Documento
Opinión

26/2024 7 de marzo de 2024

Varios autores

La desinformación como arma de guerra

Visitar la WEB Recibir BOLETÍN ELECTRÓNICO

La desinformación como arma de guerra

Resumen:

La desinformación se ha convertido en una poderosa arma de guerra en el contexto de los conflictos contemporáneos. Este trabajo, realizado por el XLIX Curso de Defensa Nacional, explora las multifacéticas dimensiones de la desinformación, destacando su impacto en la sociedad, la democracia y, particularmente, en el ámbito militar. Se enfoca en cómo la digitalización y las redes sociales han potenciado la capacidad de desinformar, alterando la opinión pública y debilitando las instituciones democráticas. Se examinan los métodos de detección y contramedidas, incluyendo la legislación y las herramientas tecnológicas, resaltando la importancia de una respuesta coordinada y multidimensional que involucre a actores gubernamentales, medios de comunicación, plataformas digitales y la sociedad civil. El documento concluye enfatizando la necesidad de una defensa activa y una educación en medios para fortalecer la resiliencia social frente a este fenómeno creciente.

Palabras clave:

Desinformación, Guerra Híbrida, Resiliencia Social, Educación en Medios

Jaime Alastuey Rivas, María Isabel García López, Francisca García Vizcaíno, Adolfo Garrido López, Fernando Mora Moret, Jesús Mª Pedrazo Majarrez, Sofía Pérez-Tejada García

Disinformation as a Weapon of War

Abstract:

Disinformation has emerged as a potent weapon in the landscape of contemporary conflicts. This study, conducted by the XLIX National Defense Course, delves into the multifaceted aspects of disinformation, highlighting its impact on society, democracy, and especially in the military sphere. It focuses on how digitalization and social media have enhanced the capacity for disinformation, skewing public opinion and undermining democratic institutions. The methods for detection and countermeasures, including legislation and technological tools, are examined, underscoring the importance of a coordinated, multidimensional response involving governmental actors, media, digital platforms, and civil society. The document concludes by emphasizing the need for active defense and media education to bolster societal resilience against this escalating phenomenon.

Keywords:

Disinformation, Hybrid Warfare, Social Resilience, Media Education

Cómo citar este documento:

ALASTUEY RIVAS, Jaime y otros. *La desinformación como arma de guerra*. Documento de Opinión IEEE 26/2024.
https://www.ieee.es/Galerias/fichero/docs_opinion/2024/DIEEEO26_2024_VVAA_Desinformacion.pdf y/o enlace bie[3] (consultado día/mes/año)

Desinformación: naturaleza de la amenaza

«El corazón del hombre necesita creer algo, y cree mentiras cuando no encuentra verdades que creer». Mariano José de Larra, 1832.

El uso de la información y la manipulación de las herramientas de comunicación de las sociedades ha sido una constante a lo largo de la historia. Hoy día es una de las mayores preocupaciones de los Estados modernos. La difusión no intencional de información bien sea veraz o falsa *("misinformación")* o el uso de información sesgada o engañosa con fines partidistas *("propaganda")* son prácticas habituales. Pero cuando hablamos de "desinformación" aportamos un valor añadido, ya que la verdadera desinformación, conlleva intencionalidad y búsqueda de un efecto desestabilizador.

Actualmente, el efecto de esta antigua práctica se ve seriamente potenciado por la propia digitalización de las sociedades. Las redes sociales e internet actúan como un poderosísimo vehículo con capacidad para difundir más información y de manera más rápida y, por lo tanto, la capacidad de influir más y de una manera más contundente y efectiva en las opiniones públicas[1]. Además, este es un vehículo barato y muy asequible, al alcance no sólo de Gobiernos, instituciones y grandes grupos, sino de toda la ciudadanía. Actores estatales y no estatales, grupos terroristas y ciudadanos al servicio de las campañas de desinformación.

¿Cómo afecta la desinformación a la sociedad y la democracia?

