campaña, medios locales dieron credibilidad a noticias falsas que atacaban al PDD y cuyo origen estaba en China, comprándose la creación, también desde China, de redes pro-Han —uno de los candidatos del KMT— en Facebook. Más tarde, se tuvo la certeza de que se incrementó el número de noticias falsas sobre el oponente de Han desde cinco provincias chinas e, incluso, se constató la intención de agentes del gobierno chino de comprar páginas en Facebook pro-Taiwán, antes de las elecciones generales de 2020. Por otro lado, en 2019 Twitter eliminó 900 cuentas que se utilizaban para socavar la credibilidad de los manifestantes prodemocracia en Hong Kong. Más tarde le siguieron Facebook y YouTube. La red estuvo activa desde 2017 para atacar a líderes opositores del PCCh como Yang Jianli, Guo Wengui, Gui Minhai o Yu Wensheng (Cook, 2020, pp. 10-11).

[11] Al menos, fue así al comienzo del COVID, ya en que al final del 2022, la técnica cambio (Europa Press, 2022)

Los mecanismos de financiación de China como actor autocrático en la era de la desinformación

China Media Group (CMG) es el principal aparato de noticias del Partido Comunista Chino (PCCh) que opera en video y radio. Formado en 2018, CMG está compuesto por China Central Television (CCTV), CGTN, China National Radio (CNR) y China Radio International (CRI). En 2022, CMG recibió un presupuesto de 2.32 mil millones de RMB (344 millones de USD), con el 96% destinado a "cultura, turismo, deportes y medios de comunicación". CMG ha financiado asociaciones con medios y periodistas extranjeros para ampliar su alcance y promover narrativas favorables a China (DFRLab, 2023). Pekín también ha trabajado para cooptar a voces prominentes en el entorno informativo internacional (Global Engagement Center [GEC], 2020b), como las élites políticas extranjeras y los periodistas (T0010/ T0093).

En determinadas ocasiones, China también ha recurrido a la creación de perfiles falsos (T0009), ya que los medios chinos difundieron noticias falsas sobre un supuesto científico suizo llamado Wilson Edwards, quien criticó a Estados Unidos por su manejo de la pandemia de COVID-19 (Davidson, 2021).

Pekín busca maximizar el alcance de los contenidos sesgados o falsos a favor del Partido Comunista de China y ha adquirido participaciones en medios de comunicación extranjeros a través de medios públicos y no públicos y ha patrocinado a personas influyentes en línea (T0100). Eso podría englobarse en su estrategia de *Thousand Talents Plan*, por el cual el país estaría reclutando a científicos en investigadores occidentales (Keown, 2018). China está reclutando a especialistas occidentales a través de Redes Sociales en Occidente. Especialmente a través de la red social de LinkedIn (Burgess, 2023). El PCCh en España está impulsando la creación o aumento de recursos de organizaciones y *think tanks* mediante la organización de eventos. (T0126 / T0057).

IRÁN

Metodología de investigación sobre Irán

El enfoque metodológico seguido se centra en el análisis de narrativas digitales alineadas con los intereses geopolíticos y estratégicos de Irán. La investigación abarca múltiples plataformas, desde Telegram hasta otros canales digitales, con el objetivo de identificar patrones de comunicación, propaganda estatal y diversas tácticas de manipulación. El propósito es comprender cómo Irán impulsa su agenda ideológica, moviliza apoyo y desacredita a sus adversarios en el entorno informativo global.

Como punto de partida, se identifican los principales medios digitales donde podrían difundirse narrativas alineadas con los intereses iraníes. El ecosistema de propaganda utilizado combina múltiples capas de medios tradicionales y digitales, operando en varios idiomas para maximizar su alcance. Esta narrativa se amplifica y distribuye a través de un conjunto de medios y canales que incluyen:

- **Medios estatales** como HispanTV, Press TV y Al-Alam. El análisis pone especial énfasis en HispanTV, por su enfoque en audiencias hispanohablantes, mientras que Press TV y Al-Alam se dirigen a públicos de habla árabe.

- **Aplicaciones de mensajería y redes sociales** como Telegram, Twitter, Facebook y YouTube, utilizadas para la movilización de contenidos y campañas.

- **Medios aliados** como Al-Mayadeen y TeleSUR, los cuales comparten agendas antioccidentales y amplifican las narrativas iraníes.

- **Otros medios** vinculados a grupos cibercriminales, que a través de campañas de ciberespionaje y *hacktivismo* contribuyen a reforzar los mensajes estratégicos de Irán.

La segunda fase de la investigación se centra en la recolección de información de los medios digitales previamente identificados para su monitorización, obtención y análisis. El contenido recopilado abarca distintos formatos, como noticias, videos, infografías, memes, análisis políticos o ideológicos, discursos oficiales y contenido multimedia original o republicado.

Durante el análisis de la narrativa iraní se identifican varios puntos clave:

- **Narrativas predominantes**: Se determina la existencia de temas recurrentes y su respectivo encuadre narrativo, alineado con los intereses de Irán, como por ejemplo las siguientes narrativas:

    - **Apoyo a la resistencia palestina,** reforzando la idea de que Irán es un aliado clave en la lucha contra la ocupación israelí.

    - **Deslegitimación de sanciones occidentales**, presentando estas sanciones como un "crimen de guerra" que afecta principalmente a la población civil iraní.

    - **Crítica a la hegemonía de Estados Unidos**, subrayando el "declive del imperialismo" y promoviendo un nuevo orden mundial multipolar en alianza con potencias como Rusia y China.

- **Alineación ideológica y geopolítica**: Se analiza si el contenido refleja posturas pro-Irán, pro-Rusia, anti-OTAN, anti-EE. UU., o favorables hacia otros actores internacionales, como China o Venezuela.

Finalmente, la fase conclusiva de la investigación se enfoca en identificar las TTP utilizados en los medios digitales alineados con la narrativa proiraní, siguiendo el marco metodológico DISARM.

Campañas de desinformación y propaganda

La narrativa desplegada por diversos medios digitales refleja una estrecha red de alianzas entre Irán y sus principales aliados, como Rusia, Siria, Palestina, Líbano y Venezuela, quienes utilizan estas plataformas como herramientas de poder blando para difundir posturas antioccidentales. Irán se posiciona como líder de la resistencia contra Estados Unidos, Israel y Arabia Saudí, promoviendo un rechazo a las intervenciones extranjeras en sus aliados y defendiendo un mundo multipolar.

HispanTV, un canal estatal iraní, refuerza el discurso oficial de Irán al ensalzar a figuras como el Ayatolá Jamenei y Bashar al-Ásad y degradando a adversarios, presentando las sanciones occidentales como agresiones injustas. En paralelo, el medio TeleSUR desde Venezuela refuerza esta narrativa mediante campañas de desprestigio contra opositores políticos y la exaltación de alianzas con Cuba e Irán, utilizando videos y noticias orientadas a dividir y debilitar gobiernos prooccidentales en América Latina.

Desde otro frente, la agencia controlada estatalmente por Rusia, Sputnik, complementa estas narrativas al atacar directamente a Estados Unidos y la OTAN, particularmente en conflictos como el de Ucrania, donde la plataforma acusa a las fuerzas occidentales de ser agresoras. Sputnik, aunque no es directamente pro-Irán, opera bajo una visión alineada con Irán al promover un orden mundial alternativo en el que las potencias emergentes desafían la hegemonía occidental. De manera similar, grupos más específicos, como Eje de la Resistencia y Mundo Multipolar ZOV en Telegram, intensifican este mensaje al resaltar el papel de la resistencia global, con especial énfasis en los vínculos entre Irán, Rusia y Palestina.

Por su parte, el medio Al Mayadeen, con sede en Líbano, respalda la causa palestina y la resistencia armada contra Israel, alineándose con los intereses de Irán, Siria y grupos como Hezbolá, mientras denuncia la hegemonía estadounidense en la región. A su vez, canales como Libertad Palestina o Palestina Hoy en Telegram utilizan imágenes y teorías conspirativas para alimentar la resistencia contra Israel. En la misma línea, medios sirios como SANA legitiman al régimen de Bashar al-Ásad, presentándolo como un defensor de la soberanía frente al terrorismo y la injerencia extranjera. Finalmente, los movimientos europeos como los Chalecos Amarillos son exhibidos como señales del colapso del modelo occidental, subrayando la narrativa de que un nuevo orden mundial, liderado por Irán y Rusia, está emergiendo para desafiar la estructura de poder actual.

El análisis de la narrativa expuesta, en conjunto con el mapeo bajo el marco DISARM, revela una serie de técnicas alineadas con evidencias potenciales de desinformación. Una de las técnicas más destacadas es la de facilitar propaganda estatal (T0002), que se utiliza para amplificar la narrativa oficial, excluyendo voces críticas. Está estrategia fortalece la legitimidad de los líderes aliados y promueve la resistencia contra occidente. Asimismo, se emplea la técnica de degradar al adversario (T0066), la cual desacredita a actores como EE. UU. e Israel, presentando sus acciones como agresiones ilegítimas y ensalzando a los aliados.

Otra técnica relevante es el acoso a oponentes (T0048), cuyo propósito es desprestigiar a líderes opositores y deslegitimar sus movimientos. Además, la técnica de responder a eventos de última hora (T0068) permite que los actores alineados reaccionen rápidamente ante crisis, moldeando la narrativa para reforzar su agenda. La publicación cruzada (T0119), por su parte, maximiza el alcance del mensaje a través de múltiples plataformas, como se observa en la difusión simultánea de contenido prorruso y antioccidental.

El uso de teorías de conspiración (T0022) es también significativo, ya que introduce narrativas que acusan a las potencias occidentales de conspirar para controlar la política global. Esta técnica se complementa con desalentar/consternar (T0078), empleada mediante la difusión de imágenes impactantes de víctimas civiles, particularmente en el conflicto palestino-israelí, con el fin de generar rechazo hacia Israel y sus aliados. Estos patrones de manipulación informativa buscan consolidar la resistencia de los aliados de Irán y debilitar la legitimidad de sus adversarios.

Adicionalmente, el uso de técnicas como la creación de contenido localizado (T0101) y determinar audiencias objetivo (T0073) permiten adaptar los mensajes a públicos específicos, optimizando su impacto. Esto incluye la creación de hashtags y artefactos de búsqueda (T0015) para viralizar contenido, como en las campañas que apoyan la causa palestina o critican las intervenciones occidentales en América Latina. Estas estrategias permiten a los actores alineados incrementar su difusión informativa, fortaleciendo su narrativa y desestabilizando a sus oponentes.

Igualmente, Irán vendría desarrollando diversas operaciones de influencia que incluyen la invitación a *influencers* extranjeros a visitar el país, supuestamente para impulsar el turismo (News, 2024); la financiación de editores concretos de sitios webs, como The Grayzone, a través de una particular agencia de comunicación propiedad del gobierno iraní (Menn, 2024) para encubrir la difusión de propaganda y desinformación; o mediante el acercamiento e instrumentalización de periodistas facilitándoles visitas con la anuencia y coordinación de organismos oficiales iranies, lo que a la postre se traduce en campañas de propaganda a favor del régimen que pueden ahondar en intentos de desprestigiar a Occidente y su estructura mediática (News, 2023). Estas operaciones requieren un análisis detallado para identificar y rastrear operaciones de influencia e injerencia extranjera, cada vez más complejas, bien mediante la adquisición o reclutamiento de redes no domésticas (T0093), bien cultivando agentes inconscientes (T0010).

Por último, hay que indicar que la identificación de elementos suficientes, a través de fuentes abiertas, que sustenten las fuentes de financiación o hipotéticas motivaciones económicas respecto los procedimientos utilizados por Irán para monetizar las estrategias basadas en las TTP indicadas, requiere de análisis más complejos y extendidos en el tiempo, sugiriéndose como líneas de trabajo a abordar en futuros Grupos de Trabajo del Foro contra las Campañas de Desinformación en el ámbito de la Seguridad Nacional.

Grupos “cyber” vinculados con Irán

En el contexto global actual, las campañas de desinformación y los ciberataques han surgido como poderosas armas utilizadas por actores estatales y grupos *hacktivistas* para influir en la percepción pública y desestabilizar a sus adversarios. Irán, en particular, ha sido identificado como uno de los principales actores en este ámbito, utilizando grupos APT (Amenazas Persistentes Avanzadas) y *hacktivistas* alineados con su ideología para llevar a cabo operaciones de espionaje, sabotaje y propaganda. Estos esfuerzos están diseñados no solo para proteger los intereses del régimen iraní, sino también para proyectar poder a nivel internacional, atacando a sus rivales regionales y globales, especialmente hacia Estados Unidos, Israel y Arabia Saudí.

En cuanto a las APT, se han identificado dos grupos presuntamente patrocinados por Irán y vinculados a los Cuerpos de la Guardia Revolucionaria Islámica (IRGC). Uno de los más relevantes es APT42, también conocido como Charming Kitten, un grupo iraní destacado en actividades de espionaje y desinformación. Su objetivo principal es ejecutar campañas dirigidas contra altos cargos de Israel y Estados Unidos, incluyendo figuras gubernamentales, políticos, diplomáticos o críticos directos de Irán, como activistas, periodistas y ciertos *think tanks*.

APT42 ha estado implicado en actividades recientes como la suplantación de *think tanks* estadounidenses y el despliegue de *malware* contra objetivos estadounidenses tras los ataques de octubre de 2023 en Israel. Además, ha llevado a cabo campañas de phishing dirigidas a medios de comunicación y organizaciones sin ánimo de lucro en EE. UU. y Oriente Medio, atacando también a personas vinculadas en las campañas presidenciales de EE. UU. en la primera mitad de 2024.

