TRABAJOS DEL FORO CONTRA LAS CAMPAÑAS DE DESINFORMACIÓN

INICIATIVAS 2024

GOBIERNO DE ESPAÑA
PRESIDENCIA DEL GOBIERNO

Catálogo de publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA, JUSTICIA Y RELACIONES CON LAS CORTES

NIPO (edición on-line): 143-24-053-2
Fecha de edición: Noviembre 2024

TRABAJOS DEL FORO CONTRA LAS CAMPAÑAS DE DESINFORMACIÓN

INICIATIVAS 2024

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.

PRESENTACIÓN

En diciembre del año 2021 se aprueba la actualmente vigente Estrategia de Seguridad Nacional (ESN21). Por primera vez una Estrategia Nacional recoge las campañas de desinformación como un riesgo para la seguridad nacional.

Desde el año 2021 hasta el actual, el riesgo que supone la desinformación para la seguridad nacional, lejos de reducirse, se ha consolidado e incluso ganado en importancia y protagonismo, pudiendo considerarse como una de las amenazas más relevantes que experimentan los sistemas democráticos actuales.

En este sentido, el informe del Foro Económico Mundial de Davos - 2024, sitúa el fenómeno de la desinformación en el primer puesto en el ranking de riesgos globales en el corto plazo (2 años vista). Resaltando, además, que la Inteligencia Artificial está siendo utilizada ya para amplificar informaciones manipuladas y distorsionadas que podrían desestabilizar sociedades

En esta misma línea, el Informe Anual de Seguridad Nacional de 2023 describe como *"las tensiones globales están llevando a un incremento de la difusión de campañas de desinformación, […] con la intención de desestabilizar y polarizar a la sociedad y socavar su confianza en las instituciones" y que "particularmente en el contexto de la guerra en Ucrania y del conflicto en la franja de Gaza, se ha detectado un aumento de las narrativas antioccidentales, antieuropeas y también, en ocasiones, antiespañolas"*.

Frente a esta amenaza, España, durante el año 2024 ha logrado consolidar el *Foro contra las campañas de desinformación en el ámbito de la seguridad nacional* como iniciativa nacional de colaboración público-privada.

Este espacio de colaboración entre instituciones públicas y sociedad civil, sector privado y academia, ha logrado afianzarse como un mecanismo eficaz para impulsar la generación e intercambio de conocimiento sobre el riesgo que la desinformación supone para nuestro Estado democrático y de Derecho y fomentar el debate sobre los mecanismos disponibles para afrontarlas, integrando para ello a los representantes de los principales sectores de la sociedad involucrados en la detección, conocimiento y posible reducción del nivel de la amenaza.

El 29 de febrero de 2024, el Plenario del Foro aprobó abordar un total de **ocho iniciativas**, cuyos resultados se recogen en este libro. Estas propuestas, llevadas a cabo por los propios vocales del Foro o por expertos de los sectores implicados, han pretendido bien ahondar en los retos planteados en los trabajos anteriores, bien cubrir el conocimiento de algunos aspectos específicos de la amenaza que aún no se habían explorado lo suficiente, o bien avanzar en el debate sobre posibles soluciones disponibles, incluyendo nuevas herramientas en el ámbito regulatorio como la Ley de Servicios Digitales (Reglamento UE DSA 2022/2065), en vigor efectiva desde febrero 2024.

En esta segunda edición de trabajos 2024, el Foro ha buscado impulsar iniciativas dinámicas que incentivaran el debate y la búsqueda de soluciones comunes entre expertos de diferentes sectores implicado en busca también de mayor alcance y repercusión. En este sentido, en el marco de las iniciativas de este año, se han desarrollado por primera vez, conferencias temáticas y paneles de discusión con grupos de expertos de amplia formación, experiencia y capacidad de comunicación.

Este libro recoge, por lo tanto, los resultados de dos tipos de trabajos del Foro desarrollados durante el año 2024: por un lado, los capítulos uno al cuatro, reflejan documentos de análisis temáticos elaborados por expertos y, por otro, los capítulos cinco y seis, recogen el resumen y las conclusiones de dos iniciativas llevadas a cabo en formato interactivo.

- El **primer capítulo** aglutina un glosario de 125 términos clave relacionados con las campañas de desinformación que facilitan la comprensión y el uso coherente de términos, evitando confusiones y proporcionando una base común para describir conceptos, técnicas y

estrategias, dada la falta de uniformidad y homogeneidad en la terminología empleada hasta ahora en la sociedad española.

- El **segundo capítulo** describe el papel que los **medios de comunicación y las direcciones de comunicación de instituciones públicas y privadas** deberían desempeñar para enfrentar eficazmente el desafío las campañas de desinformación que afectan a todo tipo de instituciones y organismos. Además, aborda cuáles, y cómo, deben ser los mecanismos de interacción, así como la relevancia y especiales consideraciones de la **comunicación durante procesos de gestión de crisis.**

- El **tercer capítulo** caracteriza las tácticas, técnicas y procedimientos de diversos actores estatales extranjeros, entre ellos, Rusia, China e Irán, para desarrollar campañas de manipulación e injerencia en la información poniendo el foco tanto en las estrategias de monetización como en los recursos económicos desplegados para sufragarlas.

- El **cuarto capítulo** desarrolla un enfoque que pretende aplicar el conjunto de lecciones aprendidas en el caso de la ciberseguridad al dominio las Injerencia y manipulación extranjera de la información (FIMI, de sus siglas en inglés), evaluando, a través de las diversas tecnologías y procedimientos, cómo se diseñan estrategias, tácticas y operaciones contra objetivos concretos.

- El **quinto capítulo** recoge las conclusiones y recomendaciones de **la conferencia** celebrada en septiembre en la facultad de Derecho de la UCM en el marco de la iniciativa sobre campañas de desinformación y promoción del discurso de odio y que contó con ponentes y asistentes expertos en ambos ámbitos. Este capítulo: **desinformación y promoción del discurso de odio**, aborda exitosamente la descripción de cómo ambas amenazas interactúan, a menudo habitualmente, así como los riesgos asociados a dicha concurrencia. Asimismo, recopila una descripción de los mecanismos existentes en la actualidad para luchar contra ambas amenazas y los retos futuros para enfrentarlas.

- El **sexto capítulo** contiene una reflexión sobre la hipótesis de la existencia de **escepticismo en la opinión pública y medios de comunicación españoles sobre las campañas de desinformación asociadas a la injerencia extranjera**. Sobre la evaluación de esta hipótesis se enumeran una serie de conclusiones y recomendaciones fundamentadas en dos paneles de discusión con expertos tanto en opinión pública como en medios de comunicación.

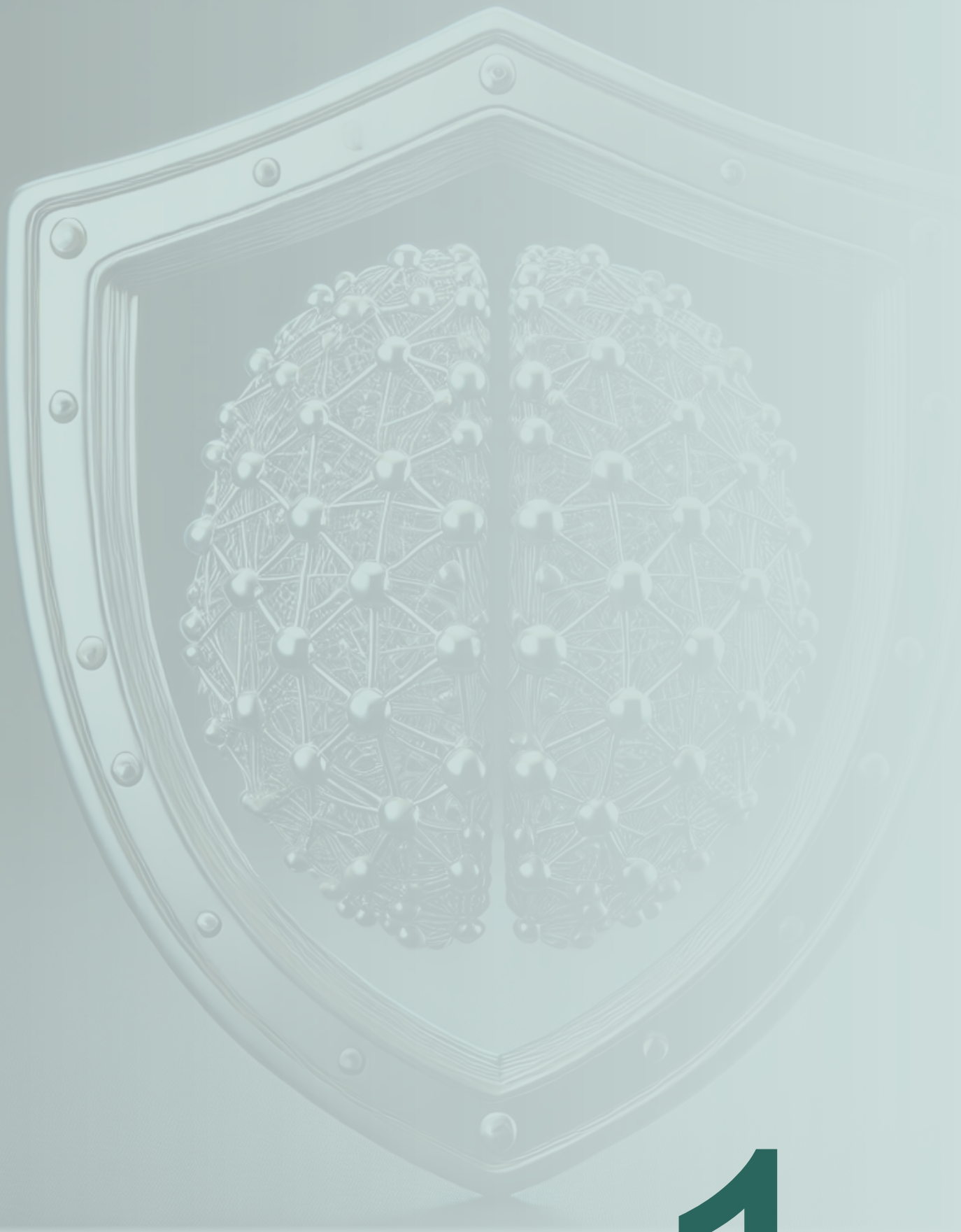
También, es necesario mencionar que algunas de las iniciativas aprobadas por el Foro en 2024 siguen desarrollándose en la actualidad, motivo por el cual sus resultados no han podido ser recogidos en el presente libro, si bien, una vez finalicen los trabajos pendientes, sus resultados se publicarán en formato digital o se integrarán junto a los trabajos de la próxima edición del Foro.

Es necesario reconocer y resaltar la implicación de la sociedad española, representada por representantes de sociedad civil, sector privado, centros de pensamiento e investigación y academia en esta iniciativa, pionera a nivel internacional en su ámbito.

Finalmente, el colofón de este prólogo está dedicado a vocales y expertos, que han participado desinteresadamente en estos trabajos 2024, poniendo a disposición del Foro, en favor de la seguridad nacional, todo su compromiso, esfuerzo personal, conocimiento y experiencia en sus respectivos ámbitos de trabajo, movidos todos ellos por el interés común de avanzar hacia una sociedad más resiliente y mejor informada para hacer frente a las campañas de desinformación y la injerencia extranjera en el espacio informativo.

Dña. Loreto Gutiérrez Hurtado
Directora del Departamento de Seguridad Nacional
y Presidenta del Foro contra las campañas de
desinformación en el ámbito de la seguridad nacional

ÍNDICE



CAPÍTULO 1

125 TÉRMINOS SOBRE DESINFORMACIÓN

Coordinadores:

Sergio Arce García

Leticia Rodríguez Fernández

Departamento de Seguridad Nacional (DSN)

Autores y colaboradores:

Mª José Establés Heras

David García Marín

Beatriz Marín García

Virginia Martín Jiménez

Concha Pérez Curiel

Elías Said Hung

Ramón Salaverria Aliaga

Astrid Wagner

INTRODUCCIÓN

La propuesta de este capítulo surge en el marco de un grupo de trabajo dependiente de la Conferencia de Rectores de las Universidades Españolas (CRUE), cuyo propósito es vincular la actividad de las universidades y centros de investigación con la comprensión y búsqueda de soluciones para el fenómeno de la desinformación.

Anteriormente, el grupo de trabajo realizó un profundo análisis de la literatura académica sobre este objeto de estudio publicada por autores con filiación en centros españoles, describió la actividad de los principales grupos de investigación que lo abordan, examinó la financiación que la Agencia Estatal de Investigación (AEI) así como otras organizaciones privadas dedicaron a proyectos vinculados y ahondó en el papel de las universidades y centros de investigación en la estrategias de seguridad nacional.

En el marco de este trabajo, y mientras el grupo analizaba las diversas publicaciones científicas relacionadas, se plantearon varios debates sobre los conceptos y términos empleados para describir las distintas técnicas y herramientas que conforman una campaña de desinformación. A diferencia de otras lenguas, como por ejemplo el inglés, en el que se llegan a describir hasta tres términos para diferenciar la desinformación (*malinformation*, *misinformation* y *disinformation*), en español, el término tiende a ser mal empleado para describir también otros supuestos como por ejemplo el desconocimiento de un hecho. Se añade el problema de la extrapolación de términos de otras lenguas, es decir, cada autor los traduce, los enmarca y los interpreta conforme a su propio criterio que no tiene por qué coincidir necesariamente con el de otros autores.

Partiendo de la identificación de esta necesidad, se plantea en este capítulo una propuesta de 125 términos fundamentales para la comprensión del fenómeno de las campañas de desinformación en el marco de la seguridad nacional. El objetivo final es ofrecer un glosario, de lectura rápida y clara, que suponga además una oportunidad para establecer criterios homogéneos en la descripción de definiciones, tácticas, y estrategias empleadas en este tipo de campañas.

La coordinación del trabajo ha estado a cargo de Sergio Arce García, profesor contratado doctor en la Universidad Internacional de la Rioja; Leticia Rodríguez Fernández, profesora titular en la Universidad de Cádiz y un representante del Departamento de Seguridad Nacional (DSN).

Para su desarrollo se contó con un grupo de expertos conformado por Mª José Establés Heras, profesora ayudante doctora en la Universidad de Castilla La Mancha (UCLM); David García Marín, profesor titular en la Universidad Rey Juan Carlos (URJC); Beatriz Marín García, analista de datos en European External Action Service (EEAS); Virginia Martín Jiménez, profesora titular en la Universidad de Valladolid (UVA); Concha Pérez Curiel, profesora titular en la Universidad de Sevilla (US); Elías Said Hung, profesor titular en la Universidad Internacional de la Rioja (UNIR); Ramón Salaverria Aliaga, catedrático en la Universidad de Navarra, y Astrid Wagner, científica titular del Instituto de Filosofía del CSIC en Madrid. Cabe destacar también a Antonio Díaz, profesor titular en la Universidad de Cádiz, que actúa como vocal del grupo de trabajo de la CRUE en el Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional.

En primer lugar, se realizó una revisión de literatura académica relacionada (artículos, capítulos de libro y libros) que permitiera recopilar aquellos términos de interés. En total, se recogieron inicialmente 160 conceptos que fueron valorados y filtrados por el grupo de trabajo, bajo criterios de relevancia y conexión con el ámbito de la seguridad. Para su descripción se asignó una media de 12 palabras por autor, que posteriormente fueron revisadas por todos los miembros del grupo, hasta alcanzar una selección final de 125 conceptos que se muestra en este capítulo. Finalmente, con el ánimo de facilitar la lectura y la comprensión de este glosario, se clasificaron los términos conforme a ocho criterios fundamentales: (1) Manipulación de la información; (2) Suplantación de identidad, manipulación y recursos tecnológicos; (3) Guerra informativa e injerencia extranjera; (4) Estrategias de control, supresión y propaganda; (5) Falacias, teorías conspirativas y pseudo-conocimiento; (6) Tácticas psicológicas, cognitivas y de percepción; (7) Manipulación algorítmica y mediática; y (8) Ciberdelitos y amenazas online.

ÁMBITO DE APLICACIÓN DEL TRABAJO

La desinformación en contextos digitales es un fenómeno relativamente reciente que tiende a la constante evolución. En consecuencia, nos encontramos ante neologismos y extranjerismos que precisan de una definición precisa, rigurosa y de utilidad para los distintos actores que participan en su comunicación, identificación, detección y resolución.

Destacan entre ellos:

- ***Sector de la comunicación, medios y verificadores***: los periodistas tanto de medios convencionales como de agencias de verificación desempeñan un papel fundamental en la identificación y en el desmentido de contenidos falsos. Igualmente, en el ecosistema comunicativo encontramos otros actores como los departamentos de comunicación, las agencias de comunicación o las agencias de publicidad, que indirectamente también pueden verse afectados. Pretendemos que este glosario sirva para identificar las tácticas de desinformación, y, en el caso de periodistas, sería una buena herramienta para homogeneizar los conceptos que se divulgan hacia la sociedad.

- ***Plataformas digitales:*** las empresas tecnológicas son agentes fundamentales en la detección de campañas de desinformación. El glosario que se propone puede ser útil para quienes realizan curación de contenido e incluso asienta una base para el desarrollo de políticas más efectivas en este ámbito.

- ***Entorno de la ciberseguridad:*** gracias a este glosario, se podría realizar una futura codificación de modalidades de desinformación mediante sistemas informáticos, con fines como la detección automática de desinformación, la búsqueda eficiente de términos, o la creación de sistemas de alerta temprana.

- ***Ámbito académico***: investigadores y académicos desempeñan un triple papel como investigadores, educadores y divulgadores. Este glosario contribuye a abrir el debate y a establecer criterios homogéneos sobre la terminología más adecuada para investigar, educar y hacer accesible el conocimiento en torno a la desinformación.

- ***Ciudadanía:*** no menos importante resulta la sociedad en su conjunto. Estimular el conocimiento de la ciudadanía en torno al funcionamiento de las campañas de desinformación y mejorar su alfabetización mediática y digital ofrece, sin duda, una oportunidad para continuar trabajando en su resiliencia y, por extensión, en la calidad democrática.

GLOSARIO DE DESINFORMACIÓN

Manipulación de la información

Arenques podridos (*Rotten herrings*). Método o técnica de difusión de propaganda negra o negativa, en la que se asocia de forma continua en el tiempo a una persona, grupo o institución a uno o varios escándalos o falsedades. Aunque la falsedad sea desmentida, queda en la mente de las personas la asociación de la acusación y el escándalo. Se suele emplear a través de redes sociales o webs de desinformación, y suele ser difundida mediante técnicas de tipo *astroturfing* para introducirse en el debate de diferentes sectores de la sociedad o medios de comunicación tradicionales. Ha sido utilizada a lo largo de la historia en numerosas ocasiones, siendo una de las técnicas más empleadas en la actualidad.

Bulo. Información falsa o engañosa que se difunde de manera intencional y con el objetivo de manipular o engañar a la audiencia. Se trata de un rumor o noticia sin fundamento que se propaga rápidamente, a menudo a través de las redes sociales y medios de comunicación. Es una afirmación o historia inventada que carece de evidencia o pruebas confiables que la respalden, convirtiéndose en un tipo de desinformación utilizada para crear confusión, generar desconfianza o influir en la opinión pública. Su equivalente en inglés es *hoax*.

Cherry-picking **(Recolección de cerezas).** Falacia de prueba incompleta o de atención selectiva, consistente en considerar válidos únicamente los datos o pruebas que confirman

la idea o postura propia mientras se descartan las informaciones que la contradicen. También se establece cuando se defiende una opinión seleccionando solo las evidencias y argumentos que la corroboran. Una manifestación de esta falacia aplicada al ámbito de la desinformación es el sesgo de confirmación (ver definición en este mismo glosario).

Debunking **(Desenmasacar/desacreditar)**. Acción de demostrar la falsedad o inexactitud de un contenido presumiblemente desinformativo utilizando estrategias y técnicas de verificación. Estas estrategias son aplicadas de forma profesional por los verificadores o *fact-checkers* (*debunkers*) a fin de etiquetar el contenido como falso, engañoso, verdadero a medias, etc. En estos procesos de *debunking*, los verificadores no solo publican la resolución final de sus verificados, sino también las técnicas y evidencias empleadas durante su ejecución.

Desinformación. Acción o estrategia que consiste en la difusión intencionada de información falsa o engañosa, descontextualizada o parcial, con el fin de confundir, persuadir y manipular a las personas. A diferencia de la información errónea, que puede ser incorrecta pero no intencional, la desinformación es deliberada y busca influir en las opiniones, creencias o comportamientos de la ciudadanía. Las fuentes desinformativas utilizan la polarización, el lenguaje emocional y sensacionalista y el discurso del odio y del miedo para debilitar a las instituciones y dañar su confianza, especialmente durante las elecciones, pero también en otros contextos no electorales.

Desórdenes informativos. Situaciones o fenómenos que alteran los procesos y flujos comunicativos y que pueden tener relación con la desinformación, la sobresaturación informativa, la manipulación, la mentira, la tergiversación y mala interpretación de hechos e informaciones, así como la limitación a su acceso y/o la censura. Su producción es intencionada y puede combinar diferentes tácticas en el proceso.

Estrategia híbrida. Empleo intencionado y sincronizado de diversas acciones de tipo político, económico, social, diplomático, militar e informacional para aprovechar la vulnerabilidad de un oponente en esos distintos ámbitos –habitualmente, un país objetivo– para ejercer coerción en su toma de decisiones políticas y obtener ventaja competitiva. De forma concreta, estas estrategias pueden incluir campañas de desinformación, ciberataques, espionaje, subversión social, sabotaje y coacción económica. Una amenaza híbrida sería la percepción real o imaginaria de poder ser llevada a cabo en un futuro.

Exageración. Amplificar y/o magnificar la importancia o desarrollo de hechos o acontecimientos o datos. En ella se destacan aspectos relevantes para el emisor y/o el receptor que puedan servir a la persuasión o a la generación de emociones intensas. Empleada con fines desinformativos sirve para captar la atención y/o generar falsas narrativas.

Factoide. Término importado del neologismo inglés *factoid*. Creencia popular sin base factual. Afirmación o dato falso, impreciso o trivial, que se convierte en un hecho supuestamente incontrovertible, a raíz de su repetición en múltiples fuentes.

Fake news. Noticia falsa o bulo. Información falsa o engañosa que se presenta y difunde de forma intencionada como noticia auténtica, para influir en la opinión y creencias de la ciudadanía. Tienen apariencia de noticias reales que imitan el formato, el estilo profesional y las páginas web de los medios de comunicación de reconocido prestigio. Las *fake news*

utilizan las tácticas de viralización para compartir contenidos con millones de usuarios en las redes sociales. Se apoyan en el sensacionalismo, las emociones, el uso de las citas inventadas y la distorsión de los hechos y del contexto espacial y temporal en el que discurren los acontecimientos. Numerosos expertos desaconsejan el uso del término, tal como recoge el primer texto del DSN en este ámbito ("Lucha contra las campañas de desinformación en el ámbito de la Seguridad Nacional. Propuestas de la sociedad civil"), publicado en 2022, y utilizar mejor la palabra "desinformación".

***Firehosing* (Manguera de falsedades)**. Táctica empleada para difundir una gran cantidad de información falsa de forma rápida y repetida, con el fin de abrumar a las audiencias, con flujos continuos e intensos de información errónea, similar al agua que sale de una manguera contra incendios (de ahí su nombre en inglés). Un escenario en que se dificulta que las personas distingan entre noticias reales y falsas, lo que impide que estos puedan verificar hechos, dada la cantidad de información errónea que opaca la información veraz.

Globo sonda. Táctica de comunicación que consiste en divulgar anticipadamente información o sugerir medidas potenciales para medir su grado de aceptación o rechazo. En la comunicación política se usa generalmente en o hacia medios de comunicación, para evaluar la reacción ciudadana ante una idea, antes de tomar acciones definitivas.

Hechos alternativos (*Alternative facts*). Tergiversación o versión sesgada de un acontecimiento, que contradice la evidencia empírica y los datos verificados. Concepto nacido y especialmente usado en comunicación política, alude a la presentación de información que no se basa en la realidad, sino en interpretaciones construidas para influir en la opinión pública o defender ciertos intereses.

Imprecisión. Falta de exactitud en la información emitida sobre una acción, expresión o dato. Se puede dar de forma consciente e intencionada en una campaña desinformativa o inconsciente cuando el emisor de la información no verifica o contrasta correctamente los hechos. En todo caso, la imprecisión en la información resulta especialmente problemática, ya que puede contribuir a la propagación de narrativas falsas o engañosas. Se puede manifestar de diferentes formas, desde la impropiedad léxica que ocasiona sesgos en la producción del relato informativo hasta la falta de pluralidad o diversidad de opiniones cuando se tratan asuntos controvertidos.

Malinformation. Utilización de información verídica o basada parcialmente en la realidad con el fin de causar daño a una persona, colectivo, organización, institución o un país. Incluye el uso político de información sensible, la revelación de información personal o confidencial o la publicidad de información comprometida obtenida mediante métodos fraudulentos. Aunque la *malinformation* se basa en información verdadera, ésta puede resultar incompleta, desactualizada o haber sufrido algún tipo de manipulación con la intención de producir descrédito, perjuicio o menoscabo en la población o entidad a la que se pretende dañar.

Manipulación informativa; FIMI (*Foreign Information Manipulation and Interference*). La manipulación informativa incluye una serie de prácticas para distorsionar y alterar el proceso comunicativo con el propósito de influir y alterar la opinión pública. FIMI describe un patrón de comportamiento, en su mayoría no ilegal, que tiene por objetivo amenazar o generar un impacto negativo en los valores democráticos y procesos políticos. Tal actividad

es de carácter manipulador, llevado a cabo de manera intencional y coordinada por parte de actores extranjeros y sus proxies dentro y fuera de su territorio.

Medias verdades. Afirmaciones que contienen elementos de verdad, pero que están incompletas, sesgadas o presentadas de forma que pueden inducir a error. Son más creíbles al incorporar elementos de verdad y más fáciles de detectar que la mentira completa.

Misinformation. Información falsa, errónea o inexacta emitida sin intención de engañar o manipular. Este tipo de desinformación puede confundir al receptor, si bien suele ser fruto de errores, negligencias o sesgos inconscientes. A diferencia de lo que sucede con la *disinformation* (que sí implica la emisión de un contenido falso de forma intencionada), la *misinformation* hace referencia a la difusión accidental de información no verídica.

Paltering. Anglicismo que puede traducirse como "falsear" o "distorsionar". Modalidad de tergiversación que consiste en seleccionar afirmaciones verdaderas que, sin embargo, se interpretan de manera torticera, de modo que el discurso en su conjunto resulta engañoso o induce a error. Se basa en hilvanar afirmaciones que no son falsas en un discurso mentiroso, lo que dificulta la refutación general del discurso. Suele emplearse por el emisor como medida de protección ante acusaciones de deshonestidad.

Posverdad. Término de uso adjetivo o sustantivo que se refiere a un entorno en el que los hechos se consideran irrelevantes o menos importantes que las creencias y opiniones personales, y se utilizan apelaciones emocionales y herramientas de desinformación para influir en la opinión pública y en el debate político. Circunstancias en las que los mecanismos de escrutinio, verificación y justificación pierden importancia frente a lo que se percibe o siente como verdadero.

Prebunking. Neologismo derivado del término inglés *debunking* ("destapar", "revelar", "desenmascarar"), que puede traducirse como "pre-desenmascaramiento". Conjunto de medidas preventivas orientadas a inmunizar o alertar anticipadamente a la ciudadanía ante mensajes falsos. Basada en la teoría sociológica de la inoculación, es una práctica usada principalmente por agencias de verificación y organizaciones que promueven la alfabetización mediática.

Superdifusor de desinformación (*Disinformation superspreader*). Individuo, entidad o agente automatizado que juega un papel crucial en la propagación de noticias falsas o contenido engañoso por su popularidad, influencia social o relevancia. Estas personas o cuentas en redes sociales tienen una gran audiencia y, a menudo, producen o comparten contenido desinformativo entre grupos poblacionales específicos, amplificando su impacto. Sus características son la intencionalidad de su acción desinformativa, la producción o propagación de narrativas atractivas que confirman creencias preexistentes entre grupos concretos y el aprovechamiento de la capacidad de viralización del contenido en las plataformas digitales.

Suplantación de identidad, manipulación y recursos tecnológicos

Bot. Abreviatura de robot. Es un programa de software diseñado para realizar tareas automatizadas en internet, sin intervención humana. Tienen la capacidad de interactuar con usuarios en tiempo real, manejar gran cantidad de volúmenes de datos y adaptarse a diferentes entornos. El mal uso de los bots genera desinformación, manipulación de la opinión pública, suplantación de la identidad, ataques coordinados a individuos, organizaciones y colectivos, saturación y corte de servicios en la red y manipulación de resultados de búsquedas de tendencias.

Camuflaje de palabras (*Leetspeak*). Tipo de escritura en la que se cambian letras por caracteres alfanuméricos a modo de cifrado, haciendo incomprensible para determinados usuarios o indetectable para algoritmos que detecten palabras malsonantes, insultantes o de odio. A través del cambio de determinadas letras por otros símbolos se pretende burlar o hacer bromas ante otros usuarios, o evitar que determinadas palabras sean identificadas como ofensivas por parte de algoritmos de foros o redes sociales. En el caso de identificación de cuentas en redes sociales, se emplean para ocultar o generar multitud de diferentes versiones de un mismo usuario, llegando al término de "cuenta matrícula" al aparecer un nombre de persona junto a diversos números y caracteres.

Catfishing. Fórmula de engaño y fraude que consiste en la creación de una identidad falsa en las redes sociales o plataformas digitales. Los *catfishers* crean perfiles falsos a través de chats, correos electrónicos, teléfono o videollamadas, usando fotos, nombres y detalles de la vida de otras personas. La manipulación emocional, el uso de historias emotivas y convincentes para mantener el engaño o la solicitud de dinero para sufragar emergencias financieras, de salud o de cualquier índole son las estrategias más comunes. Entre sus objetivos figuran el enriquecimiento fraudulento, la venganza o el simple entretenimiento.

Cheapfake. Tipo de contenido desinformativo consistente en la manipulación sencilla y burda de materiales mediáticos preexistentes en cualquiera de los formatos posibles (texto, fotografía, vídeo o audio). Las formas de manipulación pueden ser la edición o la contextualización incorrecta. A diferencia de las *deepfakes* (mucho más verosímiles, sofisticadas y complejas en su elaboración), las *cheapfakes* requieren poco esfuerzo de elaboración y escasos conocimientos tecnológicos, y se pueden crear con herramientas simples y accesibles. Aunque son más sencillas de verificar, suelen poblar los circuitos desinformativos y lograr un alto impacto.

Ciborg. Abreviatura de organismo cibernético. La imagen de ciborg corresponde a un ser que combina parte humana y componente tecnológico. En el contexto de la desinformación pueden propagar noticias falsas de manera más efectiva que elementos exclusivamente automatizados como los bots, crear consenso o disenso e influir en la percepción de la ciudadanía ante un tema, usar algoritmos para incrementar el contenido sesgado y la polarización y erosionar la confianza y la credibilidad de los públicos.

Deepfake. Técnica de inteligencia artificial que permite manipular o generar contenido audiovisual falso, como imágenes, videos o audios, de manera muy realista. Estos contenidos se crean a partir de datos de entrenamiento de aprendizaje profundo (*deep learning*), lo que permite reemplazar el rostro o la voz de una persona por la de otra, o incluso generar una

persona que no existe. Los deepfakes han sido utilizados para crear contenido engañoso, como videos de políticos o celebridades diciendo o haciendo cosas que nunca ocurrieron.

Hack&Leak operations. Técnica de manipulación informativa que combina un ataque de ciberseguridad con una operación informativa. Estas operaciones empiezan por el acceso no autorizado o intrusión a sistemas o datos (hackeo) de una organización o individuo, seguido de la divulgación selectiva de esa información robada (filtración) para manipular a la opinión pública, dañar la reputación de individuos, organizaciones o gobiernos. Los contenidos filtrados pueden ser auténticos, falsos, manipulados o una combinación de todos ellos.

Impersonation **(Clon, suplantación de identidad, *Doppelgänger*)**. Técnica de manipulación informativa mediante la cual se clona o se suplanta la identidad de entidades legítimas y reales, como por ejemplo medios de comunicación, organizaciones públicas y personas, con el objetivo de engañar al público y difundir información falsa o engañosa. Esta técnica se utiliza para aprovechar la credibilidad y confianza asociadas con la identidad suplantada, con el fin de amplificar el alcance y el impacto de la desinformación. o *deepfakes* para suplantar la identidad de figuras públicas. El término *Doppelgänger* se emplea específicamente para operaciones de influencia rusa que utilizan una red de "clones", reproduciendo diseños y dominios de medios auténticos occidentales, para difundir artículos, vídeos y/o encuestas falsas.