- Manipulando la opinión y el debate público, sus creencias y actitudes, evitando que puedan aplicar un juicio crítico sobre la información que reciben dificultando la toma de decisiones informadas. La propagación de rumores y teorías conspirativas pueden generar además pánico y alarma social. El ejemplo paradigmático es la oleada de desinformación durante la pandemia de la COVID. De hecho, la Organización Mundial de la Salud (OMS) acuñó el concepto "Infodemia" en paralelo a la pandemia por coronavirus, y ha terminado por generalizarse. La OMS emplea este anglicismo para referirse a un exceso de

[1] XXXII Seminario Internacional de Seguridad y Defensa: Amenazas desde el ciberespacio. (2020). Madrid.

información acerca de un tema, mucha de la cual son bulos o rumores que dificultan que las personas encuentren fuentes y orientación fiables cuando lo necesiten.

- Promoviendo la polarización y división de la cohesión social, generando desconfianza y hostilidad entre los grupos.
- Generando desconfianza en los medios de comunicación y en las fuentes de información confiables. No saber diferenciar entre lo que es cierto y es falso en Internet. Esto puede llevar a que las personas busquen fuentes de información alternativas o caigan en teorías de conspiración.
- Deslegitimando las instituciones democráticas, los gobiernos y los líderes políticos, manipulando intereses políticos, económicos o ideológicos, limitando la confianza en el sistema democrático en su conjunto. Facebook reconoció que hasta 126 millones de sus usuarios se vieron expuestos a publicaciones de una compañía vinculada al Kremlin llamada Internet Research Agency durante las elecciones estadounidenses de 2016. Twitter identificó 3.814 cuentas dedicadas a esta actividad. La Inteligencia estadounidense apuntó a Moscú como impulsor de una gran estrategia de noticias falsas y propaganda.

Objetivos y tácticas de desinformación

Existen varios tipos de desinformación, cada uno con sus propias características, que varían según el objetivo que se persiga y el actor que la emplea. Para poder actuar contra la desinformación es importante entender cómo funciona y ser capaz de desenmascarar sus tácticas y procedimientos. Pueden deslindarse diferentes fases y mecanismos para implementar una exitosa campaña de disrupción digital y comunicativa para desestabilizar la opinión pública de un Estado[2]:

Se difunde un relato que deforma la realidad de tres maneras: falseándola, con datos que manifiestamente contradicen los hechos; manipulándola, apelando a la componente emocional de la información; tergiversándola, mezclando informaciones reales con otras

[2] CCN-CERT (2021). desinformación en el Ciberespacio. Informe de buenas prácticas. Centro Criptológico Nacional (CNN-CERT). Ministerio de Defensa.

completamente falsas. Se diseñan teorías conspiratorias, extrayendo ciertos elementos de la compleja realidad del entorno contemporáneo, se entrelazan de tal modo que parezcan una teoría válida que finalmente se convierta en dogma.

Pero ¿qué hace de esta práctica una verdadera y exitosa amenaza?[3]:

- Su alto nivel de efectividad. Actualmente, resulta relativamente barato y fácil, y en muy poco tiempo, producir mensajes multimedia de alta calidad técnica y difundirlos eficazmente.
- La dificultad para establecer una atribución directa. Las plataformas digitales y la propia naturaleza de la red propician el surgimiento de actores anónimos, estatales y no estatales con el uso de perfiles digitales anónimos, ocultación de direcciones IP, programas para automatizar la distribución de mensajes, que dificulta establecer la trazabilidad de la información y su fuente.
- Compleja regulación y persecución. Resulta muy difícil emprender acciones contra un país o un grupo supra o subnacional al que se le acusa de iniciar una guerra de comunicación en el marco de un entramado legal lleno de vacíos regulatorios y tipos penales de difícil concreción. Además, es muy difícil establecer una relación de causalidad entre los intentos por alterar la opinión pública y los cambios en el comportamiento de los ciudadanos.