Estas acciones demuestran la sofisticación del grupo y su capacidad para realizar ciberataques en un contexto geopolítico complejo, utilizando técnicas como determinar audiencias objetivo (T0073) y la creación de expertos falsos (T0009), infiltrándose en redes y ganándose la confianza de sus víctimas.

Por otro lado, APT33, conocido también como Elfin, se especializa en ciberataques dirigidos a infraestructuras críticas, con un enfoque particular en el sector energético de países adversarios, como Arabia Saudí. Este grupo opera bajo una narrativa pro-Irán, alineándose con los intereses del régimen en su confrontación con Estados Unidos, Israel y Arabia Saudí. APT33 ha sido vinculado a la distribución de un *malware* con funciones de puerta trasera a finales de 2023, en una operación en la que los actores se hicieron pasar por una empresa estadounidense del sector espacial y de satélites. Las técnicas utilizadas por este grupo incluyen determinar fines estratégicos (T0074), lo que les permite atacar objetivos de alto valor en sectores críticos, y degradar al adversario (T0066), mediante el sabotaje de infraestructuras clave y la manipulación de información sensible.

Estos grupos no solo se enfocan en el espionaje y sabotaje, sino también en la creación de narrativas favorables al régimen iraní. A través de la combinación de ciberespionaje y campañas de desinformación, tanto APT42 como APT33 apuntan a sectores estratégicos en Estados Unidos y otras naciones occidentales.

A estas acciones se suman grupos *hacktivistas* alienados con la narrativa pro-Irán, como Cyber Av3ngers (presuntamente alineado con IRGC), ALTOUFAN TEAM, ALtahrea Team, Makhlab al-Nasr y Cyber Toufan. Estos grupos buscan debilitar a sus adversarios mediante ataques cibernéticos, utilizando estrategias como degradar al adversario (T0066), al publicar filtraciones de documentos sensibles y exponer vulnerabilidades en infraestructuras críticas. También emplean técnicas como determinar audiencias objetivo (T0073), dirigiéndose a audiencias propalestinas y proiraníes, e inundar el espacio informativo (T0049), saturando las redes sociales con propaganda visual y textual que resalta sus logros en ciberataques.

Un denominador común entre estos grupos es el uso de plataformas como Twitter y Telegram para amplificar sus actividades y, en algunos casos, coordinarse. Grupos, como Handala Hack, emplean la técnica ocultar actividad operativa (T0129), protegiendo su identidad mediante el uso de canales cifrados, mientras que otros, como Cyber Court, utilizan la técnica publicar contenido (T0115), difundiendo continuamente información sobre sus ataques. Además, los grupos *hacktivistas* suelen recurrir a técnicas para controlar el entorno informativo a través de operaciones cibernéticas ofensivas (T0123), realizando ataques que distorsionan el ecosistema informativo de sus adversarios. Ejemplos de esto incluyen la manipulación de documentos robados y la exageración de los efectos derivados de sus ataques a infraestructuras críticas israelíes, como en el caso del grupo Cyber Flood.

En conjunto, las acciones de estos grupos reflejan el alcance y la complejidad de las operaciones cibernéticas iraníes, que no solo buscan debilitar o destruir la infraestructura de sus enemigos, sino también influir en la narrativa global. Emplean técnicas de ocultación de la actividad operativa (T0129), y mantienen una estrategia a largo plazo (T0059) que permite a Irán proyectar su poder en el ciberespacio mientras protege sus intereses geopolíticos.

VENEZUELA

Venezuela, que una vez fue una de las democracias más plenas en todo Latinoamérica, ha experimentado un deterioro significativo en sus instituciones democráticas bajo el régimen de Hugo Chávez y su sucesor, Nicolás Maduro. Este proceso ha sido acompañado por un aumento en la represión digital y la censura.

En Venezuela, más de 268 emisoras de radio han sido cerradas entre diciembre de 2021 y noviembre de 2023. Esto afecta tanto a áreas rurales y urbanas, dejando muchas regiones sin acceso a noticias locales. Las estaciones de televisión también han enfrentado censura, con órdenes de CONATEL prohibiendo ciertos temas y palabras al aire. Esto ha llevado a la desaparición de segmentos de opinión y entrevistas en muchos canales. Doce de los veinticuatro estados de Venezuela no tienen periódicos impresos locales. Muchos periódicos han cerrado debido a la censura y la presión económica, incluyendo El Nacional, El Universal y Últimas Noticias. Más de 52 sitios de noticias han sido bloqueados, incluyendo Armando.info, Efecto Cocuyo, El Pitazo, La Patilla, Maduradas, Noticiero Digital, NTN24, Vivo Play y VPITV. Medios internacionales como Infobae y NTN24 también han sido bloqueados en Venezuela. La censura del país también ha afectado al bloqueo de diversas redes sociales, como X (Mitchell, 2024).

El gobierno de Nicolás Maduro ha utilizado las redes sociales de manera estratégica para llevar a cabo campañas de desinformación y manipulación de la opinión pública (T0074). El grupo conocido como Tuiteros de la Patria coordina sus publicaciones para amplificar los mensajes del gobierno, recibiendo recompensas monetarias por cumplir con objetivos de publicación (Mitchell, 2024) utilizando hashtags y lenguaje proporcionado por el Ministerio de Comunicación e Información (T0002, T0093). Además, se habrían llevado a cabo campañas coordinadas en redes sociales para desacreditar a la oposición y promover sus propias narrativas, utilizando hashtags como #MariaCorinaEsLeopoldo y #LosLujosDeLeopoldo durante las primarias de la oposición (Cocuyo chequea, 2023) en 2023 (T0015). También se han identificado redes de perfiles artificiales y trolls que amplifican mensajes progubernamentales y atacan a críticos del régimen (T0048) y el gobierno venezolano utilizó las tendencias en la plataforma X para promover sus mensajes y ocultar información desfavorable mediante la publicación masiva y coordinada de tweets con hashtags específicos (T0068). Las cuentas oficiales y las redes de trolls han atacado a medios independientes y periodistas que publican información crítica del gobierno, incluyendo campañas de difamación y la publicación de información falsa para desacreditar a los periodistas. Además, el gobierno de Maduro ha colaborado con otros regímenes autoritarios, como Rusia y China, para difundir narrativas favorables a sus intereses y atacar a sus críticos, amplificando mensajes en medios estatales y redes sociales controladas por estos países.[12]

En las últimas elecciones venezolanas, el Consejo Nacional Electoral (CNE), controlado por el gobierno, proclamó a Maduro como vencedor sin proporcionar un desglose detallado de las actas de votación, lo que generó denuncias de fraude por parte de la oposición y cuestionamientos

---

[12] Como, por ejemplo: Usa en Español [@UsaenEspanol]. (2019, 12 de marzo). Rusia usa sus organismos de desinformación patrocinados por el estado como Russia Today y Sputnik para desviar la atención del desastre humanitario del régimen de Maduro. Rusia ha gastado gran cantidad de dinero en Venezuela. Más de $17 mil millones en inversiones y préstamos. https://x.com/i/status/1105425709986664448 [video adjunto] [post] https://x.com/USAenEspanol/status/1105425709986664448

de la comunidad internacional. Los observadores electorales extranjeros que asistieron estaban compuestos principalmente por aliados del régimen (Pérez Gallardo, 2024) y la declaración del Alto Representante de la UE sobre Venezuela, emitida el 4 de agosto de 2024, expresa una profunda preocupación por los recientes acontecimientos electorales en el país al no cumplir con los estándares internacionales de integridad electoral y la falta de publicación de los registros de votación por parte del CNE (Consejo de la Unión Europea, 2024). La Unión Europea y España (junto con 21 países más) han pedido la verificación imparcial de los resultados electorales de Venezuela (Ministerio de Asuntos Exteriores, UE y Cooperación, 2024).

IMPACTO ECONÓMICO DE LAS ACTIVIDADES ANALIZADAS

Debemos discernir entre el impacto económico que genera en el actor de la amenaza desplegar sus estrategias desinformativas, en términos de coste-beneficio-eficiencia, incremento de la influencia y alcance, así como su percepción en el control narrativo y, por otro, el impacto sociopolítico que genera en la sociedad en su conjunto, pero también en los mercados financieros.

La manipulación en plataformas online, especialmente de redes sociales, encuentra facilidades tecnológicas que habilitan la creación de auténticas redes coordinadas inauténticas. Su éxito dependerá de la capacidad de aquellas para detectarlas y eliminarlas. A pesar de normativas como la Ley de Servicios Digitales, las plataformas mostrarían limitaciones significativas y desiguales en la detección y eliminación de cuentas falsas e interacciones inauténticas (Bergmanis-korats y Haiduchyk, 2024).

El uso de perfiles artificiales comerciales, que suelen enfocarse en temas como criptomonedas y apuestas, para amplificar contenido político está en aumento, especialmente en época de elecciones, lo que plantea riesgos adicionales de manipulación en procesos democráticos. Una estrategia para evitar ser detectados es dividir las campañas masivas en operaciones en menor escala para dificultar su identificación por los sistemas de clasificación de las plataformas (Bergmanis-korats y Haiduchyk, 2024).

Los servicios de manipulación en redes sociales son cada vez más accesibles y, a su vez, han reducido los costos, lo que hace económicamente viable para los distintos actores maliciosos adquirir grandes volúmenes de interacciones falsas[13] y amplificar sus campañas de desinformación. Estos servicios incluyen "paquetes" con miles de visualizaciones o "me gusta" a precios asequibles, lo cual permite monetizar estas interacciones mediante promoción de contenido (Bergmanis-korats y Haiduchyk, 2024).

---

[13] La rapidez de la manipulación dificulta la detección y los bloqueos oportunos por parte de las plataformas. En 2024, el 93% de las interacciones falsas de las registradas por el estudio, tuvieron lugar dentro de las primeras 24 horas (siendo el 100% en YouTube y TikTok, dentro de las primeras 12 horas, y el 64% en X dentro de las primeras 24 horas). La rapidez de la manipulación afecta a la eficacia de las plataformas en abordar el comportamiento manipulativo con suficiente celeridad como para mitigar su impacto.

Como se indicaba al principio, las campañas de desinformación extienden su impacto más allá del ámbito social y político, afectando también a la economía.

Efectivamente, la difusión orquestada de narrativas falsas, rumores y teorías de conspiración suele generar incertidumbre y volatilidad en los mercados, lo que a su vez puede afectar la toma de decisiones empresariales y de inversión.

Una campaña de desinformación no tendría efecto alguno sobre la economía si no fuera porque, si tiene éxito entre sus destinatarios (víctimas), si cala en la conciencia de los receptores, la reputación de la entidad, institución o sistema atacado se ve claramente afectada, perdiendo reputación y credibilidad ante quienes son sus clientes, usuarios o ciudadanos, lo que provoca finalmente el impacto deseado por el atacante, entre otros, en el ámbito de la economía.

Efectivamente, como se ha dicho, la desinformación agrava la crisis del modelo de negocio mediático, ya que la rápida difusión de contenido falso puede reducir la confianza en los medios tradicionales, afectando negativamente los ingresos publicitarios. Esta situación se ve potenciada por la dependencia de modelos de financiamiento tradicionales en la prensa y la creciente dificultad de captar la atención de las audiencias en un mercado saturado.

La aceleración de los ciclos de noticias y la economía de la atención, que recompensa el contenido que genera reacciones rápidas y masivas, favorece la diseminación de noticias falsas y polarizantes. Esto penaliza a los productores de contenido de calidad y amenaza la sostenibilidad de los medios, que enfrentan costos altos y dificultades en la automatización sin perder calidad (IBERIFIER, 2023). Sólo en EE. UU., los principales sitios de desinformación generan más de $235 millones en ingresos anuales por publicidad (Global Disinformation Index, 2022).

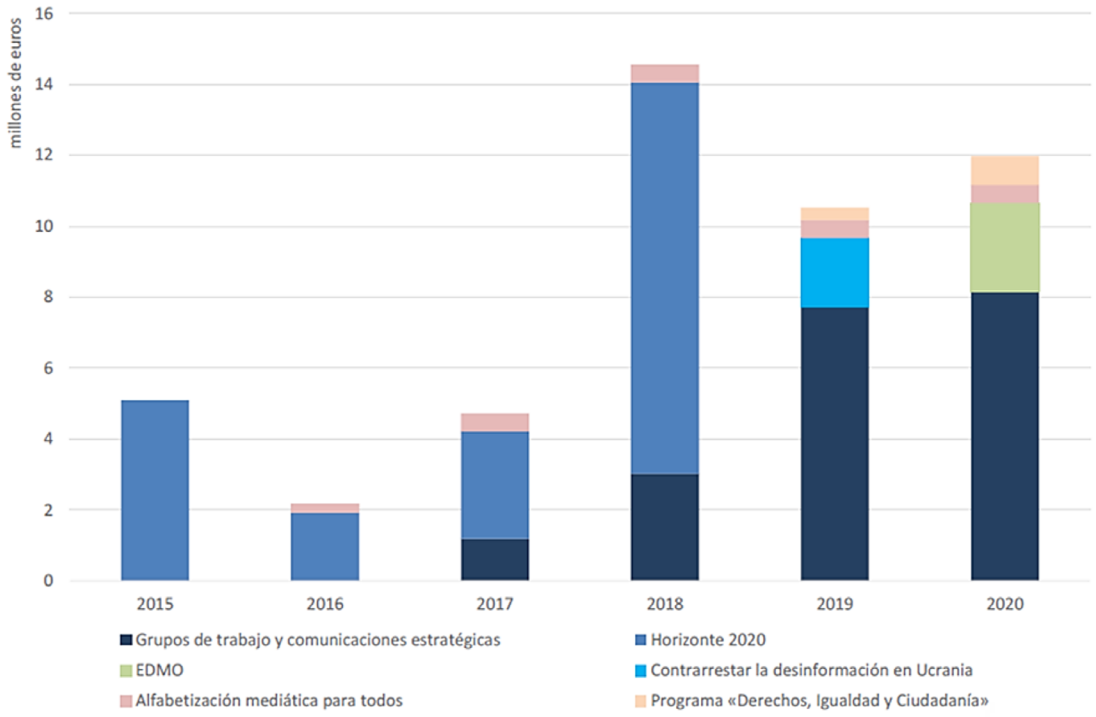
Como decimos, las informaciones manipuladas influyen en la percepción pública y pueden alterar el entorno económico, afectando decisiones de inversión y el consumo, especialmente en tiempos de elecciones o crisis políticas (Fake News and its Impact on the Economy, 2020). Todo ello sin tener en cuenta en este momento que un incesante flujo de información falsa puede impulsar la creación de regulaciones que podrían restringir la libertad empresarial, obligando a las organizaciones a invertir en estrategias adicionales a las ya existentes en materia de comunicación y gestión de crisis (Christov, 2019).