Inteligencia artificial (IA) generativa. Sistema de generación masiva de datos nuevos que imitan el contenido creado por humanos mediante el uso de algoritmos avanzados. Estos sistemas utilizan modelos de aprendizaje profundo, como redes neuronales generativas, para producir texto, imágenes, música, video y otros tipos de contenido. Los modelos generativos más conocidos incluyen las Redes Generativas Antagónicas (GAN) y los modelos de lenguaje como el CHAT-GPT (*Generative Pre-trained Transformer*). Un mal uso de la IA Generativa favorece la desinformación, la falsificación de documentos o la suplantación de identidad, a través de técnicas de *deepfakes*, con imágenes, audios y vídeos manipulados.

Killchain. Adaptando el concepto militar y de ciberseguridad a la desinformación, el modelo de *killchain* desglosa el análisis de un incidente en una serie de fases estructuradas que describen el ciclo de vida de una operación de desinformación, desde su concepción hasta su ejecución y evaluación a través de la descripción de Tácticas, Técnicas y Procedimientos (TTP). El análisis de un ataque por etapas permite a los analistas predecir, reconocer, interrumpir o prevenir dicho ataque en cada una de las etapas del incidente.

Marioneta de calcetín (*Sock puppet account*). Cuenta falsa utilizada en redes sociales para generar identidades ficticias o encubrir identidades reales. Pueden utilizarse como técnica de manipulación informativa para difundir desinformación de manera encubierta. También pueden ser utilizadas con fines de investigación para proteger y ocultar la verdadera identidad de analistas de OSINT (*Open Source INTelligence*, fuentes de inteligencia en abierto) y obtener acceso a información de algunas plataformas para la que se requiere una cuenta.

Phishing. Técnica de engaño en el ámbito informático diseñada para obtener información confidencial de una persona o institución objetivo. Consiste en enviar mensajes con el fin de ganar la confianza del destinatario y luego manipularlo para que realice acciones

indebidas. Utilizando el engaño o la adulación, se explotan diversas situaciones personales para que la víctima "muerda el anzuelo". Como técnica de ingeniería social, se enfoca en la vulnerabilidad de la mente humana en lugar del sistema informático, lo que la convierte en una de las estrategias más simples, peligrosas y efectivas, y por este motivo, de las más utilizadas.

STIX (*Structured Threat Information eXpression*). Lenguaje estandarizado utilizado para codificar e intercambiar Inteligencia sobre Ciberamenazas (CTI). En el ámbito de la desinformación permite expresar y estructurar la información sobre el análisis de la amenaza utilizando una sintaxis común. STIX permite compartir información de forma estandarizada entre analistas. Este lenguaje ha sido adoptado como estándar internacional por varias comunidades de intercambio de inteligencia, y es el estándar común adoptado por la Unión Europea y Estados Unidos para el intercambio de información estructurada sobre amenazas FIMI.

TTP; DISARM. En el contexto de manipulaciones informativas, el análisis de las Tácticas, Técnicas y Procedimientos (TTP) permite describir los patrones de comportamiento de un actor de amenaza en un marco estructurado. En conjunto, las TTP describen por fases cómo operan los actores malintencionados, desde la estrategia de planificación general hasta los métodos específicos y los procesos que utilizan para manipular la percepción pública. El análisis de los patrones de ataque es una herramienta crucial para planificar estrategias de respuesta y reacción a incidentes de manipulación informativa (*killchain*). El DISARM (*Detecting and Responding to Manipulated Media*) *Red Framework* es un catálogo de código abierto diseñado para describir TTPs en el ámbito de la desinformación, mientras que el *Blue Framework* se refiere a respuestas sugeridas frente a las mismas.

Typosquatting. Técnica de manipulación informativa utilizada por actores malintencionados que registran dominios de internet con errores tipográficos o con nombres similares a sitios web reales. Estos dominios son utilizados para confundir y dar legitimidad a contenido falso; engañar y obtener datos personales; redirigir a sitios maliciosos; o atraer tráfico para obtener ingresos publicitarios. Los actores malintencionados a menudo reservan diversos dominios similares a páginas web legítimas para generar confusión y derivar al usuario a otra página web maliciosa.

***Vishing* (*Phishing* de voz)**. Técnica en la que, a través de una llamada, audio o vídeo se suplanta la identidad de una persona, de una empresa, organización o institución pública. Su misión es obtener información personal y sensible de la víctima como un número de tarjeta o un código secreto, o el de llevar a cabo una campaña de desinformación, en los casos en los que la manipulación se lleva a cabo mediante identidad pública tal como, por ejemplo, con políticos. También se utiliza en campañas de desinformación para entrevistar a personalidades, para después publicar la información y ridiculizar a los entrevistados. El término nace de la unión de las palabras en inglés *voice* y *phishing*.

Amenazas híbridas: Acciones coordinadas y sincronizadas desplegadas para favorecer o lograr los objetivos estratégicos de actores estatales o no estatales y que, de forma deliberada, tienen el objetivo de socavar, desestabilizar y perjudicar al adversario, así como de explotar las vulnerabilidades sistémicas de los Estados y de sus instituciones democráticas. Utilizan y combinan una amplia gama de medios (desde ataques cibernéticos, campañas de manipulación de la información, maniobras políticas encubiertas y tácticas militares, entre otras) y explotan los umbrales de detección y atribución, así como las diferentes fronteras (paz-guerra, nacional-internacional, local-estatal...) y pretenden influir de diversas formas en la toma de decisiones a nivel local, estatal o institucional. Adicionalmente, se caracterizan por su ambigüedad y por la dificultad de atribuirlas a un actor concreto. En la literatura, en ocasiones, se utiliza de forma indistinta los términos de amenazas y estrategias híbridas, si bien, las primeras consisten en acciones que pueden materializarse en el futuro, mientras que las segundas, que suelen integrar las amenazas como parte de un marco o plan general, acaban materializándose para lograr un fin. La rápida evolución tecnológica y la interconectividad global han aumentado la velocidad, escala e intensidad de todos estos aspectos.

Control reflexivo: Técnicas utilizadas como medio para transmitir a un interlocutor o adversario, información especialmente preparada para predisponerle a tomar voluntariamente la decisión predeterminada deseada por el actor ejecutor de la acción. Esta ventaja táctica, que pretende conseguir el actor de la amenaza, se logra alterando factores clave en la percepción de la información por parte del oponente (que puede ser un Estado) y busca neutralizar sus puntos fuertes, haciéndole elegir vías de acción perjudiciales y que, a la vez, favorezcan los objetivos del actor ejecutor. Este proceso se basa en la comprensión minuciosa de los modelos mentales y estructuras de decisión del oponente, lo que permite moldear su percepción de la realidad y guiarle hacia elecciones estratégicas desfavorables. Este tipo de técnicas ocupan un lugar en la doctrina militar rusa, y se enmarcan dentro de la *maskirovka* (engaño), junto a las medidas activas y la *dezinformatsiya,* considerada un arte aplicado para la manipulación con el propósito de influir en decisiones estratégicas.

Cyberwarfare **(Ciberguerra)**. Uso de ataques cibernéticos por parte de naciones, estados u organizaciones para dañar, interrumpir o destruir sistemas de información, redes e infraestructuras críticas de otros países u organizaciones. Estos ataques pueden incluir infiltración para robar información, sabotaje de infraestructuras críticas y manipulación de medios de comunicación. Utiliza técnicas como *malware*, *ransomware*, ataques de denegación de servicio (DDoS) o el *phishing*, y se distingue por su naturaleza clandestina y la dificultad de atribuir los ataques, permitiendo causar daños significativos sin recurrir a la violencia física directa.

Guerra híbrida. Consiste en el uso coordinado y sincronizado de una amplia gama de instrumentos contra el adversario, graduando su intensidad y evitando en lo posible la confrontación militar directa e, incluso, cualquier posible reacción del oponente. La guerra híbrida combina el empleo de estrategias militares no convencionales y convencionales con operaciones hostiles de inteligencia, campañas de manipulación e injerencia de la información o amenazas y presiones políticas y económicas que entran en el terreno de la guerra psicológica. Acciones que buscan como fin último derrotar, debilitar o someter la voluntad del adversario. Es decir, se caracteriza por la integración en tiempo y espacio de

procedimientos convencionales con tácticas propias de la guerra irregular (propaganda, subversión, *lawfare*, ciberoperaciones o guerra informativa), mezcladas estas últimas con actos terroristas y conexiones con el crimen organizado para la financiación, obtención de apoyos y asistencia.

Guerra informativa; guerra de la información. Acciones basadas en el uso malintencionado de campañas psicológicas masivas contra la población de otro Estado con el fin de desestabilizar su sociedad y su gobierno y forzar a ese Estado a tomar decisiones en interés de su adversario, interfiriendo en su dominio informativo. Las medidas de guerra informativa suelen implementarse previamente para alcanzar objetivos políticos sin necesidad de utilizar la fuerza militar para, posteriormente, moldear una respuesta favorable de la comunidad internacional ante la utilización de la fuerza militar. Desde el punto de vista de la doctrina militar rusa, se define como el conflicto entre dos o más Estados en dicho dominio con el objetivo de infligir daños en los sistemas de información, procesos y recursos, así como en las estructuras de importancia crítica, con el fin de socavar los sistemas político, económico y social de otro Estado.

Hacktivismo. Activismo desarrollado en entornos digitales cuyo propósito suele ser llamar la atención de la opinión pública sobre asuntos políticos o sociales. En su implementación se utilizan técnicas como la modificación de espacios web (*defacing*), la filtración o revelación de información confidencial, la sobrecarga de servicios o páginas web para evitar su funcionamiento.

Hard power: Literalmente en español, poder duro, que en contraposición con el *soft power* se refiere, desde el punto de vista de las relaciones internacionales y la geopolítica, al poder nacional/estatal en términos económicos y militares. Esta forma de poder político conlleva habitualmente la coerción o imposición frente a otras realidades estatales con menor capacidad económica o militar.

Influencia extranjera; injerencia extranjera. La injerencia extranjera, a menudo realizada como parte de una estrategia híbrida más amplia, puede entenderse como los esfuerzos coercitivos, encubiertos y engañosos para perturbar la libre formación y manifestación de la voluntad u opinión de las personas por parte de un actor estatal extranjero o de sus agentes. Esta actividad normalmente persigue objetivos políticos al interferir, subvertir o afectar negativamente a los procesos, valores y procedimientos democráticos establecidos y es contrario a la soberanía y los intereses nacionales de un Estado. Por el contrario, las actividades de influencia extranjera se llevan a cabo de manera abierta y transparente, son un aspecto normal de las relaciones internacionales y la diplomacia y contribuyen positivamente al debate público.

Infoesfera; noosfera. En el ámbito digital, la infoesfera se refiere al entorno global de información que incluye todos los datos, redes y tecnologías de la información y comunicación. Comprende la totalidad de la información generada, almacenada y compartida a través de internet, bases de datos, redes sociales y otros medios digitales. Es el espacio donde ocurren las interacciones digitales y el intercambio de datos, siendo fundamental para el funcionamiento de la sociedad y la economía en la era digital. Por otro lado, la noosfera se enfoca en la dimensión del conocimiento y la conciencia colectiva facilitada por las tecnologías digitales. Representa el espacio virtual donde las mentes humanas interactúan y colaboran, transformando la información en conocimiento compartido a través de plataformas digitales, redes sociales y herramientas de colaboración en línea. La noosfera

digital abarca fenómenos como la inteligencia colectiva, el *crowdsourcing* y la colaboración en proyectos, ampliando la capacidad humana para pensar, aprender y crear colectivamente en el entorno digital.

Kompromat. Extranjerismo del ruso que alude a una información comprometida o incriminatoria, recopilada con el propósito de someter a chantaje a una persona u organización. Esta información puede incluir evidencia real o fabricada sobre actividades ilegales, inmorales o vergonzosas por parte de la persona u organización chantajeada.

Lawfare. Instrumentalización de la legislación para reforzar la legitimidad de los objetivos estratégicos, operativos o tácticos del actor de la amenaza sobre un adversario en particular, o para debilitar la legitimidad de los respectivos objetivos particulares del adversario. El *lawfare* es distinto de la mera adopción de leyes que impliquen a un Estado adversario o de la firma de un tratado, y dependerá de cómo se estén utilizando dichas leyes, con qué propósito y contra qué oponente para lograr un objetivo concreto. Además, puede utilizarse en guerras asimétricas para establecer las condiciones de un conflicto o de una negociación, lo que, en ocasiones, podría considerarse una "preparación legal" de un escenario bélico.

Medidas activas (*Active measures*). Expresión que se utilizó a lo largo del siglo XX para referirse a operaciones de influencia, como la desinformación y la propaganda, dirigidas a la desestabilización, la discordia y otras formas de subversión. Estas medidas, de carácter eminentemente ofensivo, se emplean para agredir, controlar, impedir o neutralizar acciones, y pueden abarcar desde el plano informativo hasta el físico. El término fue acuñado por dirigentes de la Unión Soviética en los años 1920, pero ganó especial difusión tras la Segunda Guerra Mundial, durante la Guerra Fría. En la actualidad, el término ha vuelto a ser bastante utilizado, especialmente en el contexto de operaciones en redes sociales. A lo largo de los años, se han establecido estudios de medidas activas dirigidas a la opinión pública, políticos, gobiernos, la comunidad académica, empresas y organizaciones no gubernamentales.

Obstruccionismo. Táctica cuyo objetivo es bloquear, retrasar o imposibilitar la consecución de determinadas propuestas, acciones o acuerdos en torno a cuestiones políticas o sociales sensibles y relevantes. En su implementación se pueden desarrollar acciones que contribuyan a ganar tiempo, como prolongar el debate de una propuesta de Ley o bloquear la aprobación de un presupuesto, entre otras. Su finalidad puede ser evitar la aprobación de dicha propuesta, desgastar a un gobierno, cambiar el enfoque sobre una cuestión que está en el debate público, generar malestar y frustración en la población, incluso afectar a la gobernabilidad.

ONG Zombi (ONG falsas; ONG desaparecidas). Son Organizaciones No Gubernamentales (ONG) que o bien han perdido sus propósito o eficacia original, se han aprovechado del nombre de alguna ONG fidedigna anterior desaparecida o directamente son falsas, que distorsionan la comunicación y la confianza en torno a causas o problemas sociales reales. Se caracterizan por generar ruido y diluir el impacto de comunicaciones auténticas, realizadas por ONG que sí existen. Su acción contribuye a obstaculizar las iniciativas sociales genuinas, favorecer la asignación errónea de recursos, fomentar la competencia por la colaboración, reducir el enfoque organizacional, perpetuar las narrativas culturales ineficaces y restar valor a un cambio social significativo. Suelen participar activamente y ejercer su influencia en las redes sociales, con el fin de movilizar apoyos, en torno a un determinado tema.

Operación psicológica (PSYOPS). Se refiere, como componente de las Operaciones de Información, al conjunto de actividades psicológicas planificadas utilizando métodos de comunicación y otros medios dirigidos a audiencias concretas para influir en las percepciones, actitudes y comportamientos, afectando el logro de objetivos políticos y militares.

Proxy. 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.

***Soft power* (poder blando)**. En contraposición con el *hard power*, este término acuñado por J. Nye se refiere a la habilidad de un estado para influir en otro sin el empleo del poder económico ni militar, sino a través del uso persuasivo de las manifestaciones culturales en todas sus variantes, los valores políticos que defiende o su modelo social. Este concepto, vinculado a la dominación a través de la no coerción, sirve en la actualidad para entender las estrategias del poder en el entorno digital dónde la atracción y cooptación resultan más eficaces que la coerción a través de la norma.

Xuanchuan. Palabra que proviene del chino y significa propaganda o publicidad. Históricamente se refiere a difusiones militares chinas, con un añadido educativo y aspecto neutro. Con el paso de los últimos años se ha expuesto como propaganda oficial, aunque debido a la asociación de propaganda en el sentido negativo occidental, se ha ido convirtiendo en el mismo concepto o sentido peyorativo a la hora de emplear esta palabra.

Estrategias de control, supresión y propaganda

Agitprop. Propaganda de agitación, resultado de la forma abreviada de “agitación” y “propaganda”. El término fue creado por la Sección de Agitación y Propaganda del Secretariado del Comité Central del Partido Comunista en la Unión Soviética en 1920. Desde la visión del teórico marxista Georgy Plekhanov, recogida también por Vladimir Lenin, ambos conceptos eran completamente distintos. La agitación se dirigía a la masa, a la calle, mientras que la propaganda se centraba en las ideas. El agitprop recoge aquellas formas culturales cuyo propósito es abiertamente político y persuasivo.

Amplificar voces extremas y conspirativas (*Junknews*). Diversas formas de propaganda, ideológicamente extremas, así como noticias, informaciones y contenidos políticos hiperpartidistas y/o conspirativos que tienen como objetivo saturar el debate público, amplificar los discursos extremos y que otras discusiones sean desplazadas. Su objetivo es afectar y reducir la confianza pública.

Astroturfing. Estrategia de comunicación aplicada a nivel de las redes sociales, mediante el uso de un número determinado de usuarios, aparentemente similares al resto (suelen tener pocos seguidores y seguidos, aunque el número tiende a aumentar, especialmente, si se tratan de cuentas reconvertidas, es decir, cuentas que varían y adaptan su foco narrativo, a la vez que obtienen ventajas de la ganancia de seguidores de las etapas previas con otras temáticas), que actúan de forma coordinada, sacando el máximo provecho del ¨anonimato aparente¨ que poseen, para la distribución, amplificación e inundación de contenidos desinformativos, destinados al posicionamiento de narrativas, la generación de tendencias o *trending topics*, y el condicionamiento del debate dentro de la opinión pública, hacia determinados temas. El término *grassroots* sería el movimiento real espontáneo desde la población o comunidad, mientras que el *astroturfing* estaría planificado haciéndose pasar por el anterior.

Blanqueo de información (*Information laundering*). Conjunto de técnicas de manipulación informativa utilizadas con el objetivo de legitimar cierto contenido informativo empleando la republicación de intermediarios que evitan atribuirla a su fuente original, ocultando con ello el origen de la información. El proceso de blanqueo informativo se divide en tres fases: La fase de emplazamiento inicial del contenido por parte de uno o diversos canales de comunicación; el proceso de superposición a través de uno o más intermediarios, a menudo interconectados, que ocultan su afiliación con el emisor original y blanquean el origen del contenido; y por último la fase de integración en el discurso público que le da mayor amplificación y legitima el contenido manipulativo.

Comunicación estratégica (*Stratcom*). Planificación de la comunicación de una organización en la que se trasladan mensajes concretos en función de sus públicos, con la finalidad de alcanzar determinados objetivos. La comunicación se alinea con la estrategia global de la organización, y busca mejorar su posicionamiento y reputación. En el campo de la seguridad suele emplearse la abreviatura *Stratcom* y alude a la comunicación realizada por gobiernos u organizaciones militares, con un sentido más amplio que un simple establecimiento de agenda o una planificación de mensajes. De esta manera, los *Stratcom* son una herramienta estratégica que contribuyen a coordinar actividades comunicativas y también capacidades operativas, que incluyen diplomacia, monitoreo estratégico, relaciones internacionales o incluso el desarrollo de políticas públicas. La planificación de este tipo de estrategias constituye una herramienta de prevención frente a acciones de guerra informativa llevada a cabo por los actores de la amenaza (por ejemplo, Estados hostiles que despliegan estrategias híbridas contra su objetivo), ya que permite identificar cuáles son las fortalezas y debilidades, las amenazas y facilita acciones efectivas de disuasión.

Deplatforming. Acción de retirar, limitar, bloquear o privar deliberadamente a ciertos actores el acceso de individuos, organizaciones o grupos que infrinjan políticas de uso de plataformas en línea, proveedores de servicios y servicios críticos. Esta medida está relacionada con la práctica de moderación del contenido determinando su idoneidad para un sitio, localidad o jurisdicción determinados y reduciendo su propagación e impacto.

Euphemesia. Término acuñado por Ralph Keyes en 2004 en su obra *The post-truth era: dishonesty and deception in contemporary life*, que alude al uso de eufemismos para no utilizar la mentira y que caracteriza los tiempos de posverdad: “Afirmaciones ambiguas que no son exactamente la verdad, pero que no son una mentira”. Los eufemismos sirven para suavizar o disfrazar el significado real de un concepto o hecho.

Jajaganda. Técnica de propaganda que hace uso del humor para camuflar la divulgación de contenidos desinformativos, destinados a la manipulación de otros usuarios en las redes sociales. A través de esta técnica se traslada un mensaje, para humillar o desprestigiar a una persona, institución o cargo. El peligro de esta técnica recae en que se dirige al plano cognitivo de los usuarios receptores, ya que afecta en la forma como piensan estos y cómo se establecen las relaciones sociales y políticas.

Lavado; marketing engañoso de falsa bandera. Práctica centrada en la búsqueda del posicionamiento de una determinada narrativa, por motivos económicos o políticos que promueven un escenario engañoso y manipulado, en el que se intenta dar la impresión de que las operaciones diseñadas están siendo llevadas a cabo por otros usuarios o entidades. Esto favorece el desvío de la culpa o la creación de un entorno que contribuye a falsas justificaciones, lo que puede socavar los procesos democráticos y la cohesión social, desde la distorsión de la realidad y la manipulación sentimental en la opinión pública.

Monetización (y desmonetización). En el ámbito digital, la monetización se refiere a las estrategias y métodos utilizados para generar ingresos a partir de contenidos, servicios o productos en línea. Esto incluye publicidad, suscripciones, ventas directas, donaciones, productos de merchandising y patrocinios que apoyen campañas como las de desinformación, generando no solo beneficios económicos sino también mayor difusión incluso fuera de internet. La desmonetización, en el contexto de la desinformación, implica la retirada de oportunidades de ingresos para aquellos que difunden información falsa, engañosa o manipulada. Las plataformas de redes sociales han adoptado medidas económicas para luchar contra la desinformación. Estas políticas incluyen la eliminación de anuncios y la restricción de ingresos para aquellos creadores de contenido que difundan información falsa o perjudicial. El objetivo principal es doble: por un lado, reducir la motivación financiera detrás de la creación y difusión de desinformación, y por otro, limitar su alcance y propagación.

Propaganda. Conjunto de técnicas y estrategias de comunicación utilizadas en el ámbito de la política, los conflictos bélicos o la publicidad para influir en las opiniones, actitudes y comportamientos del público, mediante el uso del sesgo, la exageración y la manipulación de los hechos. Recurre a la intencionalidad, la selección de la información, la emoción, la repetición del mensaje, la simplicidad y la deshumanización y la imagen negativa del adversario como forma de persuasión unilateral, sin necesidad de ofrecer argumentos o visiones equilibradas sobre los hechos. Sus consecuencias directas son la polarización, la desconfianza y la manipulación de la opinión pública y entre sus herramientas se incluye la desinformación.

Relativismo. Posición filosófica según la cual las afirmaciones sobre la verdad y la falsedad, lo correcto y lo incorrecto, así que los razonamientos que las justifican, son producto de diferentes convenciones y marcos de interpretación y evaluación y cambian con ellos. Por consiguiente, su autoridad se limita al contexto cultural, científico, religioso o incluso ideológico que les da origen. Así, en sus distintas variantes, el relativismo niega el carácter universal y absoluto del conocimiento, la verdad, los hechos o los valores.

Técnicas de supresión. Conjunto de técnicas de manipulación informativa utilizadas con el objetivo de controlar el espacio informativo mediante la eliminación o supresión de determinadas voces o mensajes en la esfera pública. Las técnicas de supresión ejercidas por parte de actores autoritarios pueden ser internas, pero también extenderse más allá

de sus fronteras y dirigirse a la diáspora fuera del territorio del país. Pueden afectar a cualquier voz crítica e independiente. La supresión puede ejercerse a través del control de los canales de distribución, la explotación de sistemas de moderación del contenido, la coerción, presión o ridiculización de individuos o mediante operaciones en el ciberespacio para alterar la trayectoria del contenido dando prioridad a algunos mensajes mientras se bloquean otros.

Whataboutism **(Responder con preguntas de acusación; contraacusación)**. Táctica retórica en la que se responde a una acusación o una pregunta difícil haciendo una contraacusación o planteando un tema diferente. Esta táctica ha encontrado terreno fértil en las redes sociales, ya que estas permiten una rápida difusión de este tipo de acciones contraargumentativas, lo que favorece discusiones fragmentadas y polarizadas. Como resultado, se socava el diálogo significativo y se fomenta un entorno digital volátil y agresivo que afecta a la transparencia y los valores democráticos en la opinión pública. Si la contraacusación se dirige hacia la persona (*ad hominem*) acusando de hipocresía e incoherencia, puede denominarse *tu quoque* ("¿y tú qué?").

Falacias, teorías conspirativas y pseudo-conocimiento

Amplificación conspiranoica. Proceso mediante el cual las teorías conspirativas se difunden y se vuelven más influyentes. El término "conspiranoia" combina las palabras "conspiración" y "paranoia" para describir una tendencia exagerada a ver conspiraciones detrás de eventos o situaciones que no necesariamente las implican. Se caracteriza por una visión distorsionada de la realidad donde se sospecha constantemente de tramas ocultas, orquestadas por grupos poderosos con intenciones malignas y por la reducción de problemas complejos a un único y sencillo esquema basado en la idea de la conspiración.

Conspiración (teoría de). Creencia que afirma que un acontecimiento o suceso está sujeto al secreto y la mala intención de grupos de poder. Esta teoría está basada en la desconfianza hacia las versiones oficiales, mediante el uso de argumentos difíciles de verificar. Los promotores de la conspiración desconfían de las instituciones, de los gobiernos, de los medios de comunicación y de los expertos. Suelen inundar con explicaciones diversas e incluso contradictorias un mismo hecho, para sobresaturar de datos sin relación empírica subyacente (causalidad) que eviten creer cualquier refutación de la misma, a pesar de los esfuerzos que tratan de buscar una correlación que confunda la opinión pública. Estas comunidades cerradas ofrecen respuestas simples ante lo complejo, se apoyan en interpretaciones subjetivas de los hechos e ignoran cualquier información o refutación que contradiga la teoría.

Deepstate **(Estado profundo)**. Supuesta red secreta de funcionarios y agentes del Estado que actúan al margen de los líderes legítimos y de las instituciones oficiales de un país. Su propósito sería proteger agendas e intereses ocultos influyendo, sin control democrático, en la política y en las decisiones del gobierno.

Defensa Chewbacca. Técnica de propaganda defensiva, que consiste en plantear argumentos sin sentido con el objetivo de confundir al atacante o acusador. Se basa en llenar de mentiras o falacias mediante la exposición de temas, ejemplos y asociaciones que no tienen relación alguna con el tema tratado, para desviar la atención y sembrar dudas.

Esta técnica puede observarse cuando, al identificar un bulo en redes sociales o sitios web, los difusores de la falsedad emplean este tipo de defensa para desviar y confundir a la audiencia. Su nombre proviene de una serie de televisión de animación llamada *South Park*.

Falacia lógica; falso dilema. Argumento que muestra, con un lenguaje polarizante, el hecho de simplificar un problema complejo y presentarlo como una disyuntiva entre dos opciones, sin considerar otras soluciones o matices. Entre las falacias lógicas informales encontramos el falso dilema (una conclusión falsa basada en una afirmación disyuntiva incorrecta que simplifica en exceso la realidad al excluir alternativas válidas) o la falacia de causa cuestionable (la identificación incorrecta de una causa).

Falacia de autoridad. Error de razonamiento que basa la validez de una afirmación únicamente en su atribución a una persona o entidad, generalmente con un prestigio, sin considerar la evidencia o los argumentos subyacentes. Se confía en la reputación de la persona en lugar de la solidez del argumento o la evidencia. Aumenta la susceptibilidad a desinformación que hace referencia a falsos expertos. Se suele emplear a nivel político.

Falsa equivalencia. Sugerir o asumir que son igualmente válidos dos (o más) puntos de vista, cuando está empíricamente/científicamente demostrado que uno (o alguno de ellos) está mucho más próximo a la verdad o es, en realidad, el único verídico. En el contexto de la desinformación, esto sucede cuando se da el mismo peso a argumentos basados en evidencias y a afirmaciones falsas, sesgadas o inexactas, lo que lleva a un empobrecimiento de la comprensión de la realidad. El problema de la falsa equivalencia se vincula con la acción de ciertos medios de comunicación y plataformas digitales que, en ocasiones, ejercen como altavoces de cualquier tipo de relato para evitar ser acusados de sesgos ideológicos o censura.

Freedom Convoy. Movimiento promovido por camioneros canadienses que estaban en contra de las restricciones gubernamentales por la pandemia de la Covid-19. La movilización estuvo acompañada de la circulación de una gran cantidad de información falsa o engañosa en las redes sociales y medios digitales con el objetivo de polarizar la opinión pública. Algunos de los elementos de desinformación asociados a este evento incluyeron teorías conspirativas sobre las verdaderas motivaciones y financiación del convoy o noticias falsas sobre el nivel de apoyo popular o sobre la supuesta ilegalidad de las medidas restrictivas sanitarias.

La gran mentira (*The big lie*). Técnica de propaganda que consiste en lanzar una campaña basada en una mentira muy evidente de ser falsa, pero que provoca una fuerte reacción emocional, como asco, repulsión o miedo en alta intensidad. Esta técnica aprovecha el hecho de que una respuesta emocional intensa suele desplazar el pensamiento racional, permitiendo que la mentira persista en el subconsciente a pesar de su evidente falsedad. Mencionada por Adolf Hitler en 1925, esta estrategia suele ir asociada junto a la técnica de "arenques podridos", ya que la repetición constante de la mentira puede llegar a convertirla en una percepción aceptada como realidad.

Love jihad; Romeo jihad **(Yihad romántica)**. Se trata de una teoría de conspiración de carácter antimusulmán que afirma que hay un supuesto plan organizado por la comunidad musulmana para convertir a mujeres no musulmanas al islam a través de relaciones amorosas y matrimonios interreligiosos. Esta noción se basa en la idea de que los hombres musulmanes estarían deliberadamente seduciendo y casándose con mujeres de otras

religiones con el objetivo de aumentar la población musulmana. La "yihad romántica" se considera una narrativa engañosa y se percibe como un intento de demonizar y estigmatizar a la comunidad musulmana, al presentar las relaciones interreligiosas como parte de una supuesta conspiración, cuando en realidad no hay evidencia creíble que sustente tales afirmaciones.

Manosfera; machosfera. Son dos términos que hacen referencia a una red de sitios web, foros y comunidades en línea que promueven ideologías misóginas, antifeministas y de supremacía masculina asociados a movimientos de extrema derecha. Algunos ejemplos incluyen grupos de hombres que se definen como *incels* (involuntariamente célibes), MGTOW (hombres que rechazan el matrimonio y las relaciones con mujeres), los MRA (los activistas por los derechos de los hombres) y otros que promueven nociones de masculinidad tóxica.

Negacionismo. Actitud que consiste en la negación sistemática o el rechazo obstinado de hechos o eventos históricos, científicos o sociales ampliamente aceptados y empíricamente verificados. Desde el punto de vista psicológico, este comportamiento se explica como mecanismo para evitar una realidad psicológicamente incómoda. Las motivaciones que hay detrás pueden ser políticas, ideológicas, religiosas, emocionales o simplemente de carácter económico. Este rechazo dogmático no debe confundirse con el escepticismo científico inherente al proceso de investigación que incluye la constante revisión de datos, hipótesis, teorías y resultados.

Pastilla roja (*Red pill*). Término empleado en los subgrupos de la manosfera/machosfera, así como en el de extrema-derecha, en contraposición con la pastilla azul (*blue pill*) y hace referencia a aquellos varones que consideran que han tomado conciencia de la verdadera realidad en un contexto en el que denuncian, según su percepción misógina, que el feminismo ha impuesto un control autoritario y manipulador sobre el mundo y sus dinámicas sociopolíticas. Su origen proviene de la película Matrix (1999) y de una escena en la que el protagonista, Neo, debe optar entre seguir viviendo de manera ignorante en una realidad manipulada (si toma la píldora azul) o abrir los ojos a la verdad de la realidad (si opta por la roja).

Pensamiento posfáctico. Forma de razonamiento en la que las emociones y las creencias personales tienen más influencia que los hechos objetivos y la evidencia verificable. Se caracteriza por la indiferencia de las personas respecto a la distinción entre verdad y mentira, realidad y ficción, opinión y conocimiento. Una mentalidad que tiende a conceder gran importancia a las narrativas a través de las cuales se construyen hechos alternativos.