Efectos de la desinformación en el ámbito militar y su impacto como arma de guerra

La OTAN caracteriza la guerra híbrida «el uso de amenazas de actividades a veces encubiertas, militares y paramilitares, convencionales y no convencionales, actos de sabotaje, coerción, desinformación o propaganda, y acciones civiles de todo tipo para influenciar a un adversario». La desinformación es un componente de esa guerra híbrida[4]. Nuestra Estrategia de Seguridad Nacional la incluye en su enumeración de las

[3] CCN-CERT. Documento sobre detección de la información. https://www.redgealc.org/site/assets/files/12292/desinformacion_g.pdf

[4] CIDOB-Las estrategias de la OTAN en respuesta a los conflictos híbridos. (s.f.). Obtenido de: https://www.cidob.org/es/articulos/cidob_report/n_8/las_estrategias_de_la_otan_en_respuesta_a_los_conflictos_hibridos

amenazas a la seguridad nacional. El ámbito militar pues, se ve afectado de manera trascendental por esta nueva arma que nos sitúa en un escenario bélico inédito.

Estas potenciales amenazas se empiezan a tratar al máximo nivel en las principales instituciones europeas. En la visita del *XLIX Curso de Defensa Nacional* al Cuartel General de la OTAN en Bruselas, dos altos funcionarios resaltaron la importancia que esta problemática está adquiriendo en las estrategias de los aliados. *"Indudablemente, a pesar del componente de guerra convencional que tiene la agresión militar de Rusia a Ucrania, los nuevos dominios comienzan a estar muy presentes. No es algo que esté muy desarrollado* -admitió uno de los ponentes-. *Pero indudablemente tanto las estrategias nacionales de ciberseguridad como las medidas que está tomando la UE, son tenidas muy en cuenta dentro la OTAN",* subrayó.

Las guerras se libran en muy diversos frentes, simultáneamente. Los escenarios bélicos, los campos de batalla, cada vez más híbridos y grises, ya no se desarrollan sólo en tierra, mar y aire, o incluso en el espacio exterior y en el ciberespacio. Hay un sexto ámbito de actuación: el ámbito cognitivo, la *mente*. El ámbito cognitivo se refiere al espacio específico relacionado con la gestión de la información y la influencia, que afecta a las percepciones, actitudes, emociones y comportamiento de las personas involucradas en un conflicto [5].

La desinformación es "arma de guerra", tanto cuando es utilizada antes de un conflicto real, para difundir información falsa o engañosa con el objetivo de desestabilizar un país y allanar el terreno en un conflicto armado (por ejemplo, manipulando la opinión pública para sembrar la discordia y el caos en un determinado país, desestabilizar a los gobiernos y las instituciones…) como en el marco del propio conflicto, para justificar acciones violentas o agresivas, dificultar la toma de decisiones informadas en el ámbito internacional erosionando la confianza entre los países y las organizaciones internacionales (dañando su reputación), para provocar confusión y la adopción de políticas equivocadas…

[5] CALVO ALBERO, J., ANDRÉS MENÁRGUEZ, D., PEIRANO, M., MORET MILLÁS, V., PECO YESTE, M., & DONOSO RODRÍGUEZ, D. (2020). *Implicaciones del ámbito cognitivo en las Operaciones Militares.* Centro Superior de Estudios de la Defensa Nacional (CESEDEN). Instituto Español de Estudios Estratégicos (ieee).

Si un estado sufre una campaña desinformativa es fundamental conocer de dónde procede, su atribución y qué individuos, organizaciones o instituciones se encuentran detrás, como clave para defenderse de dichas campañas.

Alerta social ante un escenario incierto

El fotógrafo alemán Boris Eldagsen fue premiado en los prestigiosos *Sony World Photography Awards 2023* con una imagen realizada a través de inteligencia artificial. El artista fue galardonado en la categoría "Creativo". Pero después de que la Organización Mundial de Fotografía diera a conocer a los ganadores el pasado 13 de abril, Eldagsen reconoció que no era una fotografía real y renunció al galardón. Declaró que su fin había sido comprobar si una creación como la suya podía colarse entre las candidatas como una más. No solo lo hizo, sino que ganó el certamen. Recientes imágenes como las del Papa Francisco con un abrigo blanco de plumón o la de Donald Trump violentamente detenido por un grupo de policías han disparado las alarmas sobre la Inteligencia Artificial (IA), capaz de producir imágenes hiperrealistas que en realidad no han existido nunca.