EFECTOS DEL IMPACTO ECONÓMICO DE LAS CAMPAÑAS DE DESINFORMACIÓN	
Volatilidad en los Mercados Financieros	Inestabilidad en los mercados financieros. Por ejemplo, la difusión de información falsa sobre la salud financiera de una empresa puede llevar a ventas masivas de sus acciones, causando una caída abrupta en su valor. Un caso notable fue la desinformación sobre la empresa de tecnología Zoom Video Communications en marzo de 2020 (Krenz, 2022), donde se reportaron falsamente vulnerabilidades de seguridad, provocando caídas temporales en su cotización. Las fluctuaciones del mercado no sólo afectan a las empresas directamente implicadas sino también a los inversores y otros actores del mercado, generando un clima de incertidumbre y desconfianza que puede extenderse a todo el sistema financiero. A largo plazo, esta volatilidad puede desincentivar la inversión extranjera y reducir el crecimiento económico.
Impacto en la confianza del consumidor o en el ciudadano	La difusión de noticias falsas puede erosionar la confianza del consumidor en las marcas y empresas, lo que puede llevar a una disminución en el consumo y en las ventas. Esto puede tener un efecto negativo en la economía, especialmente en sectores como el comercio minorista y los servicios. Por ejemplo, durante la pandemia de COVID-19, la difusión de información falsa sobre productos básicos y alimentos generó pánico y escasez innecesaria. Lo mismo cabe decir cuando la víctima son los ciudadanos, pertenecientes a un grupo, a una región, a un estado o a una comunidad política. La erosión de la confianza generada por la campaña de desinformación puede claramente desincentivar a los ciudadanos a seguir participando activamente en el sistema, dejando de pagar impuestos, por ejemplo.
Costes de mitigación	Los gobiernos y las empresas deben invertir recursos significativos para detectar y contrarrestar la desinformación, lo que incluye la implantación de herramientas tecnológicas avanzadas, la formación de personal y la generación de campañas de concienciación pública (Heikkinen, 2021).

EFECTOS DEL IMPACTO ECONÓMICO DE LAS CAMPAÑAS DE DESINFORMACIÓN	
Pérdida de competitividad	La desinformación también puede dañar la reputación de las empresas y los países, afectando su competitividad en el mercado global. Por ejemplo, un país que es visto como un blanco fácil para campañas de desinformación puede ser percibido como inestable, desalentando la inversión extranjera y el turismo. Además, las empresas que son objeto de desinformación pueden ver dañada su reputación a largo plazo, incluso después de que la información falsa haya sido desmentida. La pérdida de confianza puede resultar en una disminución en las ventas y en la capacidad de atraer nuevos clientes, afectando negativamente su posición en el mercado.
Impacto en la política económica	La desinformación puede influir en la toma de decisiones políticas, llevando a la adopción de políticas económicas inadecuadas o mal informadas. Por ejemplo, durante la campaña del Brexit, se difundió mucha información engañosa sobre los beneficios y consecuencias económicas de abandonar la Unión Europea, lo que afectó la votación y las decisiones políticas posteriores (Brändle et al., 2021). Las políticas basadas en desinformación pueden tener efectos a largo plazo, perjudicando el crecimiento económico y la estabilidad financiera. Además, la polarización política resultante de la desinformación puede dificultar la implementación de políticas económicas necesarias y la cooperación entre diferentes actores políticos.

En resumen, las campañas de desinformación representan una amenaza significativa para la estabilidad económica y financiera de los países atacados.

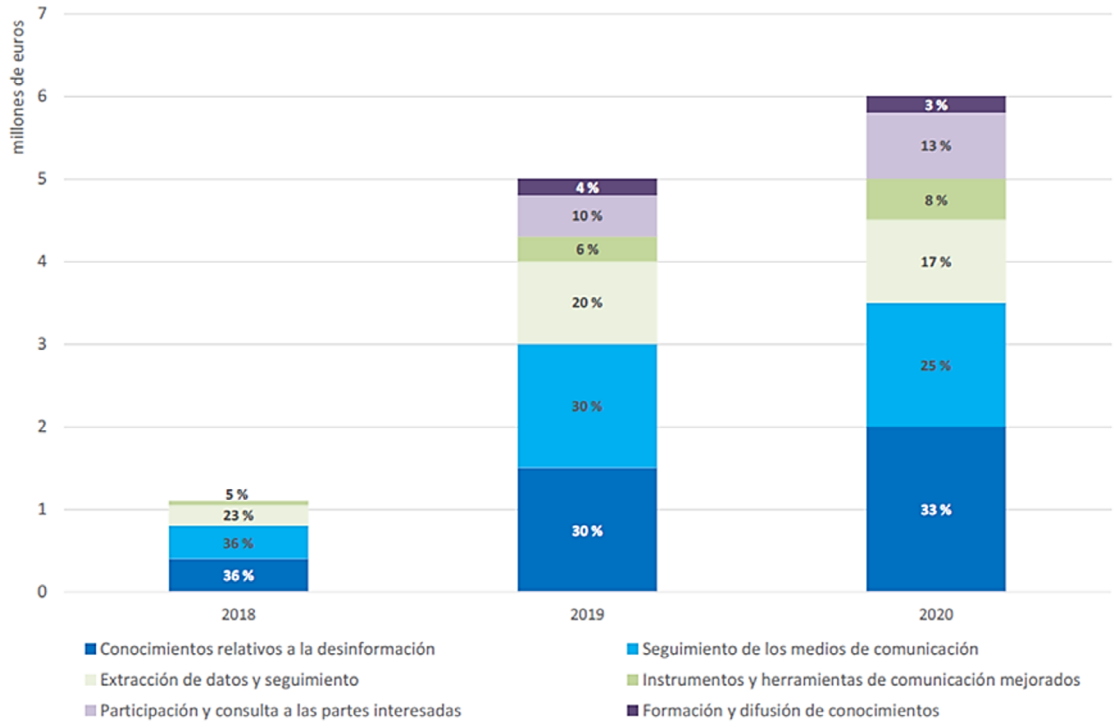
El Informe Especial del Tribunal de Cuentas Europeo (2021), recoge algunos datos especialmente significativos en relación con los esfuerzos económicos que viene acometiendo la Unión Europea para contrarrestar las campañas de desinformación.



Financiación total destinada por la UE a la lucha contra la desinformación en el período 2015-2020. (Fuente: Tribunal de Cuentas Europeo, a partir de la información proporcionada por la Comisión y el SEAE).

El SEAE se ha mostrado especialmente activo en la lucha contra la desinformación, asignando partidas presupuestarias a los diferentes Grupos de Trabajo constituidos en el StratCom[14]. La figura siguiente muestra el reparto de tales fondos en el periodo señalado.

14 https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en



Financiación aportada por la acción preparatoria «StratCom Plus» a diferentes capacidades de los grupos de trabajo StratCom del SEAE (2018-2020). (Fuente: Tribunal de Cuentas Europeo, a partir de datos del SEAE.)

Aunque todavía claramente insuficiente, la Unión Europea ha venido asignando en los últimos años dotaciones presupuestarias para combatir los riesgos derivados de las campañas de desinformación.

La tabla siguiente muestra la inversión realizada por la UE en acciones destinadas a combatir la desinformación durante el periodo 2015-2020.

Entidad	Línea presupuestaria	Financiada por	Título	Dotación presupuestaria						Total
				2015	2016	2017	2018	2019	2020	
SEAE	19 06 01	Prerrogativa de la Comisión (FPI)	Divulgación de información sobre las relaciones exteriores de la UE					298 200		298 200
	19 06 77 01	Acción preparatoria (FPI)	Acción preparatoria «StratCom Plus»				1 100 000	3 000 000	4 000 000	8 100 000
	1200	SEAE	Agentes contractuales			1 187 000	1 128 942	2 098 697	2 159 748	6 574 387
	2214	SEAE	Capacidad de comunicación estratégica				800 000	2 000 000	2 000 000	4 800 000
DG Redes de Comunicación, Contenido y Tecnologías	09 04 02 01	Horizonte 2020	Liderazgo en tecnologías de la información y de las comunicaciones	3 115 736		2 879 250	10 885 524			16 880 510
	09 03 03	MCE - telecomunicaciones	Observatorio Europeo de Medios Digitales						2 500 000	2 500 000
	09 05 77 04	Proyecto piloto	Proyecto piloto «Alfabetización mediát ca para todos»		245 106	500 000				745 106
	09 05 77 06	Acción preparatoria	Acción preparatoria «Alfabetización mediát ca para todos»				499 290	500 000	500 000	1 499 290
ERC	08 02 01 01	Horizonte 2020	Reforzar la investigación en las fronteras del conocimiento mediante las act vidades del Consejo Europeo de Investigación	1 980 112	1 931 730	149 921	150 000			4 211 763
FPI	19 02 01 00	Instrumento en pro de la Estabilidad y la Paz	Contrarrestar la desinformación en el sur y el este de Ucrania					1 934 213		1 934 213
DG Justicia	33 02 01	Programa «Derechos, Igualdad y Ciudadanía»	Estudio del impacto de las nuevas tecnologías en la celebración de elecciones libres y limpias					350 000		350 000
	33 02 01	Programa «Derechos, Igualdad y Ciudadanía»	Actividades de promoción de los derechos de ciudadanía de la Unión (por ejemplo, un evento para la Red de Cooperación Electoral o relacionado con el informe sobre la ciudadanía)						376 000	376 000
	34 02 01	Programa «Derechos, Igualdad y Ciudadanía»	Estudios e investigaciones sobre ámbitos específicos relacionados con la ciudadanía de la Unión (red de representantes del mundo académico y otros)						434 000	434 000
DG Comunicación	16 03 02 03	Presupuesto operativo	Herramientas de información y comunicación en línea y en formato impreso					91 603	62 249	153 852
	16 03 01 04	Presupuesto operativo	Comunicación de las Representaciones de la Comisión, Diálogos con los ciudadanos y Acciones de asociación						132 000	132 000
	08 02 05 00	Presupuesto institucional	Actividades horizontales de Horizonte 2020					110 000		110 000
DG Informática para el SEAE	26 03 77 09	Acción preparatoria «Soluciones de análisis de datos para la elaboración de políticas»						251 421		251 421
TOTAL				5 095 848	2 176 836	4 716 171	14 563 756	10 634 134	12 163 997	49 350 742

Gasto de la UE destinado a acciones para combatir la desinformación (en euros).
(Fuente: Tribunal de Cuentas Europeo, a partir de datos proporcionados por la Comisión y el SEAE).

Finalmente, el cuadro siguiente muestra la evaluación de proyectos contra la desinformación (proyectos piloto, acciones preparatorias, Horizonte 2020).