Plan Kalergi (Conspiración antisemita). Teoría conspirativa antisemita, que afirma que un grupo de judíos y otras élites internacionales están conspirando para destruir la identidad racial y cultural de Europa mediante la inmigración masiva y la mezcla racial. Esta teoría se basa en una falsa interpretación de los escritos de Richard von Coudenhove-Kalergi, quien propuso una unión europea en la década de 1920, y que suele estar promovida por comunidades y grupos alt-right y de extrema derecha que se distinguen por la promoción de teorías de la conspiración y/o discursos de odio.

Pseudo-escepticismo. Se refiere a las posturas negacionistas que se autodefinen como escépticas. Incluye todas las variantes del negacionismo: histórico (reinterpretaciones subjetivas e interesadas de la historia), científico (rechazo de la evidencia y de los consensos científicos), tecnológico (profunda desconfianza frente a desarrollos tecnológicos) y político

(negación de hechos políticos, demográficos o sociales). No debe confundirse ni con el escepticismo inherente a la práctica científica ni con el escepticismo filosófico.

Pseudociencia. Campo cognitivo que pretende ser científico, pero no cumple algunas características fundamentales de la práctica científica por lo cual choca inevitablemente con teorías científicas aceptadas. Los siguientes criterios ayudan a distinguirla de las ciencias: pseudociencias postulan entidades cuya existencia no se puede demostrar, defienden concepciones espiritualistas, no tienen lógica ni procedimientos de control objetivos, no desarrollan nuevos problemas e hipótesis y tienen poca continuidad con otras disciplinas. Sus afirmaciones no suelen ser falsables y, por tanto, las teorías subyacentes apenas evolucionan a través de la investigación.

Tácticas psicológicas, cognitivas y de percepción

Alfabetización mediática; educación mediática / digital / transmediática. Facultad de consultar y evaluar críticamente contenidos en medios de comunicación, así como de crear contenido digital. Esta competencia implica entender cómo funcionan los medios, reconocer sus diferentes tipos y formatos, y desarrollar habilidades críticas para interpretar la información que publican. Se aplica a entornos mediáticos tanto digitales como analógicos.

Avaricia cognitiva. Proceso mental por el que los seres humanos ahorran esfuerzos en el procesamiento de la información o en la toma de decisiones. En lugar de realizar un análisis meticuloso de los datos obtenidos aplicando para ello un razonamiento lógico, se prefiere procesar la información de forma superficial utilizando claves emocionales o atajos mentales que llevan a interpretar la realidad de la forma más simple. Esta situación resulta especialmente prevalente en contextos de sobreinformación como el actual, donde cualquier persona está expuesta a múltiples estímulos imposibles de interpretar con total atención.

Cámara de eco. Entorno donde se comparten de manera recurrente creencias, ideas o datos alineados, propiciando su amplificación y refuerzo. La información, sea verdadera o falsa, circula y se redifunde sin ser cuestionada por los miembros del grupo del filtro burbuja (ver definición en glosario) ni contrastada con perspectivas externas, creando una realidad distorsionada y polarizada.

DARVO (*Deny, Attack and Reverse Victim and Offender*, en español: Negar, Atacar e Invertir Víctima y Agresor). Técnica reactiva y manipuladora que consiste en negar la evidencia y defenderse atacando, invirtiendo las figuras de víctima y agresor. Este comportamiento es común en los agresores cuando son señalados como tales. Primero, niegan la agresión o abuso; luego, atacan al agredido intentando desacreditarlo como persona o grupo; finalmente, se posicionan como víctimas en lugar de agresores. Esta técnica se emplea para silenciar a personas o grupos mediante críticas y para culpabilizar a la víctima del ataque.

Disonancia cognitiva. Teoría propuesta en 1957 por el psicólogo Leon Festinger, que explica la necesidad que tienen las personas de que sus creencias y actitudes sean coherentes entre sí, y el malestar que surge cuando no lo son. La tendencia a la búsqueda de la coherencia interna de las creencias interiorizadas y los comportamientos hace que

se genere tensión ante determinadas actitudes propias o, incluso, ante ideas ajenas que vienen a romper esa armonía interna. Esta sensación incómoda impulsa al individuo a intentar reducir el malestar con un intento de cambio de conducta o con la defensa de sus creencias o actitudes a través del autoengaño.

Dominio cognitivo. Control sobre un conjunto de habilidades y procesos mentales relacionados con el aprendizaje, el conocimiento y la comprensión. Incluye funciones como la percepción, el sistema sensoriomotor, la atención, la memoria, el pensamiento y el razonamiento que facilitan la toma de decisiones y el pensamiento crítico. La desinformación trata de socavar de manera subliminal la autonomía respecto a estas capacidades cognitivas, influencia que se consigue mediante la gestión de la información que la audiencia objetivo recibe.

Efecto *rabbit hole* (Realidad paralela). Tendencia a caer en un ciclo interminable de contenido en línea. Se trata de un efecto psicológico y adictivo en el que una persona se ve atrapada en una sucesión interminable de contenido relacionado a través de plataformas *online*, redes sociales, foros o webs de noticias. El término proviene de la novela *Las aventuras de Alicia en el país de las maravillas*, de Lewis Carroll, donde la protagonista cae por una madriguera y entra en un mundo de fantasía y desorientación.

Efecto silbato de perro (*Dog whistle*). Técnica de oratoria y propaganda que consiste en el empleo de lenguaje de doble sentido. Esta técnica se basa en que determinados grupos tienen conocimientos, lenguajes o significados específicos que solo ellos entienden, mientras que para la población en general, el mensaje tiene otro significado más inocuo. De esta manera, es posible comunicar ideas a un grupo particular sin llamar la atención del resto de la población. El nombre proviene de los silbatos para perros, que emiten sonidos a frecuencias no audibles para el oído humano.

***Epistemic flooding* (Inundación epistémica)**. Trastorno del procesamiento cognitivo causado por sobreinformación. Se produce en entornos como las redes sociales, donde las personas están expuestas regularmente a más información y datos de los que pueden procesar cuidadosamente. La sobreoferta de imágenes, datos y texto, y la velocidad a la que se consumen dificultan la identificación de información fiable, así como aumentan su capacidad de influencia.

Filtro burbuja; burbuja epistémica. Término acuñado en 2011 por Eli Pariser como *filter bubble* en inglés, para referirse al efecto sesgado que generan los algoritmos con los que en Internet se seleccionan los contenidos que se reciben al navegar en el entorno digital. Este mecanismo de selección aísla ideológicamente a las personas en burbujas epistémicas, donde no tienen cabida contenidos no alineados con sus puntos de vista y en las que se genera una cámara de eco que reafirma las creencias propias y lo que se considera verdadero.

Galope de Gish (*Gish Gallop*). Técnica de propaganda y réplica en debates que consiste en emitir una multitud de mensajes en un corto período, donde la cantidad y rapidez de los argumentos prevalecen sobre su veracidad. Esta técnica se basa generalmente en medias verdades, falsedades o tergiversaciones, impidiendo que el oponente tenga tiempo para verificar o refutar los numerosos mensajes en tan poco tiempo. Proviene su nombre de un creacionista llamado Gish, que empleaba esta técnica contra los defensores de la teoría de la evolución.

Influencia por persuasión / sugerencia. Proceso intencionado de personas o grupos dirigido a influir y cambiar la actitud, creencia o decisión de otros mediante una estrategia directa, que utiliza argumentos lógicos y claros o una estrategia indirecta que recurre a sutilezas, sugerencias implícitas y manipulación emocional. La persuasión tiene como principal objetivo convencer a la otra parte de la validez de un argumento y requiere de una comunicación eficaz que incluye creatividad, apelación a los sentimientos, capacidad de escucha, claridad y adaptación al público objetivo. El mal uso de la persuasión puede derivar en la desinformación, la propaganda política o el marketing engañoso, entre otras consecuencias negativas.

Infodemia / sobreinformación. Deriva de la fusión entre las palabras información y epidemia. Alude a la situación de abundancia excesiva de información sobre un tema o aspecto concreto donde se mezcla la información verídica y correcta con datos falsos, rumores e informaciones inexactas, sesgadas y malintencionadas. Esta sobrecarga informativa –amplificada y distribuida a una audiencia mundial gracias al uso de las tecnologías digitales– excede la capacidad limitada de procesamiento del individuo; lo que puede acarrear graves consecuencias, sobre todo en contextos de crisis o emergencias.

Luz de gas (*Gaslighting*). Estrategia de abuso y manipulación que busca que la otra persona cuestione su propia percepción de la realidad. El término tiene su origen en la obra de teatro del mismo nombre de Patrick Hamilton, estrenada en 1938 y que ha contado con posteriores adaptaciones cinematográficas. La trama muestra a un hombre que maltrata a su mujer haciendo pequeños cambios en el hogar, como el nivel de la luz de gas, haciéndole creer que nada ha cambiado para que ella empiece a dudar de su cordura. En la actualidad, desfigurando el sentido original del término, se emplea para referirse a la estrategia de mentir reiteradamente a alguien con el fin de manipularlo y controlarlo.

Metralleta de preguntas (*Sealioning*; *JAQoff*). Técnica de ataque o acoso que consiste en lanzar continuamente preguntas y solicitudes de pruebas, manteniendo una apariencia muy cortés y tranquila, con el objetivo de desorientar a la otra parte. Similar al Galope de Gish o la ametralladora de falacias, esta técnica se diferencia en plantear preguntas constantes y acusar de falta de pruebas, en lugar de presentar numerosos argumentos. El propósito es provocar el enfado del oponente, para luego presentarse como la parte ofendida o agraviada. Es una técnica muy utilizada en el troleo en redes sociales, principalmente para silenciar a una persona o institución. Al lograr callar a la otra parte, se hacen parecer aceptables afirmaciones de escasa verosimilitud.

***Misperceptions* (percepciones erróneas)**. Ideas o creencias incorrectas sobre un hecho, relacionadas con factores como información sesgada, prejuicios personales o falta de conocimiento sobre el acontecimiento. La percepción errónea está basada en la inexactitud, la generalización y extrapolación de casos individuales a un contexto general o el sesgo de confirmación por el que las personas conceden más importancia a la información que confirma sus creencias preexistentes. Las consecuencias derivadas de este uso son la toma de decisiones errónea y la pérdida de confianza en la fuente promotora.

Manipulación algorítmica y mediática

Clickbait. Anglicismo que la RAE sugiere traducir por términos como "ciberanzuelo", "cibercebo" o "anzuelo/cebo de clics", entre otros. Práctica empleada en marketing y en medios digitales, que consiste en adulterar el contenido mediante fórmulas sensacionalistas, ambiguas o engañosas, especialmente en su titular, con el fin de que el público lo visite movido por la curiosidad. Una vez que el usuario accede al contenido, este suele resultar decepcionante o no corresponder con la expectativa inicial.

Creepypasta. La traducción literal al español sería "pasta terrorífica", si bien se suele utilizar la voz inglesa. Se trata de una forma de contenido digital que combina elementos de ficción y horror para crear una experiencia de miedo o perturbación en el lector. Estas historias también pueden ser utilizadas para propagar desinformación y bulos, ya que pueden contener elementos de verdad, pero se mezclan con detalles ficticios y se difunden de manera intencional para crear una sensación de miedo o paranoia. Esto puede llevar a que los lectores compartan la historia sin verificar su veracidad, contribuyendo así a la propagación de desinformación.

Curación algorítmica. Selección y filtrado de información que los algoritmos realizan en función de las preferencias y comportamientos de los usuarios. Es aplicado fundamentalmente en las búsquedas realizadas en buscadores de información y redes sociales y afecta al acceso de información pues a través de dicha curación se limita la exposición de los individuos a otras opiniones o perspectivas.

Micro-targeting. La microsegmentación o microfocalización es una estrategia propia de la comunicación estratégica y el marketing, que consiste en identificar públicos específicos y personalizar el mensaje acorde a los datos que se han recogido de los usuarios. Con ella, el emisor consigue que la aceptación de los mensajes sea mayor y más efectiva. En estrategias de desinformación es empleada para identificar audiencias más vulnerables y aumentar la probabilidad de creencia sobre contenidos falsos, manipulados o medias verdades.

Partidismo (*Partisanship*). Tendencia a apoyar de manera incondicional a un partido político, grupo o ideología, sin considerar críticamente sus argumentos, incluso si estos se basan en afirmaciones engañosas. Esta adhesión inquebrantable puede llevar a un sesgo en el juicio y en la toma de decisiones, donde la lealtad al grupo político prima sobre el análisis objetivo de las evidencias.

Perfil psicográfico. Categorización psicológica, ideológica, socioeconómica y etnodemográfica de una persona a partir de sus datos personales, sus búsquedas y movimientos en Internet, que crea patrones no sólo de sus preferencias explícitas y conscientes, sino también sobre lo que le atrae y repele por debajo del nivel de acción consciente. Estos perfiles permiten crear contenidos personalizados que van dirigidos a unos individuos determinados, mejorando así la eficacia de cualquier tipo de campaña de tipo *microtargeting* o individualizada.

Periodismo amarillo. Tipo de periodismo sensacionalista y exagerado, que prioriza los aspectos más truculentos, escandalosos o espectaculares de la realidad, en detrimento de la objetividad y el rigor informativo. Se caracteriza por el uso de titulares llamativos, lenguaje

dramático, imágenes impactantes y la distorsión o exageración de los hechos, con el objetivo de atraer la atención del público y generar mayor impacto emocional, incluso a costa de la veracidad. En concreto, sacrifica los principios éticos y profesionales del periodismo en favor de intereses comerciales y la búsqueda de sensacionalismo, y contribuye a la desinformación y la manipulación de la opinión pública.

Polarización. La polarización es la división creciente de la sociedad en grupos con ideas, opiniones o intereses opuestos. Ocurre cuando las posiciones ideológicas de los individuos o grupos se alejan hacia los extremos opuestos, lo que puede dificultar el consenso y aumentar el conflicto social. Se suele distinguir entre la polarización ideológica, que se refiere a un desplazamiento de los partidos en su perfil y posicionamiento hacia los extremos del espectro político, y la polarización afectiva, referente a las emociones y afectos de simpatía u hostilidad hacia los partidos, sus líderes y sus votantes, y que se mide en el nivel de crispación en el espacio público. Igualmente se trata de un recurso de comunicación utilizado por grupos de interés (ej. grupos políticos), para atraer usuarios mediante la explotación de plataformas digitales, mediante el uso de discursos que pueden incluir discursos de odio y contenidos desinformativos. Implica la combinación de fenómenos sociopolíticos y comunicativos en los que la retórica basada en expresiones de odio conduce a la propagación de los prejuicios y la intolerancia en las sociedades contemporáneas.

Pseudomedio. Publicación que emula a los medios periodísticos en su estructura y formato, y que se caracteriza por incumplir los principios éticos y estándares profesionales del periodismo. El término alude sobre todo a publicaciones digitales, aunque también puede aplicarse a medios en otras plataformas. Los pseudomedios se caracterizan por su apuesta por la polarización, el activismo ideológico, el fomento de teorías conspirativas y una tendencia generalizada a la difusión de contenidos falsos, no contrastados y extremadamente sesgados o partidistas.

Sesgo (bias / prejuicios). Es una forma de prejuicio, de carácter inconsciente o subconsciente, y vinculado a las heurísticas cotidianas, que contribuye, generalmente, a apoyar u oponerse a una cosa, persona u organizaciones sobre otras. El sesgo se produce cuando la información o el contenido divulgado se presenta de forma parcialmente veraz o manipulada, para favorecer ciertos intereses, opiniones o perspectivas sobre otros. A menudo la presencia del sesgo en las redes sociales se manifiesta de diversas formas, y puede influir en las diferentes perspectivas de individuos, grupos sociales o instituciones. Ejemplo de ello, es a través de los algoritmos que distribuyen los contenidos que se suelen mostrar en las redes sociales, los cuales ayudan a adaptar lo que vemos en función de nuestro comportamiento y preferencias anteriores.

Sesgo de confirmación. Tipo de sesgo cognitivo que consiste en la tendencia a favorecer, buscar, interpretar y recordar información que confirma las creencias, hipótesis o expectativas previas de una persona, dando menos consideración a alternativas o evidencia contraria. Algunas características clave del sesgo de confirmación serían: se trata de un error sistemático en el razonamiento inductivo, se manifiesta cuando se reúne o recuerda información de manera selectiva o se interpreta sesgadamente, es más fuerte cuando la información tiene contenido emocional o cuando las creencias están firmemente arraigadas, lleva a interpretar una evidencia ambigua como apoyo a las posiciones existentes, o también es un sesgo que puede explicar fenómenos como la polarización de actitudes, la perseverancia de creencias falsas y la percepción de correlaciones ilusorias.

Verificación (*fact-cheking*). Acción destinada a la comprobación de la autenticidad y/o validez de datos o afirmaciones. En el escenario digital, se añade además la comprobación de las fuentes y la identidad de sus emisores. Es una herramienta crucial para combatir la desinformación. El impacto de la verificación depende de múltiples factores, incluyendo la plataforma utilizada, el tipo de contenido y la predisposición ideológica de los usuarios. Para aumentar la difusión de su trabajo y desmentir públicamente los contenidos falsos, los verificadores suelen emplear distintos canales y redes sociales en su difusión.

Ciberdelitos y amenazas online

Ataque mariposa (*Butterfly attack*). Técnica similar al *astroturfing*, pero con un enfoque diferente: en lugar de apoyar temas o grupos con la ilusión de un movimiento de base, se utiliza para infiltrarse, dividir y desactivar comunidades, campañas y grupos ya existentes. El método consiste en que grupos de impostores o troles se infiltran en estos grupos o campañas, ya sea en redes sociales o en la vida real, con el objetivo de provocar divisiones mediante engaños y desinformación. Una vez dentro, se identifican y explotan las diferencias y prejuicios presentes en el grupo, introduciendo confusión y desacreditando al colectivo. El nombre empleado se basa en el comportamiento de las mariposas, que cambian sus patrones de aleteo para confundir a sus depredadores, de ahí su nombre propuesto por Patrick Ryan en 2017.

Capitalismo de vigilancia. Modelo económico y social que se caracteriza por la recolección y explotación masiva de datos personales de los usuarios, con el objetivo de generar beneficios a través de la predicción y modificación de su comportamiento. Este sistema se basa en la captura de información detallada sobre las actividades, preferencias y hábitos de las personas, a través de diversos dispositivos y plataformas digitales. Dicha información es luego analizada y monetizada por grandes empresas tecnológicas, que la utilizan para desarrollar productos y servicios personalizados, así como para influir en la toma de decisiones de los individuos. El capitalismo de vigilancia ha sido criticado por su impacto en la privacidad, la autonomía y la libertad de las personas, al convertir sus datos en una mercancía valiosa que es comercializada sin su consentimiento pleno. Asimismo, se ha señalado que este modelo puede profundizar las desigualdades sociales y consolidar el poder de unas pocas corporaciones a escala global.

Ciberocupación. Es una forma de ciberdelito en el que una persona compra o registra un nombre de dominio igual o similar a uno existente, con la intención de sacar provecho de una marca registrada, nombre comercial o personal reconocido socialmente. Este tipo de delitos suelen ser empleados para la creación de páginas de phishing, estafas o encuestas falsas, con el interés final de recopilar datos de usuarios, para robarles o secuestrar la identidad digital de estos en internet.

Ciberseguridad. Conjunto de prácticas, tecnologías y procesos diseñados para proteger sistemas, redes y dispositivos informáticos, así como los datos que contienen, frente a ataques, daños o accesos no autorizados. Esta disciplina abarca diversas áreas como la seguridad de la red, información y aplicaciones, y la protección de dispositivos. También incluye la gestión de identidad y acceso, la respuesta a incidentes, y la recuperación ante desastres, asegurando la continuidad del proceso.

Contenido dañino (*Harmful content*). Contenidos difundidos a través de los escenarios de medios tradicionales o en digitales, que tienen un impacto negativo y persistente durante un período significativo de tiempo, una vez diseminados. Están destinados a causar daño, hacia una persona o grupo social específico. Este tipo de contenidos se manifiesta de diversas formas, a través de la incitación al odio, el lenguaje ofensivo, la intimidación, el acoso, así como la exposición de contenidos desinformativos.

Discurso de odio (*hate speech*). Cualquier forma de expresión que ataca o utiliza un lenguaje hostil, incívico, amenazante, ofensivo, discriminatorio o de violencia expresa, en referencia a un grupo o a una persona en función de su etnia, nacionalidad, raza, género, ascendencia, religión, vulnerabilidad u otras formas de identidad como la ideología política. idioma, origen económico o social, discapacidad, estado de salud u orientación sexual, entre otras. Este tipo de discurso tiene una naturaleza pública, y persigue causar daño e incitar a acciones violentas o discriminatorias, pues denotan la presencia de un móvil de odio o discriminación y la narrativa tiene la aptitud o idoneidad para generar un clima de odio.

Doxing **(Doxeo)**. Técnica de propaganda o difusión de mensajes que consiste en revelar de manera pública e intencionada los datos personales privados de una persona, grupo o institución. Esta estrategia busca extorsionar al difundir aspectos como el lugar de residencia, números de teléfono, información sobre la familia, aspectos personales, correos electrónicos, fotografías, entre otros. El objetivo no solo es señalar y dañar a la persona aludida, sino también asustar, amenazar o avergonzarla para que deje de realizar las actividades que desempeñaba anteriormente. Esta técnica ha sido empleada contra periodistas, políticos, militares, activistas, empresarios, deportistas, entre otros.

Granja de *bots*; granja de troles. Término que alude a la organización masificada de *bots* o troles, coordinados para la creación masiva y difusión de mensajes falsos en redes sociales, a partir de contenidos desinformativos, abusivos y violentos dirigidos hacia una persona o colectivo, o bien alrededor de unos determinados temas de interés. La presencia de este tipo de granjas sirve para generar confusión, manipular o dividir la opinión pública, realizar fraudes, o ayudar a realzar determinadas marcas o usuarios, con fines comerciales o sociales.

Offline / online violence. Estrategia que persigue llevar las acciones de violencia online al mundo físico u offline. Se busca con ello lograr un mayor impacto de las campañas en línea, desarrollando acciones en ambos campos, y establecer mayores interconexiones a través de la interacción física de las personas afines. Este tipo de maniobras puede suponer la puesta en marcha de una manifestación vinculada a un movimiento de protesta en línea, el uso de medios tales como radio, prensa o la publicidad en general para reforzar el mensaje ideológico o la puesta en marcha de foros físicos dónde reunir adeptos.

Trol. Persona con identidad real oculta que publica en las redes sociales, webs o plataformas mensajes provocadores o dañinos de manera intencionada con un objetivo ideológico concreto: generar desinformación, boicotear o entorpecer la conversación, ocasionar daño… Sus acciones son conocidas con el término trolear. Muchas veces los troles no actúan de manera individual ni aislada, sino de forma coordinada formando parte de lo que se conoce como granja de trolls (véase definición en el glosario).

CONCLUSIONES Y PROPUESTAS

En el presente capítulo se han recogido 125 términos fundamentales para la comprensión del fenómeno de la desinformación, con implicaciones en la seguridad nacional y el ámbito digital. Este glosario tiene como objetivo proporcionar conocimiento sobre diversos aspectos del ámbito que impactan en la sociedad. Su propósito es reunir, difundir y dar a conocer técnicas y elementos clave empleados en este contexto. Está dirigido a medios de comunicación, expertos, técnicos, el sector educativo y académico, y, sobre todo, a la sociedad en general como una herramienta de utilidad.

Si bien esta es una primera propuesta que buscaba aunar miradas de distintos expertos en la materia, conviene lógicamente una revisión y ampliación periódica, bien sea a través de este Foro contra las Campañas de Desinformación en el ámbito de la Seguridad Nacional o a través de publicaciones similares. La propia evolución del fenómeno implica que algunos de estos conceptos puedan llegar a quedar obsoletos, por lo que convendría su correspondiente revisión con el ánimo de que sea útil y pertinente.

Dado que la desinformación es global y afecta a la realidad de distintos países, su correspondiente traducción a otros idiomas permitiría su aplicación en otros contextos, ampliando a la vez la mirada sobre tácticas y herramientas que trascienden las fronteras nacionales. A su vez, se abriría la posibilidad de establecer marcos internacionales comunes, facilitando la colaboración y entendimiento entre expertos e investigadores de distintas regiones. Traducciones que también serían de interés en el campo de la alfabetización mediática y digital.

Los nuevos retos relacionados con la desinformación como la inteligencia artificial, los potenciales regulatorios globales, las realidades inmersivas, la privacidad o la criptografía tendrán que ser también retratados a futuro. Si bien, esta propuesta es un primer paso, valioso y necesario, tener un lenguaje común es esencial para empoderar a ciudadanos, académicos y profesionales en la lucha contra la manipulación y la desinformación.

REFERENCIAS BIBLIOGRÁFICAS

Aguilar, D. (2023, 22 de agosto). How to Use Sock Puppet Accounts to Gather Social Media Intelligence. Maltego.com. https://www.maltego.com/blog/how-to-use-sock-puppet-accounts-to-gather-social-media-intelligence/

Arce-García, S., Said-Hung, E., y Mottareale-Calvanese, D. (2023). Tipos De campaña Astroturfing De Contenidos Desinformativos Y Polarizados En Tiempos De Pandemia En España. Revista ICONO 14. *Revista científica De Comunicación Y Tecnologías Emergentes, 21*(1). https://doi.org/10.7195/ri14.v21i1.1890.

Carrasco Rodríguez, B. (2020). Information Laundering in Germany. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/cuploads/pfiles/nato_stratcom_coe_information_laundering_in_germany_final_web.pdf

Comisión Europea (2020, 3 de diciembre). Plan de Acción para la Democracia Europea. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0790

Comisión Europea (2023). Developing a better understanding of information suppression by state authorities as an example of foreign information manipulation and interference. https://cordis.europa.eu/programme/id/HORIZON_HORIZON-CL2-2023-DEMOCRACY-01-02/es

C-Informa (2022, 29 de noviembre). ¿Fake, Trolls, Astroturfing? Conoce estos y otros conceptos en el Glosario sobre desinformación. Cazadores de Fake News. https://www.cazadoresdefakenews.info/fake-trolls-astroturfing-conoce-estos-y-otros-conceptos-en-el-glosario-sobre-desinformacion/ de Goelj, M.W.R. (2023). Reflexive Control: Influencing Strategic Behavior. Parameters, 53(4), https://doi.org/10.55540/0031-1723.3262

Disarm Foundation (2019). Disarm Framework. https://www.disarm.foundation/framework

EUDisinfoLab (2024, 13 de agosto). What is the Doppelgänger operation? List of resources. Disinfo.eu. https://www.disinfo.eu/doppelganger-operation/

EUvsDisinfo (2021, 25 de agosto). Modus Trollerandi Part 5: Provocations. EUvsDisinfo.eu. https://euvsdisinfo.eu/modus-trollerandi-part-5-provocations/

Foro contra las Campañas de Desinformación en el ámbito de la Seguridad Nacional (2023). Trabajos 2023. Departamento de Seguridad Nacional. https://www.dsn.gob.es/es/documento/foro-contra-campa%C3%B1as-desinformaci%C3%B3n-%C3%A1mbito-seguridad-nacional-trabajos-2023

Giles, K., Sherr, J., y Seaboyer, A. (2018). Russian reflexive control. Royal Military College of Canada. https://www.researchgate.net/publication/328562833_Russian_Reflexive_Control

Goldenziel, J.I. (2021). Law as a Battlefield: The U.S., China, and the Global Escalation of Lawfare. Cornell Law Review, 106(5). https://www.cornelllawreview.org/2021/09/23/law-as-a-battlefield-the-u-s-china-and-the-global-escalation-of-lawfare/

Harper, N. (2020, 17 de diciembre). No, you're not 'just asking questions.' You're spreading disinformation. Minnesota Reformer. https://minnesotareformer.com/2020/12/17/no-you-re-not-just-asking-questions-youre-spreading-disinformation/

HybridCoE (2023). Hybrid threats as a concept. https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

NSS (2024, 4 de enero). *Defining foreign influence and interference*. Tel Aviv University. https://www.inss.org.il/publication/influence-and-interference/

Lupiáñez Lupiáñez, M. (2023). Cómo hacer frente a un ataque cognitivo: Prototipo de detección de la propaganda y manipulación en operaciones psicológicas dirigidas a civiles durante un conflicto. *Revista del Instituto Español de Estudios Estratégicos, 22*, 61-93. https://revista.ieee.es/article/view/6058/7348

Mercenaries, C., Maurer, T., & Mannan, S.H. (2019). Projecting Power: How States Use Proxies in Cyberspace. https://jnslp.com/wp-content/uploads/2020/04/Projecting_Power_How_States_Use_Proxies_in_Cyberspace.pdf

Ministerio de Defensa ruso (2011). Conceptual Views Regarding the Activities of the Armes Forces of the Russian Federation in the Information Space (CCDCOE, Trad). CCDCOE.org (2018). https://ccdcoe.org/uploads/2018/10/Russian_Federation_unofficial_translation.pdf

Oasis Open Europe Fundation (2021, 25 de enero). *STIX Version 2.1*. Oasisopen.org. https://www.oasis-open.org/standard/6426/

OTAN (2024, 7 de mayo). Countering hybrids threats. https://www.nato.int/cps/en/natohq/topics_156338.htm

Parliament of Australia (2020). Third parties and foreign actors. https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Electoral_Matters/2019Federalelection/Report/section?id=committees/reportjnt/024439/73871#:~:text=Electoral/foreign%20interference%20involves%20interfering,focused%20on%20advancing%20specific%20issues

Presidencia del Gobierno (2017). Estrategia de Seguridad Nacional 2017. *Departamento de Seguridad Nacional*. https://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf

Presidente de la Federación de Rusia (2000, 9 de septiembre). Doctrina de seguridad de la información de la Federación de Rusia. https://base.garant.ru/182535/

Rid, T. (2020). *Desinformación y guerra política*. Crítica.

Rodríguez-Fernández, L. (2021). *Propaganda digital. Comunicación en tiempos de desinformación*. UOC.

Sessa, M.G. (2023, 30 de marzo). Disinformation glossary: 150+ terms to understand the information disorder. *Disinfo.eu*. https://www.disinfo.eu/publications/disinformation-glossary-150-terms-to-understand-the-information-disorder/

Sharma, S. (2023, 20 de diciembre). The biggest names pranked by Russian duo Lexus and Vovan, from Prince Harry to Elton John. *The Independent*. https://www.independent.co.uk/news/world/europe/russian-lexus-vovan-leo-varadkar-prank-call-b2467203.html

Sitaraman, G. (2023). Deplatforming. *The Yale Law Journal, 133*(2), 419-668. https://www.yalelawjournal.org/article/deplatforming

Strategic Communications, Task Forces and Information Analysis -STRAT.2- Data Team (2023). *1st EEAS Report on Foreign Information Manipulation and Interference Threats Towards a framework for networked defence*. European Union External Action. https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf

Think Tank (2021). Strategic communications as a key factor in countering hybrid threats. *European Parliament*. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)656323

Voyager, M. (2018). Russian Lawfare – Russia's Weaponisation of International And Domestic Law: Implications For The Region And Policy Recommendations. *Journal on Baltic Security, 4*(2). https://doi.org/10.2478/jobs-2018-0011

Zabrisky, Z. (2020, 4 de marzo). *Big Lies and Rotten Herrings: 17 Kremlin Disinformation Techniques You Need to Know Now*. BylineTimes. https://bylinetimes.com/2020/03/04/big-lies-and-rotten-herrings-17-kremlin-disinformation-techniques-you-need-to-know-now/

CAPÍTULO 2

EL PAPEL DE LOS MEDIOS DE COMUNICACIÓN Y LAS DIRECCIONES DE COMUNICACIÓN EN EL COMBATE CONTRA LA DESINFORMACIÓN

Coordinadores:

Emilio Lliteras Arañó

Miguel Lopez Quesada

María Penedo

Departamento de Seguridad Nacional

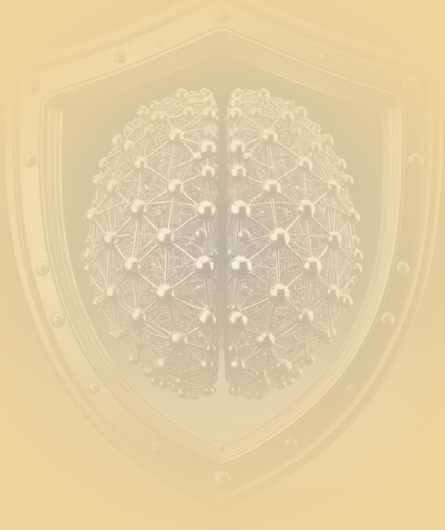
Autores y colaboradores:

Emilio Lliteras Arañó

Miguel López-Quesada

María Penedo

Fernando Romero Valderrama



CONTEXTO

La desinformación es un concepto antiquísimo y permanente que siempre se ha utilizado para conseguir posiciones de privilegio en todo tipo de sociedades.