Hay ejemplos recientes que permiten vislumbrar el alcance de estas nuevas tecnologías. La inteligencia artificial aprendió a pintar como lo haría Rembrandt. *The Next Rembrandt* es una obra realizada por algoritmos y análisis de datos para generar por medio de Inteligencia Artificial un nuevo cuadro del pintor holandés Rembrandt (1609 – 1699). El proyecto fue una investigación multidisciplinaria de 168.263 fragmentos de las 346 pinturas de Rembrandt. En 2019, la compañía tecnológica china Huawei anunció que un algoritmo de IA fue capaz de completar los dos últimos movimientos de la Sinfonía nº8, la composición inacabada que Franz Schubert comenzó en 1822, 197 años antes. La situación se hace extensiva a la irrupción de los *deep fakes*, que funcionan a través de modelos de redes neuronales generativas, el denominado *deep learning*. Esta tecnología de inteligencia artificial se puede utilizar maliciosamente para engañar a Gobiernos, poblaciones, causar conflictos internacionales, dañar la imagen de una persona o sacar un provecho ilegítimo.

Este escenario ha llevado a líderes tecnológicos de la talla de Steve Wozniak, Jaan Tallinn o Elon Musk a unirse para reclamar que se paralicen temporalmente los grandes experimentos con inteligencia artificial (IA) por los riesgos que pueden entrañar

para la sociedad. En un documento que tuvo gran repercusión, los firmantes solicitaron que dicha paralización de los entrenamientos se aproveche para *"desarrollar e implementar un conjunto de protocolos de seguridad compartidos para el diseño y desarrollo avanzados de IA",* que sean auditados y supervisados por expertos externos independientes. *"Esto no significa una pausa en el desarrollo de la IA en general, simplemente un paso atrás de la carrera peligrosa hacia modelos de caja negra impredecibles cada vez más grandes con capacidades emergentes"*, indicaron en la misiva, publicada en el *Future of Life Institute*[6]*.*

En España, y bajo el título de *"Pienso, luego existo. IA: Es el momento de pararse a pensar"* (17 de abril de 2023), un artículo del presidente de Telefónica, José María Álvarez-Pallete, reflexiona en la web de la compañía sobre la necesidad de pensar la forma en que la humanidad va a utilizar los avances en inteligencia artificial. El directivo considera que *"ha llegado la hora de parar y pensar como sólo los humanos somos capaces de hacerlo. Ha llegado la hora de parar y redactar un nuevo contrato social. Para decidir y determinar cuáles son los derechos y obligaciones básicas de personas y máquinas en este nuevo mundo".*

Todo ello crea un campo de cultivo en el que la desinformación campa a sus anchas. Hay que tener en cuenta que las noticias falsas aprovechan sesgos cognitivos de los seres humanos para que, paradójicamente, nos resulten más atractivas que las noticias verdaderas. *"Tendemos a filtrar la información que nos llega quedándonos con aquella que refuerza nuestras creencias previas, y descartamos aquella que nos desafía".* Esto se conoce como sesgo confirmatorio. Por otro lado, *"tendemos a buscar argumentos y conclusiones que concuerdan con nuestras creencias, en vez de buscar argumentos que las contradicen".* Esto se denomina razonamiento motivado. Las redes sociales actúan como amplificadores, multiplicando el impacto de una noticia falsa, gracias a la participación de los propios usuarios en la viralización de la misma. Esta se ve también favorecida por la propia naturaleza de los algoritmos que regulan la difusión de información dentro de estas plataformas[7].

[6] Europa Press (2021). La UE aprueba ocho observatorios de medios digitales contra la desinformación y España lidera uno. https://www.europapress.es/sociedad/noticia-ue-aprueba-ocho-observatorios-medios-digitales-contra-desinformacion-espana-lidera-uno-20210622185801.html

[7] Instituto de Ingeniería del Conocimiento, Univ. Autónoma

Defensa activa

Marco normativo

El Sistema de Seguridad Nacional, regido por la Ley 36/2015, fija en su artículo 11 la obligación de que las Administraciones Públicas con competencias en materia de Seguridad Nacional establezcan mecanismos de coordinación e intercambio de información para detectar y neutralizar riesgos y amenazas, entre las que se encuentra la desinformación.