Número de proyecto	Tipo de proyecto	Países	Duración del proyecto (real)	Estado	Vínculo directo con otros proyectos	Importe de la subvención (en euros)	¿Resultó adecuado el seguimiento de la Comisión?	Criterio 1 Pertinencia relat va a la desinformación	Criterio 2 Resultados tangibles y sostenibles	Criterio 3 Escala y alcance suficientes
1	Horizonte 2020	Reino Unido (objetivos: Alemania, Francia, Polonia, Suecia, Reino Unido / Brasil, Canadá, China, México, Rusia, Ucrania, Estados Unidos, Taiwán)	Enero de 2016 - diciembre de 2020	En curso	Sí	1 980 112	Existe una presentación de informes continua e independiente en forma de auditoría y un informe científico.			El proyecto produjo, principalmente, documentos de investigación. La mayoría de las presentaciones de estos documentos se han producido fuera de la UE. Tras la salida del Reino Unido de la UE, se desconoce de qué modo podrá esta investigación seguir benef ciando a la Unión.
2	Horizonte 2020	Reino Unido	Julio de 2017 - enero de 2019	Finalizado	Sí	149 921	Existe una presentación de informes continua e independiente en forma de auditoría.			No existe ningún tipo de indicio de que el proyecto vaya a ir más allá de una prueba de concepto y, si así sucede, se desconoce si el público se beneficiará tanto como el sector privado en el caso de que el producto final acabe comercializándose.
3	Horizonte 2020	Grecia	Enero de 2016 - diciembre de 2018	Finalizado	Sí	3 115 737	Existe un dictamen experto e independiente e informes de evaluación.			La herramienta producida por el proyecto estaba enfocada, principalmente, a los expertos y no resultó lo suficientemente intuitiva para el público general (se requirieron dos proyectos posteriores para precisar los resultados y para mejorar la escala y el alcance del proyecto).
4	Horizonte 2020	Italia	Enero de 2018 - diciembre de 2020	En curso	No	2 879 250	El proyecto sigue en curso en la actualidad. Existe una presentación de informes continua acompañada de una primera evaluación.		Se ha observado un punto débil, ya que uno de los componentes del soporte lógico está obsoleto, por lo que el proyecto no está empleando métodos de última generación en este ámbito.	
5	Horizonte 2020	Irlanda, Grecia, Italia, Chipre, Austria, Portugal, Rumanía, Reino Unido	Enero de 2018 - noviembre de 2021	En curso	Sí	2 454 800	Se realizó una revisión independiente a distancia en julio de 2020, facilitada por la DG Redes de Comunicación, Contenido y Tecnologías.		Un proyecto bien gestionado que precisa de algunas medidas correctoras para situar el foco en determinados componentes clave, y una elaboración más detallada de su difusión y explotación.	Puntos débiles en la ejecución de la difusión y en las estrategias de explotación empresarial.
6	Horizonte 2020	Chequia, Irlanda, España, Austria	Diciembre de 2018 - noviembre de 2021	En curso	Sí	2 753 059	Se están llevando a cabo revisiones independientes a distancia (fecha de inicio: agosto de 2020).			Existe incertidumbre acerca de cómo interactuarán las plataformas en línea centralizadas con la herramienta.
7	Horizonte 2020	Francia, Italia, Polonia, Rumanía, Reino Unido	Diciembre de 2018 - noviembre de 2021	En curso	Sí	2 505 027	Se realizaron tres evaluaciones individuales en diciembre de 2019 y una evaluación general en febrero de 2020. Además, entre enero y abril de 2020, se llevó a cabo una revisión del proyecto.			
8	Horizonte 2020	Dinamarca, Grecia, Italia	Noviembre de 2018 - abril de 2021	En curso	Sí	987 438	El proyecto fue revisado por tres controladores independientes y evaluado por el jefe de proyecto.		El proyecto sigue en curso en paralelo a un proyecto similar en ese ámbito.	
9	Horizonte 2020	Bélgica, Bulgaria (C), Alemania, Grecia, Francia, Reino Unido	Diciembre de 2018 - noviembre de 2021	En curso	Sí	2 499 450	Ausencia de contribución y de esfuerzos coordinados por parte de la Comisión al inicio del proyecto.		Se están comprobando los resultados en la fase de prototipo. Esto puede conllevar determinados riesgos. Ausencia de directrices por parte de la Comisión; además, las ideas sobre cómo pueden ser sostenibles los resultados se limitan a iniciativas asociadas vinculadas a sus propios contactos, socios o clientes.	
10	Horizonte 2020	Suiza/Reino Unido	Septiembre de 2018 - noviembre de 2019 (en un principio, febrero de 2020)	Finalizado	Sí	150 000	A petición del Tribunal, el jefe de proyecto se preocupó de recopilar la información necesaria para establecer cómo se aprovecharon los resultados.			Los resultados fueron explotados, principalmente, por una empresa estadounidense.
11	Proyecto piloto	Bélgica, Rumanía, Francia, Croacia, Polonia, Finlandia, Estados Unidos	Enero de 2018 - enero de 2019	Finalizado	No	125 000	El seguimiento del proyecto se llevó a cabo mediante diversos indicadores cualitativos y cuantitat vos.			
12	Proyecto piloto	España, Italia, Malta, Portugal, Reino Unido	2016	Finalizado	Sí	171 057	El seguimiento por parte de la Comisión no fue evidente.		Tan solo se desarrollaron cursos de formación sostenibles en uno de los cinco países.	Los resultados del proyecto tuvieron un alcance limitado.
13	Proyecto piloto	Bélgica, Grecia, España, Italia, Letonia, Lituania, Hungría, Malta, Austria, Polonia, Portugal, Rumanía, Eslovaquia	2017	Finalizado	No	118 445	Presentación de informes continua y producción de un informe técnico y de una evaluación final independiente.			Problemas de sostenibilidad. En su autoevaluación final, el proyecto destacó la ausencia de una estrategia de alfabetización mediática general.

Número de proyecto	Tipo de proyecto	Países	Duración del proyecto (real)	Estado	Vínculo directo con otros proyectos	Importe de la subvención (en euros)	¿Resultó adecuado el seguimiento de la Comisión?	Criterio 1 Pertinencia relat va a la desinformación	Criterio 2 Resultados tangibles y sostenibles	Criterio 3 Escala y alcance suficientes
14	Proyecto piloto	Polonia	Julio de 2018 – junio de 2019	Finalizado	No	127 590	**Tan solo existe una evaluación de una página que no analiza los resultados.**	**El proyecto mezcla la verificación de datos con los derechos de las mujeres y el sexismo, por lo que su pertinencia en lo que respecta a la desinformación es escasa.**	**La página web creada por el proyecto ya no está operativa.**	
15	Proyecto piloto	Bélgica, Austria, Portugal	2017	Finalizado	No	122 815			**Se llevó a cabo una tormenta de ideas y se elaboraron libros blancos, pero no existen herramientas específicas.**	**El proyecto se suspendió debido a la insolvencia del coordinador.**
16	Proyecto piloto	Dinamarca, Irlanda, Grecia, Chipre, Portugal	Julio de 2018 – junio de 2019	Finalizado	No	131 150	**No existe ningún indicio de que se esté llevando a cabo un seguimiento continuo. La evaluación final es de 133 palabras y no contiene ninguna recomendación.**	**El proyecto se centra en el pensamiento creativo en general.**	**Los productos o resultados no son cuantificables.**	**El proyecto fue un ejercicio aislado y no puede reproducirse o prolongarse con facilidad**
17	Acción preparatoria	Bélgica, Bulgaria, Alemania, España, Croacia, Rumanía, Italia, Letonia	Julio de 2019 - agosto de 2020 (prórroga sometida a debate)	En curso	No	124 546,72	**Se produjo un informe de ejecución técnica provisional.**			
18	Acción preparatoria	Dinamarca, Alemania, España, Francia, Italia, Países Bajos, Polonia, Finlandia	2018	En curso	Sí	214 556	**El proyecto realizó un seguimiento estrecho de las acciones con indicadores claramente definidos.**			
19	Acción preparatoria	España, Francia, Rumanía, Suecia	2018	En curso	Sí	159 380	**El proyecto sigue en curso en la actualidad y la calidad del informe técnico es buena. También se elaborará un informe independiente.**			
20	Acción preparatoria	Grecia, España, Lituania, Finlandia	Agosto de 2019 - agosto de 2020 (prórroga sometida a debate)	En curso	No	86 630	**La presentación de informes tan solo exigió un informe de evaluación intermedia tras un período de siete meses. Algunos documentos no se encontraban disponibles inmediatamente y tuvieron que remitirse por correo.**			**El proyecto está encontrando dificultades de financiación.**

No completado
Completado parcialmente
Completado
S. O.

El ANEXO II representa una clasificación de las TTP relevantes en el análisis de las acciones de manipulación informativa, asignadas en función de su coste e impacto.

Los datos presentados provienen de un riguroso análisis de información llevado a cabo por VIGINUM, el organismo francés encargado de la vigilancia y monitoreo de la manipulación de información.[15]

Asimismo, el estudio se ha complementado con investigaciones del SEAE, que aborda el fenómeno de la Manipulación y la Interferencia de Información Extranjera (SEAE, 2023, 2024) en la región europea.

Este análisis se ha llevado a cabo en coordinación con los sistemas de alerta temprana, cuya aproximación se desarrolló en el capítulo 6 de la primera entrega de los trabajos del Foro contra las Campañas de Desinformación en el ámbito de la Seguridad Nacional (2023), y se amplió para el propio SEAE, orientados a la identificación y prevención de incidentes FIMI. En este sentido, el cuadro no cuantifica datos, sino que ofrece una aproximación cualitativa de las tácticas en función de los incidentes revisados.

La valoración de cada técnica es una síntesis de observaciones empíricas y experiencias recientes sobre el coste e impacto que las acciones han tenido en la audiencia.

Los valores asignados en cada dimensión, coste e impacto, reflejan:

- Coste: la inversión estimada en recursos y esfuerzos necesarios para ejecutar cada táctica, evaluada según incidentes previos.

- Impacto: una medida cualitativa del alcance y la influencia observada de cada técnica en la audiencia o en los objetivos de manipulación, según las evaluaciones de impacto realizadas en incidentes concretos.

Este tipo de análisis resulta especialmente útil para comprender la efectividad relativa de cada técnica y priorizar la implementación de estrategias de contramedidas.

Al identificar qué tácticas son particularmente efectivas o de bajo coste para los actores que llevan a cabo manipulación de información, las instituciones pueden optimizar sus sistemas de alerta y respuesta, minimizando la vulnerabilidad de las audiencias a las manipulaciones informativas externas.

---

[15] La información de este análisis está disponible en su repositorio público en GitHub de VIGINUM (véase https://github.com/VIGINUM-FR)

ANÁLISIS DE DOCUMENTOS LEGALES PARA ABORDAR LA AMENAZA

Desde 2018 y hasta el momento presente, las instituciones de la Unión Europea y España han venido publicando documentos -tanto de naturaleza legal como informativa- en relación con las denominadas “amenazas híbridas” y, más concretamente, con posibles mecanismos de lucha contra uno de sus elementos más perturbadores y dañinos: las campañas de desinformación.

Siendo el propósito del presente trabajo el análisis de las implicaciones económicas de dichas campañas de desinformación, tanto en lo que se refiere al posible beneficio para los atacantes como a los perjuicios que su perpetración comporta para las víctimas, en cuanto al gasto requerido para habilitar mecanismos de prevención, disuasión, detección y recuperación, se ha hecho un recorrido por todos aquellos documentos significativos emanados de la Unión Europea y de España, arrancando dicho análisis con la publicación en 2018 del primer Code of Practice on Disinformation, y concluyendo con el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial, pasando por el Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales) o el Reglamento (UE) 2024/1083 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se establece un marco común para los servicios de medios de comunicación en el mercado interior y se modifica la Directiva 2010/13/UE (Reglamento Europeo sobre la Libertad de los Medios de Comunicación), sin olvidar a las normas nacionales españolas implicadas en mayor o menor medida en la regulación del tema tratado, como es, entre otra normativa analizada, el Real Decreto 444/2024, de 30 de abril, por el que se regulan los requisitos a efectos de ser considerado usuario de especial relevancia de los servicios de intercambio de vídeos a través de plataforma, en desarrollo del artículo 94 de la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual.

Se ha pretendido con todo ello desarrollar un estudio (ver ANEXO III) lo más completo posible, tratando de no dejar fuera del análisis ninguna aportación (nacional o europea) que pueda servir para alcanzar el objetivo perseguido.

CONCLUSIONES Y PROPUESTAS

La lucha contra la desinformación requiere un esfuerzo coordinado a nivel global, involucrando a gobiernos, empresas tecnológicas, mundo académico, medios de comunicación, periodistas y la sociedad civil en su conjunto, especialmente para identificar la motivación económica de las campañas de desinformación. Es necesario implementar medidas para fortalecer la resiliencia de las sociedades ante la manipulación informativa y promover un entorno digital más transparente y confiable.

Las campañas de desinformación, además de su impacto social y político, representan una seria amenaza para la estabilidad económica de los países, si bien, es clave abordar, por el contrario, el impacto económico que genera en los actores estatales desplegar sus estrategias desinformativas, en términos de coste-beneficio-eficiencia, incremento de la influencia y alcance, así como su percepción en el control narrativo. El impacto sobre la audiencia objetivo se intensifica en tiempos de elecciones o crisis, que son vistas como escenarios de vulnerabilidad para erosionar las democracias, las instituciones e influir en la opinión pública.

El sector de los medios de comunicación se ve particularmente afectado por la desinformación, ya que la rápida propagación de contenido falso erosiona la confianza en las fuentes tradicionales de información, provocando que las audiencias modifiquen sus patrones de consumo de información desplazándose hacía sitios webs alternativos que utilizan la desinformación como modelo de negocio, ya que se ven beneficiadas por el aumento del tráfico y, por ende, incrementan los ingresos por publicidad.

Los gobiernos deben destinar recursos considerables para combatir la desinformación, lo que implica la implementación de medidas y protocolos de detección y prevención, así como campañas de concienciación pública. En este sentido, a nivel europeo, la Unión Europea ha incrementado la financiación destinada a combatir la desinformación, aunque todavía se considera insuficiente.

Es esencial comprender que la desinformación no solo genera un coste para los gobiernos y empresas que buscan combatirla, sino que también beneficia a los actores que la impulsan. Estos actores, a menudo con motivaciones políticas o ideológicas, buscan obtener réditos económicos a través de la desestabilización, manipulación de mercados, o incluso extorsión.

Para ello, se propone la metodología del modelo DISARM como herramienta de análisis de las tácticas, técnicas y procedimientos (TTP) desplegadas por las campañas de desinformación identificar el componente económico de las campañas de desinformación. La literatura revela la existencia de métodos de bajo coste y alto impacto, lo que hace que estas campañas sean altamente rentables para sus perpetradores.

Más en detalle, a continuación, se pormenorizan los distintos países objeto de análisis, haciendo especial referencia a la posible vinculación y derivadas económicas de las TTP identificadas:

- Rusia: utiliza una amplia gama de TTP (que incluye la financiación de sitios web, uso de plataformas de micromecenazgo o *wallets* de criptomonedas), desde operaciones sofisticadas y costosas hasta tácticas más directas y de bajo coste. Esta variabilidad, además de la ofuscación de las transacciones, dificulta el

seguimiento del flujo monetario, la identificación de los beneficiarios finales y la evaluación del retorno de la inversión en desinformación.