El repertorio de procedimientos para desinformar es inmenso pero en estos momentos, las mayores amenazas están asociadas a Internet, el uso interesado de las redes sociales y de la inteligencia artificial, lugares donde en muchos casos no existe transparencia ni responsabilidad social ni jurídica respecto del emisor de los mensajes, mientras los algoritmos premian la visibilidad de los contenidos más extremos y de los contenidos más afines a nuestros sesgos personales, con independencia de la responsabilidad de la fuente que los origine. En este contexto, la lucha contra la desinformación está resultando una necesidad profunda y urgente. Para combatir los augurios de quienes vaticinan la muerte de las democracias liberales, es fundamental establecer con decisión y con carácter inmediato un sistema que preserve y garantice la prevalencia de las democracias frente a los diferentes totalitarismos interesados en enmascarar la verdad.

El derecho universal a recibir información veraz (Desantes Guanter, 1997) supone el reconocimiento del ejercicio de profesiones que defiendan la libertad de información tanto en los medios como en las fuentes.

¿Cómo hacer frente a esta emergencia global de la desinformación sin lesionar derechos y libertades fundamentales en las democracias liberales?

Existe un consenso generalizado sobre la necesidad de impulsar la alfabetización mediática de manera transversal. De forma paralela, es preciso recordar que las democracias han luchado y prevalecido contra la mentira y el abuso de poder, conceptos indisolubles, gracias a la defensa de la verdad por parte de los medios de comunicación, los agentes políticos y sociales y la ciudadanía.

Rastrear, identificar procedencias, garantizar autorías profesionalizadas capaces de soportar y asumir responsabilidades, verificar y contrastar, son ingredientes indispensables en el complejo mundo de la información pública que forman parte de un entramado indispensable si queremos identificar las democracias liberales como salvaguarda válida de convivencia.

MEDIOS DE COMUNICACIÓN Y DIRECCIONES DE COMUNICACIÓN, FRENO Y BARRERA CONTRA LA DESINFORMACIÓN

En un momento en el que la defensa de la verdad resulta estratégica, medios de comunicación, departamentos y direcciones de comunicación de empresas e instituciones están llamados a desempeñar un papel fundamental. Son pilares básicos en la construcción de una sociedad donde prevalezca la verdad, la pluralidad y la confianza frente a aquellos que, sirviéndose del anonimato y amparados en la ausencia de responsabilidad editorial de las redes sociales, trabajan por la extensión de la mentira, la polarización y la desconfianza. La visibilidad de la firma y de la marca, así como la plena asunción de la responsabilidad reputacional, social y jurídica por sus informaciones y mensajes, son contrapunto necesario ante la oscuridad y opacidad de las redes sociales y los algoritmos.

Se trata de profesionales cualificados, sometidos a una deontología, responsables ante la sociedad en la que difunden sus mensajes. De poco sirven los más sofisticados avances en la manera de generar y distribuir la información sin unos intermediarios creíbles cuyo único objetivo se oriente al derecho del ciudadano y la sociedad en su conjunto a recibir información veraz.

Medios de comunicación, periodistas y directores de comunicación -como organizaciones y profesionales- con suficiente formación, pericia, habilidades comunicativas probadas y sobre todo con una identificación deontológica profunda y responsabilidad jurídica plena, se hacen totalmente indispensables en la lucha eficaz contra la desinformación.

Son muchos los factores que han contribuido a la eclosión de la mentira como arma política, económica y militar, utilizada para radicalizar, polarizar y socavar los valores de las democracias. Nos fijaremos aquí en uno que afecta de lleno a periodistas, medios y departamentos y directores de comunicación. Hablamos del fin de la intermediación periodística, proclamado por algunos hace no tantos años como la clave para alcanzar el sueño de la democracia real. Ejercida tradicionalmente por los medios de comunicación en colaboración con los departamentos de comunicación, la citada intermediación ha sido demonizada, pero hoy, una década después, es reivindicada como esencial. ¿Qué ha sucedido para este cambio de percepción sobre el valor y la función de los medios de comunicación tradicionales y los también tradicionales departamentos de comunicación públicos y privados?

El advenimiento del llamado "periodismo ciudadano", del que se dijo que iba a acabar con la dependencia de los medios de comunicación como intermediarios necesarios para llegar a grandes audiencias, ha llenado las redes sociales de engaños, bulos e invenciones, extendidos sin control por un ejército anónimo de constructores de mentiras con intereses ocultos. En el mejor de los casos ese "periodismo ciudadano" es apenas "periodismo aficionado" sin contexto ni contraste, carente de las obligaciones deontológicas y profesionales de los periodistas en ejercicio. En los casos más extremos ha sido utilizado como coartada por profesionales del odio y la mentira, ayudados por *bots* y cuentas falsas, que ejercen su actividad con alto grado de impunidad, favorecida por la ausencia de una regulación que les haga efectivamente responsables de los daños originados por la desinformación difundida.

Respecto a la percepción de la ciudadanía sobre los medios de comunicación, los periodistas que en ellos trabajan y su utilidad como fuente acreditada y solvente en este desigual combate, valgan estos datos extraídos del I Estudio sobre desinformación de la Unión de Televisiones Comerciales en Abierto (UTECA) y la Universidad de Navarra (UTECA & Universidad de Navarra, 2022), de junio de 2022. Un 84,6% de los encuestados indicó que prefiere informarse por los medios de comunicación frente a las

redes sociales por contar con equipos profesionales de periodistas que verifican, contrastan y analizan las informaciones. Asimismo, para el 80,1% prensa, radio y televisión son la mejor garantía frente a la proliferación de la desinformación.

Aun así, el 88,1% admite que las personas tienden a creer más aquellos mensajes recibidos que coinciden con su forma de pensar. Sobre la importancia que otorgan a los medios de comunicación, al ser preguntados sobre cómo combatir la difusión de la desinformación, la primera opción, respondida por un 53,4%, es evitar el reenvío de mensajes anónimos; en segunda posición (un 43,4%) citan informarse por televisión, prensa y radio para evitar ser engañados. De los datos del citado barómetro cabe deducir que la ciudadanía aprecia la existencia de medios de comunicación y periodistas que ofrecen autoridad, jerarquía informativa, veracidad y contexto, bajo los principios deontológicos de organizaciones profesionales responsables y transparentes.

Sabido es que la mentira se extiende con mayor rapidez, pues la ausencia de rigor la hace más ligera. Ante esta realidad, medios y directores de comunicación están llamados a actuar como muro de contención, sirviéndose del rigor, la veracidad, el contraste y la responsabilidad para revalidar cada día su condición de fuente autorizada y referencial.

Medios de comunicación, periodistas y directores de comunicación han de contribuir a democracias sólidas en las que se respete la verdad. El ejercicio responsable de su función es elemento fundamental que los distingue de los desinformadores.

Fomentar una sociedad plural, desde los distintos ámbitos de actuación institucional, pública o privada, es también una forma de combatir la desinformación en lo que compete a su objetivo de lograr una uniformidad de pensamiento.

El compromiso ético y la responsabilidad jurídica de los medios de comunicación y las direcciones de comunicación son asimismo determinantes contra la desinformación.

En momentos como los actuales, es especialmente relevante la actuación de los profesionales de la información conforme a los más elevados estándares éticos de su profesión, contrastando las informaciones antes de su publicación e identificando siempre a quien asume la información difundida bajo su marca informativa. No obstante, medios de comunicación, periodistas y directores de comunicación no están exentos de cometer errores en su ejercicio diario. Cuando sucede, disponen de protocolos internos para responder con profesionalidad, transparencia y eficacia, aplicando los códigos deontológicos propios del ejercicio profesional del periodismo y la comunicación corporativa. Asimismo, las personas naturales o jurídicas que se sientan afectadas por la información publicada por un medio de comunicación tienen la capacidad de ejercer frente al medio en cuestión su derecho de rectificación, al amparo de lo previsto en la Ley Orgánica 2/1984 reguladora del Derecho de Rectificación, estando obligado el medio de comunicación a publicar esta rectificación. Este derecho no asiste a las personas físicas o jurídicas frente a la información difundida por redes sociales.

Precisamente para ahondar en esta autoexigencia de responsabilidad, existe un rico tejido asociativo profesional, donde se reflexiona y comparten buenas prácticas de manera constante. Ejemplo de este compromiso es el documento, de abril de 2021, “Periodistas y directores de comunicación. Un compromiso ético para el futuro”[1], firmado por FAPE, APM, APIE y DIRCOM. Igualmente existen libros de estilos y códigos deontológicos en numerosos medios de comunicación, de obligado seguimiento para sus periodistas. En el ámbito nacional, el código deontológico de la FAPE es un compendio de buenas prácticas para los miembros de las asociaciones de la prensa de España.

---

[1] Disponible en: https://www.dircom.org/wp-content/uploads/2022/01/Documento_Buenas-Practicas_ES_DBPPD.pdf

VALORES, HERRAMIENTAS Y PROCEDIMIENTOS DE LOS MEDIOS DE COMUNICACIÓN ANTE LA PROLIFERACIÓN DE LA DESINFORMACIÓN

Los medios de comunicación son un instrumento eficaz y central en el combate contra la extensión de la desinformación, tanto por su condición de organizaciones profesionales y jerarquizadas de periodistas como por estar dotados de controles editoriales internos y asumir la responsabilidad sobre sus contenidos y ante la sociedad en la que operan. En un mundo en el que muchos actores buscan extender la desconfianza y la confusión, los medios de comunicación ofrecen contexto, contraste, análisis y autoría.

La verificación en fuentes acreditadas es consustancial al oficio del periodismo. Ese modo de actuar está recogido en los códigos deontológicos de las asociaciones del sector, así como en los manuales de estilo, buenas prácticas y protocolos y procedimientos internos de medios públicos y privados.

Entre sus valores más apreciados se encuentra la propia marca periodística y la reputación asociada, que convierten a los medios en la fuente principal a la que recurre la ciudadanía cuando desea contrastar la veracidad de un mensaje de actualidad recibido por otros canales (UTECA y Universidad de Navarra, 2022).

Ese valor de la marca se complementa, crece y reafirma con el valor de la firma. Al contrario de lo que sucede con los bulos y falsedades que circulan con impunidad y de forma anónima por las redes sociales y servicios de mensajería instantánea, los medios reivindican la autoría de los contenidos que difunden bajo el poder prescriptor de la marca y la firma de sus informaciones. Estos elementos otorgan a la información difundida la garantía de credibilidad de la que otros soportes carecen.

En cuanto a la organización del trabajo, son entidades responsables, que ejercen un control editorial interno de las publicaciones para garantizar —más allá de errores puntuales— la veracidad e idoneidad de los contenidos a difundir, excluyendo aquellos que fomentan el odio o la violencia. Asimismo, jerarquizan las informaciones, siguiendo criterios profesionales desde el pluralismo y la diversidad de enfoques.

Ante las campañas interesadas que desacreditan como desinformación cualquier opinión difundida públicamente contraria a una determinada forma de pensar, es recomendable que las acciones de alfabetización mediática incidan en la diferencia entre opinión y desinformación, siendo ésta la divulgación premeditada de falsedades con el fin de perjudicar a un tercero. Si la opinión de parte está sustentada sobre un hecho o dato cierto, no puede ser descalificada como desinformación. Disentir de una opinión forma parte de la libertad de expresión; señalar una opinión como desinformación contribuye a fomentar la confusión y la desconfianza hacia los medios. La diversidad de opiniones y enfoques sobre un mismo hecho cierto enriquece el debate y es ejemplo de pluralismo mediático y social.

Los medios de comunicación se enfrentan a desafíos constantes y a tentaciones a las que no deben sucumbir. En la nueva era de la Inteligencia Artificial, será preciso extremar los controles internos y el recurso a fuentes acreditadas y de confianza, además de una formación y permanente actualización de conocimientos técnicos para discernir lo auténtico en medio del aluvión de imágenes falsas técnicamente perfectas.

VALORES, HERRAMIENTAS Y PROCEDIMIENTOS DE LAS DIRECCIONES DE COMUNICACIÓN DE LOS ÁMBITOS PÚBLICO Y PRIVADO

Los directores y las directoras de comunicación de empresas e instituciones, como cabeza visible de los departamentos de comunicación, son en estos momentos uno de los principales instrumentos para luchar contra la desinformación. Su figura se identifica con la conciencia social de su organización y asume el compromiso de su responsabilidad con toda la sociedad, porque su primera y principal responsabilidad social corporativa está relacionada precisamente con la veracidad de sus mensajes.

Son los periodistas los principales responsables de la verificación de la verdad, y en lo que dicha verdad tiene que ver con las organizaciones, públicas o privadas, el director de comunicación es también un transmisor profesional de información veraz (fundamental para los medios de comunicación) desde una perspectiva de parte o fuente. Su propósito es servir de contrapunto garantizador en esa realidad compleja de la información pública, con la aceptación del nuevo concepto teórico de "periodismo de fuente" (Fernández del Moral, 2020) como instrumento al servicio del director de comunicación que resulta estratégico a la hora de garantizar la veracidad de las informaciones difundidas desde el departamento de comunicación.

Precisamente por su capacidad de enlazar a los medios con las fuentes, y de generar y/o trasladar información de agentes sociales tan importantes como las empresas o las instituciones, el director o directora de comunicación tiene un papel estratégico en las organizaciones, y por tanto debe formar parte de la alta dirección de su organización y sus órganos decisorios (comité de dirección o similar).

Empresas e instituciones deben regir sus políticas de comunicación con criterios de veracidad, comprensión y claridad en la información que facilitan a los medios, sus clientes y la sociedad en general. Las direcciones de comunicación también tienen sus compromisos éticos en su relación con los grupos de interés y deben abstenerse de fomentar, financiar o primar medios, redes o perfiles que fomenten la desinformación. Al igual que los medios de comunicación, son responsables de las informaciones "de parte" transmitidas a medios y periodistas, ya sea en versión "off the record" (no atribuible) o para su publicación.

MEDIOS DE COMUNICACIÓN Y DEPARTAMENTOS DE COMUNICACIÓN, UNA INTERACCIÓN NECESARIA

La relación y comunicación fluida de medios y periodistas con directores y departamentos de comunicación es una práctica que ayuda a desmontar bulos y mentiras, de la que se beneficia la sociedad en su conjunto, pues amplía la eficacia del combate contra la desinformación.

Los medios de comunicación son soportes informativos muy apreciados por empresas e instituciones como intermediarios necesarios para su comunicación con la sociedad, por tratarse de organizaciones profesionales de periodistas con responsabilidad editorial, que contrastan, verifican y disponen de mecanismos de rectificación si publican informaciones erróneas.

Igualmente, las direcciones de comunicación son utilizadas por los medios de comunicación como fuente de información confiable, responsable y transparente.

La obligación y el compromiso de los medios de comunicación y periodistas de contrastar y verificar las informaciones antes de su difusión ha de tener su justa correspondencia en la respuesta ágil y veraz del director de comunicación, siempre bajo el respeto a la autonomía y criterios profesionales de las partes.

En su relación con medios y periodistas, los directores de comunicación ejercen funciones de "periodismo de fuente", suministradores autorizados de una información clave y veraz para frenar campañas orquestadas de desinformación contra empresas e instituciones que buscan generar desconfianza, daños reputacionales y económicos.

Para los medios de comunicación, los departamentos y directores de comunicación son una fuente fundamental para la confirmación de la veracidad de informaciones, mensajes e imágenes anónimas viralizados por internet que, en muchas ocasiones, circulan con apariencia de veracidad. Asimismo, facilitan a los medios el contacto con expertos de reconocido prestigio y credibilidad en materias muy diversas, en las que la necesidad de testimonios con conocimiento, autoridad y confianza son fundamentales para contrarrestar desinformaciones que pueden afectar a materias tan sensibles como la seguridad nacional, la salud, la economía o las relaciones internacionales, entre otras.

Estamos, pues, ante una interacción, ayudada por un ejercicio profesional honesto y autocrítico, que contribuye a una sociedad mejor informada y, por tanto, más preparada para enfrentarse con criterio a las falsedades y bulos que circulan sin control por internet.

En definitiva, la defensa de la verdad pasa por una estrecha colaboración entre los profesionales de los medios y la comunicación institucional y corporativa, que ejercen una función social insustituible.

LA COMUNICACIÓN COMO BARRERA CONTRA LA DESINFORMACIÓN EN SITUACIONES DE CRISIS

En un entorno marcado por la saturación de información, las situaciones de crisis se han integrado como parte de nuestra cotidianidad, con todas las implicaciones que ello conlleva. La desinformación, que en situaciones comunes ya plantea un desafío significativo, se intensifica de manera exponencial en estos escenarios. Una crisis, caracterizada por la incertidumbre y la urgencia, genera un contexto en el que la toma de decisiones debe realizarse con rapidez y precisión. Los mensajes se difunden a gran velocidad, las expectativas de las audiencias se multiplican y la información disponible es limitada.

Uno de los aspectos más destacados de los profesionales de la comunicación en estos escenarios es su capacidad para responder con agilidad y eficacia. Los directores de comunicación están entrenados para gestionar situaciones de crisis en tiempo récord, tomando decisiones informadas incluso cuando la información es escasa. Esta agilidad es fundamental para mitigar los efectos negativos que la desinformación puede tener en un entorno de crisis. A pesar de la falta de información completa, no se puede dejar de responder a las preguntas ni de mantener el pacto implícito con las audiencias. Esto genera expectativas que, junto con las presiones inherentes a la situación, deben ser gestionadas correctamente.

A menudo, las crisis exceden el ámbito de una sola empresa o institución, lo que requiere un enfoque colaborativo y cooperativo con diversos *stakeholders*. En escenarios donde la desinformación prevalece y se manifiesta de manera recurrente, los directores de comunicación deben priorizar el fortalecimiento de sus vínculos con los medios de comunicación como primer punto de acción. La creación de confianza mutua es esencial para garantizar que la información distribuida cumple con los controles de calidad y los estándares profesionales adecuados.

La colaboración público-privada adquiere un papel fundamental en la gestión eficaz de crisis. Es crucial contar con mecanismos de coordinación que estén casi automatizados, permitiendo que, cuando se detecte una crisis, la información se comparta rápidamente entre las partes involucradas. Esto incluye a organismos públicos y privados que deben trabajar de manera conjunta para responder a las amenazas de manera más eficiente. Un ejemplo de esta colaboración exitosa es la creación de una cultura en las empresas, donde los incidentes críticos, como los ciberataques, no se esconden, sino que se reportan inmediatamente a las autoridades competentes. Este proceso de reporte inmediato y la instalación de sistemas de detección temprana, como balizas en servidores, permite que las amenazas sean identificadas rápidamente, beneficiando tanto a la organización afectada como al sistema de seguridad nacional en su conjunto.

Esta colaboración también implica una cierta cesión de soberanía por parte de las empresas, permitiendo que las autoridades instalen herramientas de monitoreo en sus sistemas. A cambio, estas organizaciones reciben alertas tempranas y protección adicional. No se trata solo de buscar ayuda cuando surge una crisis, sino de construir redes de colaboración sistémica que funcionen como una red de seguridad estructural. Es, en esencia, como crear un “ejército en la sombra,” que, aunque no esté activado constantemente, está preparado para responder de manera cohesionada y eficiente cuando se requiere.

Las autoridades públicas desempeñan un papel crucial en la gestión de crisis. Mantener relaciones institucionales estables con las administraciones públicas es vital para abordar cualquier duda

sobre la información que se recibe o se distribuye. Esto es especialmente relevante para las empresas internacionalizadas que deben desarrollar vínculos sólidos con oficinas diplomáticas, embajadas y consulados. Asimismo, es fundamental fomentar relaciones profesionales y sólidas con los departamentos de Asuntos Exteriores, los servicios de inteligencia y otros organismos gubernamentales.

La tecnología, que en muchos casos se ha considerado un aliado en la comunicación y la gestión de información, también puede convertirse en un elemento contraproducente, especialmente en el contexto de la desinformación. La pérdida de credibilidad de instituciones, empresas e incluso ONGs es un fenómeno creciente en la sociedad civil (Edelman, 2023) y, frente a estos desafíos, contamos con muy pocas herramientas efectivas.

Por ello, la gestión de crisis implica una anticipación mediante la escucha social, la inteligencia contextual y la prevención con sistemas preestablecidos. Estos incluyen simulacros, actualización de procedimientos de crisis y protocolos, entrenamiento permanente y diálogo constante con los indicadores que pueden ayudar a identificar crisis.

Una de las claves para ejecutar una gestión de crisis eficaz es haber establecido previamente los canales de comunicación adecuados y mantener una relación activa con los diversos públicos involucrados. Esto requiere tener canales de comunicación propios operativos. Es decir, debemos contar con canales alternativos listos para entrar en funcionamiento en caso de que los sistemas principales fallen. Esta previsión garantiza que la comunicación fluya ininterrumpidamente, permitiendo a la organización responder con agilidad y mantener la confianza del público incluso en los momentos más críticos.

Otro aspecto crucial en la gestión de crisis es la importancia de comprender la psicología de masas y aplicar conocimientos sociológicos para responder a los mecanismos de desinformación. Las empresas, debido a su constante investigación del consumidor y detección de tendencias, tienen una ventaja significativa. Han sido capaces de identificar preocupaciones emergentes como el ecologismo, la economía circular, las fibras textiles naturales o el turismo sostenible antes que muchos otros actores. Sin embargo, no se está utilizando este análisis de tendencias para anticipar desinformación o percepciones erróneas que puedan instalarse en la mente de los consumidores, quienes son simultáneamente votantes y ciudadanos. Las empresas pueden ser aliadas cruciales en la gestión de crisis y en la anticipación de posibles crisis, gracias a su capacidad de escucha permanente del consumidor a través de estudios de opinión, estudios de mercado y análisis de tendencias de consumo.

Además, estos agentes tienen diversas maneras de comunicarse con los consumidores, como la publicidad, las relaciones públicas y la comunicación a través de *influencers*. Estas capacidades pueden ser aprovechadas para trasladar mensajes importantes a la sociedad, convirtiéndose en un apoyo valioso en la lucha contra la desinformación.

En situaciones de crisis, además de las encuestas tradicionales, es vital considerar el análisis del sentimiento en redes sociales. Este sentimiento en línea, sin embargo, no siempre refleja la realidad. Con frecuencia, está distorsionado por campañas orquestadas que utilizan *bots* y la influencia de líderes de opinión, quienes a veces no son representativos de la opinión pública auténtica. Por ello, es esencial desarrollar y aplicar mecanismos que permitan distinguir entre líderes de opinión genuinos y aquellos que son más artificiales, menos espontáneos o auténticos. Los profesionales de la comunicación están constantemente evaluando la fiabilidad de las fuentes de información, una tarea que se vuelve cada vez más crucial en un entorno digital donde muchos aceptan como verdad lo que leen en internet sin cuestionarlo.

Es igualmente importante reconocer que incluso entre las fuentes consideradas fiables, siempre existe la posibilidad de que alguien esté intentando manipular la información para su beneficio propio. En todos los fenómenos de desinformación a los que nos enfrentamos, debemos entender que la desinformación

puede provenir de cualquier lado. No existen actores totalmente buenos o malos; la desinformación es una herramienta utilizada por diferentes entidades, independientemente de su alineación geopolítica. A veces, esta desinformación es estructural y forma parte de una estrategia consciente. En determinados contextos, puede darse el caso de que una sociedad en su conjunto, incluyendo a los comunicadores, se convierta en parte activa de una campaña de desinformación, contribuyendo a la creación y perpetuación de una narrativa falsa que se integra en la cosmovisión de la comunidad.

Cuando la desinformación se vuelve estructural y es adoptada por la sociedad, esta puede llegar a contribuir activamente a su propagación porque encaja con ciertos intereses o creencias preexistentes. En estos casos, la desinformación no solo se convierte en una herramienta para influir en la opinión pública, sino en un virus que transforma la percepción de la realidad para grandes sectores de la población. Este fenómeno es especialmente peligroso cuando la desinformación se relaciona con cuestiones de identidad, como raza, género o religión. Cuando una sociedad entera adopta y hace suya la desinformación, el éxito de esta se vuelve profundo y duradero, con consecuencias significativas para el progreso social y económico.

Un punto clave en la gestión de crisis es la capacidad que tiene una sociedad para unirse en torno a una visión común del conflicto. Sin embargo, esta cohesión se da en muy pocas áreas. En muchos temas, como la inmigración o ciertos desafíos sociales, las sociedades están divididas, y no existe esa sensación de peligro compartido que une a todos bajo un mismo objetivo. En sociedades donde se vive permanentemente en un estado de crisis, la percepción de amenaza es constante, lo que genera una cohesión interna fuerte. En cambio, en sociedades más estables y prósperas, donde la normalidad fluye sin interrupciones significativas, esta sensación de unidad y enfoque compartido se diluye, lo que puede debilitar la respuesta colectiva ante crisis graves.

Para complementar estos esfuerzos en la gestión de la desinformación, tanto en situaciones de crisis como en el día a día, es importante considerar la creación de un cuerpo profesional de técnicos de comunicación del Estado.

Estos profesionales, formados en técnicas avanzadas de comunicación y en la lucha contra la desinformación, desempeñarían un papel crucial tanto en la comunicación exterior, a través de servicios diplomáticos y embajadas, como en la administración pública a nivel estatal y local, abarcando ministerios, diputaciones y corporaciones locales. Contar con un cuerpo del Estado especializado en comunicación permitiría no solo una gestión más eficaz de los contenidos comunicativos, sino también una respuesta rápida y coordinada ante amenazas de desinformación o campañas de injerencia.

La formación de estos técnicos podría realizarse mediante habilitaciones específicas o a través de mecanismos de oposición, garantizando así una base sólida de profesionales que comparten conocimientos, técnicas y un enfoque común en la gestión de la comunicación pública. Esta estructura capilar permitiría la actualización constante de los profesionales, facilitando la transmisión de recomendaciones precisas en situaciones de crisis.

Integrar a estos técnicos de comunicación del Estado en una red más amplia, que incluya a comunicadores del sector privado y del tercer sector, crearía una malla de profesionales capaz de frenar eficazmente bulos, manipulación informativa y otras formas de desinformación. Esta red cohesionada y proactiva serviría como una barrera protectora frente a la manipulación informativa, contribuyendo significativamente a la estabilidad y la confianza en las instituciones públicas y privadas.

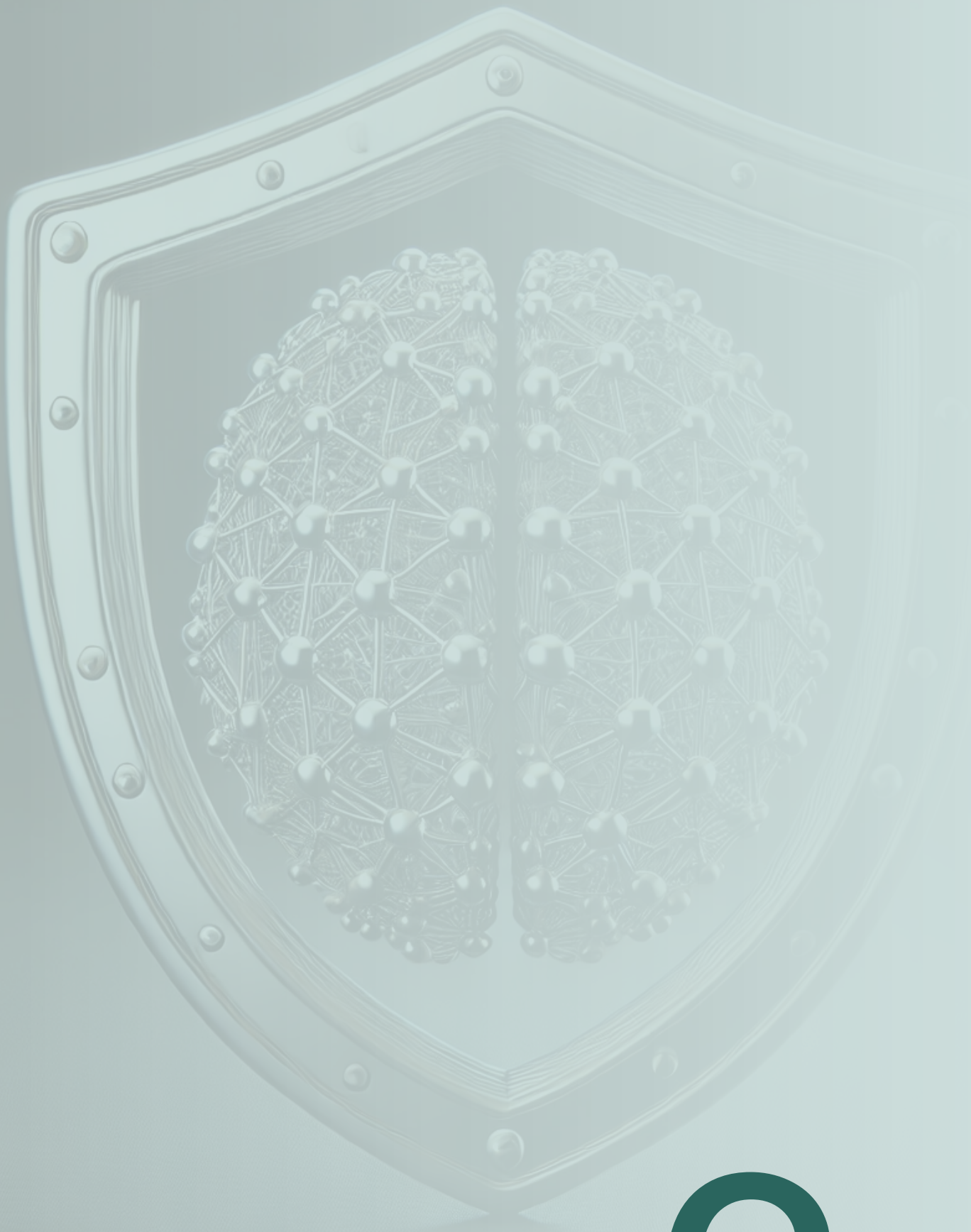
REFERENCIAS BIBLIOGRÁFICAS

Desantes Guanter, J. (1997). Fundamentos del Derecho de la información. Madrid: Confederación Española de Cajas de Ahorro.

Edelman. (2023). Edelman Trust Barometer: Global Report. Obtenido de https://www.edelman.com/sites/g/files/aatuss191/files/2023-03/2023%20Edelman%20Trust%20Barometer%20Global%20Report%20FINAL.pdf

Fernández del Moral, J.-V. (2020). Periodismo de fuente. En J. Villafañe, Diccionario de la reputación y de los intangibles empresariales. Madrid: Villafañe y As.

UTECA, y Universidad de Navarra. (2022). I Estudio sobre la desinformación en España. Obtenido de https://uteca.tv/wp-content/uploads/2022/06/INFORME-SOBRE-I-ESTUDIO-DES-INFORMACION-ESPANA-DE-UTECA-Y-LA-UNIVERSIDAD-DE-NAVARRA-a.pdf



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.

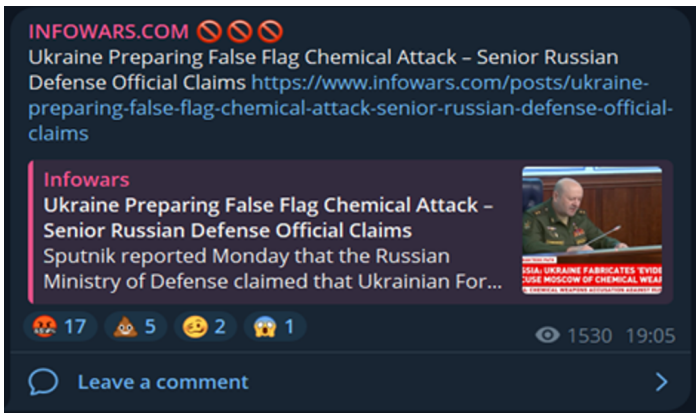
y cuándo poner el esfuerzo económico, sin realmente descartar ninguna de las opciones. Esta estrategia claramente se contrapone a la de otros países incluidos dentro de este estudio, que cuentan con situaciones diferentes a la de Rusia. Podríamos compararlo con el caso de Venezuela, que cuenta con menos 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.