La Estrategia de Seguridad Nacional de 2021, ya reconoce explícitamente a la desinformación como una amenaza a la seguridad, especialmente en el contexto de procesos electorales. El Consejo de Seguridad Nacional publicó la Orden PCM/1030/2020 por la que se aprueba el Procedimiento de Actuación contra la Desinformación. De acuerdo con dicho Procedimiento, en España la labor de coordinación radica en el Departamento de Seguridad Nacional de Presidencia de Gobierno. También presidido por este Departamento cabe señalar el Foro contra las campañas de desinformación en el ámbito de la Seguridad Nacional [8].

Herramientas para la defensa activa

Nacional

El mencionado Procedimiento de Actuación contra la Desinformación, cuyo propósito general es, «establecer medios de funcionamiento y mecanismos dirigidos a evaluar de manera continua el fenómeno de la desinformación a nivel global y particularmente para España», establece una estructura multi-ministerial y multi-sectorial para abordar la desinformación de forma integral.

Para ejecutar este plan nacional, el Gobierno ha diseñado una estructura específica, compuesta por seis entidades: el Consejo de Seguridad Nacional, el Comité de Situación, la Secretaría de Estado de Comunicación, la Comisión Permanente contra la

[8] Departamento de Seguridad Nacional (2022). Informe Anual de Seguridad Nacional 2022. Gobierno de España. https://www.dsn.gob.es/es/actualidad/sala-prensa/informe-anual-seguridad-nacional-2022

desinformación, las autoridades públicas competentes y, por último, el sector privado y la sociedad civil.

Además, se establecen cuatro niveles diferentes de activación que sirven tanto para la detección de campañas de desinformación y su análisis ante unos posibles impactos en la Seguridad Nacional, como para el apoyo en la gestión de situaciones de crisis derivadas de dichas campañas:

- Nivel 1. detección, alerta temprana y análisis técnico de campañas de desinformación.
- Nivel 2. evaluación de impacto, propuesta de medidas y coordinación interministerial por parte de la Comisión Permanente contra la Desinformación.
- Nivel 3. gestión estratégica y política por parte del Comité de Situación.
- Nivel 4. dirección política y adopción de medidas al más alto nivel por parte del Consejo de Seguridad Nacional.

Del mismo modo, también se establece la gestión de posibles campañas de desinformación en el ámbito de la UE, ya que el problema de la desinformación no afecta exclusivamente a España.

En el ámbito de los órganos de seguridad, la Constitución Española encomienda a las Fuerzas y Cuerpos de Seguridad la misión de proteger el ejercicio de derechos y libertades, lo que incluye la protección frente a la desinformación cuando ésta pretende socavarlos. El Centro Nacional de Inteligencia, la Comisaría General de Información de la Policía Nacional y el Servicio de Información de la Guardia Civil cuentan con unidades especializadas en el análisis e investigación de campañas de desinformación y su impacto en la seguridad.

Por su parte, la Ley 36/2015 de Seguridad Nacional establece que las Fuerzas Armadas, desde sus capacidades de inteligencia e información militar, deben apoyar al Sistema de Seguridad Nacional proporcionando información y análisis sobre riesgos y amenazas, entre ellos la desinformación.

El artículo 11 de la Ley de Seguridad Nacional entra de lleno en la cuestión de la interacción entre órganos nacionales de seguridad al indicar que, en el marco del Sistema de Seguridad Nacional, las Administraciones Públicas con competencias en los

ámbitos de especial interés de la Seguridad Nacional, estarán obligadas a establecer mecanismos de coordinación e intercambio de información, especialmente en relación con los sistemas de vigilancia y alerta ante posibles riesgos y amenazas.

Más allá del sector público, otros actores están llamados a involucrarse en la defensa frente a la desinformación. Los medios de comunicación, las plataformas digitales, los centros de investigación y las universidades están aportando análisis, detección de campañas y propuestas. Un ejemplo es el observatorio IBERIFIER, que aglutina entidades españolas y portuguesas para monitorear la desinformación. La articulación de estos esfuerzos contribuye a generar resiliencia social frente a la desinformación.

Otros actores relevantes son las empresas tecnológicas, cuya colaboración es vital para combatir la viralización de campañas de desinformación a través de sus plataformas. Asimismo, organizaciones de la sociedad civil especializadas en verificación de datos y alfabetización mediática son claves para sensibilizar a la ciudadanía e impulsar su participación activa en esta lucha.