- China: utiliza su poder económico para expandir su influencia a través de la desinformación. Invierte en medios de comunicación estatales y plataformas digitales para difundir propaganda y controlar la narrativa. Ha intensificado su estrategia de desinformación desde la pandemia de la COVID-19 y apoya la creación de un "mundo multipolar" en oposición a Occidente, reforzando su influencia entre otros, mediante la cooptación de voces en redes sociales para mejorar su imagen en el extranjero. La identificación del componente económico presenta una dificultad alta y ésta radica en la opacidad y la complejidad de sus redes de influencia.

- Irán: se enfoca en difundir propaganda antioccidental y movilizar apoyo para su agenda geopolítica. A través de grupos cibercriminales y *hacktivistas*, despliega campañas de desinformación dirigidas, entre otros, a EE. UU., Israel, utilizando tanto medios estatales como plataformas digitales (Telegram o X) para maximizar el alcance de sus narrativas y desacreditar a sus adversarios. Identificar el impacto económico de la desinformación es particularmente difícil a través de fuentes abiertas, las TTP no ofrecen información suficiente sobre los mecanismos de financiación o la monetización de sus campañas.

- Venezuela: ha incrementado el control de los medios y utiliza las RRSS para desacreditar a la oposición y promover narrativas progubernamentales. El uso de redes de perfiles artificiales y *trolls*, o la financiación de grupos que amplifican su narrativa, son TTP con una clara motivación económica.

De manera transversal a los países objeto de análisis, se considera extremadamente complejo determinar, a través de fuentes abiertas, la existencia de retribuciones directas o indirectas, por parte de actores estatales, a perfiles concretos que muestran indicios de alineamiento con la propaganda de aquellos, lo que no es óbice para que la promoción de dichos perfiles por los medios y canales oficiales de ciertos actores estatales facilita el reconocimiento popular, identificarlos como voces autorizadas y, por consiguiente, consiguen ampliar la audiencia a la que se dirigen los contenidos.

Aproximarnos al reto planteado por los actores estatales extranjeros y sus proxies, que utilizan las campañas de desinformación como modelo de negocio, para obtener financiación propia con la que seguir sufragando su estructura digital o para reclutar agentes de influencia fuera de sus fronteras, utilizando particulares TTP, requiere, en primer lugar, abordar si España cuenta con legislaciones menos gravosas y lesivas que el Código Penal que resuelvan la amenaza planteada y, en segundo lugar, contar con un amplio consenso entre expertos de reconocido prestigio de ámbitos distintos para abordar como sería la respuesta integral a las campañas de desinformación orquestas y qué soluciones han planteado los países democráticos aliados.

Esta respuesta integral iría desde el planteamiento de la necesidad de tipificar nuevos delitos, sancionar la financiación y apoyo logístico extranjero, extracción de responsabilidades a proxies y agentes de influencia domésticos, fortalecimiento de la cooperación internacional, potenciar la ciberinteligencia y mecanismos corregulatorios, hasta medidas que supongan la pérdida de los efectos, bienes, medios o instrumentos vinculados a dichas campañas de desinformación.

ANEXOS

ANEXO I: IDENTIFICACIÓN Y DESCRIPCIÓN DE LAS TTP

TTP	DESCRIPCIÓN
T0002: Facilitate State Propaganda	Diversos perfiles o medios no oficiales de los países señalados en este informe (incluidos influencers) divulgan las narrativas oficiales de sus gobiernos.
T0003: Leverage Existing Narratives	Utilizar narrativas existentes dentro de un territorio capaces de crear mucha polarización social.
T0009: Create Fake Experts	Inventarse perfiles que les ayuden a divulgar sus contenidos.
T0010: Cultivate Ignorant Agents	Promocionar a perfiles para que actúen como altavoz de los intereses del país dictatorial (apareciendo en sus medios, escribiendo para sus publicaciones, etc.).
T0011: Compromise Legitimate Accounts	Apoderarse de cuentas legítimas o ya existentes.
T0013: Create Inauthentic Websites	Crear páginas falsas de medios occidentales para engañar a los ciudadanos. Un método parecido a los ciberataques de phishing. Ejemplo reciente lo encontramos en la campaña rusa de *Doppelgänger*.
T0015: Create Hashtags and Search Artifacts	Crear *hashtags* artificiales para intentar crear un contenido *Trending Topic*.
T0016: Create Clickbait	Emplear titulares llamativos que empujen a un potencial lector a leer el contenido de la noticia.
T0017: Conduct Fundraising	Utilización de plataformas alternativas de pago como financiación (Youtube, X, Tipee, Patreon, GoFundMe, etc.)
T0018: Purchase Targeted Advertisements	Dirigir anuncios publicitarios a audiencias concretas.
T0019: Generate Information Pollution	Generar ruido mediático sobre un tema, creando artificialmente un debate inexistente.
T0022: Leverage Conspiracy Theory Narratives	Utilizar narrativas conspiranoicas ya existentes dentro de un territorio.

TTP	DESCRIPCIÓN
T0029: Online Polls	Manipular encuestas falsas en redes sociales. En este punto también estarían comprendidas las encuestas tendenciosas.
T0043: Use Chat Apps	La mensajería directa a través de aplicaciones de chat es un método de entrega cada vez más extendido. Estos mensajes suelen estar automatizados y los nuevos métodos de entrega y almacenamiento los hacen anónimos, virales y efímeros. Se trata de un espacio difícil de monitorizar, pero también para generar reconocimiento o notoriedad.
T0045: Use Fake Experts	Utilizar a individuos para que se hagan pasar por supuestos especialistas y, así, vender la versión oficial.
T0046: Use Search Engine Optimization	Manipular métricas de participación en el contenido (Twitter, Meta, Telegram).
T0047: Censor Social Media as a Political Force	Utilizar la censura para eliminar contenido no deseado.
T0048: Harass Opponents	Desprestigiar a oponentes tanto nacionales como extranjeros y tanto reales como perfiles de redes sociales.
T0049: Flooding the Information Space	Saturar las redes sociales con contenido sobre un tema concreto.
T0057: Organize Events	Organización de eventos. En este punto se incluyen el alquiler de recintos o salas en donde realizar eventos.
T0059: Play the Long Game	Planificar el mensaje y permitir que crezca orgánicamente sin amplificarlo artificialmente.
T0066: Degrade Adversary	Técnica que persigue degradar la imagen o la capacidad de actuar de un adversario.
T0068: Respond to Breaking News Event or Active Crisis	Responder o comentar una noticia de última hora, donde unos hechos poco claros y una información incompleta aumentan la especulación, los rumores y las teorías de conspiración, que son todas vulnerables a la manipulación.
T0072: Segment Audiences	Técnica consistente en segmentar al público objetivo de una campaña de desinformación. Un ejemplo lo podemos encontrar en cómo Rusia fomenta la Leyenda Negra en Latinoamérica.

TTP	DESCRIPCIÓN
T0073: Determine Target Audiences	Se trata de una acción dirigida a perfiles concretos. Un caso lo podemos encontrar en la "Operación Sobrecarga", una campaña de desinformación en favor del Kremlin por la cual los *factchekers* de diversos países son inundados con peticiones de investigación sobre temas no relevantes de forma que no puedan centrarse en lo importante.
T0074: Determine Strategic Ends	Estrategia que persigue minar la confianza institucional, reputacional y económica en un país adversario del Kremlin.
T0075: Dismiss	Responder a las críticas desestimándolas, lo que podría consistir en argumentar que los críticos utilizan un criterio diferente para la víctima que para otros actores o para ellos mismos, o argumentar que sus críticas son tendenciosas.
T0076: Distort	Cambiar el marco en el que se expone una narrativa.
T0077: Distract	Desviar la atención hacia una narrativa o actor diferente, por ejemplo, acusando a los críticos de la misma actividad de la que ellos mismos han sido acusados (por ejemplo, brutalidad policial).
T0078: Dismay	Amenazar a los periodistas que publican o informan de una noticia.
T0079: Divide	Crear conflictos entre subgrupos, para ensanchar las divisiones en una comunidad.
T0080: Map Target Audience Information Environment	Analizar el espacio de información en sí, incluido el análisis de redes sociales, el tráfico web y las encuestas de medios.
T0081: Identify Social and Technical Vulnerabilities	La identificación de vulnerabilidades sociales y técnicas determina los puntos débiles del entorno informativo del público objetivo para su posterior explotación. Las vulnerabilidades incluyen cuestiones políticas decisivas, infraestructuras de ciberseguridad débiles, vacíos de datos en los motores de búsqueda y otras debilidades técnicas y no técnicas en el entorno de información del público objetivo. La identificación de vulnerabilidades sociales y técnicas facilita la posterior explotación de las debilidades identificadas para avanzar en los objetivos de la operación.

TTP	DESCRIPCIÓN
T0086: Develop Image-based Content	Creación y edición de artefactos visuales falsos o engañosos, a menudo relacionados con una o más narrativas específicas, para su uso en una campaña de desinformación. Esto puede incluir fotografiar situaciones de la vida real, reutilizar imágenes digitales existentes o utilizar tecnologías de creación y edición de imágenes. En este punto encontramos aquellas generadas también por herramientas de Inteligencia Artificial (IA).
T0087: Develop Video-based Content	Creación y edición de videos falsos o engañosos, a menudo relacionados con una o más narrativas específicas, para su uso en una campaña de desinformación.
T0088: Develop Audio-based Content	Creación y edición de artefactos de audio falsos o engañosos, a menudo alineados con una o más narrativas específicas, para su uso en una campaña de desinformación. Esto puede incluir la creación de contenido de audio completamente nuevo, la reutilización de artefactos de audio existentes (incluidas falsificaciones pobres) o el uso de tecnologías de creación y edición de audio generadas por IA (incluidas las *deepfakes*). También, puede incluir la exhibición de videos de situaciones supuestamente reales, la reutilización de videos existentes o el uso de tecnologías de creación y edición de videos generados por IA (incluidos los *deepfakes*). En este punto se encuentran aquellos videos que, pese a que su contenido visual sea cierto, el audio no lo es o ha sido manipulado aumentando o eliminando contenido.
T0089: Obtain Private Documents	Obtener documentos que no están disponibles al público, por cualquier medio, ya sea legal o ilegal, que requiera muchos o pocos recursos. Estos documentos pueden incluir documentos auténticos no públicos, documentos auténticos no públicos que hayan sido alterados o documentos no auténticos que pretendan aparentar ser documentos auténticos no públicos. Todos estos tipos de documentos pueden "filtrarse" durante etapas posteriores de la operación (Operaciones de *Hack & Leak*).
T0093: Acquire/Recruit Network	Adquisición de una red existente pagando, reclutando o ejerciendo control sobre los líderes de la red existente.
T0095: Develop Owned Media Assets	Un activo mediático en propiedad se refiere a una agencia u organización a través de la cual una operación de influencia puede crear, desarrollar y alojar contenidos y narrativas. Los medios de comunicación propios incluyen sitios web, blogs, páginas de redes sociales, foros y otras plataformas que facilitan la creación y organización de contenidos.

TTP	DESCRIPCIÓN
T0096: Leverage Content Farms	Uso de los servicios de proveedores de contenido a gran escala para crear y amplificar artefactos de campaña a escala. Esta técnica sólo puede ser desarrollada por países con significativos recursos económicos.
T0100: Co-opt Trusted Sources	Incorporar a personas de confianza para divulgar una campaña de desinformación.
T0101: Create Localized Content	El contenido localizado se refiere al contenido que atrae a una comunidad específica de personas, a menudo en áreas geográficas definidas. Una operación puede crear contenido localizado utilizando el idioma y los dialectos locales para llegar a su público objetivo y combinarse con otras noticias y redes sociales locales. El contenido localizado puede ayudar a una operación a aumentar la legitimidad, evitar la detección y complicar la atribución externa. En este punto destacan los periódicos locales.
T0114: Deliver Ads	Difusión de contenidos a través de cualquier medio de pago o publicidad.
T0115: Post Content	Difusión de contenidos a través de medios propios (activos que controla el operador/agente de la amenaza).
T0116: Comment or Reply on Content	Difusión de contenidos respondiendo o comentando a través de medios propios (activos que controla el operador).
T0119: Cross-Posting	La publicación cruzada se refiere a publicar el mismo mensaje en múltiples foros de Internet, plataformas o cuentas de redes sociales o grupos de noticias, de manera simultánea.
T0123: Control Information Environment through Offensive Cyberspace Operations	Control del entorno informativo a través de operaciones ofensivas en el ciberespacio, utilizando herramientas y técnicas cibernéticas para alterar la trayectoria del contenido en el espacio informativo con el fin de priorizar los mensajes de la operación o bloquear los mensajes de la oposición.
T0126: Encourage Attendance at Events	Fomentar la asistencia o participación en ciertos eventos, impulsados por organismos oficiales, *think tanks*, Universidades, etc.
T0127: Physical Violence	Se refiere al uso de la fuerza para herir, abusar, dañar o destruir. Una operación de influencia puede llevar a cabo o alentar la violencia física para disuadir a los oponentes de promover contenido conflictivo o llamar la atención sobre las narrativas de la operación utilizando el valor del impacto.

TTP	DESCRIPCIÓN
T0128: Conceal People	Ocultar la identidad o procedencia de una cuenta de campaña y activos personales para evitar su eliminación y atribución. Borrando las cuentas o cambiando el nombre de estas una vez el mensaje se haya publicado.
T0129: Conceal Operational Activity	Ocultar la actividad operativa de la campaña para evitar su eliminación y atribución.
T0130: Conceal Infrastructure	Ocultar la infraestructura de la campaña para evitar la eliminación y atribución. Puede ser la eliminación de grupos de Reddit o Telegram.
T0131: Exploit TOS/ Content Moderation	Aprovechar las debilidades en los Términos de Servicio y las Políticas de Moderación de Contenido de las plataformas para evitar eliminaciones y acciones en la plataforma. Por ejemplo, cuando Twitter fue adquirida por Trump, las reglas de moderación se relajaron mucho.
T0132: Measure Performance	Realizar evaluaciones periódicas del éxito de una campaña de desinformación.
T0133: Measure Effectiveness	Métrica utilizada para medir el estado actual del sistema. Se persigue analizar si el método usado ayuda a logar el objetivo perseguido.