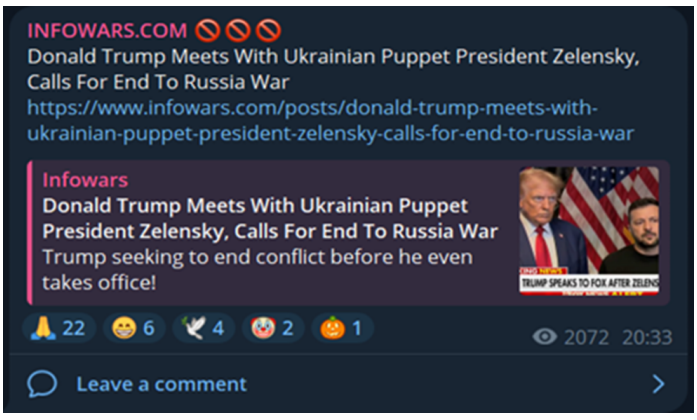
¿Acción directa o a través de terceros?

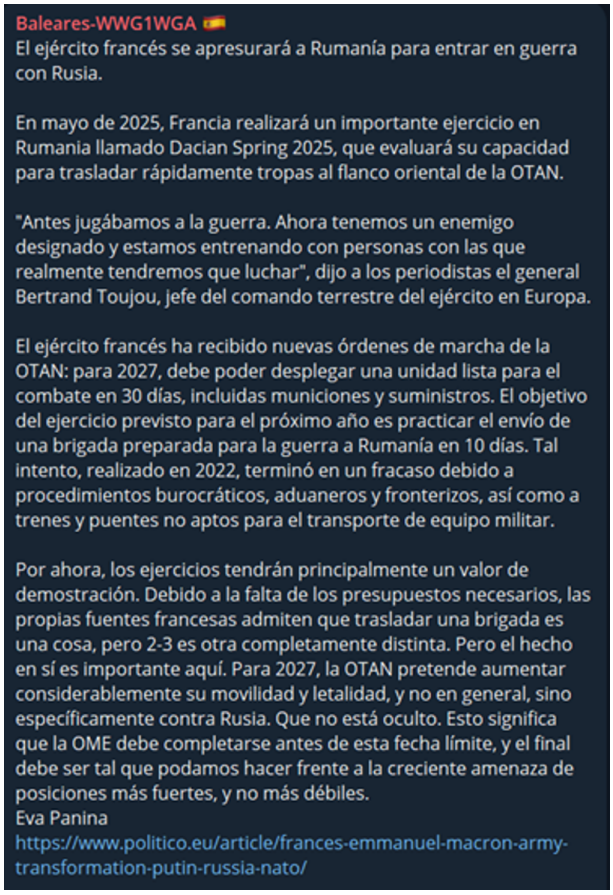
Dentro de las 55 TTP identificadas para el estudio, se han evaluado si Rusia, de acuerdo a las acciones pasadas identificadas bajo su autoría en investigaciones ya publicadas como las ya mencionadas y otras como RNN (VIGINUM, 2023) y Matriochka (VIGINUM, 2024b), la investigación Roller Coaster del medio 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:

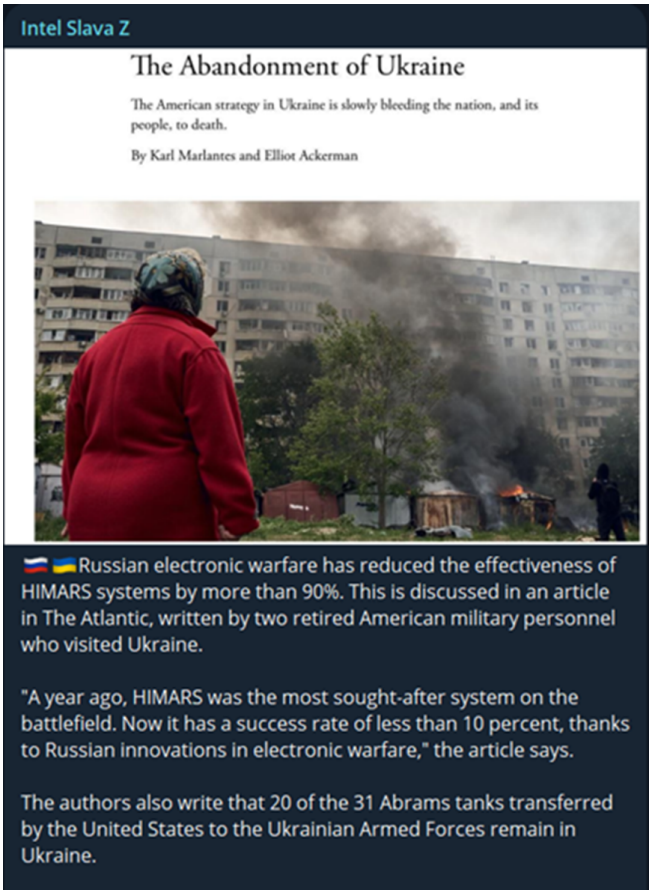
- Aprovechar narrativas basadas en teorías de conspiración (T0022). Por ejemplo, pieza informativa publicada en 2023 por la agencia estatal rusa Sputnik (Sputnik, 2023).

- 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).

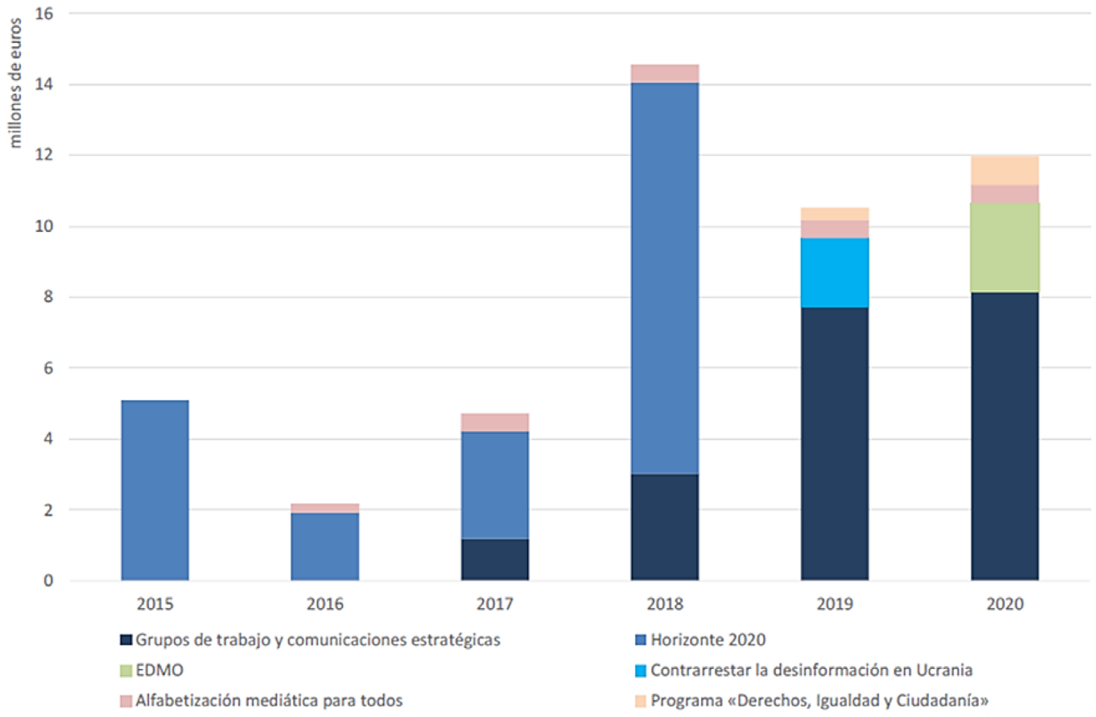
Como decimos, las informaciones manipuladas influyen en la percepción pública y pueden alterar el entorno económico, afectando decisiones de inversión y el consumo, especialmente en tiempos de elecciones o crisis políticas (Fake News and its Impact on the Economy, 2020). Todo ello sin tener en cuenta 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.

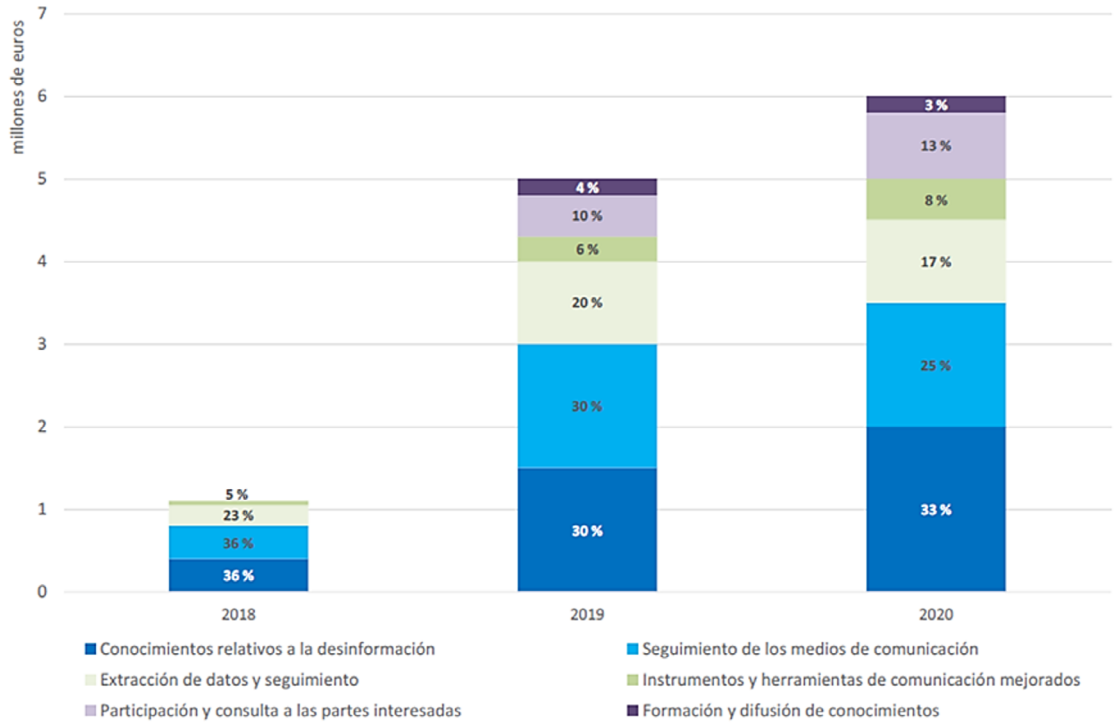
El Informe Especial del Tribunal de Cuentas Europeo (2021), recoge algunos datos especialmente significativos en relación con los esfuerzos económicos que viene acometiendo la Unión Europea para contrarrestar las campañas de desinformación.



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.

Evaluación de proyectos contra la desinformación (proyectos piloto, acciones preparatorias, Horizonte 2020)
(Fuente: Tribunal de Cuentas Europeo)

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/

CAPÍTULO 4

INGENIERÍA DE LA DESINFORMACIÓN: INFRAESTRUCTURA TECNOLÓGICA DE LAS OPERACIONES DIGITALES EN CAMPAÑAS DE MANIPULACIÓN

Coordinadores:

Fran Casino

Ministerio del Interior – Oficina de Coordinación de Ciberseguridad (OCC)

Autores y colaboradores:

Marc Almeida Ros

David Arroyo Guardeño

Ivan Homoliak

Andrés Marín López

Rafael Mata Milla

Constantinos Patsakis

Oscar Walsch

INTRODUCCIÓN

El capítulo tendrá por objeto realizar un doble ejercicio de trasvase de conocimiento involucrando tres dominios que, si bien tienen características específicas, en la actualidad suelen aparecer combinados en el contexto concreto de las operaciones de influencia y en campañas de manipulación. En efecto, tal y como se pone de relieve en (Gioe y Smith, 2024, capítulo 8), elementos de desestabilización desde la esfera cibernética pueden aprovechar situaciones de conflicto o violencia para amplificar sus efectos, de forma que la interrelación entre ciberespionaje, cibercrimen y la ciberguerra es cada día más patente (Shapiro, 2023).

En este capítulo analizaremos las fases de la denominada *killchain* según define Mitre para el caso de las *Advanced Persistent Threats* (APT). Dicho análisis estar a acompañado de una evaluación a alto nivel de los diferentes estadios vinculados a *Advanced Persistent Manipulations* (APM). Se establecerá una relación entre el dominio cibernético de las APT y el informacional de las APM. Tal relación se llevará a término poniendo de relieve tanto elementos de infraestructura de redes como servicios de internet empleados para diseñar y ejecutar ataques de desinformación contra objetivos específicos. El enfoque adoptado en el capítulo pretende aplicar el conjunto de lecciones aprendidas en el caso de la ciberseguridad al dominio FIMI (*Foreign Information Manipulation and Interference*), evaluando a través de las diversas tecnologías y procedimientos cómo se diseñan estrategias, tácticas y operaciones contra objetivos concretos en base a su matriz de vulnerabilidades. Dichas vulnerabilidades engloban no sólo aspectos tecnológicos (Mirza et al., 2023), sino que también incluyen el conjunto de elementos psico-sociales que hacen más plausible emplear narrativas concretas contra una sociedad o segmento social específico.

A lo largo del capítulo la caracterización de herramientas, servicios y plataformas pondrá de relieve el carácter dual del ecosistema digital. Así, herramientas que en primera instancia son diseñadas para proteger la privacidad de los usuarios al navegar en Internet se constituyen en piezas clave de las estrategias de atacantes en operaciones de información de cara a bien desplegar ofensivas bajo falsa bandera, bien simplemente para dificultar por parte de los objetivos una posterior "ciberatribución". Ésta será dependiente de la capacidad de extraer indicadores y entidades a partir de trazas de sistemas, monitorización de redes y de información en foros en abierto, pero también en la *Deep Web* y la *Darknet*. La conexión entre actores, entre actores y medios, y entre actores e intenciones nos permitirá tanto comprender fenómenos FIMI como anticiparlos. De esta forma, en el capítulo se contextualizarán el conjunto de herramientas, servicios y estándares para relacionar conexiones casuales entre los diversos elementos del ecosistema FIMI y el uso de elementos y técnicas de infraestructura de red.

RELACIÓN ENTRE LOS ATAQUES INFORMACIONALES Y LAS ESTRATEGIAS AVANZADAS DE CIBERATAQUE

La denominada cadena de ataque o *killchain* describe las distintas fases de ataque de APT de acuerdo con el paradigma definido por MITRE ATT&ACK (Strom et al., 2018). Los ataques APT que cuentan con clara y definida esponsorización por parte de estados suelen estar combinados con estrategias híbridas de desestabilización. Así, las fases de exfiltración de información en la cadena de ataque de APT puede nutrir la configuración de las fases de selección de objetivos y de elección de medios y herramientas para desplegar operaciones de influencia y manipulación (Ahmad et al., 2019). En este sentido, cabe destacar el carácter crítico de toda brecha de datos, en especial aquellas que afectan a datos personales que habilitan el perfilado de ciudadanos (The UN Report on Disinformation: a role for privacy, 2021). Dicho perfilado es una información de gran relevancia en la configuración de ataques de ingeniería social y en la fabricación de contenidos viralizantes y que aprovechen sesgos, preferencias y vulnerabilidades psico-sociales de potenciales objetivos (Shapiro, 2023).

A continuación, analizaremos en detalle la relación entre los diversos componentes y elementos del ecosistema del *malware* de los cuales se nutren tantos las APT como las acciones de influencia en el ámbito FIMI. Para ello emplearemos como referencia el esquema de la Figura 1, detallando el nivel de criticidad del mercado de datos y de herramientas en la *Dark Web* (*Dark Web Marketplace*, DWM), el acceso y uso de software malicioso y de paquetes de utilidades para realizar phishing (*PhaaS*, *Phishing as a Service*) y ataques de ingeniería social. Además, se pondrá de relieve el carácter dual de tecnologías como la inteligencia artificial (*Malicious AI Generated Content*, MAIGC) y las fuentes abiertas de inteligencia (*Open source Intelligence*, OSINT).

Reconocimiento	OSINT
Ingeniería social	MAIGC
Despliegue inicial	PHAAS
Movimiento lateral	MAAS
Cifrado y exfiltración	RAAS
Recolección y secuestro	DWM

Figura 1: Estructura integral de las APT

MALWARE COMO SERVICIO (MaaS)

El uso instrumental de información y de software por parte de agentes extranjeros constituye un elemento cada vez más presente en el denominado fenómeno FIMI. El análisis en profundidad de incidentes como la inestabilidad provocada por los servicios de inteligencia rusos en 2019 en Georgia (Greenberg, 2020) pone de relieve estrategias complejas de ataque que combinan el uso de software malicioso y operaciones de influencia e información.

La configuración del dominio cruzado entre lo cibernético (los bits) y lo informacional (los bytes) queda claramente patente en la estrategia y operativa de ataque puesta en marcha desde 2006 por Rusia en Georgia (Beehner et al., 2018), siendo especialmente significativa toda la dinámica de generación y distribución de software malicioso o *malware* a partir del dominio StopGeorgia.ru.

"La configuración del dominio cruzado entre lo cibernético (los bits) y lo informacional (los bytes) queda claramente patente en la estrategia y operativa de ataque puesta en marcha desde 2006 por Rusia en Georgia"

El *malware* es una amenaza crítica para las organizaciones y las personas en todo el mundo. En las últimas décadas, hemos sido testigos de la evolución del *malware* desde simples programas diseñados para causar disrupciones menores, hasta convertirse en herramientas sofisticadas empleadas en operaciones de cibercrimen altamente organizadas. En este contexto, el *MaaS* ha emergido como un modelo de negocio lucrativo que facilita a los delincuentes cibernéticos el acceso a herramientas de ataque complejas sin necesidad de poseer habilidades técnicas avanzadas (Patsakis et al., 2024). En el contexto específico de FIMI, hay que tener en cuenta los servicios y proveedores del ecosistema de producción y distribución de *malware* como potenciales *proxies* para diseñar, desplegar y coordinar estrategias combinadas de desestabilización de un adversario (Borghard y Lonergan, 2016a). Es aquí donde el *MaaS* adquiere relevancia significativa e importancia creciente, siendo de especial importancia la dificultad creciente de realizar atribución y actividad FIMI y de evitar ser víctimas de ataques de falsa bandera (Skopik y Pahi, 2020).

El *MaaS* es un modelo de negocio en el que desarrolladores de *malware* ofrecen sus herramientas y servicios a otros delincuentes a cambio de un pago, generalmente en forma de criptomonedas para mantener el anonimato (Casino et al., 2021). Este modelo opera de manera similar al Software como Servicio (*SaaS*) en la industria legítima, donde los usuarios pue-den suscribirse o alquilar software sin necesidad de gestionarlo o desarrollarlo por sí mismos. En el caso de *MaaS*, los "clientes" son delincuentes que desean ejecutar ataques cibernéticos, pero carecen de las habilidades técnicas necesarias para desarrollar *malware* por su cuenta. Al ofrecer servicios como kits de *malware*, infraestructura de comando y control (C&C por sus siglas en inglés), servicios de ofuscación y evasión, y soporte técnico, el *MaaS* ha democratizado el acceso al cibercrimen, haciéndolo más accesible y rentable para una amplia gama de actores (Davidson, 2021), incluyendo aquellos que directamente o indirectamente participan en FIMI (Borghard y Lonergan, 2016a).

De cara a realizar la correcta conexión entre estrategias combinadas de acción informacional y cibernética en FIMI partiremos de marcos de referencia basados en estándares como DAD-CDM[1] y otras iniciativas encuadradas dentro de la plataforma OASIS[2]. La adecuada articulación de los

1 https://dad-cdm.org/
2 https://www.oasis-open.org/

estándares definidos en el marco de OASIS permite crear grafos de relaciones entre actores y entre actores y acciones, lo que habilita el análisis de causalidad y/o ciberatribución. A continuación, describimos en detalle los componentes, actores y funcionamiento de *MaaS*.

Componentes del MaaS

El ecosistema de *MaaS* está compuesto por varios componentes clave que facilitan la operación y éxito de este modelo de negocio:

- **Kits de *Malware***: Estos son paquetes de software que contienen todo lo necesario para ejecutar un ataque. Los kits de *malware* suelen incluir el código malicioso, instrucciones detalladas sobre cómo utilizarlo, y en algunos casos, herramientas adicionales como *exploit kits* o *loaders* que ayudan a distribuir el *malware*. Estos kits están diseñados para ser fáciles de usar, permitiendo que incluso aquellos con poca experiencia técnica puedan ejecutar ataques efectivos (Meland, et al., 2020).

- **Infraestructura de C&C**: La infraestructura de C&C es esencial para la mayoría de los tipos de *malware*, especialmente aquellos que requieren comunicación continua con el atacante. Los servidores de C&C permiten a los atacantes gestionar de manera remota las máquinas infectadas, enviar comandos, exfiltrar datos y actualizar el *malware* en respuesta a nuevas medidas de seguridad. Los proveedores de *MaaS* suelen ofrecer acceso a servidores de C&C como parte de su paquete, lo que facilita la gestión y control de las campañas de *malware* (Huang, et al., 2018).

- **Servicios de ofuscación y evasión**: Para que el *malware* sea efectivo, debe ser capaz de evadir la detección por parte de las soluciones de seguridad. Los proveedores de *MaaS* a menudo incluyen servicios de ofuscación, que alteran el código del *malware* para hacerlo menos detectable por los sistemas de antivirus. Además, pueden implementar técnicas de evasión, como el uso de empaquetadores personalizados o la inserción de código en procesos legítimos para evitar ser detectados (Patsakis et al., 2024).

- **Soporte técnico y actualizaciones**: En el modelo *MaaS*, los desarrolladores de *malware* no solo venden su software, sino que también ofrecen soporte técnico para garantizar que los clientes puedan utilizarlo de manera efectiva. Esto puede incluir ayuda con la configuración del *malware*, la resolución de problemas, y la provisión de actualizaciones para hacer frente a nuevas medidas de seguridad. Al igual que en el SaaS, los proveedores de *MaaS* buscan mantener satisfechos a sus clientes para asegurar una fuente constante de ingresos (Huang et al., 2018).

Actores Clave en el Ecosistema de MaaS

El ecosistema de *MaaS* se nutre de una variedad de actores, cada uno desempeñando un papel específico en la cadena de valor del cibercrimen. A continuación, se describen los principales actores involucrados:

- **Desarrolladores de *Malware*:** Estos son los actores más técnicos en el ecosistema de *MaaS*. Son responsables de crear y mantener el software malicioso que se distribuye a través de los mercados de *MaaS*. Los desarrolladores de *malware* suelen ser programadores altamente cualificados con un profundo conocimiento de las vulnerabilidades del software, las técnicas de evasión de seguridad y las estrategias de ataque cibernético. Estos individuos o grupos a menudo operan en la clandestinidad, aprovechando foros de la *Darknet* y otros canales privados para vender sus productos (U.S. Department of Justice, 2022).

- **Operadores de *MaaS*:** Los operadores de *MaaS* son responsables de gestionar la infraestructura que sustenta estos servicios. Esto incluye no solo la distribución de kits de *malware*, sino también el mantenimiento de servidores y la provisión de servicios de soporte y actualización. Los operadores de *MaaS* actúan como intermediarios entre los desarrolladores de *malware* y los clientes, asegurando que los primeros reciban su compensación mientras los segundos obtienen las herramientas necesarias para llevar a cabo sus ataques (Europol, 2021).

- **Afiliados:** Los afiliados son un grupo clave dentro del ecosistema *MaaS*. A menudo carecen de las habilidades técnicas para desarrollar su propio *malware*, pero están dispuestos a distribuir el *malware* proporcionado por los operadores de *MaaS*. A cambio, los afiliados reciben una comisión ba-sada en los ingresos generados por las campañas de *malware* que llevan a cabo. Un ejemplo paradigmático de este modelo es el "*Ransomware*-as-a-Service" (RaaS), el cual permite a los operadores de *ransomware* maximizar su alcance y ganancias sin necesidad de involucrarse directamente en la distribución del *malware* (Europol, 2023a).

- **Clientes/Criminales:** Los clientes de *MaaS* son los actores que adquieren servicios de *malware* para llevar a cabo sus propias operaciones delicti-vas. Estos pueden ser individuos o grupos organizados, y sus motivaciones varían desde el lucro financiero hasta la venganza personal o el espionaje. Los clientes de *MaaS* pueden carecer de habilidades técnicas avanzadas, pero gracias a los servicios proporcionados por los operadores de *MaaS*, pueden lanzar ataques efectivos con una inversión mínima en términos de tiempo y recursos (Cable, s.f.).

- **Intermediarios y revendedores:** Además de los actores directamente involucrados en la creación y distribución de *malware*, existen intermediarios y revendedores que facilitan las transacciones entre los diferentes actores del ecosistema. Estos intermediarios pueden ofrecer servicios como el cambio de criptomonedas, el acceso a servidores comprometidos, o la reventa de kits de *malware* a nuevos clientes (Europol, 2023b).

Funcionamiento de los Mercados de MaaS

Los mercados de *MaaS* han adoptado muchas de las características de los negocios virtuales legítimos, lo que facilita a los delincuentes la compra de servicios de *malware*. Estos mercados suelen operar en la *Darknet*, donde los proveedores de *MaaS* publican anuncios detallados de sus productos y servicios, que incluyen descripciones de las funcionalidades del *malware*, precios, y en algunos casos, reseñas de otros usuarios.

- ***Ransomware*-as-a-Service (RaaS):** El RaaS es uno de los modelos más prevalentes en los mercados de *MaaS*. En este modelo, los operadores de *ransomware* proporcionan el software necesario para cifrar los datos de las víctimas y exigir un rescate a cambio de la clave de descifrado. Los afiliados se encargan de distribuir el *ransomware*, a menudo a través de correos electrónicos de *phishing* o mediante la explotación de vulnerabilidades en sitios web o aplicaciones. A cambio, los afiliados reciben un porcentaje de los pagos de rescate que logran recolectar. Este modelo ha demostrado ser extremadamente rentable, tanto para los operadores de RaaS como para sus afiliados (Meland et al., 2020).

- **Exploit Kits y *Phishing*-as-a-Service:** Además del *ransomware*, los mercados de *MaaS* también ofrecen kits de exploits y servicios de *phishing*. Los *exploit kits* son paquetes de software que explotan vulnerabilidades en software popular (como navegadores web o sistemas operativos) para instalar *malware* en las máquinas de las víctimas. El *Phishing-as-a-Service*, por otro lado, proporciona plantillas de correos electrónicos y páginas web fraudulentas que los delincuentes pueden utilizar para robar credenciales de inicio de sesión u otra información sensible. Estos servicios son populares porque permiten a los delincuentes lanzar ataques dirigidos sin necesidad de desarrollar sus propias herramientas (Meland et al., 2020).

- **Servicios de *botnets*:** Las *botnets* son redes de ordenadores comprometidos que los delincuentes pueden controlar de manera remota. En los mercados de *MaaS*, es posible alquilar acceso a *botnets* para realizar una variedad de ataques, incluidos DDoS, el envío masivo de spam, o el minado de criptomonedas. Los operadores de *botnets* mantienen y actualizan las redes comprometidas, asegurando que sigan siendo efectivas y difíciles de detectar por las soluciones de seguridad. Este servicio permite a los delincuentes escalar sus operaciones rápidamente y sin necesidad de infraestructura propia (Huang et al., 2018).

Desafíos y Amenazas para la Seguridad Cibernética

El crecimiento de *MaaS* plantea numerosos desafíos para la seguridad cibernética. La naturaleza descentralizada y anónima de estos servicios dificulta la identificación y persecución de los responsables. Además, la facilidad de acceso a herramientas de ataque sofisticadas ha reducido la barrera de entrada al cibercrimen, permitiendo que más actores participen en actividades delictivas sin necesidad de un conocimiento técnico profundo.

- **Evolución Rápida de las Amenazas:** Uno de los desafíos más significativos que presenta el *MaaS* es la rápida evolución de las amenazas. Los desarrolladores

de *malware* y los operadores de *MaaS* están en constante competencia con las soluciones de seguridad, actualizando y mejorando sus productos para evitar la detección. Esto significa que las organizaciones deben estar en alerta constante y actualizar regularmente sus sistemas para protegerse contra las nuevas variantes de *malware* (Casino et al., 2022).

- **Impacto Económico y Social**: El cibercrimen facilitado por *MaaS* tiene un impacto devastador en la economía global. Además de los costos directos asociados con la recuperación de ataques de *malware*, las organizaciones también enfrentan pérdidas de reputación, pérdida de confianza de los clientes, y posibles sanciones legales y regulatorias. En el ámbito social, los ataques facilitados por *MaaS* también pueden poner en peligro la infraestructura crítica, como los servicios de salud, energía y transporte, con consecuencias potencialmente catastróficas (Freeze, 2022).

- **Colaboración Internacional y Medidas de Mitigación**: Para enfrentar la amenaza del *MaaS*, es crucial una colaboración internacional. Los cibercriminales operan a menudo desde múltiples jurisdicciones, lo que dificulta su persecución por parte de las autoridades nacionales. Las agencias de seguridad deben trabajar juntas para compartir información y coordinar esfuerzos para desmantelar estas redes. Además, las organizaciones deben adoptar un enfoque proactivo en su ciberseguridad, invirtiendo en tecnologías avanzadas de detección y respuesta, y educando a sus emplea-dos sobre las amenazas más recientes (Europol, 2021; Casino et al., 2022).

INFRAESTRUCTURA Y CAMPAÑAS DE DESINFORMACIÓN

Los actores de amenaza que realizan campañas de desinformación necesitan usar estructuras y medios técnicos desde los que apoyarse para lograr sus objetivos, siendo especialmente relevante todo el conjunto de herramientas, servicios y plataformas que permiten diferir la causa de una estrategia FIMI de su consecuencia. A lo largo de esta sección haremos énfasis en los recursos tecnológicos que permiten ofuscar la actividad FIMI, impidiendo la identificación de actores e intereses.

Tal y como aparece recogidos en trabajos como (Huang et al., 2018), en el contexto actual existe una paulatina división de tareas y de especialización de las herramientas y servicios para cibercrimen, en sentido global, pero también en el caso particular de actividades ilícitas en la fabricación, instrumentalización y explotación de contenido fabricado o descontextualizado. Dicho de otra forma, en los últimos 10 años se ha producido una transformación *fordiana* del ecosistema del cibercrimen y de la guerra cognitiva y ataques reputacionales.

"En los últimos 10 años se ha producido una transformación fordiana del ecosistema del cibercrimen y de la guerra cognitiva y ataques reputacionales."

Estructura y elementos

Algunos ejemplos de las estructuras y medios técnicos usados son los siguientes:

- **VPN y *proxies* residenciales.** Una VPN, del inglés Virtual Private Network, permite navegar a través de Internet impidiendo la interceptación de la información que intercambiamos. Si bien el uso de servicios de VPN no garantiza el anonimato, pueden ser usados como una capa más de seguridad que proteja la identidad final del actor de amenaza, aumentando la dificultad de su atribución. El esfuerzo por parte de fuerzas y cuerpos de seguridad del estado a la hora de llevar a cabo investigaciones sobre direcciones IP que procedan de servicios de VPN es costoso en tiempo y en coordinación, especialmente si los propios servicios de VPN no son cooperativos y siguen políticas de no almacenamiento de registros de actividad de sus usuarios o clientes. Como se destacará más adelante a destacar más adelante, aquí existe la circunstancia dual de que proteger la privacidad puede ayudar a dificultar labores de atribución en investigaciones de ilícitos en el dominio ciber y, concretamente, en el ecosistema FIMI. Es más, si la infraestructura de red usada está distribuida de forma internacional, entonces la labor del investigador requiere la coordinación entre distintos marcos jurisdiccionales que no son siempre compatibles y que dificultan la necesaria colaboración.

  En el caso de los servidores *proxy*, un usuario se conecta a este servicio para no acceder de forma directa a un servicio o plataforma en Internet. El servidor *proxy* actúa de intermediario entre un cliente y un servidor final, de forma que se añade una capa extra entre ambos. Existen diversos tipos de servidores *proxy*, siendo especialmente relevantes los servidores *proxy* anónimos y los residenciales. En los servidores *proxy* anónimos la dirección IP del cliente es modificada, de forma que la plataforma o servicio al que accede un cliente no conocerá la dirección de origen. Esto permite enmascarar la acción de ataque de un cibercriminal o de un actor en campañas de desinformación, pero el grado de protección dependerá del tipo de servidor. En el caso de los *proxies* residenciales el servidor está ubicado en emplazamientos concretos no dependientes de ningún centro de datos o proveedor de servicios, de forma que una autoridad judicial tendría más dificultades de cara a conseguir la colaboración de este proveedor de servicio *proxy*.

