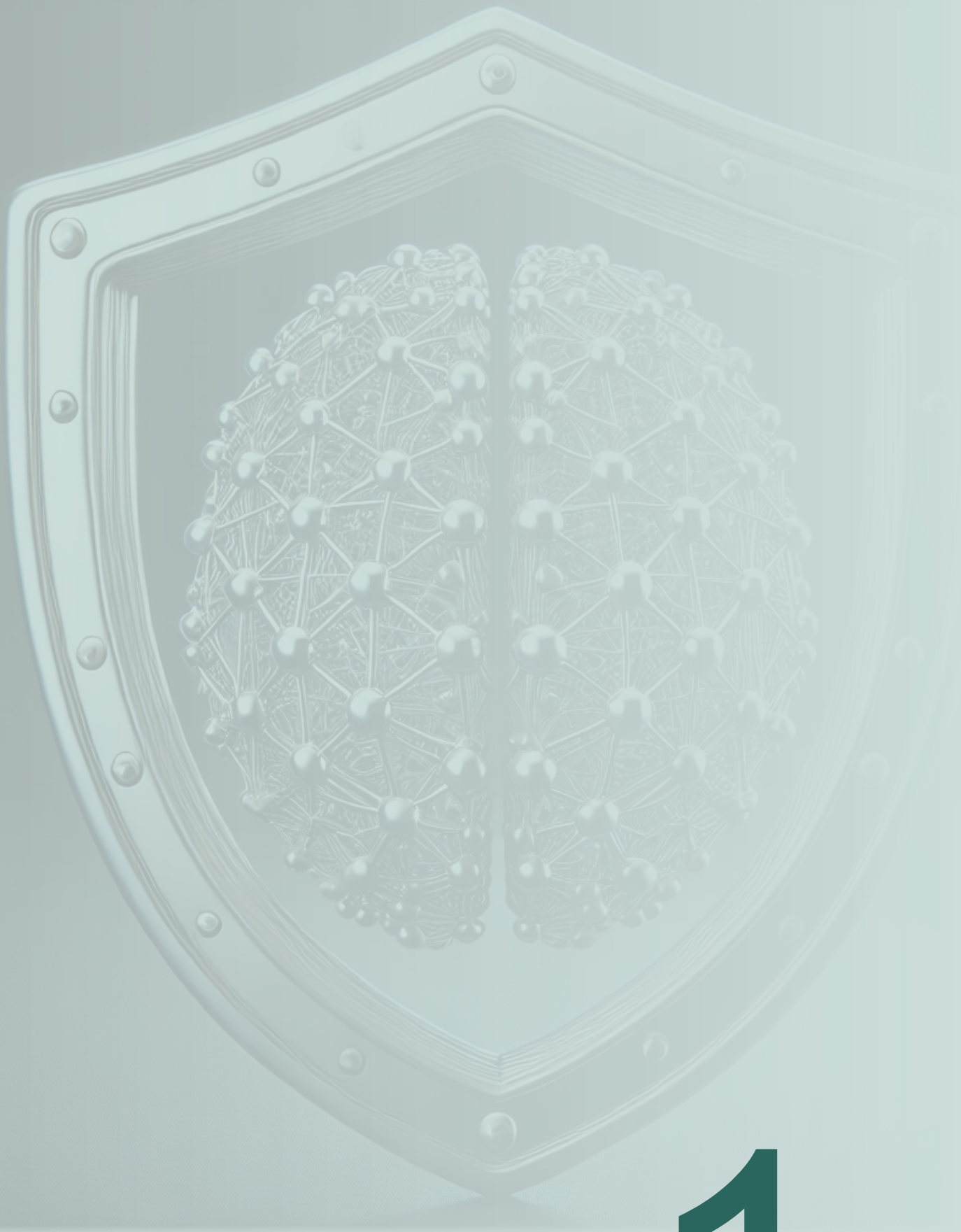
TRABAJOS DEL FORO CONTRA LAS CAMPAÑAS DE DESINFORMACIÓN

INICIATIVAS 2024

CAPÍTULO 1

125 TÉRMINOS SOBRE DESINFORMACIÓN

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/