ANEXO II: RELACIÓN DE COSTE E IMPACTO POR TTP

TTP	Coste	Impacto
T0002: Facilitate State Propaganda	3	3
T0003: Leverage Existing Narratives	1	2
T0009: Create Fake Experts	2	3
T0010: Cultivate Ignorant Agents	2	2
T0011: Compromise Legitimate Accounts	2	3
T0013: Create Inauthentic Websites	2	3
T0015: Create Hashtags and Search Artifacts	1	2
T0016: Create Clickbait	1	1
T0017: Conduct Fundraising	1	2
T0018: Purchase Targeted Advertisements	3	3
T0019: Generate Information Pollution	1	2
T0022: Leverage Conspiracy Theory Narratives	1	2
T0029: Online Polls	2	2
T0043: Use Chat Apps	1	2
T0045: Use Fake Experts	2	3
T0046: Use Search Engine Optimization	2	3
T0047: Censor Social Media as a Political Force	3	3

T0048: Harass Opponents	2	3
T0049: Flooding the Information Space	2	3
T0057: Organize Events	2	3
T0059: Play the Long Game	2	3
T0066: Degrade Adversary	3	3
T0068: Respond to Breaking News Event or Active Crisis	2	3
T0072: Segment Audiences	1	2
T0073: Determine Target Audiences	1	2
T0074: Determine Strategic Ends	2	3
T0075: Dismiss	1	2
T0076: Distort	1	2
T0077: Distract	1	2
T0078: Dismay	1	2
T0079: Divide	1	3
T0080: Map Target Audience Information Environment	2	3
T0081: Identify Social and Technical Vulnerabilities	2	3
T0086: Develop Image-based Content	2	2
T0087: Develop Video-based Content	2	2
T0088: Develop Audio-based Content	2	2

T0089: Obtain Private Documents	2	3
T0093: Acquire/Recruit Network	3	3
T0095: Develop Owned Media Assets	3	3
T0096: Leverage Content Farms	3	3
T0100: Co-opt Trusted Sources	3	3
T0101: Create Localized Content	2	3
T0114: Deliver Ads	2	3
T0115: Post Content	1	2
T0116: Comment or Reply on Content	1	2
T0119: Cross-Posting	2	3
T0123: Control Information Environment through Offensive Cyberspace Operations	3	3
T0126: Encourage Attendance at Events	2	3
T0127: Physical Violence	3	3
T0128: Conceal People	3	3
T0129: Conceal Operational Activity	3	3
T0130: Conceal Infrastructure	3	3
T0131: Exploit TOS/Content Moderation	2	3
T0132: Measure Performance	2	2
T0133: Measure Effectiveness	2	3

ANEXO III: NIVEL DE ALINEAMIENTO/EFICACIA ESTIMADA DE NORMATIVA NACIONAL Y EUROPEA FRENTE A LA AMENAZA

LEYENDA

Nivel de alineamiento y/o eficacia estimada de los documentos relacionados en respuesta a las TTP:

- **Efecto SIGNIFICATIVO**
- **Efecto MODERADO**
- **Efecto BAJO**

	Ley 13/2022, de 7 de julio, **General de Comunicación Audiovisual.**	Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE **(Reglamento de Servicios Digitales).**	Real Decreto 1138/2023, de 19 de diciembre, por el que se regulan el **Registro estatal de prestadores del servicio de comunicación audiovisual, de prestadores del servicio de intercambio de vídeos a través de plataforma y de prestadores del servicio de agregación de servicios de comunicación audiovisual y el procedimiento de comunicación previa de inicio de actividad.**	Reglamento (UE) 2024/900 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, sobre **transparencia y segmentación en la publicidad política**.	Reglamento (UE) 2024/1083 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se establece un marco común para los servicios de medios de comunicación en el mercado interior y se modifica la Directiva 2010/13/UE **(Reglamento Europeo sobre la Libertad de los Medios de Comunicación).**
TTP	**Artículos aplicables**				
T0002: Facilitate State Propaganda	art. 42		art. 12	arts. 1 y 8	art. 6
T0003: Leverage Existing Narratives	art. 78				
T0009: Create Fake Experts			art. 12	arts. 11 y 12	
T0010: Cultivate Ignorant Agents	art. 79	art. 22			art. 18
T0011: Compromise Legitimate Accounts	arts. 14 y 15		art. 36		
T0013: Create Inauthentic Websites	art. 9	arts. 9,10	art. 27	art. 11	
T0015: Create Hashtags and Search Artifacts					
T0016: Create Clickbait	art. 78		art. 12	arts. 11 y 12	
T0017: Conduct Fundraising	arts. 14 y 15	art. 67	art. 13		
T0018: Purchase Targeted Advertisements	arts. 14 y 15	art. 44		art. 18	
T0019: Generate Information Pollution	art. 78			art. 13	
T0022: Leverage Conspiracy Theory Narratives					
T0029: Online Polls	arts. 14 y 15	art. 25			

T0043: Use Chat Apps					
T0045: Use Fake Experts			art. 12		
T0046: Use Search Engine Optimization	arts. 14 y 15				
T0047: Censor Social Media as a Political Force	arts. 14 y 15				arts. 3,17
T0048: Harass Opponents		arts.9,34	art. 32	art. 15	
T0049: Flooding the Information Space	arts. 14 y 15	arts. 34, 35	art. 20	arts. 11 y 12	
T0057: Organize Events	art. 78				
T0059: Play the Long Game	arts. 14 y 15				
T0066: Degrade Adversary	art. 78	arts. 9,10			
T0068: Respond to Breaking News Event or Active Crisis	arts. 14 y 15				
T0072: Segment Audiences	art. 78	art. 44		art. 18	
T0073: Determine Target Audiences	DA5[a]	art. 44		art. 18	art. 20
T0074: Determine Strategic Ends	art. 78	arts. 34,35			
T0075: Dismiss		arts. 9,10			
T0076: Distort					
T0077: Distract					
T0078: Dismay	art. 78				
T0079: Divide	arts. 14 y 15				
T0080: Map Target Audience Information Environment	art. 78	art. 34			art. 6
T0081: Identify Social and Technical Vulnerabilities					
T0086: Develop Image-based Content	art. 98	art. 100			
T0087: Develop Video-based Content	art. 98	art. 100			
T0088: Develop Audio-based Content	arts. 14 y 15				
T0089: Obtain Private Documents					

T0093: Acquire/Recruit Network			art. 12		
T0095: Develop Owned Media Assets	art. 78		art. 12		
T0096: Leverage Content Farms	art. 78	arts. 34,35			
T0100: Co-opt Trusted Sources	art. 42	art. 22			art. 6
T0101: Create Localized Content	arts. 14 y 15				
T0114: Deliver Ads	arts. 14 y 15	arts. 9,10	art. 13	art. 18	
T0115: Post Content		arts. 9,10			
T0116: Comment or Reply on Content	arts. 14 y 15	arts. 9,10			
T0119: Cross-Posting	arts. 14 y 15	art. 35			
T0123: Control Information Environment through Offensive Cyberspace Operations		arts. 34,35			
T0126: Encourage Attendance at Events					
T0127: Physical Violence	art. 78	art. 67			
T0128: Conceal People	arts. 14 y 15	art. 30			art. 6
T0129: Conceal Operational Activity		art. 30			
T0130: Conceal Infrastructure		art. 67			
T0131: Exploit TOS/Content Moderation	arts. 14 y 15	art. 34			
T0132: Measure Performance	art. 78				
T0133: Measure Effectiveness	arts. 14 y 15				

	The Strengthened Code of Practice on disinformation 2022	Plan de Acción contra la desinformación.	**Directrices** de la Comisión para los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño para la **reducción de los riesgos sistémicos en los procesos electorales de conformidad con el artículo 35, apartado 3, del Reglamento (UE) 2022/2065**	Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 **(Reglamento de Inteligencia Artificial).**
TTP	**Artículos aplicables**			
T0002: Facilitate State Propaganda	Comp. 4 al 13	Pilar 1 / Acción 1	secciones 3.2.1(c) (iv) / 3.2.27	
T0003: Leverage Existing Narratives	Comp. 18	Pilar 4 / Accs 7, 9		
T0009: Create Fake Experts	Comp. 14	Pilar 3 / Acción 6	secciones 3.2.1 (c)(iii) / 3.2.1 (c)(iv) / 3.2.1 (c)(v)	art. 52
T0010: Cultivate Ignorant Agents				
T0011: Compromise Legitimate Accounts			sección 3.2.1(h)	
T0013: Create Inauthentic Websites	Comp. 1	Pilar 1 / Acción 1	secciones 3.2.1 (h) / 3.2.1 (i)	art. 50
T0015: Create Hashtags and Search Artifacts	Comp. 14 / Med. 14.1	Pilar 1 / Acción 1		
T0016: Create Clickbait			sección 3.2.1 (c)(ii)	
T0017: Conduct Fundraising	Comp. 1 / Med. 1.1	Pilar 3 / Acción 6	sección 3.2.1€	
T0018: Purchase Targeted Advertisements	Comp. 2 /Meds. 2.1, 2.2	Pilar 3 / Acción 6		arts. 50 y 52
T0019: Generate Information Pollution				

T0022: Leverage Conspiracy Theory Narratives	Comp. 18	Pilar 4 / Accs 7, 9		
T0029: Online Polls				
T0043: Use Chat Apps	Comp. 25 / Med. 25.2	Pilar 3 / Acción 6		
T0045: Use Fake Experts	Comp. 14	Pilar 3 / Acción 6	secciones 3.2.1 (c)(iii) / 3.2.1 (c)(iv) / 3.2.1 (c)(v)	art. 52
T0046: Use Search Engine Optimization	Med. 14.1	Pilar 1 / Acción 1		art. 5
T0047: Censor Social Media as a Political Force	Cons. (c)	Introducción		
T0048: Harass Opponents	Comp. 48	Pilar 3 / Acción 6	sección 3.2.1(h) / 3.2.1(i)	
T0049: Flooding the Information Space			sección 3.2.1(d)	art. 110
T0057: Organize Events				
T0059: Play the Long Game				
T0066: Degrade Adversary			sección 3.2.1 (b)	
T0068: Respond to Breaking News Event or Active Crisis				
T0072: Segment Audiences			sección 3.112	
T0073: Determine Target Audiences			sección 3.112	
T0074: Determine Strategic Ends				
T0075: Dismiss				
T0076: Distort				
T0077: Distract	Comp. 21	Pilar 4 / Acción 9		
T0078: Dismay				
T0079: Divide				

T0080: Map Target Audience Information Environment			sección 3.112	
T0081: Identify Social and Technical Vulnerabilities				
T0086: Develop Image-based Content				art. 52
T0087: Develop Video-based Content				art. 52
T0088: Develop Audio-based Content				
T0089: Obtain Private Documents				
T0093: Acquire/Recruit Network			sección 3.2.1(i)	
T0095: Develop Owned Media Assets			sección 3.2.1(c)	
T0096: Leverage Content Farms				
T0100: Co-opt Trusted Sources				
T0101: Create Localized Content	Comp. 30	Pilar 4 / Acción 8		
T0114: Deliver Ads				arts. 50 y 52

T0115: Post Content				
T0116: Comment or Reply on Content				
T0119: Cross-Posting				
T0123: Control Information Environment through Offensive Cyberspace Operations				
T0126: Encourage Attendance at Events				
T0127: Physical Violence				
T0128: Conceal People				
T0129: Conceal Operational Activity				
T0130: Conceal Infrastructure				
T0131: Exploit TOS/Content Moderation				arts. 117 y 118
T0132: Measure Performance	Comps. 34, 38 al 44	Pilar 1 / Acción 1		
T0133: Measure Effectiveness				

ANEXO IV: CRIPTODIVISAS COMO MÉTODO DE FINANCIACIÓN

En los últimos años, las criptomonedas han surgido como un método de financiación para facilitar campañas de desinformación y operaciones de interferencia a nivel global. Actores estatales y no estatales aprovechan el aparente anonimato y carácter transnacional de las criptomonedas para financiar, organizar y mantener redes que buscan desestabilizar democracias y sembrar desconfianza en las instituciones. Los pagos en criptomonedas permiten a estos actores adquirir infraestructura digital, como servidores y servicios de alojamiento en línea, fundamentales para crear y gestionar sitios web de noticias falsas, redes de *bots* y perfiles en redes sociales que amplifican sus campañas de influencia.

La Oficina de Control de Activos Extranjeros (OFAC) ha identificado numerosas direcciones de criptomonedas vinculadas a individuos y organizaciones que participan en estas campañas de desinformación, y ha impuesto sanciones a quienes financian y apoyan estas actividades.

Las criptomonedas, como Bitcoin y USDT, se han utilizado para recolectar donaciones que financian operaciones militares y propaganda, con actores como el medio de desinformación ruso SouthFront y el grupo paramilitar Task Force Rusich. SouthFront, por ejemplo, solicitando cripto donaciones en su página web, dando instrucciones a sus seguidores para transferir fondos desde billeteras personales, evitando de esta manera intermediarios. Específicamente en el caso de Task Force Rusich, grupo vinculado a la guerra en Ucrania, se ha encontrado evidencia de la utilización de criptomonedas para financiar la compra de equipos militares y difundir propaganda que apoya los objetivos del gobierno ruso.