  Al igual que en el caso de las VPN, el uso de *proxies* residenciales puede favorecer el acceso a información restringida de forma geográfica. De igual forma, su uso por actores de amenaza puede intentar engañar en una investigación sobre el origen real de la amenaza, al situarse en terceros países que también pueden tener interés en la difusión de desinformación. El uso de *proxies* residenciales es parte del arsenal desplegados, por ejemplo, por APT29, grupo que ha estado especialmente activo en Ucrania antes de la crisis de 2014, y volvió a realizar campañas activas de *phishing* a partir de finales de 2018. En el marco de FIMI, es especialmente importante la conexión entre APT29 y acciones diplomáticas por parte de Rusia (Cunningham, 2020).

- ***SIM Swapping* y SMS *Phishing*.** El intercambio de SIM se ha asociado de forma habitual a estafas relacionadas con las finanzas, sin embargo, adquiere un nuevo papel en las campañas de desinformación. Además de poder conceder acceso total o parcial a un dispositivo o servicio, y por tanto ser usado con fines de ciberespionaje o para acceder a otros elementos relacionados con la fuente que contengan

información de interés, esta técnica podría permitir la adquisición de medios de difusión legítimos, como cuentas de usuario en redes sociales que sean reputadas y cuenten con una gran audiencia de su interés.

Está técnica tiene otras implicaciones al permitir tanto la difusión de desinformación como la desacreditación de la víctima suplantada. De la misma forma que el *SIM Swapping*, el *phishing* puede ser usado para adquirir acceso a una cuenta legítima, permitiendo la difusión de información a una mayor audiencia. También permite la adquisición de información real que puede ser manipulada para realizar desinformación, como en el caso de David Satter, cuya cuenta de correo fue accedida de forma ilegal, lo que permitió que se modificaran sus correos electrónicos con vistas a publicar información falsa en relación con una supuesta operación financiada por EE. UU. para desestabilizar a Rusia (Hulcoop et al., 2017).

El ecosistema del *phishing* mediante SMS ha adquirido también una especial relevancia en los últimos tiempos. El conjunto de sistemas de alojamiento de servidores para campañas de *phishing* y de ingeniería social da una idea del grado de sofisticación de este tipo de actividad (Nahapetyan et al., 2024), así como del conjunto de retos en lo relativo a la supervisión de proveedores de servicios y de plataformas según lo establecido por el acta europea de servicios digitales o Digital Services Act (DSA). La recolección de servicios de hosting, patrones de generación de certificados digitales mediante el análisis de los logs de *Certificate Transparency*, o la identificación y trazabilidad de kits de desarrollo de campañas de *phishing* son elementos cruciales de cara al desarrollo de estrategias de contención frente a FIMI.

- **Inteligencia Artificial Generativa y suplantación (*Human Spoofing*).** El uso de Inteligencia Artificial permite generar desinformación tanto basada en texto como multimedia. Los *Large Language Models*, o Modelos de Lenguaje Extensos, pueden generar información verosímil y convincente sobre el asunto a desinformar. Permiten además la generación masiva de desinformación, llevando entonces a la infoxicación. La IA puede ser también usada para el refinamiento de la desinformación, intentando que la información sea más persuasiva, mejorando su calidad, o adaptándola a la audiencia objetivo. Aunque la mayoría de los modelos de lenguaje estén censurados o prevengan este tipo de conductas, son fácilmente eludibles por medio de distintas técnicas, cadenas de pensamiento, o el uso de modelos no censurados o protegidos, entre otros (Barman et al., 2024).

  En el caso de la generación de imágenes, si antes generalmente se necesitaba una imagen que poder descontextualizar, ahora directamente se puede fabricar. Esto es especialmente interesante con modelos como Flux, que no contemplan por ejemplo la censura de personajes reconocidos, y donde la dificultad para diferenciar las imágenes generadas de las reales es cada vez mayor. El acceso a estas tecnologías es fácilmente asequible, ya que no requiere conocimientos técnicos, y las especificaciones requeridas para ejecutar este software no son tan demandantes como se puede pensar. El *Human Spoofing*, mediante el uso de IAs generativas como las reseñadas anteriormente, pone a disposición de actores de desinformación la posibilidad de suplantar de forma muy verosímil a personajes públicos, ya no solo para la difusión del contenido creado, sino para el

"El Human Spoofing, mediante el uso de IAs generativas como las reseñadas anteriormente, pone a disposición de actores de desinformación la posibilidad de suplantar de forma muy verosímil a personajes públicos"

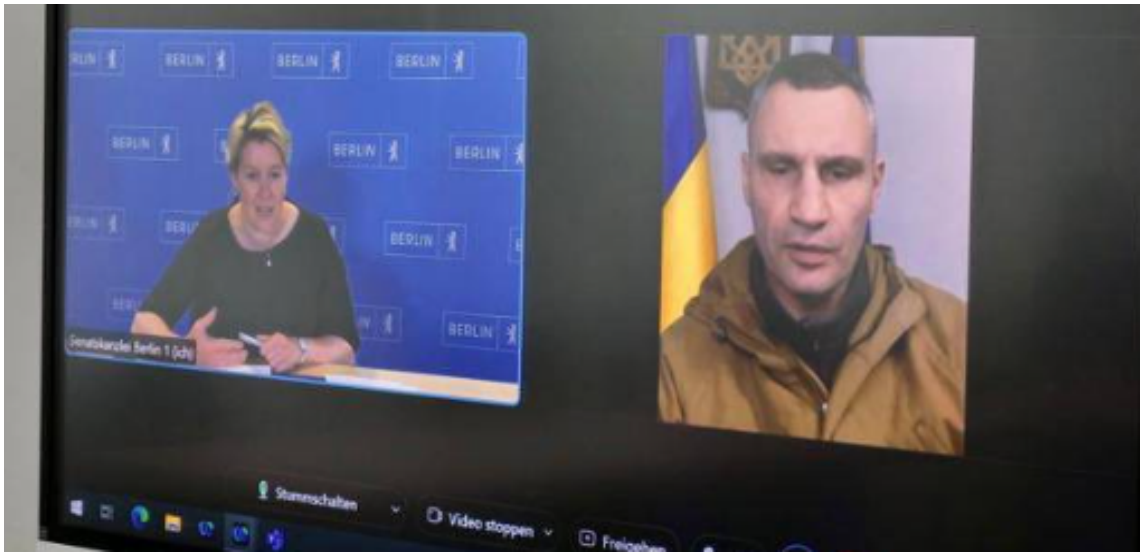


Figura 2. Alcaldesa de Berlín siendo manipulada mediante la suplantación de identidad del alcalde de Kiev Vitali Klitschko. Fuente: Fishcer (2022).

engaño y el uso de ingeniería social para con otros. Un ejemplo de esto es la falsa videollamada mantenida entre el alcalde de Madrid y su supuesto homólogo en Kiev, un acto que podría ser catalogable entre la broma y la guerra híbrida (Twomey et al., 2023).

- **Redes sociales, influencia y búsqueda de talento.** El uso combinado de redes sociales, las dinámicas multiplataforma y el despliegue de acciones coordinadas. La democratización en el acceso a canales de generación y distribución de contenido facilita el despliegue de operaciones para influir en la toma de decisión. Desde el punto de vista de su investigación, los servicios de mensajería instantánea con cifrado de extremo a extremo suponen en este sentido un gran desafío, en la medida que impiden una interceptación directa de tráfico e impulsan coordinación entre fuentes y medios de manipulación (Hoseini et al., 2024; Hanley y Durumeric, 2024). Entre las aplicaciones de redes sociales, plataformas e incluso foros en la *Deep Web*, cabe destacar el despliegue de infraestructura para la formación y reclutamiento de talento en la esfera del cibercrimen (Wang et al., 2023; Pandey, 2022).

Tecnologías de uso dual

Definimos tecnologías de uso dual como aquellas tecnologías que pueden ser usadas tanto para fines civiles como militares. En este caso, hacemos uso del término para referirnos a aquellas tecnologías que, además de su uso civil, permiten ser usadas por actores de amenaza para realizar operaciones de desinformación. Las tecnologías de uso dual por excelencia son las redes sociales. Sin embargo, en este apartado nuestra atención se dirige hacia la infraestructura necesaria para la realización de operaciones de desinformación.

- **Marketing digital.** El marketing digital se ha consolidado como una herramienta esencial para las empresas y organizaciones que buscan promocionar sus productos y servicios. A través de estrategias como el posicionamiento en buscadores (SEO) y la publicidad en redes sociales, las marcas pueden llegar a audiencias específicas de manera eficiente y efectiva. Sin embargo, las mismas técnicas y plataformas utilizadas para fines comerciales pueden ser empleadas para llevar a cabo operaciones de influencia y desinformación. Actores de amenaza pueden aprovechar las herramientas de segmentación y análisis de datos para identificar y dirigirse a audiencias vulnerables, difundiendo información falsa o manipulada para influir en opiniones, comportamientos o decisiones políticas (Domenico et al., 2021).

  Por ejemplo, durante procesos electorales, actores estatales o no estatales han utilizado campañas de desinformación en redes sociales para sembrar discordia, polarizar a la sociedad o desacreditar a candidatos. Mediante la creación de contenido engañoso y el uso de *bots* y perfiles falsos, pueden amplificar mensajes y hacerlos parecer más legítimos o populares de lo que realmente son. Así, existen grupos organizados que están financiados por estados o prestan sus servicios para efectuar campañas de manipulación en redes sociales. Este es el caso de las denominadas granjas de *trolls* y/o *bots* (Hughes y Waismel-Manor, 2021), o del uso de infraestructura militar en desuso para relacionar actividades de soporte para el cibercrimen y la ciberguerra (Caesar, 2020). Además, técnicas de microsegmentación o los sistemas de recomendación (Deldjoo et al., 2024) permiten adaptar mensajes específicos a grupos particulares, aumentando la efectividad de la manipulación (O Fathaigh et al., 2021).

- **Wikipedia.** La enciclopedia cooperativa es uno de los sitios web más visitados globalmente, sirviendo como fuente de información accesible y gratuita para millones de personas. La participación de cualquier persona en su edición es a su vez su principal ventaja y desventaja. Desde la óptica de las campañas de desinformación e influencia, esta capacidad es susceptible de ser explotada por actores de amenaza mediante la edición maliciosa y el sesgo de contenido, los ataques de edición coordinados, la manipulación de fuentes y referencias, o la divulgación de fuentes y referencias aparentemente legitimas pero que constituyen parte de la campaña de desinformación.

  Aunque la mayoría de los engaños en Wikipedia se detectan rápidamente y tienen poco impacto, un pequeño número de ellos sobreviven mucho tiempo y reciben muchas visitas (Kumar, West, y Leskovec, 2016). Existen formas de clasificar automáticamente si un artículo dado es engañoso, consiguiendo una precisión mayor al de la revisión manual realizada por moderadores humanos. Según el

artículo anteriormente citado, el lector humano tiende a considerar los artículos cortos como contenido engañoso, mientras que en realidad es en grandes artículos donde es más propenso el engaño, así como se demuestra que la capacidad para evadir la moderación de contenido malicioso es baja sin herramientas automáticas especializa-das. Esto hace de la Wikipedia un escenario idóneo para la divulgación de desinformación, dadas sus características de edición y acceso abierto, y el masivo tráfico que recibe.

- **Open Source Intelligence.** La inteligencia de fuentes abiertas, OSINT por sus siglas en inglés, ha constituido desde hace años una gran fuente de información gracias a su fácil accesibilidad, gran disponibilidad de información y bajo coste económico en comparación con otro tipo de fuentes. La proliferación de la tecnología y el acceso masivo a internet han transformado la manera en que se recopila y analiza la información. La inteligencia de fuentes abiertas se ha convertido en una herramienta esencial para extraer datos relevantes de un océano de información disponible públicamente. Su facilidad para ser obtenida ha permitido que sea activamente explotada tanto por servicios de inteligencia como por organizaciones o particulares, consiguiendo ventajas estratégicas y una mejora en la toma de decisiones en diversos sectores.

  Aunque su uso está ampliamente extendido y aceptado, es necesario reconocer la importancia de la desinformación y manipulación en este campo. Un actor de amenaza podría realizar infoxicación mediante la generación de contenido artificial erróneo o ligeramente falso, así como fabricación de información sesgada que pueda ser malinterpretada por actores enemigos o competidores (Flamer, 2023).

- **Internet Archive.** Los servicios de archivado web, como *Wayback Machine* (del Internet Archive) o Archive.is, permiten almacenar páginas web de manera automatizada o a demanda, posibilitando que cualquier usuario acceda a la información incluso si ha sido eliminada o modificada, o simplemente sin visitar el sitio original. Estos servicios desempeñan un papel crucial en la preservación de la historia digital, facilitando la investigación académica y el acceso a información que, de otro modo, podría perderse.

  Sin embargo, aunque su propósito legítimo es evidente, se ha observado que algunos actores malintencionados utilizan esta tecnología con diversos fines, como la propagación de información errónea, retractada o desinformación; el acceso a noticias de medios contrarios a sus ideales con el fin de reducir los ingresos publicitarios de dichos medios; la evasión de medidas de censura durante la difusión de contenido desinformativo en redes sociales; y la captura de publicaciones en redes sociales y noticias que podrían ser eliminadas debido a controversias (Zannettou et al., 2018; Acker y Chaiet, 2020) .

- **Uso de servicios cloud legítimos como estrategia de evasión.** El uso de servicios legítimos para llevar a término ciberataques es algo que se ha venido observando de forma habitual en el caso del despliegue de *botnets* y sistemas C&C (Al lelah et al., 2023). Dado el carácter excesivamente central de algunas plataformas, ca-be estimar como de alta criticidad todo uso instrumental de los servicios de dicha plataforma para eludir los sistemas de filtrado y de control de seguridad de instituciones, organizaciones y empresas (Alcantara, 2024).

DISCUSIÓN, RETOS Y DESAFÍOS

Esta sección resume las ideas obtenidas del análisis anterior, destacando las implicaciones de las campañas de desinformación y ofreciendo una perspectiva sobre los pasos futuros. Los puntos principales de discusión se centran en los avances tecnológicos necesarios para mitigar la amenaza de la desinformación.

Desarrollo de estándares y procedimientos para la identificación de actores, herramientas y terceros interpuestos en el dominio FIMI. Desde el punto de vista de la atribución de campañas y acciones de injerencia externa, la asociación entre estados y actores del ecosistema MaaS constituye un reto tecnológico y metodológico. La extensión de los tradicionales proxies en el dominio del enfrentamiento tácito y militar se amplifica gracias a los medios cibernéticos. La sofisticación y especialización en lo relativo a servicios, productos y plataformas para creación y distribución de contenido fabricado y malware contribuye a incrementar el carácter poliédrico del concepto de proxy o, mejor dicho, de ciber-proxy (Borghard y Lonergan, 2016b). El análisis de riesgos y amenazas asociados a los diversos tipos de proxies en el ámbito cibernético demanda el desarrollo de procedimientos de identificación, anotación y distribución de evidencias e inteligencia a nivel nacional y transnacional. En este sentido, a nivel europeo sería interesante incorporar a la red de ISAC soluciones tecnológicas derivadas de marcos teóricos para el análisis de riesgo y la atribución de acciones FIMI.

Firma Digital y Protocolos Seguros para la Verificación de Contenidos. Las campañas de desinformación pueden combatirse eficazmente adoptando protocolos seguros y firmas digitales que autentiquen el origen y la integridad del contenido. Técnicas como los Entornos de Ejecución Confiable (TEE) y las Pruebas de Conocimiento Cero (ZK-SNARKs) están emergiendo como opciones viables para verificar la autenticidad de la información. Estas técnicas criptográficas garantizan que se conserve la autoría original del contenido digital, reduciendo el potencial de que se difunda contenido manipulado o fabricado sin control. Implementar tales protocolos en entornos donde la IA Generativa puede fabricar desinformación será crucial en el futuro.

"Las campañas de desinformación pueden combatirse eficazmente adoptando protocolos seguros y firmas digitales que autentiquen el origen y la integridad del contenido"

Un caso de estudio bien conocido de lucha contra la desinformación utilizando zk-SNARKs es la protección de imágenes digitales. Las cámaras necesitan un elemento seguro para producir firmas en imágenes o videos capturados. Este elemento seguro actúa de manera similar a un TEE, aunque se describe con mayor precisión como un sistema de firma a prueba de manipulaciones o elemento seguro. Algunas compañías ya han contribuido a un estándar conocido como firmas C2PA (Coalition for Content Provenance and Authenticity) (C2PA, 2024), que no se centra necesariamente en hardware seguro, sino en vincular contenido multimedia con metadatos confiables, como la geolocalización. C2PA permite a los usuarios equilibrar privacidad y autenticidad, por ejemplo, adjuntando la geolocalización a una imagen mientras revelan selectivamente la información que eligen compartir. De esta manera, cualquiera con acceso a una imagen de alta resolución, como una foto de 30MP y su firma correspondiente, puede demostrar que una cámara autenticada capturó la imagen en un lugar específico. Este mecanismo ayuda a combatir la desinformación, como la difusión de fotos falsas de zonas de conflicto. Posibles ataques, como tomar una foto

de una imagen impresa, siguen siendo un vector de ataque separado que debe abordarse independientemente.

Preservación de la Integridad durante modificaciones de contenido. Las agencias de noticias y redes de televisión a menudo modifican fotos y videos originales antes de publicarlos. Modificaciones como recortar, cambiar el tamaño o convertir a escala de grises resultan en la pérdida de la vinculación original entre el medio firmado y sus metadatos. Esto presenta un desafío significativo para mantener la integridad del contenido durante el proceso de modificación. Para abordar este problema, zk-SNARKs pueden emplearse para preservar la vinculación entre la imagen original y las modificaciones. Definiendo un circuito que represente las transformaciones aplicadas al medio original, es posible retener la firma y la vinculación, incluso después de que el contenido haya sido alterado. Varios autores han discutido este enfoque (Datta et al., 2024), aunque uno de los mayores desafíos identificados fue la sobrecarga computacional significativa asociada con la generación de pruebas zk-SNARK. Su método requería grandes cantidades de memoria, hasta 64GB, para generar una sola prueba, lo que lo hacía poco práctico para una adopción generalizada. Sin embargo, un artículo más reciente (Della Monica et al., 2024) optimizó este enfoque aplicando un principio de dividir y con-quistar. Propusieron dividir una imagen en mosaicos y modificar el protocolo C2PA para firmar mosaicos agregados utilizando una estructura de árbol de Merkle. Este método permite la generación de pruebas zk-SNARK para mosaicos individuales, reduciendo significativamente la carga computacional. Como resultado, este enfoque optimizado permite la generación de pruebas zk-SNARK incluso en hardware común, como solo 4GB de RAM.

Si bien los enfoques para imágenes estáticas han mostrado resultados prometedores, el contenido de video presenta un desafío computacional mucho mayor ya que hace que la generación de pruebas zk-SNARK sea significativamente más lenta y demande más recursos. Se están llevando a cabo investigaciones para paralelizar el proceso de generación de pruebas zk-SNARK utilizando hardware de GPU, lo que ha mostrado mejoras de velocidad de hasta 4 veces. Sin embargo, estos esfuerzos aún no logran la eficiencia computacional requerida para el procesamiento en tiempo real o a gran escala de videos.

Detección automatizada de desinformación usando IA y Big Data. Las LLMs y su capacidad para generar información falsa convincente plantea un desafío. La sobrecarga de información ya es un problema prevalente, y la capacidad de la IA para producir grandes cantidades de información falsa agravará este problema (Xu et al., 2023). Abordar la sobrecarga de información requerirá tanto soluciones técnicas (p. ej., mejores algoritmos de filtrado y sistemas automatizados de verificación) así como esfuerzos educativos para mejorar la alfabetización mediática de la sociedad. En este contexto, la automatización de la detección de desinformación mediante sistemas basados en IA que aprovechen correlaciones semánticas y técnicas de procesamiento de lenguaje natural (NLP) es fundamental. Sin embargo, aún quedan desafíos por abordar en cuanto a la escalabilidad y precisión de dichos sistemas. Además, el mantenimiento de bases de datos continuamente actualizadas para rastrear fuentes conocidas de desinformación jugar´ un papel vital en la efectividad de estos sistemas de IA (Mansurova et al., 2024).

Expertos en la verificación de noticias. Si bien los sistemas automatizados juegan un papel importante, no se puede ignorar la participación de expertos en la verificación de la exactitud y legitimidad de contenido. El rol de verificadores, periodistas y expertos de diferentes campos debe fortalecerse para contrarrestar la creciente influencia de la desinformación generada por IA. Integrar la retroalimentación de expertos en los sistemas de IA para señalar con-tenido falso podría crear un sistema híbrido robusto (Mahmud et al., 2023). Además, el concepto de “experto” en sí

requiere definiciones que puedan usarse para identificar al personal adecuado y sus habilidades y comportamientos, entre otras características, en diferentes contextos de información. Esto constituye una línea de investigación en sí misma.

Tecnologías emergentes en la protección de contenido verificado: Blockchain y Registros Inmutables. La correcta curación de noticias a través de expertos, su eficiente anotación y distribución requiere de la existencia de protocolos y procedimientos que garanticen su custodia e integridad. La tecnología Blockchain ofrece otra solución potencial para contrarrestar la desinformación mediante la creación de registros digitales inmutables de con-tenido. Esto permitiría rastrear la información a medida que se propaga en diferentes plataformas, garantizando que las alteraciones o manipulaciones del contenido original sean visibles, rastreables y verificables. Este enfoque podría ser particularmente efectivo en plataformas de noticias y redes sociales, donde la información falsa puede difundirse rápidamente (Fraga-Lamas y Fernandez-Carames, 2020).

Colaboración multidisciplinaria en la lucha contra la desinformación. El enfoque de modelado de amenazas en ciberseguridad puede servir para caracterizar mejor el perfil de atacantes en el arco de la desinformación, sus patrones de ataque, sus objetivos preferenciales y las técnicas que usan de forma más habitual (Mirza et al., 2023). Ahora bien, para ello se requiere un enfoque colaborativo que abarque múltiples disciplinas. Expertos en ciberseguridad, fuerzas del orden, análisis de datos, psicología y análisis semántico deben trabajar juntos para desarrollar contramedidas efectivas. Esta colaboración interdisciplinaria también debe extenderse a los legisladores, asegurando que el marco legal evolucione junto con los avances tecnológicos (Casino, et al., 2022). Los protocolos diseñados para detectar y mitigar la desinformación deben estar fundamentados en estándares legales, proporcionando tanto privacidad como seguridad (Ramasauskaite, 2023).

Desafíos en la atribución cibernética. Uno de los desafíos persistentes en la lucha contra la desinformación es el tema de la atribución cibernética. Identificar la fuente de la desinformación, especialmente en casos que involucran campañas patrocinadas, requiere herramientas sofisticadas y cooperación internacional. Si bien se han logrado avances, particularmente con el uso de IA y OSINT, las tácticas en evolución de los actores maliciosos hacen que la atribución sea cada vez más difícil. Las operaciones de falsa bandera, infraestructuras de Internet anonimizadas (p. ej., VPN, proxies) y el uso de canales de comunicación encriptados dificultan la labor de identificar a los actores de campañas de desinformación. Los esfuerzos futuros deben centrarse en mejorar los marcos de atribución cibernética para responsabilizar a los responsables a nivel internacional (Maesschalck, 2024).

CONCLUSIONES

Este capítulo ha explorado la compleja interacción entre las campañas de desinformación, los avances tecnológicos y los impactos sociopolíticos resultan-tes. A lo largo del capítulo, hemos visto cómo la desinformación y las campañas cibernéticas sofisticadas se nutren a menudo de infraestructuras organizadas y plataformas que aprovechan el malware y las tecnologías de IA. Las APM reflejan las etapas de las ATP, donde la guerra de información opera junto con los ciberataques, difundiendo contenido manipulado que puede potencialmente desestabilizar a la sociedad.

El MaaS ejemplifica la mercantilización de herramientas de cibercrimen, que permiten incluso a actores no técnicos orquestar campañas de desinformación. Este proceso se refuerza a través de la evolución de botnets, ransomware y modelos de phishing como servicio. En paralelo, mientras que las herramientas de IA permiten la generación de contenido falso o modificado a gran escala, también allanan el camino para su detección. En resumen, identificamos varias tecnologías y estrategias clave que deben ser exploradas, como el uso de blockchain para la integridad del contenido, la mejora de la eficiencia de zk-SNARK, la necesidad colaboración interdisciplinaria y, finalmente, abordar los desafíos de la atribución cibernética.

REFERENCIAS BIBLIOGRÁFICAS

Acker, A., y Chaiet, M. (2020, 28 de septiembre). The weaponization of web archives: Data craft and COVID-19 publics. *Harvard Kennedy School (HKS) Misinformation Review*. https://doi.org/10.37016/mr-2020-41

Ahmad, A., Webb, J., Desouza, K. C., y Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security, 86*, 402– 418.

Alcantara, J. M. (2024, 23 de marzo). Phishing with cloudflare workers: Transparent phishing and html smuggling. *Netskope*. https://www.netskope.com/blog/phishing-with-cloudflare-workers-transparent-phishing-and-html-smuggling

Al lelah, T., Theodorakopoulos, G., Reinecke, P., Javed, A., y Anthi, E. (2023). Abuse of cloud-based and public legitimate services as command-and-control (c&c) infrastructure: a systematic literature review. *Journal of Cybersecurity and Privacy, 3 (3)*, 558–590.

Barman, D., Guo, Z., y Conlan, O. (2024). The Dark Side of Language Models: Exploring the Potential of LLMs in Multimedia Disinformation Generation and Dissemination. *Machine Learning with Applications, 16*, *100545*. https://doi.org/10.1016/j.mlwa.2024.100545

Beehner, L., Collins, L., Ferenzi, S., Person, R., y Brantly, A. F. (2018). Analyzing the russian way of war: Evidence from the 2008 conflict with Georgia. *Modern War Institute*. Disponible en: https://mwi.westpoint.edu/wp-content/uploads/2018/03/Analyzing-the-Russian-Way-of-War.pdf

Borghard, E. D., y Lonergan, S. W. (2016a). Can states calculate the risks of using cyber proxies? *Orbis, 60 (3)*, 395-416. https://doi.org/10.1016/j.orbis.2016.05.009

Borghard, E. D., y Lonergan, S. W. (2016b). Can states calculate the risks of using cyber proxies? *Orbis, 60 (3)*, 395–416.

C2PA. (2024). Coalition for content provenance and authenticity specification. *c2pa.org*. https://c2pa.org/specifications/specifications/2.0/specs/C2PA_Specification.html

Cable, J. (s.f.). Ransomwhere — ransomwhe.re. https://ransomwhe.re/.

Caesar, E. (2020, 27 de julio). The cold war bunker that became home to a dark-web empire. *The New Yorker.* https://www.newyorker.com/magazine/2020/08/03/the-cold-war-bunker-that-became-home-to-a-dark-web-empire

Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M., Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *IEEE Access, 10*, 25464-25493. https://ieeexplore.ieee.org/document/9720948

Casino, F., Lykousas, N., Katos, V., y Patsakis, C. (2021). Unearthing mali-cious campaigns and actors from the blockchain dns ecosystem. *Computer Communications, 179*, 217–230.

Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., y Patsakis, C. (2022). Sok: Cross-border criminal investigations and digital evidence. *Journal of Cybersecurity, 8 (1)*. https://doi.org/10.1093/cybsec/tyac014

Cunningham, C. (2020). *A Russian Federation Information Warfare Primer*. The Henry M. Jackson School of international Studies. University of Washington. https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/

Datta, T., Chen, B., y Boneh, D. (2024). VerITAS: Verifying image transformations at scale. *Cryptology ePrint Archive*. https://eprint.iacr.org/2024/1066

Davidson, R. (2021). The fight against *malware* as a service. *Network Security, 2021 (8)*, 7–11. https://doi.org/10.1016/S1353-4858(21)00088-X

Deldjoo, Y., Jannach, D., Bellogin, A., Difonzo, A., y Zanzonelli, D. (2024). Fair-ness in recommender systems: research landscape and future directions. *User Modeling and User-Adapted Interaction, 34 (1)*, 59–108. https://doi.org/10.48550/arXiv.2205.11127

Della Monica, P., Visconti, I., Vitaletti, A., y Zecchini, M. (2024). Trust nobody: Privacy-preserving proofs for edited photos with your laptop. *Cryptology ePrint Archive*. https://eprint.iacr.org/2024/1074

Domenico, G. D., Sit, J., Ishizaka, A., y Nunan, D. (2021, enero). Fake news, social media and marketing: A systematic review. Journal of Business Research, 124 , 329–341. https://doi.org/10.1016/j.jbusres.2020.11.037

Europol. (2021). DarkMarket: world's largest illegal dark web marketplace ta-ken down. https://www.europol.europa.eu/media-press/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down

Europol. (2023a). 288 dark web vendors arrested in major marketplace seizure. https://www.europol.europa.eu/media-press/newsroom/news/288-dark-web-vendors-arrested-in-major-marketplace-seizure

Europol.(2023b).Takedown of notorious hacker marketplace selling your identity to criminals. https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-notorious-hacker-marketplace-selling-your-identity-to-criminals

Fishcer, D. (2022, 1 de julio). Fake Video Calls Aim to Harm Ukraine. *Refugees Human Rights Watch*. https://www.hrw.org/news/2022/07/01/fake-video-calls-aim-harm-ukraine-refugees

Flamer, N. (2023). 'The enemy teaches us how to operate': Palestinian hamas use of open source intelligence (osint) in its intelligence warfare against Israel (1987-2012). *Intelligence and National Security, 38 (7)*, 1171–1188. https://dx.doi.org/10.1080/02684527.2023.2212556

Fraga-Lamas, P., y Fernandez-Carames, T. M. (2020). Fake news, disinformation, and deepfakes: Leveraging distributed ledger technologies and block-chain to combat digital deception and counterfeit reality. *IT professional, 22 (2)*, 53–59.

Freeze, D. (2022). Cybercrime to cost the world 8 trillion annually in 2023. *Cybercrime Magazine*. https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

Gioe, D. V., y Smith, M. W. (2024). *Great power cyber competition: Competing and winning in the information environment*. Routledge. Taylor & Francis.

Greenberg, A. (2020, 20 de febrero). The US Blames Russia's GRU for Sweeping Cyberattacks in Georgia. *Wired*. https://www.wired.com/story/us-blames-russia-gru-sweeping-cyberattacks-georgia/

Hanley, H. W., y Durumeric, Z. (2024). Partial Mobilization: Tracking Multilingual Information Flows amongst Russian Media Outlets and Telegram. *Proceedings of the International AAAI Conference on Web and Social Media, 18*, 528–541. https://doi.org/10.48550/arXiv.2301.10856

Hoseini, M., de Freitas Melo, P., Benevenuto, F., Feldmann, A., y Zannettou, S. (2024). Characterizing Information Propagation in Fringe Communities on Telegram. *Proceedings of the International AAAI Conference on Web and Social Media, 18*, 583–595. https://doi.org/10.1609/icwsm.v18i1.31336

Huang, K., Siegel, M., y Madnick, S. (2018). Systematically understanding the cyber attack business: A survey. *ACM Computing Surveys (CSUR), 51(4).* https://doi.org/10.1145/3199674

Hughes, H. C., y Waismel-Manor, I. (2021). The Macedonian Fake News Industry and the 2016 US Election. *Political Science & Politics, 54 (1)*, 19-23. https://doi.org/10.1017/S1049096520000992

Hulcoop, A., Scott-Railton, J., Tanchak, P., Brooks, M., y Deibert, R. (2017). *Tainted Leaks: Disinformation and Phishing with a Russian Nexus*. Citizen Lab Research Report, University of Toronto. https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/

Kumar, S., West, R., y Leskovec, J. (2016). Disinformation on the Web: Impact, Characteristics, and Detection of Wikipedia Hoaxes. *Proceedings of the 25th International Conference on World Wide Web,* 591-602. https://doi.org/10.1145/2872427.2883085

Maesschalck, S. (2024). Gentlemen, you can't fight in here. Or can you?: How cyberspace operations impact international security. *World Affairs, 187(1)*, 24-36. https://doi.org/10.1002/waf2.12004

Mahmud, M. A. I., Talukder, A. T., Sultana, A., Bhuiyan, K. I. A., Rahman, M. S., Pranto, T. H., y Rahman, R. M. (2023). Toward News Authenticity: Synthesizing Natural Language Processing and Human Expert Opinion to Evaluate News. *IEEE Access, 11*, 11405-11421. https://doi.org/10.1109/ACCESS.2023.3241483

Mansurova, A., Mansurova, A., y Nugumanova, A. (2024). QA-RAG: Exploring LLM Reliance on External Knowledge. *Big Data and Cognitive Computing, 8(9)*, 115. https://doi.org/10.3390/bdcc8090115

Meland, P. H., Bayoumy, Y. F. F., y Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. *Computers & Security, 92*, 101762. https://doi.org/10.1016/j.cose.2020.101762

Mirza, S., Begum, L., Niu, L., Pardo, S., Abouzied, A., Papotti, P., y Pöpper, C. (2023). Tactics, threats & targets: Modeling disinformation and its mitigation. *Network And Distributed System Security (NDSS) Symposium*. https://doi.org/10.14722/ndss.2023.23657

Nahapetyan, A., Prasad, S., Childs, K., Oest, A., Ladwig, Y., Kapravelos, A., y Reaves, B. (2024). On SMS *phishing* tactics and infrastructure. *2024 IEEE Symposium on Security and Privacy (SP)*, 1-16. https://doi.org/10.1109/SP54263.2024.00169.

O Fathaigh, R., Dobber, T., Zuiderveen Borgesius, F., y Shires, J. (2021). Micro-targeted propaganda by foreign actors: An interdisciplinary exploration. *Maastricht Journal of European and Comparative Law, 28 (6)*, 856–877.

Pandey, R. (2022). Exploring HackTown: A College for Cybercriminals. *Isaca.*org. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/exploring-hacktown-a-college-for-cybercriminals

Patsakis, C., Arroyo, D., y Casino, F. (2024). The malware as a service ecosystem. *arXiv preprint*. https://doi.org/10.48550/arXiv.2405.04109

Patsakis, C., Casino, F., y Lykousas, N. (2024). Assessing LLMs in Malicious Code Deobfuscation of Real-world Malware Campaigns. *Expert Systems with Applications, 256 (6)*, 124912. http://dx.doi.org/10.1016/j.eswa.2024.124912

Ramasauskaite, O. (2023). *The role of collaborative networks in combating digital disinformation*. 2. International Conference on Economics "Regional Development - Digital Economy" : proceedings book. December 21-23, 2023 / Baku, Azerbaijan / The Scientific-Research Institute of Economic Studies under the Azerbaijan State University of Economics (UNEC), 432-437. https://vb.mruni.eu/object/elaba:184652082/

Shapiro, S. J. (2023). *Fancy Bear Goes Phishing: The Dark History of the Information Age, in Five Extraordinary Hacks*. Random House.

Skopik, F., y Pahi, T. (2020). Under false flag: using technical artifacts for Ccyber attack attribution. *Cybersecurity, 3*, 8. https://doi.org/10.1186/s42400-020-00048-4

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., y Thomas, C. B. (2018). Mitre att&ck: Design and philosophy. En Technical report. The MITRE Corporation.

Twomey, J., Ching, D., Aylett, M. P., Quayle, M., Linehan, C., y Murphy, G. (2023). Do deepfake videos undermine our epistemic trust? A thematic analysis of tweets that discuss deepfakes in the Russian invasion of Ukraine. *PLOS ONE, 18 (10)*, e0291668. https://doi.org/10.1371/journal.pone.0291668

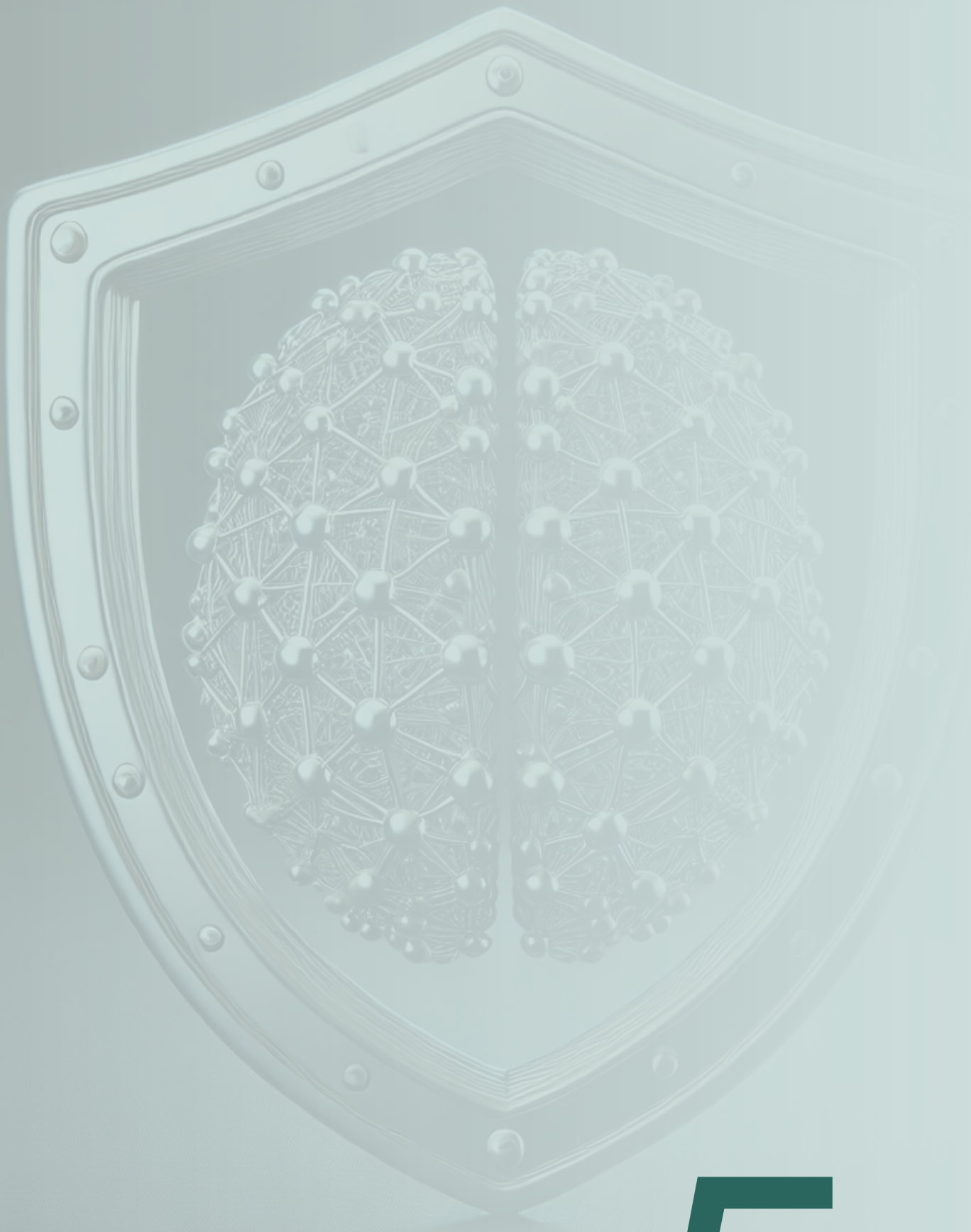
The UN report on disinformation: a role for privacy. (2021, 17 de mayo). Privacyinternational.org. https://privacyinternational.org/news-analysis/4515/un-report-disinformation-role-privacy

U.S. Department of Justice. (2022). *Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace*. https://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace

Wang, Y., Roscoe, S., Arief, B., Connolly, L., Borrion, H., y Kaddoura, S. (2023). The Social and Technological Incentives for Cybercriminals to Engage in Ransomware Activities. En Arief, B., Monreale, A., Sirivianos, M., Li, S. (Eds.), *Security and Privacy in Social Networks and Big Data. SocialSec 2023. Lecture Notes in Computer Science*, 14097. Springer, Singapore. https://doi.org/10.1007/978-981-99-5177-2_9

Xu, D., Fan, S., y Kankanhalli, M. (2023). Combating misinformation in the era of generative AI models. En Proceedings of the 31st acm international conference on multimedia. *Association for Computing Machinery,* pp. 9291-9298. https://doi.org/10.1145/3581783.3612704

Zannettou, S., Blackburn, J., De Cristofaro, E., Sirivianos, M., y Stringhini, G. (2018, junio). Understanding Web Archiving Services and Their (Mis)Use on Social Media. *Proceedings of the International AAAI Conference on Web and Social Media, 12 (1)*. https://doi.org/10.1609/icwsm.v12i1.15018



CAPÍTULO 5

CAMPAÑAS DE DESINFORMACIÓN Y PROMOCIÓN DEL DISCURSO DE ODIO

Coordinadores:

Mario Hernández Ramos

Miguel Camacho Collados

Departamento de Seguridad Nacional

Autores y colaboradores:

Rubén Arcos Martín

Jesús Díaz Carazo

Carlos Edmundo Arcila

Carmen Girón Tomás

Beatriz Marín Garcia

María Teresa Martín Valdivia

Unidad de delitos de odio y discriminación de la Fiscalía General del Estado

Unidad Especializada contra la Criminalidad Informática de la Fiscalía General del Estado

INTRODUCCIÓN

El riesgo que las campañas de desinformación suponen para alentar y promover el discurso de odio contra determinados colectivos en el seno de los países democráticos ha sido ya foco de atención del Parlamento Europeo (Szakács & Bognár, 2021), el Servicio Europeo de Acción Exterior (EEAS Stratcom Division, 2023) y el Centro Europeo de Excelencia para la Lucha contra las Amenazas Híbridas (Hoogensen Gjørv & Jalonen, 2023), especialmente cuando estas campañas son promovidas por actores estatales hostiles que buscan generar división social. Además, estas campañas también se despliegan en terceros países (principalmente de África y Europa del Este) como una forma de atacar a Occidente y el modelo de democracia liberal, con el consiguiente riesgo que esto genera en los colectivos de estos países.

A esto se le une, la creciente preocupación por el potencial que tiene la desinformación para promover la radicalización violenta, especialmente cuando adopta la forma de teoría de la conspiración que presenta a ciertos grupos o colectivos como una amenaza (Red de Concienciación sobre la Radicalización (RAN), 2020).

Por ello, el 29 de febrero de 2024 el Foro contra las campañas de desinformación en el ámbito de la seguridad nacional acordó la creación de un grupo de trabajo con el objetivo principal de analizar el riesgo que las campañas pueden suponer para el fomento del discurso de odio, con especial atención a España, y discutir los posibles instrumentos o iniciativas para limitar su impacto en nuestra sociedad. Asimismo, el grupo tendría como objetivo fomentar la concienciación y el conocimiento sobre esta amenaza entre los diferentes actores de la sociedad civil y la administración pública implicados en la protección de los colectivos que puedan ser objetivo de estas campañas de desinformación.

Para coordinar este grupo de trabajo se designó a Mario Hernández Ramos y a Miguel Camacho Collados, así como al Departamento de Seguridad Nacional, por parte de la administración pública, como coordinadores. El grupo de trabajo se conformó con las personas que figuran al inicio de este capítulo.

DESARROLLO DE LA INICIATIVA

A fin de alcanzar el objetivo de conocer mejor la amenaza y el marco actual para abordarla, así como para fomentar la concienciación sobre la misma en el seno de las comunidades vinculadas tanto a la lucha contra las campañas de desinformación como a la lucha contra el discurso de odio, se consideró la realización de una jornada con expertos en la materia.

Esta jornada se celebró el 18 de septiembre en la Facultad de Derecho de la Universidad Complutense de Madrid y contó con la colaboración del Instituto de Derecho Parlamentario en el marco del proyecto de investigación "Fortalecimiento de la democracia y el Estado de Derecho a través de la inteligencia artificial"[1]. La sesión estuvo organizada en cuatro paneles, dirigidos a abordar diferentes aspectos de la amenaza o de las posibles herramientas disponibles para limitar sus efectos.

El primer panel, orientado a conocer mejor esta amenaza, las técnicas empleadas y cómo se vinculan en la actualidad los fenómenos de las campañas de desinformación y el discurso de odio, estuvo formado por Beatriz Marín, del Servicio Europeo de Acción Exterior; Ruben Arcos Martín, profesor contratado Doctor de la Universidad Rey Juan Carlos; Alicia Moreno Delgado, profesora de la Universidad Internacional de La Rioja; Raquel Godos, de EFE Verifica; y Alejandro González, del Departamento de Seguridad Nacional, como moderador.

El segundo panel estuvo dedicado a conocer las actuales herramientas normativas y legales con las que cuenta España frente a estas amenazas y los retos y oportunidades de nuevos instrumentos como la Ley de Servicios Digitales. La mesa contó con Miguel Ángel Aguilar, Fiscal de Sala Coordinador de la Unidad de los Delitos de Odio y Discriminación de la Fiscalía General del Estado; Karoline Fernández de la Hoz Zeitler, Directora del Observatorio Español del Racismo y la Xenofobia del Ministerio de Inclusión, Seguridad Social y Migraciones; Carlos Aguilar Paredes, de la Comisión Nacional de los Mercados y la Competencia; y Alfonso Peralta Gutiérrez, Juez de Primera Instancia e Instrucción; y estuvo moderada por Rafael Bustos Gisbert, Catedrático de Derecho Constitucional de la Universidad Complutense de Madrid.

En tercer lugar, se abordaron las oportunidades que la tecnología ofrecía para detectar estas amenazas o para contrarrestarlas desde el campo de la comunicación. El panel estuvo integrado por Emilio Delgado López Cózar, catedrático de la Universidad de Granada; David Blanco Herrero, investigador posdoctoral en la Universidad de Ámsterdam (Países Bajos); Gavin Abercrombie, profesor ayudante en la Universidad Heriot Watt (Reino Unido); Flor Miriam Plaza del Arco, investigadora en la Universidad Bocconi (Italia); y estuvo moderado por Maite Martín Valdivia, catedrática de la Universidad de Jaén y Carlos Arcila Calderón, profesor titular de la Universidad de Salamanca.

El último panel puso el foco en la alfabetización mediática y el papel del tercer sector y reunió a expertos en la materia como Manuel Gértrudix Barrio, catedrático de la Universidad Rey Juan Carlos de Madrid; Alberto Izquierdo Montero, profesor ayudante doctor de la UNED; Pablo Hernández Escayola, Coordinador de Investigación Académica de Maldita.es; Natalia Sancha, del Servicio Europeo de Acción Exterior; Marisa Gómez, directora de la Plataforma de ONG de Acción Social; y Carmen Girón Tomás, doctoranda en Derecho y Ciencias Sociales, UNED, quien coordinó el panel.

La conferencia contó con un público de más de setenta asistentes del ámbito académico, expertos de organizaciones de la sociedad civil y centros de pensamiento, así como representantes de la administración pública.

---

[1] Proyecto financiado por Ministerio de Ciencia e Innovación con PID2021-122677NB-I00.

CONCLUSIONES

Conceptualización de la amenaza

Las campañas de desinformación son entendidas hoy en día en el ámbito de la seguridad nacional como patrones de comportamiento de carácter manipulativo llevados a cabo de forma coordinada e intencional con el objetivo de menoscabar los principios, valores y procesos democráticos. El carácter manipulativo puede apreciarse en la construcción del mensaje (por ejemplo, mediante el uso de *deepfakes*), en la fuente (por ejemplo, mediante la suplantación de medios de comunicación o cuentas oficiales) o en la distribución (por ejemplo, mediante el uso de cuentas automáticas o *bots*).

Los actores que despliegan este tipo de campañas de desinformación con objetivos geopolíticos suelen utilizar vulnerabilidades existentes en la sociedad, ya sea en el ámbito social, económico, político o histórico. En este sentido, en los últimos años cada vez se ha observado la utilización de la identidad como vector de ataque, entre ellas, las vinculadas a género, orientación sexual, raza, etnia o religión.

Estas campañas a menudo tienen como objetivo el fomento de divisiones sociales, menoscabando la cohesión social, así como el ataque a líderes políticos o sociales contrarios a los intereses de los actores hostiles que despliegan las campañas. Estas, además, pueden disuadir a un grupo social de participar en la vida pública y en el proceso político, lo cual genera un menoscabo del sistema democrático. Este tipo de estrategias deben entenderse como acciones de influencia coercitiva (Alonso-Villota & Arcos, 2024).

Entre las estrategias de las campañas de desinformación que usan la identidad como vector, se identifican: la acusación a una persona de tener esa identidad, el intento de modificar la percepción que se tiene en la sociedad sobre esa identidad, el fomento del acoso en línea o incluso la promoción de acciones de acoso o delitos de odio en el plano físico.

Actualmente, en España, los análisis realizados en el ámbito académico han puesto de manifiesto que los discursos de odio en Internet predominantes son de temática racista. En este sentido, los análisis de los verificadores han constatado que la desinformación asociada al discurso racista o xenófobo es la predominante en el ecosistema español. Por ejemplo, el 20% de la desinformación desmentida por los verificadores durante las elecciones al Parlamento Europeo de 2024 estaba dirigida a vincular criminalidad e inmigración.

Si bien no toda la desinformación identitaria puede ser considerada discurso de odio, uno de los retos a afrontar es conocer en qué grado estas campañas de desinformación pueden fomentar el odio, la discriminación o incluso, la violencia contra los grupos sociales objetivo. En este sentido, este tipo de campañas de desinformación suelen extenderse en el tiempo, generando un flujo continuo de eventos y narrativas que deben ser analizadas en su conjunto para poder evaluar el riesgo de radicalización. Otro factor de análisis importante es tratar de identificar a los actores sistemáticos que difunden las campañas de desinformación.

Además de utilizar un enfoque global con participación de toda la sociedad para abordar esta amenaza y promover una educación para el ciudadano con competencias adecuadas, es necesario valorar la realización de análisis anticipatorios para futuros escenarios o situaciones que puedan ser explotadas por este tipo de campañas y, de este modo, ser capaces de desplegar respuestas preventivas como el *prebunking* y la alerta de medios y verificadores.

Por último, es necesario avanzar en la protección de los actores de la sociedad civil que trabajan en la exposición y concienciación de esta amenaza, que en los últimos años se han visto expuesto a acciones de acoso, *lawfare* o incluso amenazas por parte de los actores estatales que difunden estas campañas.

Marco legal y normativo

Las características definitorias de la democracia española y del ordenamiento jurídico, principalmente el carácter normativo de la Constitución y determinados derechos fundamentales, condicionan las respuestas que puedan ofrecerse al discurso del odio desde el Derecho y los poderes públicos. España no es una democracia militante; eso implica que no se puede garantizar la libertad de expresión a través de la censura y, aunque no es un derecho ilimitado, tiene un carácter prioritario, incluso sobre otros derechos fundamentales. El disfrute de todos los derechos fundamentales exige regulaciones y medidas proporcionales y decisiones ponderadas. En consecuencia, ninguna autoridad pública puede erigirse en guardián de la verdad. La libertad de expresión es un pilar esencial de toda sociedad democrática y, por ello, han de extremarse las cautelas al decidir la eventual retirada de contenidos impuesta por autoridades administrativas y judiciales, siempre basándose en un marco normativo e institucional respetuoso con los valores y principios constitucionales.

En España existe una variedad normativa y de protocolos, tanto jurídicamente vinculante como de *soft law*, para combatir el discurso de odio *online*, ofreciendo así diversas posibilidades, desde la regulación de las plataformas y medios hasta la sanción administrativa y penal.

Destacan la Ley de Servicios Digitales (DSA) (esto es, el Reglamento (UE) 2022/2065, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales por el que se modifica la Directiva 2000/31/CE, Reglamento de Servicios Digitales), la Decisión Marco 2008/913/JAI del Consejo, de 28 de noviembre de 2008, relativa a la lucha contra determinadas formas y manifestaciones de racismo y xenofobia mediante el Derecho penal, la Recomendación de la Comisión Europea contra al Racismo y la Intolerancia (ECRI) del Consejo de Europa nº 15 sobre discurso de odio del año 2016, la Recomendación para combatir el discurso de odio del Consejo de Europa (aprobado por el Comité de Ministros el 20 de mayo de 2022) y el Protocolo para combatir el discurso de odio ilegal en línea (firmado por el Ejecutivo, el Poder Judicial y la Fiscalía), además del resto del ordenamiento jurídico nacional aplicable como el Código Penal (CP).

La utilización de dichas herramientas varía en función de las distintas modalidades de discursos de odio: en primer lugar, el penalmente relevante; en segundo lugar, el no penalmente relevante, pero con respuesta administrativa o civil; y, en tercer lugar, los mensajes ofensivos sin respuesta jurídica, pero a la que hay que responder con una contranarrativa.

Así, en principio, mentir consciente o involuntariamente, es decir faltar a la verdad, no debería comportar responsabilidades penales. Conforme a lo anterior y teniendo en cuenta que uno de

los principios que rigen el Derecho Penal es el de intervención mínima, se debe excluir *a priori* de cualquier responsabilidad penal, sin perjuicio de otro tipo de responsabilidades, la divulgación involuntaria de contenidos falsos o tendenciosos.

La desinformación penalmente relevante debe reunir cuatro elementos: que sea carente de verdad; difundida deliberadamente (la motivación ha de ser discriminatoria); dolosa; y orientada a influir y manipular la opinión pública.

La hipotética respuesta normativa a este comportamiento no está lo suficientemente clara en nuestro Código Penal dentro del catálogo de conductas tipificadas en los diferentes apartados del art. 510 CP. Pero se reflexiona sobre la posibilidad de abrir, en algunos casos excepcionales y desde una perspectiva de política criminal, el delicado debate sobre la necesidad de perseguir penalmente aquellos comportamientos en los que con manifiesto y consciente desprecio a la verdad se difunden públicamente contenidos falsos o deliberadamente manipulados en los que su autor se ha hecho o se ha podido hacer un representación razonable de que de sus publicaciones van a generar entre la población reacciones de odio, hostilidad, violencia o discriminación, humillación, menosprecio etc. contra personas o grupos por motivos discriminatorios.

Esto surge porque en la actual regulación de nuestro Código Penal existen ciertas dificultades para encajar la conducta de difundir bulos o *fake news* en los tipos delictivos existentes del art. 510 del CP.

Del análisis de las conductas incardinadas en el art. 510.1.A) y el art. 510.2.A) del CP, se desprende que la difusión de bulos podría encajar mejor en los actos de lesión a la dignidad de los colectivos hacia el que se dirige el bulo del segundo de los preceptos, pero la falta de previsión específica en este artículo para estos comportamientos hace difícil su encaje, dejando un amplio margen a su interpretación.

No hay jurisprudencia sobre desinformación en el marco de delitos de odio. Los únicos dos casos juzgados hasta el momento han sido resueltos mediante sentencias de conformidad.

Para el caso de que los hechos no sean considerados delictivos, podrían constituir una infracción administrativa sancionable, lo que requiere la tramitación de un rápido expediente administrativo con el objetivo de no dejar impune estas conductas. La eficacia en la aplicación del régimen jurídico del Derecho administrativo sancionador (Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación y Ley 4/2023, de 28 de febrero, para la igualdad real y efectiva de las personas trans y para la garantía de los derechos de las personas LGTBI), exige establecer de forma inminente mecanismos ágiles de coordinación dado que la competencia sancionatoria está repartida entre las diferentes Comunidades Autónomas, a fin de garantizar una respuesta administrativa uniforme en todo el Estado, rápida y ágil; también es necesario implementar nuevas soluciones legislativas para poder perseguir los hechos cometidos por internet y redes sociales en los que en muchas ocasiones no puede establecerse un lugar concreto de comisión; por tanto, todo ello exige una autoridad administrativa sancionadora no vinculada a una sede territorial autonómica.

En muchas ocasiones para la determinación de los responsables de estas conductas se precisa la identificación del titular de la cuenta de la red social en la que se están llevando a efecto las mismas. Tal posibilidad no se ve limitada a la investigación de delitos graves pues, al tratarse de datos de abonado que no afectan al derecho fundamental al secreto de las comunicaciones y obtenidos con la finalidad de facilitar la operatividad y agilidad de las investigaciones, el art. 588 ter m) de

la LECrim permite que puedan ser directamente recabados por el Ministerio Fiscal o la Policía Judicial en cualquier clase de investigaciones y sin necesidad de autorización judicial. Quedan con ello superados los obstáculos que planteaban los operadores de comunicaciones para la entrega de esta clase de datos con el argumento de que de que los mimos eran conservados junto con los datos de tráfico que están obligados a conservar en aplicación de la Ley 25/2007, de Conservación de Datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones - dictada en desarrollo de la Directiva 2006/24/CE posteriormente anulada por el TJUE en Sentencia a 8 de abril de 2014 – en la que se limita el acceso a los datos (de tráfico) conservados por los operadores de comunicaciones a la investigación, detección y enjuiciamiento de un delito grave exigiendo autorización judicial para su obtención.

Por su parte y en lo que se refiere al ámbito administrativo no han de olvidarse las posibilidades que ofrece el art. 10 de la DSA en base al cual, las autoridades judiciales o administrativas nacionales pertinentes, sobre la base del Derecho de la Unión aplicable o del Derecho nacional aplicable en cumplimiento del Derecho de la Unión, podrán emitir órdenes de información a los prestadores de servicios intermediarios para que informen sobre el/los destinatarios de un servicio en el marco del cual se ha publicado el discurso de odio. Dada su relevancia en esta materia el principal reto a afrontar es a agilización e impulso del desarrollo normativo interno que permita su aplicación. También ha de tenerse en cuenta las facultades que ostenta la AEPD en el marco de las investigaciones que le competen (art. 51 de la LOPD).

Cuestión distinta es la referida a la identificación de los responsables de las concretas publicaciones constitutivas de discurso de odio que hayan podido llevarse a cabo en una determinada red social en aplicación de los procedimientos sancionadores existentes en materia de discurso de odio (Ley 15/2022 o Ley 4/2023, entre otros) que sigue presentando algunos retos. Al respecto, ha de tenerse en cuenta que la obtención de las direcciones IP y otros datos de conexión vinculados a dicha publicación, al tratarse de datos de tráfico, exigen la necesidad de autorización judicial, de conformidad con lo establecido en el art. 588 ter j) de la LECrim que, por aplicación de los criterios rectores del art. 588 bis a) de la misma norma, se verá restringida a los supuestos en que dicha medida se estime proporcionada.

La relevancia de la Ley de Servicios Digitales (DSA), que pone el foco en las grandes plataformas (*Very Large online Platforms*, VLOP), está fuera de toda duda, pero para que pueda desplegar su eficacia en España es necesario que se dote de competencias a nivel estatal a la Comisión Nacional del Mercado de la Competencia (CNMC). A partir de la lectura de dicha ley, puede destacarse que el concepto de desinformación tiene tres elementos principales: en primer lugar, la falsedad del contenido; en segundo lugar, la intención de hacer daño; y, en tercer lugar, la sistemática en la propagación.

Partiendo de una base de corregulación con códigos de conducta para las VLOP, fruto del acuerdo entre la Comisión Europea y las plataformas, la Ley de Servicios Digitales puede contribuir de las siguientes maneras: en primer lugar, designación a los denominados alertadores fiables para la notificación de contenidos como actores privilegiados, defendiendo la libertad de expresión de los medios fiables (conectando esto con el Reglamento de Medios); en segundo lugar, dado que los contenidos son difundidos por plataformas, puede obligar a una plataforma a analizar los riesgos sistémicos, a crear fórmulas de mitigación de riesgos (con la supervisión de las agencias estatales y la agencia europea), a promocionar una acción conjunta de autocontrol y supervisión, a desmonetizar este tipo de contenidos, e incluso creando protocolos de crisis; en tercer lugar, tomando medidas sobre la transparencia en las reglas de moderación de contenidos, ya sea prohibiendo patrones oscuros, la elaboración de

perfiles sobre la base de datos protegidos para publicidad, u obligando a crear repositorios de anuncios.

El Protocolo para combatir el discurso de odio ilegal en línea es una herramienta de utilidad en lucha contra el discurso de odio en internet, del que podría destacarse la acreditación y la formación de los comunicantes fiables por parte de la Administración y las empresas proveedoras de servicios de alojamiento de datos (apartado IV), para identificar así discursos de odio (a diferencia con la DSA, por la que se puede formar, pero no acreditar). La entrada en vigor de la DSA y la creación de la nueva figura del Coordinador de Servicios Digitales exigirá la modificación del contenido del citado Protocolo para dar una nueva respuesta coordinada en la retirada de contenidos ilícitos.

De la aplicación de este protocolo puede deducirse que la mayoría del discurso de odio detectado reúne cuatro elementos: en primer lugar, el grupo de los más afectados, que en la actualidad son personas del norte de África, musulmanes, raza negra; en segundo lugar, el tipo de discurso, destacando un 53% deshumanización grave y discurso agresivo explícito un 54%; en tercer lugar, vinculación a eventos sobre inseguridad ciudadana; y en cuarto y último lugar, uso de información falsa.

Ámbito tecnológico

La tecnología juega un papel dual en el contexto de la desinformación y el discurso de odio. Por un lado, se ha constatado que las herramientas tecnológicas pueden amplificar estos problemas. Las redes sociales y las plataformas digitales son usadas para diseminar desinformación de manera rápida y masiva, fomentando la polarización social y el discurso de odio. La reciente democratización de los modelos de lenguaje avanzados, como los modelos de IA generativa, puede empeorar esta situación al facilitar la creación de contenido manipulado y falso de manera más sutil y efectiva.

Por otro lado, tenemos la responsabilidad de aprovechar estas mismas tecnologías para contrarrestar estos efectos negativos. Los avances en la inteligencia artificial y las tecnologías de procesamiento de lenguaje natural pueden utilizarse ya no solo para detectar patrones de comportamiento inapropiados (como discursos de odio, ofensividad, desinformación) sino también para mitigarlos mediante la generación de contranarrativas que nos permitan contrarrestar estos discursos de odio mediante discursos positivos que favorezcan una interacción digital mucho más respetuosa y constructiva.

La rápida evolución en los últimos años de la inteligencia artificial generativa y, en especial de los modelos lingüísticos de gran tamaño (LLM), ha centrado el foco en muchos investigadores que trabajan en la detección de discurso en línea y en la creación de contranarrativas.

Sin embargo, el uso de estos modelos para la detección del discurso de odio plantea algunos retos, como la necesidad de contar con modelos entrenados en los idiomas de interés (castellano y lenguas cooficiales), de avanzar en la detección de sarcasmo e ironía, y en la adaptabilidad a la ambigüedad del lenguaje y la evolución temporal del mismo, así como a la diversidad lingüística regional. Por otro lado, existen algunos factores que se consolidan como oportunidades para el uso de estos modelos, entre ellos la existencia de numerosos recursos en español para poder entrenar estos modelos, la capacidad de los mismo de tener un aprendizaje continuo, o la cada vez mayor cooperación multidisciplinar de expertos, desde sociólogos y psicólogos hasta especialistas en el ámbito del Derecho.

Los elevados niveles de información que se observan actualmente en las redes sociales hacen que la detección del discurso de odio automatizada no sea suficiente ya que, aunque se detecte, no existen suficientes recursos para hacerle frente de forma manual. Por ello, estos modelos de inteligencia artificial también están siendo probados para las labores de mitigación y generación automática de contranarrativas. De esta forma, se elabora una alternativa a la del bloqueo o eliminación de estos mensajes que es menos lesiva con la libertad de expresión y se integra como un posible mecanismo en la prevención de la radicalización.

La generación de contranarrativas se basa en la creación automática o supervisada de respuestas a mensajes de odio en las que se ofrece una visión alternativa y positiva. Actualmente se han estudiado diferentes estrategias de contranarrativas, si bien no todas tienen la misma efectividad, dependiendo de cada situación y del público al que van dirigidas. Del mismo modo que los actores hostiles que promueven o difunden campañas de desinformación explotan las vulnerabilidades existentes en las sociedades objetivo, la defensa frente a la desinformación y la influencia hostil en el entorno de información mediante narrativas positivas debe partir de un análisis, no sólo de nuestras vulnerabilidades y de qué nos divide, sino también de nuestras fortalezas y de aquello que nos mantiene unidos y cohesionados como sociedad democrática, plural y respetuosa con las diferencias en las características identitarias existentes.

Actualmente, estos diseños requieren de una implementación más extensa y de la necesidad de mejorar los mecanismos para evaluar la efectividad de las contranarrativas.

Por otro lado, aunque poco a poco se ha avanzado en el estudio de los algoritmos de promoción y recomendación de contenido de las plataformas, es necesario seguir progresando para entender las implicaciones para el fomento de la polarización, así como comprender cómo las dinámicas de sobreestimulación que promueven los modelos actuales de atención de algunas redes impactan negativamente en los mecanismos cognitivos necesarios para la correcta evaluación e integración de la información.