Además, estos grupos emplean servicios de venta de cuentas robadas y de alojamiento en servidores anónimos, que también aceptan pagos en criptomonedas. En la *darknet*, existen plataformas que venden cuentas comprometidas de redes sociales, facilitando a los actores de desinformación hacerse pasar por usuarios reales y alcanzar grandes audiencias de manera masiva. Estos servicios, a menudo en idiomas extranjeros como el ruso, permiten la adquisición de cuentas a gran escala y brindan a los actores maliciosos la capacidad de escalar sus campañas sin ser detectados. A la par, proveedores de infraestructura *offshore*, como el servicio de alojamiento web Shinjiru, ofrecen anonimato para sitios de propaganda, permitiendo que las campañas de desinformación se mantengan activas sin riesgo de supervisión regulatoria.

El impacto de estas campañas financiadas con criptomonedas es especialmente evidente en su combinación con redes de *trolls* y *bots* que amplifican los mensajes.

Grupos paramilitares y actores prorrusos utilizan plataformas de mensajería como Telegram para pedir donaciones en criptomonedas, las cuales se destinan a operaciones de desinformación y actividades militares. Las investigaciones muestran que algunos de estos actores han recibido millones de dólares en criptomonedas, fondos que luego fluyen a cuentas de intercambio donde se convierten en moneda fiduciaria para financiar diversas actividades ilícitas.

El análisis de la cadena de bloques, o *blockchain*, permite a los investigadores rastrear transacciones y conectar a los actores y organizaciones que financian estas redes de desinformación.

El rastreo de criptomonedas se ha convertido en una herramienta indispensable para las agencias de seguridad que buscan identificar y desarticular a los autores y financiadores detrás de estas redes de influencia global. Dado que las criptomonedas suelen ser usadas por los actores involucrados en campañas de desinformación, la actividad en la cadena de bloques contiene indicadores y evidencias que pueden ayudar a las agencias gubernamentales e investigadores en general, a identificar, analizar y, en relación con aquellos, detener a los actores maliciosos, en el caso de presuntas actividades delictivas. Con el tiempo, las empresas de análisis del *blockchain* han colaborado con agencias públicas para rastrear transacciones en criptomonedas vinculadas a diversas actividades ilícitas para que analistas e investigadores puedan usar técnicas de rastreo de criptomonedas tanto para ampliar su comprensión de las redes criminales como para interrumpirlas de manera efectiva.

REFERENCIAS BIBLIOGRÁFICAS

Abril, G. (2022, 22 de octubre). Xi Jinping, según la propaganda. *El País*. https://elpais.com/internacional/2022-10-22/xi-jinping-segun-la-propaganda.html

Abril, G. y Bonet Bailén, I. (2022, 27 de noviembre). Las protestas se extienden en China contra la política de covid cero. *El País*. https://elpais.com/internacional/2022-11-27/las-protestas-contra-las-politicas-de-covid-cero-se-extienden-por-shanghai-y-otras-ciudades-de-china.html

AFP. (2023, 19 de septiembre). *US politicians, commentators misrepresent fictional pride flag skit*. https://factcheck.afp.com/doc.afp.com.33VL6VA

Aguirre, M. (2022). Una nueva y diferente Guerra Fría. *OBSERVARE - JANUS 2022 - O país que somos o(s) mundo(s) que temos: um roteiro para o conceito estratégico na próxima década*, 102-103. http://hdl.handle.net/11144/5547

Araújo, H. (2022, 1 de noviembre). Malos tiempos para los pensadores chinos. *El País*. https://elpais.com/ideas/2022-11-01/malos-tiempos-para-los-pensadores-chinos.html

Arteaga, F. y Simón, L. (2021). La OTAN se actualiza: el concepto estratégico de Madrid. *Real Instituto Elcano*, (106). Disponible en: https://media.realinstitutoelcano.org/wp-content/uploads/2021/12/ari106-2021-arteaga-simon-otan-se-actualiza-concepto-estrategico-madrid.pdf

Arteaga, F., y Simón, L. (2022). El Concepto Estratégico de Madrid: una (auto)evaluación de los resultados. *Real Instituto Elcano,* (51). Disponible en: https://www.realinstitutoelcano.org/analisis/el-concepto-estrategico-de-madrid-una-autoevaluacion-de-los-resultados/

Bartolomé, M. C. (2021). Redes sociales, desinformación, cibersoberanía y vigilancia digital: una visión desde la ciberseguridad. *Revista Estudios en Seguridad Internacional, 7(2)*, 167-185.

Belinchón, G. (2022, 8 de julio). El cine de propaganda nunca ha desaparecido: ahora se lanzan a él chinos y rusos. El País. https://elpais.com/cultura/2022-07-08/el-cine-de-propaganda-nunca-ha-desaparecido-ahora-se-lanzan-a-el-chinos-y-rusos.html

Bergmanis-Korats, G., y Haiduchyk, T. (2024). Social Media Manipulation for Sale: 2024 Experiment on Platform Capabilities to Detect and Counter Inauthentic Social Media Engagement. *NATO Strategic Communications Centre of Excellence*. https://stratcomcoe.org/publications/social-media-manipulation-for-sale-experiment-on-platform-capabilities-to-detect-and-counter-inauthentic-social-media-engagement/311

Bradshaw, S., Bailey, H., y Howard, P. N. (2020). Industrialized Disinformation. 2020 Global Inventory of Organized Social Media Manipulation. *Oxford Internet Institute*. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/02/CyberTroop-Report20-Draft9.pdf

Brändle, V. K., Galpin, C., y Trenz, H. J. (2021). Brexit as 'politics of division': social media campaigning after the referendum. *Social Movement Studies, 21(1-2)*, 234–253. https://doi.org/10.1080/14742837.2021.1928484

Brime, I. (2021, 14 de marzo). La obsesión multipolar de China. *El Español*. https://www.elespanol.com/blog_del_suscriptor/opinion/20210314/obsesion-multipolar-china/565763420_7.html

Burgess, C. (2023, 30 de agosto). The Dark Side of LinkedIn: China's Espionage Playground. *Clearance Jobs*. https://news.clearancejobs.com/2023/08/30/the-dark-side-of-linkedin-chinas-espionage-playground/

Center for Defense Reforms. (2024). *Toy Soldiers: NATO military and intelligence officers in Russian active measure*. https://ftn.news/toy-soldiers-nato-military-and-intelligence-officers-russian-active-measures

Centro Criptológico Nacional [CCN]. (2019). *Desinformación en el ciberespacio*. CCN-CERT BP/13. https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/3552-ccn-cert-bp-13-desinformacion-en-el-ciberespacio-1/file.html

Chan, K. y Thornton, M. (2022, 19 de septiembre). China's Changing Disinformation and Propaganda Targeting Taiwan. *The Diplomat*. https://thediplomat.com/2022/09/chinas-changing-disinformation-and-propaganda-targeting-taiwan/

Cheung, R. (2022, 19 de octubre). Anti-Xi Jinping Posters Are Spreading in China via AirDrop. *Vice*. https://www.vice.com/en/article/wxn7nq/anti-xi-jinping-posters-are-spreading-in-china-via-airdrop

Christov, A. (2019). ECONOMY OF THE FAKE NEWS: BUSINESS SIDE AND EFFECTS. *Eastern Academic Journal, 4*, 1-7. https://www.e-acadjournal.org/pdf/article-19-4-1.pdf

Cocuyo chequea (2023, 22 de noviembre). #CiberalianzaAlDescubierto: El Mazo y las redes anónimas se unen para desinformar. *Efectococuyo*. https://pulse.internetsociety.org/es/blog/internet-censorship-verging-on-service-blocking-ahead-of-venezuela-elections

Condliffe, J. (2017, 14 de junio). Fake News Is Unbelievably Cheap to Produce. *MIT Technology Review*. https://www.technologyreview.com/2017/06/14/151233/fake-news-is-unbelievably-cheap/

Consejo de la Unión Europea. (2024). *Venezuela: Declaración del Alto Representante, en nombre de la UE, sobre los acontecimientos consecutivos a las elecciones*. [Nota de prensa]. https://www.consilium.europa.eu/es/press/press-releases/2024/08/04/venezuela-statement-by-the-high-representative-on-behalf-of-the-eu/

Cook, S. (2020, 11 de enero). Beijing's Global Megaphone. The Expansion of Chinese Communist Party Media Influence since 2017. *Freedom House*. https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone

Corera, G. (2020, 19 de julio). Why did MI5 name Christine Lee as an 'agent of influence'? *BBC.* https://www.bbc.com/news/uk-62179004

Davidson, H. (2021, 11 de agosto). Chinese media in fake news claims over Swiss scientist critical of US. *The Guardian*. https://www.theguardian.com/world/2021/aug/11/chinese-media-fake-news-claims-swiss-scientist-wilson-edwards-critical-of-us

De la Cal, L. (2022a, 5 de junio). Desesperados por escapar de China: “No podía aguantar la extrema política de restricciones”. *El Mundo*. https://www.elmundo.es/internacional/2022/06/05/628618b021efa0801d8b45b8.html

De la Cal, L. (2022b, 1 de julio). La nueva era ‘democrática’ de Hong Kong según Xi Jinping: una ciudad que solo puede ser gobernada por patriotas. *El Mundo*. https://www.elmundo.es/internacional/2022/07/01/62bea4f0fdddfff53c8b45f5.html

De la Cal, L. (2022c, 7 de agosto). China exprime la artillería propagandística con vídeos a la norcoreana. *El Mundo*. https://www.elmundo.es/internacional/2022/08/07/62ee82e6fc6c83e91f8b45cc.html

De la Cal, L. (2022d, 24 de noviembre). China empieza a rebelarse contra el ‘Covid cero’: violentas protestas en la mayor fábrica de iPhone del mundo. *El Mundo*. https://www.elmundo.es/internacional/2022/11/24/637dee80e4d4d8704f8b45b2.html

Delage, F. (2019). China y la gobernanza económica global: hacia un orden pluralista. *Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades,* 21(42), 133-153.

Departamento de Seguridad Nacional (2022, 27 de septiembre). *Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional: propuestas de la sociedad civil*. Catálogo de publicaciones de la Administración General del Estado. https://www.dsn.gob.es/es/documento/lucha-contra-campa%C3%B1as-desinformaci%C3%B3n-%C3%A1mbito-seguridad-nacional-propuestas-sociedad-civil

Departamento de Justicia de EE. UU. (2024, 4 de septiembre). *Two RT Employees Indicted For Covertly Funding And Directing U.S. Company That Published Thousands Of Videos In Furtherance Of Russian Interests*. https://www.justice.gov/usao-sdny/pr/two-rt-employees-indicted-covertly-funding-and-directing-us-company-published

DISARM (2022). *DISARM Framework Explorer.* https://disarmframework.herokuapp.com/

DFRLab. (2023, 12 de enero). How China funds foreign influence campaigns. *Medium*. https://medium.com/dfrlab/how-china-funds-foreign-influence-campaigns-72d547ad0771

Dubow, B., Greene, S., y Rzegocki, S. (2022, 28 de septiembre). Tracking Chinese Online Influence in Central and Eastern Europe. *Center for European Policy Analysis (CEPA)*. https://cepa.org/comprehensive-reports/tracking-chinese-online-influence-in-central-and-eastern-europe/

Economist Intelligence Unit. (2023). *Democracy Index 2023*. https://www.eiu.com/n/campaigns/democracy-index-2023/

Europa Press. (2022, 25 de diciembre). China oculta ahora sus casos diarios de Covid ante la avalancha de nuevos contagios. *El Confidencial*. https://www.elconfidencial.com/mundo/2022-12-25/china-oculta-ahora-sus-casos-diarios-de-covid-ante-la-avalancha-de-contagios_3547742/

Fake News and its Impact on the Economy (2020, 11 de agosto). Priority Consultants. https://priorityconsultants.com/fake-news-and-its-impact-on-the-economy/

Foro contra las Campañas de Desinformación en el ámbito de la Seguridad Nacional. (2023). Trabajos 2023. Presidencia del Gobierno. https://www.dsn.gob.es/sites/dsn/files/Foro%20Campa%C3%B1as%20Desinfo%20GT%202023%20Accesible.pdf

Freedom House. (2024). *Freedom in the world 2024*. https://freedomhouse.org/sites/default/files/2024-02/FIW_2024_DigitalBooklet.pdf

Gadzynska, I., Mikhalkov, S. Tymoshenko, M., Lytvynov, V., Kelm, N., y Drozdova, Y. (2024). *Roller Coaster. From Trumpists to Communists. The forces in the U.S. impeding aid to Ukraine and how they do it*. https://texty.org.ua/projects/112617/roller-coaster/

Global Disinformation Index (2022, 8 de noviembre). Ad-funded Elections Integrity Disinformation. *Disinformationindex.org*. https://www.disinformationindex.org/research/2022-11-08-ad-funded-elections-integrity-disinformation/

Global Engagement Center. (2020a). *Pilares del Ecosistema de Desinformación y Propaganda de Rusia*. https://www.state.gov/wp-content/uploads/2020/08/Pilares-del-Ecosistema-de-Desinformacioi%CC%80n-y-Propaganda-de-Rusia.pdf

Global Engagement Center. (2020b). How the People's Republic of China Seeks to Reshape the Global Information Environment. *Department of State*. Disponible en: https://www.state.gov/gec-special-report-how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment/

Global Influence Operations Report. (2022, 20 de julio). *German Intelligence Says China Seeks to Instrumentalize Diaspora Groups and Journalists; 'Win Over' Politicians as Lobbyists*. https://www.global-influence-ops.com/german-intelligence-says-china-seeks-to-instrumentalize-diaspora-groups-and-journalists-win-over-politicians-as-lobbyists/

González Enríquez, C., y José Martínez, J. (2022). Barómetro del Real Instituto Elcano. Edición especial: guerra en Ucrania y Cumbre de la OTAN, junio de 2022. *Real Instituto Elcano*. Disponible en: https://www.realinstitutoelcano.org/encuestas/barometro-especial-guerra-en-ucrania-y-cumbre-otan/

Graham, E. (2022, 8 de diciembre). China's Reported Manipulation of Twitter Draws Lawmaker Questions. *Nextgov/FCW.* https://www.nextgov.com/cybersecurity/2022/12/chinas-reported-manipulation-twitter-draws-lawmaker-questions/380642/

Hao, Z. (2022, 28 de junio). How NATO began with confrontation and ends with poisoning world peace? *Global Times*. https://www.globaltimes.cn/page/202206/1269264.shtml

Heikkinen, D. (2021). An analysis of fake news and its effects on the economy and society. *Cyber News, Research, and Commentary Journal, 1(2)*, 7-12. https://mpra.ub.uni-muenchen.de/116027/1/MPRA_paper_116027.pdf

Hernández, E. (2022, 26 de junio). Entrevista con Javier Solana. El actor importante es China, no Rusia. *El Confidencial*. https://www.elconfidencial.com/espana/2022-06-26/javier-solana-entrevista_3448509/

Hernández, E. y García L.M. (2021). Chinese strategic thinking. The fundamentals of the Chinese model of world governance. *Sinología Hispánica. China Studies Review, 12*(1), 1-32.