Alfabetización mediática, concienciación y el papel del tercer sector

La alfabetización mediática e informacional es un reto esencial para combatir eficazmente la desinformación. En el ámbito académico, no es solo importante incluir en el BOE un *currículum* sobre desinformación sino promover los esfuerzos para que llegue de forma efectiva a las aulas.

Además, la capacidad actual de la alfabetización en el ámbito educativo no es suficiente, dado que la capacidad de actuar de la academia es limitada. En el actual entorno informativo los medios de comunicación y las plataformas digitales son los que tienen mayor capacidad de llegar a todos los públicos.

La formación a la ciudadanía, y en especial a los jóvenes, ha de incidir en mejorar su capacidad para detectar bulos, trabajando el pensamiento crítico, el análisis del contexto, la evaluación con indicadores, previamente facilitados, para que sirvan para analizar los condicionamientos a la credibilidad de la fuente. Esto aplica tanto al medio escrito como al audiovisual, e incluso al acústico.

También el avance en el conocimiento de las diferentes tácticas utilizadas en la difusión de discurso de odio y desinformación son esenciales para informar la alfabetización mediática.

Así, por ejemplo, los mensajes que contienen un componente de odio son más propensos a ser compartidos; sin embargo, tienden a disminuir su credibilidad en general. Este factor es relevante a la hora de avanzar en el plano de la concientización y alfabetización.

Por otro lado, el rol a desempeñar por las familias, en colaboración con los docentes es esencial para facilitar el trabajo en las aulas de la aceptación del desacuerdo, el disenso, la diversidad de perspectivas, del conflicto, inherente a las relaciones sociales, para ayudar a confrontar y aun a prevenir el discurso de odio en las redes sociales. La educación se ha mostrado eficaz para interrumpir el proceso que activa el odio y la violencia.

También la verificación de la comunicación, cualquiera que sea el medio que se utilice, se ha demostrado como un elemento eficaz para detectar y neutralizar la desinformación desapercibida, aunque requiere de una alta especialización, recursos y tiempo. Además, no es suficiente con el señalamiento o etiquetado como desinformación, sino que es necesario explicar por qué es desinformación. La colaboración entre verificadores y la transparencia metodológica a la hora de trabajar estos asuntos también son clave. En este sentido, mecanismos como las notas de comunidad o sistemas de etiquetado de contenido fruto de trabajo colectivo de los usuarios agregando contexto o verificaciones en contenido engañoso, es un complemento de la moderación de contenido que debiera potenciarse.

A su vez, los profesionales, no solo de ciencias de la información, sino de todo tipo de medios de comunicación social, salvaguardada la libertad de expresión, precisan de ejercicios de formación y sensibilización sostenidos en el tiempo, con enfoque de interculturalidad e interseccionalidad. Es importante incluir a los educadores en los debates en la formulación de estrategias, no solo de alfabetización mediática sino, también, de comunicación. Con esto se puede tener en cuenta y valorar también los efectos a largo plazo de las mismas. También es necesario concienciación en el ámbito empresarial para limitar la monetización de este tipo de campañas, eliminando o limitando la motivación lucrativa.

Actualmente, las organizaciones del tercer sector carecen de recursos y procedimientos comunes para abordar esta amenaza. La cooperación con otros actores de la sociedad civil, como los verificadores, ha dado buenos resultados para entender mejor esta amenaza.

En este sentido, la DSA constituye el instrumento preciso en la actualidad para articular la colaboración responsable triangulada, precisa entre las autoridades nacionales, los prestadores de servicios digitales globales, marcadamente, las redes sociales pero no exclusivamente, y las organizaciones de la sociedad civil, idóneamente a través de plataformas que las aglutinen y las empoderen, para trascender a los procesos participativos actuales, y posicionarse como prescriptores estratégicos a considerar, para colaborar en establecer las bases de las políticas públicas y argumentarios especializados para prevenir y luchar contra la desinformación y el discurso de odio.

Por último, y debido a la dimensión internacional de la desinformación, es importante colaborar con el resto de países para que impulsen mecanismos de concientización y alfabetización, así como promover que las herramientas de detección y los recursos de moderación en los diferentes idiomas sean suficientes. Con ello, se avanzará en limitar el impacto que estas campañas pueden tener sobre los colectivos en terceros países y también limitar su difusión, evitando que se trasladen a nuestro país por la permeabilidad de las redes o, incluso, a través de la diáspora. A la hora de impulsar acciones de comunicación o alfabetización en otras regiones es esencial atender a las circunstancias culturales y sociales de aquellas, a fin de evitar amplificar el propio efecto de la desinformación.

RECOMENDACIONES

Es necesario avanzar en el plano de la **concienciación** para entender y documentar mejor esta amenaza y sus efectos y para tener una base para implicar a todos los actores de la sociedad que deben aunar esfuerzos para luchar contra la misma.

Las narrativas están identificadas. Las estrategias también comienzan a estar identificadas. La identificación plena de ambas (narrativa más estrategia) permitirá identificar de manera cada vez más elaborada la intencionalidad *prima facie* (especialmente si usamos inteligencia artificial para ello). Esto puede suponer un avance muy significativo para la lucha contra los discursos de odio porque tendremos uno de los elementos más difíciles (la intención del autor) en su definición. Obviamente en caso de controversia será solo una identificación provisional susceptible de revisión judicial posterior.

Parece prometedor proceder a la identificación de los "actores". Tanto más posible si hemos desarrollado el punto anterior (identificación de narrativas, estrategias e intencionalidad). Podría explorarse la posibilidad de que los actores habituales de desinformación para creación de discurso de odio puedan ser tratados como algo parecido a "organización criminal".

En el **ámbito normativo**, será necesario valorar una reforma del art. 510 CP para incluir la persecución penal de la difusión pública y maliciosa de contenidos manifiestamente falsos en las condiciones expuestas anteriormente. En este sentido, debería valorarse la posibilidad de abrir el debate jurídico, sin prejuzgar un resultado concreto, tanto a nivel nacional como europeo, sobre la oportunidad desde una perspectiva de política criminal de crear nuevo tipo delictivo específico, con todas las cautelas y limitaciones apuntadas, para perseguir penalmente aquellos comportamientos en los que, de manera concertada y coordinada, con manifiesto y consciente desprecio a la verdad se difunden públicamente contenidos falsos o deliberadamente manipulados en los que su autor se representa o pueda representarse razonablemente que de sus publicaciones se van a generar entre la población reacciones de odio, hostilidad, violencia o discriminación, humillación o menosprecio contra personas o grupos por motivos discriminatorios, todo ello con el fin de evitar una interpretación forzada del actual delito de lesión de la dignidad por motivos discriminatorios previsto en el art. 510.2.A) del CP, dado que existen verdaderas dificultades para incluir la conducta consistente en difusión de bulos. La redacción del nuevo delito debería limitarse a los supuestos de intencionalidad directa de la acción de expandir bulos o de llevar a cabo la acción con dolo eventual o culpa consciente para no dejar atípica ninguna conducta.

No obstante, no se deben usar herramientas excesivas en la respuesta sancionatoria ni en la posible amenaza a los propios valores defendidos. Una respuesta colaborativa y graduada parece mucho más aconsejable. Se debería poder acudir a la vía administrativa para los hechos que no sean graves y que no supongan una puesta en peligro del colectivo al que atacan.

Es necesario mejorar en la regulación y aplicación del régimen administrativo sancionador y en la posibilidad de cesión de datos de tráfico para procedimientos administrativos sancionadores y civiles de vulneración del derecho al honor, intimidad o propia imagen, así como en la coordinación entre instituciones estatales y autonómicas para garantizar la efectiva imposición de sanciones y evitar su prescripción. Se han de implementar soluciones para garantizar una respuesta coordinada, uniforme y útil en el ámbito administrativo sancionador que implique a todas las administraciones estatales y autonómicas para limitar el alcance y efectos de estas amenazas; en

todo este proceso, penal y administrativo, deberá jugar un papel clave el Coordinador de Servicios Digitales en el marco del Reglamento de Servicios Digitales en la retirada de contenidos ilícitos penales y administrativos para lo cual se tienen que efectuar las habilitaciones normativas precisas de forma urgente.

Por último, es necesario implementar de forma urgente las previsiones de la DSA (Reglamento 2022/2065 del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales) y del protocolo de retirada de contenidos ilícitos en internet.

Por otro lado, uno de los principales retos **en el campo tecnológico** es la transferencia de las diferentes investigaciones que se están desarrollando en el marco de la detección y respuesta a estas amenazas. Es necesario identificar posibles oportunidades para la implementación efectiva de estas tecnologías.

La utilización de herramientas de inteligencia artificial en la lucha contra la desinformación vinculada al discurso de odio parece la vía más prometedora, pero todavía no está suficientemente desarrollada. Se plantean dificultades técnicas y jurídicas. De ahí se deducen dos necesidades: en primer lugar, incrementar los esfuerzos en términos de recursos materiales y humanos para el diseño de herramientas eficaces; en segundo lugar, asegurar la interdisciplinariedad en el diseño para la inclusión de los valores éticos y jurídicos que se pretenden defender.

El uso de herramientas de inteligencia artificial requiere, a su vez, una supervisión adecuada de éstas y su consideración como herramientas de alto riesgo. Eso supondría cubrir exigencias técnicas (Reglamento de IA de la UE) y establecer los procedimientos para que los poderes públicos las autoricen, reconozcan, implanten y supervisen (gobernanza de la lucha con inteligencia artificial contra los discursos de odio basados en desinformación).

En el ámbito de la **alfabetización mediática**, es esencial identificar estrategias para garantizar que esta llegue realmente a los ciudadanos. Para ello es necesario implicar a los medios de comunicación y a las plataformas digitales, así como garantizar que los currículos académicos sobre desinformación se implanten de forma efectiva en todas las aulas.

Además, sería interesante no sólo una contranarrativa sino también un enfoque de exposición pública o contramarca, revelando a la sociedad las operaciones de influencia, desinformación e intentos de manipulación a la población española.

Por último, es necesario avanzar en la formación de las **organizaciones del tercer sector**, explorando mecanismos de cooperación con otros actores como los verificadores, la academia o las plataformas digitales. Además, es interesante fomentar el desarrollo de procedimientos comunes que faciliten el trabajo de las organizaciones en esta materia.

GOBIERNO DE ESPAÑA · PRESIDENCIA DEL GOBIERNO · GABINETE DE LA PRESIDENCIA · DEPARTAMENTO DE SEGURIDAD NACIONAL · FORO CONTRA LAS CAMPAÑAS DE DESINFORMACIÓN EN EL ÁMBITO DE LA SEGURIDAD NACIONAL

Colabora · INSTITUTO DE DERECHO PARLAMENTARIO

CONFERENCIA CAMPAÑAS DE DESINFORMACIÓN Y PROMOCIÓN DEL DISCURSO DEL ODIO

Aula Polivalente II de la Facultad de Derecho de la Universidad Complutense de Madrid
Pl. Menéndez Pelayo, 4, Madrid

MIÉRCOLES 18 DE SEPTIEMBRE DE 2024

09:45 **Bienvenida**

10:00 **Definición y valoración de la amenaza**
- Beatriz Marín, Servicio Europeo de Acción Exterior.
- Ruben Arcos, Universidad Rey Juan Carlos de Madrid.
- Alicia Moreno Delgado, Universidad Internacional de La Rioja.
- Raquel Godos, EFE Verifica.
- Alejandro González, Departamento de Seguridad Nacional.

11:45

12:00 **Marco legal y normativo**
- Miguel Ángel Aguilar, Fiscal de Sala Coordinador de la Unidad de los Delitos de Odio y Discriminación de la Fiscalía General del Estado.
- Julio del Valle de Iscar, Director General para la Igualdad Real y Efectiva de las Personas LGTBI+ del Ministerio de Igualdad.
- Karoline Fernández de la Hoz Zeitler, Directora del Observatorio Español del Racismo y la Xenofobia del Ministerio de Inclusión, Seguridad Social y Migraciones.
- Carlos Aguilar Paredes, Comisión Nacional de los Mercados y la Competencia.
- Alfonso Peralta Gutiérrez, Juez de Primera Instancia e Instrucción.
- Rafael Bustos Gisbert, Catedrático de Derecho Constitucional de la Universidad Complutense de Madrid.

13:45

Pausa comida

15:45 **Retos y oportunidades de las nuevas tecnologías**
- Emilio Delgado López Cózar, Universidad de Granada.
- David Blanco Herrero, University of Amsterdam (Países Bajos).
- Gavin Abercrombie, Heriot Watt University (Reino Unido).
- Flor Miriam Plaza del Arco, Bocconi University (Italia).
- Maite Martín Valdivia, Universidad de Jaén.
- Carlos Arcila Calderón, Universidad de Salamanca.

17:30

15:45 **Comunicación estratégica, alfabetización mediática y el papel del tercer sector**
- Manuel Gértrudix Barrio, Universidad Rey Juan Carlos de Madrid..
- Alberto Izquierdo Montero, UNED.
- Pablo Hernández Escayola, Maldita.es.
- Natalia Sancha, Servicio Europeo de Acción Exterior.
- Marisa Gómez, Plataforma de ONG de Acción Social.
- Carmen Girón Tomás, Doctoranda en Derecho y Ciencias Sociales, UNED.

19:10

ANEXO: Agenda de la conferencia celebrada el 18 de septiembre de 2024

REFERENCIAS BIBLIOGRÁFICAS

Alonso-Villota, M., & Arcos, R. (2024). The Coercion-Manipulation-Persuasion Framework: Analyzing the Modus Operandi of Systems of Non-State Actors. Terrorism and Political Violence. doi:10.1080/09546553.2024.2357082

EEAS Stratcom Division. (2023). FIMI targeting LGBTIQ+ people: Well-informed analysis to protect human rights and diversity. Servicio Europeo de Acción Exterior. Obtenido de https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-LGBTQ-Report.pdf

Hoogensen Gjørv, G., & Jalonen, O. (2023). Identity as a tool for disinformation: Exploiting social divisions in modern societies. Centro Europeo de Excelencia para la Lucha contra las Amenazas Híbridas. Obtenido de https://www.hybridcoe.fi/wp-content/uploads/2023/11/20231108-Hybrid-CoE-SA-34-Identity-as-a-tool-for-disinformation-WEB.pdf

Red de Concienciación sobre la Radicalización (RAN). (2020). The Impact of Conspiracy Narratives on Violent RWE and LWE Narratives. Comisión Europea. Obtenido de https://home-affairs.ec.europa.eu/system/files/2021-01/ran_c-n_concl_pap_impact_consp_narr_on_vrwe_vlwe_24-25_112021_en.pdf

Szakács, J., & Bognár, É. (2021). The impact of disinformation campaigns about migrants and minority groups in the EU. Parlamento Europeo. Obtenido de https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/653641/EXPO_IDA(2021)653641_EN.pdf

CAPÍTULO 6

ESCEPTICISMO MEDIÁTICO Y DE LA OPINIÓN PÚBLICA ESPAÑOLA ANTE LA EXISTENCIA DE CAMPAÑAS DE DESINFORMACIÓN QUE AFECTAN A LA SEGURIDAD NACIONAL

Coordinadores:

Emilio Andreu

Departamento de Seguridad Nacional

Autores y colaboradores:

Maria Inmaculada López Núñez

María Penedo Jiménez

Jordi Rodríguez Virgili

INTRODUCCIÓN

¡Ojalá! que el escepticismo fuera el de Hume, aquél que rescató a Kant de su "sueño dogmático", como confesó el propio filósofo de Königsberg. Pero no. Lejos de su origen etimológico –skeptesthai, examinar, observar con detenimiento, en griego clásico-, hemos de referirnos, ineluctablemente, a ese territorio mental situado en medio de la nada, entre el tedio y la indiferencia.

Nadie razonable duda de las injerencias extranjeras, las de Rusia, especialmente, contra los países de la Unión Europea y de la OTAN, para minar la confianza social en esas organizaciones multilaterales, en particular, y, en general, contra los pilares del sistema democrático basado en reglas. Un terreno este que, de suyo, se encuentra ya abonado, a tenor de los resultados que ofrece la "Encuesta Sobre Tendencias Sociales" que elabora el CIS. La última, de octubre de 2023, dibujaba un panorama desolador en los porcentajes marginales de mínima-máxima confianza de la sociedad respecto a las principales organizaciones políticas e institucionales.*(veasé tabla)*

La actual irrelevancia de los *mass media* no solo la observamos en España. El último informe del "Instituto Reuters para el Estudio del Periodismo", correspondiente a 2024, detecta que apenas el 40% de los encuestados en 47 países afirma que confía en la mayoría de las noticias. No es nueva esa renuencia del público a creer en lo que le informan la prensa, radio y televisión. Así, en 1991, el 67 por ciento de los franceses no otorgaba la menor confianza a lo que la imprenta o las ondas les contaban, según un sondeo realizado por el instituto privado de encuestas ESOP (Études et Sondages d'Opinion Publique). Un fenómeno que los expertos de hace 33 años achacaban a la manipulación mediante la avalancha de informaciones travestidas de espectáculo.

Volviendo a la actualidad, en la era de las redes sociales y de mensajería instantánea, esos *mass media* de quinta generación, parece haber quedado abolido el aforismo, atribuido a Agustín de Hipona, de "contra facta non valent argumenta", contra hechos no caben argumentos. Al contrario, la verdad y los hechos no importan, estarían superados por las narrativas posfactuales.

El 29 de febrero de 2024 el Foro contra las campañas de desinformación en el ámbito de la seguridad nacional acordó la creación de un grupo de trabajo con el objetivo principal de conocer si era plausible o no la hipótesis de unos medios de comunicación y una opinión pública escépticos ante las alarmas sobre el aparato desinformativo, de actores estatales que recurren de forma reiterada a estas tácticas, como Rusia.

Es imprescindible conocer el punto de partida de la opinión pública en cuanto a concienciación y conocimiento sobre estas amenazas, ya que las mismas condicionarán y serán explotadas por las estrategias de los actores hostiles y deben de ser tenidas en cuenta en la formulación de políticas públicas dirigidas a la concienciación y la alfabetización mediática.

Para coordinar este grupo de trabajo se designó a Emilio Andreu, vocal del Foro en representación de las asociaciones de periodistas, así como al Departamento de Seguridad Nacional como coordinador por parte de la administración pública. El grupo de trabajo se conformó con los expertos que figuran al comienzo de este capítulo.

Pregunta 4
En general, ¿podría valorar de 1 a 10 la confianza que Ud. tiene en estos momentos en cada una de estas organizaciones políticas e institucionales, entendiendo que el 10 representaría "la máxima confianza" y el 1 "la mínima confianza"?

Grados de valoración	1 mínima confianza	2	3	4	5	6	7	8	9	10 máxima confianza	N.S.	N.C.	(N)
En los partidos políticos	26,3	8,3	10,3	11,8	18,3	11,3	7,0	3,6	1,0	1,1	0,3	0,7	(4.121)
En los sindicatos	29,6	7,9	9,8	9,3	14,8	10,1	8,4	4,9	1,6	1,6	1,5	0,4	(4.121)
En el Gobierno de España	33,7	6,8	6,6	8,7	11,5	9,2	9,7	7,4	2,6	3,1	0,3	0,4	(4.121)
En el Parlamento español	21,2	7,4	8,9	11,1	17,9	11,1	10,0	6,4	1,9	2,7	1,1	0,3	(4.121)
En los medios de comunicación social (prensa, radio, televisiones)	19,3	9,7	11,8	12,5	18,9	10,9	7,9	5,0	1,3	1,8	0,3	0,5	(4.121)
En la Justicia	12,4	6,6	8,4	10,3	18,5	13,9	13,9	10,2	2,4	2,6	0,4	0,2	(4.121)
En la Constitución de 1978	6,9	2,9	4,4	5,3	12,4	9,8	12,3	16,9	11,9	14,6	1,9	0,6	(4.121)

TABLA: "Encuesta Sobre Tendencias Sociales" que elabora el CIS. Octubre 2023

DESARROLLO DE LA INICIATIVA

El objetivo de este grupo era analizar si en la conversación pública española se trivializan las injerencias extranjeras para minar la confianza social en las instituciones. El grupo de expertos estimó que la forma de valorar este posible escepticismo sobre las campañas de desinformación era a través de dos grupos de discusión.

El grupo de discusión es una técnica de investigación cualitativa que consiste en reunir a un conjunto de informantes para que expresen su opinión, debatan y contesten a preguntas en torno a un tema de interés para el investigador. Está constatada la utilidad de este método de investigación en la validación de hipótesis o propuestas.

El grupo de expertos decidió realizar dos grupos distintos: uno más enfocado a la opinión pública y otro centrado en la función de los medios de comunicación. Ambos están íntimamente relacionados, como se pudo comprobar en los debates, pero se consideró que diferenciando estos ámbitos se ganaría profundidad en la conversación.

Por tanto, se celebraron dos grupos de discusión dirigidos a evaluar la hipótesis de si existe escepticismo en España ante la existencia de campañas de desinformación que afectan a la seguridad nacional, tanto en el ámbito de la opinión pública como en los medios de comunicación.

El grupo de expertos seleccionó a los "informantes" que iban a participar en ambos grupos. En el panel de Opinión Pública se contó con la experiencia de:

- Sergio Hernández. Responsable de EFEVerifica.
- Helena Matute. Catedrática de Psicología Experimental en la Universidad de Deusto.
- Andrés Medina. Socio fundador de Gravitas.
- José Javier Olivas. Investigador y profesor del Departamento de Ciencia Política y de la Administración de la UNED.
- Hélène Verbrugghe. Public Policy Manager para España y Portugal de Meta.

Para el panel de medios de comunicación:

- César González Antón, director de La Sexta Noticias.
- Jose Antonio Zarzalejos, presidente del Comité editorial de Elconfidencial.
- María Rosa Berganza Conde, catedrática de Comunicación Política y directora de Center for Media and Political Communication Research de la Universidad Rey Juan Carlos.
- Xavier Colás, periodista.

Previamente a la reunión, se les explicó la dinámica y se les envió las preguntas centrales:

- Pregunta de investigación: ¿Existe escepticismo en la opinión pública española respecto a la existencia de campañas de desinformación que afectan a la seguridad nacional?. Breve exposición de los argumentos que justifiquen su respuesta.

Preguntas para elaborar la exposición inicial:

- Según los datos del Eurobarómetro "Ciudadanía y Democracia" (EB 528), el 72% de los ciudadanos españoles está de acuerdo (54% totalmente de acuerdo, 28% más bien de acuerdo) en que las injerencias extranjeras en nuestro sistema democrático constituyen un problema grave que hay que atajar A la luz de estos resultados, parecería que la respuesta a la pregunta de investigación es negativa. ¿Está usted de acuerdo con esta interpretación?. En caso contrario, ¿cómo lo explicaría?.

- Desde su conocimiento y experiencia profesional, ¿qué factores considera relevantes en la percepción de las campañas de desinformación por parte de la ciudadanía que podrían contribuir o mitigar el escepticismo hacia éstas?.

En el caso del grupo de medios de comunicación, la pregunta de investigación era la misma, pero las cuestiones de apoyo variaban ligeramente:

- Tanto en caso de respuesta afirmativa o negativa de la pregunta de investigación (con los matices pertinentes), ¿cuáles creen que son las causas principales de esta percepción por parte, sobre todo, de los medios de comunicación?.

- Desde su conocimiento y experiencia profesional, ¿qué puede hacer el periodismo y los medios de comunicación para mantener/aumentar la toma de conciencia por parte de la opinión pública hacia las campañas de desinformación?.

A los dos grupos, se les facilitó enlaces a diversos informes y encuestas sobre la percepción de la desinformación en España.

El primer grupo de discusión tuvo lugar el jueves 26 septiembre en el Complejo de la Moncloa. Los miembros del grupo de expertos Inmaculada López Núñez, profesora en el Departamento de Psicología Social, del trabajo y diferencial de la Universidad Complutense de Madrid, y Jordi Rodríguez Virgili, profesor de Comunicación Política de la Universidad de Navarra, moderaron el debate. El resto de miembros del grupo de expertos acudió a la sesión, pero no intervinieron.

El segundo grupo se desarrolló el jueves 3 de octubre en la sede de la Asociaciones de la Prensa de Madrid. Los miembros del grupo de expertos Emilio Andreu, vocal de la Federación de Asociaciones de Periodista de España (FAPE), y María Penedo, directora de comunicación de la Unión de Televisiones Comerciales Asociadas (UTECA), moderaron el debate. El resto de miembros del grupo de expertos acudió a la sesión, pero no intervinieron.

En base a las discusiones de ambos paneles y a la propia experiencia y conocimiento de los miembros del grupo, se extrajeron las conclusiones y recomendaciones más comunes o interesantes, sin que ello refleje unanimidad en los expertos o en el grupo de trabajo sobre las mismas.

CONCLUSIONES

Existe concienciación sobre el riesgo genérico de la desinformación y de la injerencia extranjera. Sin embargo, falta concienciación sobre el objetivo concreto de la amenaza y cómo afecta al ciudadano; no hay percepción de amenaza concreta. Algunas posibles causas son:

- Falta de información que llega al ciudadano medio sobre estas amenazas.
- La ocultación, minimización o ridiculización en España de las acciones de injerencia extranjera.
- El ciudadano puede tener la percepción de ser tratado como víctima de la desinformación y que solo la Administración Pública del Estado o el Gobierno debe combatirla. No se le hace corresponsable para combatirla o, al menos, minimizarla.
- La politización de los casos de injerencia extranjera. La dinámica partidista y la polarización favorecen la politización de estas cuestiones, lo cual puede ser aprovechado por los actores hostiles.
- La complejidad de la amenaza: aunque las estrategias de manipulación no son nuevas, las tácticas utilizadas y su complejidad dificultan, por un lado, su identificación y exposición y, por otro, que la sociedad pueda percibir la intensidad de la manipulación y, por ende, cómo se materializa la amenaza.
- El acoso/ataque a los actores de la academia, verificadores o sociedad civil que trabajan en la identificación de estas amenazas, limita su exposición pública y la denuncia de estas tácticas de forma más abierta.
- El aumento del fenómeno de "desconexión mediática", "fatiga mediática" o "evitación de noticias" puede generar la percepción de no exposición a la amenaza o incluso desinterés por la misma.
- La percepción de una amenaza interior al sistema democrático y la prosperidad dificultan la percepción de la amenaza exterior, quedando relegada a un segundo plano. En este sentido, algunas encuestas apuntan a una sociedad disgustada con el funcionamiento de la democracia en nuestro país.
- Los principales actores responsables de la concienciación sobre la amenaza no son los que gozan mayores niveles de confianza en la sociedad (gobierno, responsables políticos y medios de comunicación).
- Las campañas de desinformación de actores estatales extranjeros son un continuo, lo cual dificulta su identificación y exposición. Uno de los principales objetivos de las campañas de desinformación no es vender una mentira sino conseguir que la gente no crea en nada generando desconfianza en general. De esta forma se busca que la ciudadanía se vuelva escéptica y se desconecte de la vida pública, socavando la cohesión social y, por ende, fragilizando el modelo de Estado.

- Esta sociedad cada vez más desconectada de la vida pública, cuando conecta lo hace de manera polarizada, con lo que se refuerza el sesgo de confirmación donde se puede llegar a aplaudir o, al menos, minimizar la desinformación que daña al adversario político. Esta desconexión también se deriva de una saturación informativa.

- La amenaza del enemigo exterior en la historia española se remonta a tiempos lejanos, invasión francesa, mientras que los conflictos más recientes han sido internos. Esto puede dificultar la percepción de una amenaza exterior frente a la doméstica.

- La falta de una cultura de Seguridad y Defensa. Existe la percepción de que hablar de una cultura de Seguridad y Defensa es un tema de épocas pasadas, vinculado a valores ideológicos, políticos y no a valores democráticos.

Los medios de comunicación encuentran diferentes dificultades a la hora de transmitir la información relativa a las campañas de desinformación asociadas a las injerencias extranjeras. Entre ellas:

- La Seguridad Nacional no está en la agenda de los medios. La Seguridad Nacional no tiene un perfil definido que permita englobar las noticias que le afectan. Es un término considerado amplio y ambiguo en la opinión pública.

- No existe un circuito informativo bien definido en materia de seguridad nacional al que los periodistas puedan acudir para requerir información sobre estos asuntos.

- No hay suficientes portavoces oficiales con capacidad de comunicación y conexión con las audiencias para intervenir en la conversación pública sobre estos asuntos.

- Lo anterior también deriva en una escasa especialización entre los periodistas en materia de seguridad nacional.

Además, el sistema de medios de comunicación suele ser un objetivo principal de los actores hostiles que, en la actualidad, aprovechan algunas de las vulnerabilidades existentes en el modelo de este sector para degradar la confianza de la sociedad en los mismos y dirigir a los ciudadanos a fuentes “alternativas”, como canales de redes sociales y aplicaciones de mensajería, para fomentar un consumo de información no contrastada. Algunas de estas vulnerabilidades vienen derivadas del nuevo marco, fruto de la disrupción tecnológica.

Actualmente los medios de comunicación siguen siendo el referente en nuestro país para que los ciudadanos se informen, tal como refleja el I Estudio sobre la desinformación en España, realizado por UTECA y la Universidad de Navarra en 2022, y que recoge como el 84,6% de los encuestados sigue prefiriendo los medios de comunicación frente a las redes sociales para informarse y el 80,9% de los encuestados afirma que son la mejor garantía frente a la proliferación de la desinformación. Sin embargo, esto no significa que el sector aborde algunos retos:

- El anonimato de las redes sociales contribuye a la polarización y falta de contraste de lo publicado, una situación que se ha reproducido en las secciones de comentarios de las informaciones o foros de los periódicos, asimismo amparados en el anonimato.

- Eliminar las barreras que existían para entrar en el sector de la producción y difusión de contenidos (también periodísticos) ha generado un entorno competitivo caótico, en el que aparecen y desaparecen negocios informativos nuevos, propuestas 'periodísticas' de todo tipo, que compiten en un mercado de la atención cada vez más desestructurado y atomizado. En ese mercado, la debilidad económica e institucional de los medios tradicionales favorece prácticas de influencia y control sobre ellos.

- El sector de los medios debe competir de forma desigual frente a otros, sobre todo el tecnológico. Los medios de comunicación, sujetos a regulaciones más estrictas, compiten en desigualdad de condiciones.

- La descapitalización de los medios tradicionales, con redacciones más pequeñas y peor remuneradas y con menos recursos, dificulta tener periodistas especializados, enviar corresponsales o desarrollar investigaciones en profundidad.

- El actual contexto social exige la transmisión de mensajes atractivos con el fin de competir con las narrativas desinformadoras que recurren a mensajes sensacionalistas o alarmistas frente a los hechos. Actualmente, dato no gana a relato. Una realidad que obliga a los periodistas contar el dato que contrarresta esas desinformaciones de una forma atractiva, con emoción, pasión e intensidad.

RECOMENDACIONES

Fomentar la alfabetización mediática y la concienciación:

- Impulsar la alfabetización mediática y la concienciación (para entender mejor la amenaza y el impacto que puede tener en la esfera cercana de la persona y también para poner en valor la información de calidad frente a la saturación informativa actual).

- Procurar que la información sobre actos de injerencia extranjera no sea minimizada, sin tampoco llegar a exagerarla. Igualmente evitar su ocultación, ridiculización o politización. Fomentar una cultura transparencia que simplifique el acceso a los datos a periodistas, investigadores y ciudadanos.

- Promover una ciudadanía activa, concienciar sobre el papel y responsabilidad de los ciudadanos en el consumo de información y que son y parte activa en la lucha contra la desinformación. La labor de la ciudadanía puede ser clave identificando, denunciando y evitando compartir contenidos no veraces y manipulados.

- Realizar estudios más específicos dirigidos a conocer mejor la percepción ciudadana y la banalización de las amenazas e injerencias extranjeras.

- Promover una cultura de Seguridad y Defensa Nacional entre la ciudadanía. Concienciar sobre el concepto de Defensa Nacional como valor democrático.

- Fomentar la transmisión de mensajes atractivos con el fin de competir con las narrativas desinformadoras y promover la concienciación y la alfabetización mediática, tanto en el marco de la labor de comunicación de los medios como de la Administración Pública.

Promover la inclusión de la Seguridad Nacional en la agenda mediática:

- Establecer un circuito informacional en el ámbito de la Seguridad Nacional, identificando puntos de contacto claros para periodistas y promoviendo la formación de los mismos en la materia.

- Impulsar la formación de periodistas en el ámbito de la seguridad nacional.

- Favorecer una labor más didáctica por parte de los medios de comunicación sobre las injerencias extranjeras· Necesidad de construir relatos atractivos que permitan llegar a la sociedad·

- Impulsar la presencia de portavoces oficiales expertos en seguridad nacional con capacidad para comunicar de una forma eficaz, creíble y cercana.