Hernández, O. (2022, 29 de noviembre). La prensa oficialista, 'bombero' de Pekín: "Las medidas 'covid cero' son el único camino correcto". *El Confidencial*. https://www.elconfidencial.com/mundo/2022-11-29/prensa-china-silencia-protestas-medidas-covid-cero_3530868/

IBERIFIER. (2023). *Analysis of the impact of disinformation on political, economic, social and security issues, governance models and good practices: the cases of Spain and Portugal*. https://iberifier.eu/2023/06/21/report-analysis-impact-disinformation-june-2023/

International Republican Institute. (28 de septiembre de 2022). *Coercion, Capture, and Censorship: Case Studies on the CCP's Quest for Global Influence*. https://www.iri.org/resources/coercion-capture-and-censorship-case-studies-on-the-ccps-quest-for-global-influence/

Keown, A. (2018, 27 de noviembre). China's 'Thousand Talents Plan' Recruits Western Scientists and Researchers. *BioSpace*. https://www.biospace.com/china-s-thousand-talents-plan-recruits-western-scientists-and-researchers

Kerr, N. (2023, 22 de junio). What RFK Jr., now a presidential candidate, has said about Ukraine, vaccines, the economy and more. *ABC News.* https://abcnews.go.com/Politics/rfk-jr-now-presidential-candidate-ukraine-vaccines-economy/story?id=100247005

Krenz, N. (2022, 13 de marzo). An Analysis of the 2020 Zoom Breach. *Cloud Security Alliance*. https://cloudsecurityalliance.org/blog/2022/03/13/an-analysis-of-the-2020-zoom-breach

Ling, L. (2022a, 1 de septiembre). How China's Party Congress Actually Works. The Diplomat. https://thediplomat.com/2022/08/how-chinas-party-congress-actually-works/

Ling, L. [@lingli_vienna]. (2022b, 5 de septiembre). I *wrote a long-form piece for The Diplomat, explaining how the Party Congress works. I also identify the formally authorized group who makes the final approval of nominated candidates for the membership of the Central Committee. Main takeaways. A thread*. X. https://twitter.com/lingli_vienna/status/1566798991781765120

Ling, L. [@lingli_vienna]. (2022c, 7 de septiembre). Th*read about my last [thread] on How the Party Congress Actually Works. This [thread] includes: A correction Some response to questions posted to me about the Chairmen-league Standing Committee (SCOCL). Its members sit in the front row. Ordinary members of the League sit at the back*. X. https://x.com/lingli_vienna/status/1567543444997914631

Luna, J. (2022, 28 de noviembre). Entrevista Joshua Kurlantzick. "China igualará pronto a Rusia en fake news", *La Vanguardia*. https://www.lavanguardia.com/internacional/20221128/8621009/china-igualara-pronto-rusia-fake-news.html

M. Martin, C. (2021, 11 de agosto). "The PRC: International Stimulus, Strategic Culture and Resulting Domestic Policies". *The Defence Horizon.* https://www.thedefencehorizon.org/post/the-prc-international-stimulus-strategic-culture-and-resulting-domestic-policies

Menn, J. (2022, 27 de noviembre). Twitter grapples with Chinese spam abscuring news of protest. *The Washington Post*. https://www.washingtonpost.com/technology/2022/11/27/twitter-china-spam-protests/

Menn, J. (2024, 2 de junio). News site editor's ties to Iran, Russia show misinformation's complexity. *The Washington* Post. https://www.washingtonpost.com/technology/2024/06/02/gray-zone-russia-iran-support/

Milosevich-Juaristi, M. (2020, 20 de abril). ¿Por qué hay que analizar y comprender las campañas de desinformación de China y Rusia sobre el COVID-19? *Real Instituto Elcano*. Disponible en: https://www.realinstitutoelcano.org/analisis/por-que-hay-que-analizar-y-comprender-las-campanas-de-desinformacion-de-china-y-rusia-sobre-el-covid-19/

Ministerio de Asuntos Exteriores, UE y Cooperación. (2024). *Declaración conjunta sobre Venezuela*. [Nota de prensa] https://www.exteriores.gob.es/es/Comunicacion/Comunicados/Paginas/2024_COMUNICADOS/20240816_COMU044.aspx

Mitchell, R. (2024, 26 de julio). La censura en Internet roza el bloqueo de servicios antes de las elecciones en Venezuela. *Internetsociety*. https://pulse.internetsociety.org/es/blog/internet-censorship-verging-on-service-blocking-ahead-of-venezuela-elections

News. (2023, 19 de junio). Viaje de periodistas españoles a Irán: "Los occidentales tergiversan las realidades del país". *Agencia de Noticias de la República Islámica (IRNA)*. https://es.irna.ir/news/85145576/Viaje-de-periodistas-espa%C3%B1oles-a-Ir%C3%A1n-Los-occidentales-tergiversan

News. (2024, 7 de febrero). Iranian Authorities Bet on Foreign Influencers to Boost Tourism. *Iranwire*. https://iranwire.com/en/news/125094-iranian-authorities-bet-on-foreign-influencers-to-boost-tourism/

Nimmo, B. (2022, 27 de septiembre). Removing Coordinated Inauthentic Behavior From China and Russia. *Meta*. https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia/

National Intelligence Council. (2020, 7 de abril). *Cyber Operations Enabling Expansive Digital Authoritarianism*. https://www.dni.gov/files/ODNI/documents/assessments/NICM-Declassified-Cyber-Operations-Enabling-Expansive-Digital-Authoritarianism-20200407--2022.pdf

Novelo, A. (2024, 13 de junio). RFK Jr. offers foreign policy views on Ukraine, Israel, vows to halve military spending. *CBS News*. https://www.cbsnews.com/news/rfk-jr-foreign-policy-views-ukraine-israel-military-spending/

Países Bajos. (2022). *Government-wide strategy for effectively tackling disinformation*. Ministry of the Interior and Kingdom Relations. Directorate-General for Public Administration and Democratic Rule of Law/Democracy and Governance Directorate. https://www.government.nl/documents/parliamentary-documents/2022/12/23/government-wide-strategy-for-effectively-tackling-disinformation

Papadogiannakis, E., Papadopoulos, P., P. Markatos, E., y Kourtellis, N. (2023). Who Funds Misinformation? A Systematic Analysis of the Ad-related Profit Routines of Fake News sites.

En *Proceedings of the ACM Web Conference 2023*, 2765-2776. https://doi.org/10.48550/arXiv.2202.05079

Parlamento del Reino Unido (2024). *Disinformation: sources, spread and impact*. https://researchbriefings.files.parliament.uk/documents/POST-PN-0719/POST-PN-0719.pdf

Parlamento Europeo (2021). *Strategic communications as a key factor in countering hybrid threats.* European Parliamentary Research Service, Scientific Foresight Unit (STOA). https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)656323

Parlamento Europeo (2022). *Final Report on Foreign interference in all democratic processes in the European Union.* European Parliament resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation (2020/2268(INI)). https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064_EN.html

Pérez Gallardo, M. (2024, 27 de julio). ¿Quiénes serán los observadores electorales en las presidenciales de Venezuela? *France24*. https://www.france24.com/es/am%C3%A9rica-latina/20240727-quienes-ser%C3%A1n-los-observadores-electorales-en-las-presidenciales-de-venezuela

Priego, A. (2022, 27 de junio). Los seis ejes de la cumbre de la OTAN en Madrid. *The Conversation*. https://theconversation.com/los-seis-ejes-de-la-cumbre-de-la-otan-en-madrid-185882

Pollard, M. Q. y Goh, B. (2022, 28 de noviembre). Blank sheets of paper become symbol of defiance in China protests. *Reuters*. Blank sheets of paper become symbol of defiance in China protests | Reuters

Repnikova, M. (2022, 21 de junio). The Balance of Soft Power. *Foreign Affairs*. https://www.foreignaffairs.com/china/soft-power-balance-america-china

Sammarco, A. (2024, 5 de abril). RFK Jr. Repeats Russian Propaganda on Ukraine. *Los Angeles Magazine*. https://lamag.com/news-and-politics/rfk-jr-repeats-russian-propaganda

Radio Televisión Española (2022, 28 de noviembre). *La movilización contra la política 'COVID cero' deja las mayores protestas en China en 30 años* [Vídeo]. RTVE. https://www.rtve.es/play/videos/telediario-2/movilizacion-contra-covid-cero-deja-mayores-protestas-china-treinta-anos/6746415/

Rathbone, J. P., y Sevastopulo, D. (2022, 29 de agosto). "On a par with the Russians": rise in Chinese espionage alarms Europe. *Financial Times*. https://www.ft.com/content/282aed88-de6e-4356-8a46-5718943853c4

Reuters (2022, 7 de julio). U.S. counterintelligence warns of China stepping up influence operations. *Reuters*. https://www.reuters.com/world/us/us-counterintelligence-warns-china-stepping-up-influence-operations-2022-07-06/

Servicio de Vigilancia y Protección contra Injerencias Digitales Extranjeras. [VIGINUM]. (2023). *RRN: A complex and persistent information manipulation campaign*. https://www.sgdsn.gouv.fr/files/files/Publications/20230719_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_EN.pdf

Servicio de Vigilancia y Protección contra Injerencias Digitales Extranjeras. [VIGINUM]. (2024a). PORTAL KOMBAT. *A structured and coordinated pro-Russian propaganda network.* https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf

Servicio de Vigilancia y Protección contra Injerencias Digitales Extranjeras. [VIGINUM]. (2024b). MATRYOSHKA. A pro-Russian campaign targeting media and the fact-checking Community. https://www.sgdsn.gouv.fr/files/files/20240611_NP_SGDSN_VIGINUM_Matriochka_EN_VF.pdf

Servicio Europeo de Acción Exterior [SEAE]. (2023). *1st EEAS Report on Foreign Information Manipulation and Interference Threats*. Strategic Communications, Task Forces and Information Analysis (STRAT.2). https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

Servicio Europeo de Acción Exterior [SEAE]. (2024). *2nd EEAS Report on Foreign Information Manipulation and Interference Threats*. Strategic Communications, Task Forces and Information Analysis (STRAT.2). https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

Sputnik. (2023, 26 de julio). *Robert f. Kennedy Jr: Occidente "torpedeó" la paz en Ucrania "porque queremos la guerra con Rusia"*. https://noticiaslatam.lat/20230726/robert-f-kennedy-jr-occidente-torpedeo-la-paz-en-ucrania-porque-queremos-la-guerra-con-rusia-1141941972.html

Solymos, K. K., y Panyi, S. (2023). Imam, Soldier, Diplomat, Interpreter: Meet the Hungarian NewsFront's Propagandists. *VSquare*. https://vsquare.org/newsfront-russia-hungary-disinformation-telegram-propaganda/

The Associated Press. (2020, 2 de junio). China delayed releasing coronavirus info, frustrating WHO. *The Associated Press*. https://apnews.com/article/united-nations-health-ap-top-news-virus-outbreak-public-health-3c061794970661042b18d5aeaaed9fae

Tribunal de Cuentas Europeo. (2021*). Informe Especial 09/2021: El impacto de la desinformación en la UE: una cuestión abordada, pero no atajada*. https://www.eca.europa.eu/es/publications/SR21_09

Universidad de Bonn (2024, 2 de julio). *Fake News Harms the Economy*. https://www.uni-bonn.de/en/news/134-2024

Wu, J. y Lam O. (2017). The Evolution of China's Great Firewall: 21 Years of Censorship. *Global Vocies Advox*. Disponible en: https://advox.globalvoices.org/2017/08/30/the-evolution-of-chinas-great-firewall-21-years-of-censorship/

Yam, K. (2022, 3 de octubre). Right-wing disinformation ramps up on WeChat ahead of midterms, report finds. *NBC News.* https://www.nbcnews.com/news/amp/rcna50539

Zubor, Z. (2023, 11 de octubre). A new form of fake news: clickbaiters and Russian propagandists mass-produce staged videos*. Atlatszo.* https://english.atlatszo.hu/2023/10/11/a-new-form-of-fake-news-clickbaiters-and-russian-propagandists-mass-produce-staged-videos/