Llaman la atención algunos aspectos del citado Procedimiento de Actuación contra la Desinformación:

- Si bien el protocolo reconoce que «los medios de comunicación, las plataformas digitales, el mundo académico, el sector tecnológico, las organizaciones no gubernamentales y la sociedad en general juegan un papel esencial en la lucha contra la desinformación», en el sistema nacional de lucha contra las noticias falsas no estaría representada ninguna asociación profesional de periodistas o de medios de comunicación, cuando precisamente estos medios podrían tener un papel activo a la hora de detectar y evitar la divulgación de *fake news*.
- El Procedimiento tampoco hace alusión a la eventualidad de hacer gestiones ante las grandes compañías tecnológicas para que procedan a eliminar de sus plataformas contenidos vinculados a campañas de desinformación, independientemente de que la decisión última queda en manos de los gestores de las mencionadas compañías.
- En la composición de la estructura diseñada por el Gobierno para combatir la desinformación han quedado fuera organismos públicos o gubernamentales dedicados a la ciberseguridad, así como unidades militares específicas, entidades

que podrían suponer un importante apoyo y que podrían aportar experiencia e inteligencia.

Internacional

En el plano internacional, España participa en iniciativas de coordinación para la lucha contra la desinformación tanto en la Unión Europea como en la OTAN. Así, desde la UE se ha acuñado el concepto FIMI [9], que incluye una caja de herramientas al servicio de los Estados y toma la desinformación como parte destacada, haciendo hincapié en el comportamiento manipulador, en contraposición a la veracidad del contenido difundido. Por otro lado, la Alianza Atlántica colabora en el desarrollo de metodologías conjuntas para identificar y contrarrestar campañas de propaganda extranjera.

Tal y como refiere el documento "Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional. Propuestas de la sociedad civil", se suceden iniciativas europeas de todo tipo cuyo fin es la lucha contra este tipo de dinámicas:

- El Plan de Acción para la Democracia Europea (Comisión Europea, 2020), publicado el 3 de diciembre de 2020.
- El Código de buenas prácticas de la Unión en materia de desinformación (Comisión Europea, 2018).
- La propuesta de reglamento conocida como Ley de Servicios Digitales (Comisión Europea, 2020b).
- La propuesta de legislación para garantizar una mayor transparencia en el ámbito del contenido patrocinado en un contexto político.

Como complemento a lo anterior, hay que destacar los trabajos desarrollados en la Comisión Especial sobre la Injerencia Extranjera en todos los Procesos Democráticos en la Unión Europea, en particular la desinformación (INGE), que citan expresamente a España, junto a otros Estados Miembros, como objetos de desinformación e injerencia rusa, concretamente en nuestro caso en relación con el PROCES y algunos elementos independentistas catalanes [10].

[9] Unión Europea (2021). *Joint Communication on Foreign Information Manipulation and Interference.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021JC0031

[10] Unión Europea (2022). Informe sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea.

Fuera del marco UE, pero dentro del europeo, hay que nombrar el Grupo de Trabajo Horizontal para el Fortalecimiento de la Resiliencia y para contrarrestar las Amenazas Híbridas del Consejo de Europa [11].

Cómo detectar una campaña de desinformación

Detectar una campaña desinformativa en medios digitales puede ser difícil, pero existen algunos indicadores que pueden ayudarnos a identificarla. Algunos son:

- La fuente de la información. Es muy importante verificar la credibilidad y reputación de la fuente que publica o comparte la información, ya que simulan ser un individuo o institución real. En general, son medios de comunicación que no ofrecen una línea editorial transparente y no citan de donde provienen sus informaciones y datos. Asimismo, no tiene enlace a fuentes oficiales. En relación con los responsables de estos medios, no se identifica a ninguna persona o institución como responsable, ni se facilita información de contacto. En algunas ocasiones, cuentan entre sus colaboradores con individuos que carecen de experiencia y reconocimiento en el sector de la comunicación y que apenas tienen un historial profesional o de publicaciones. En general, las noticias aparecen sin firmar o firmadas únicamente por un número reducido de personas.
- La fecha de la información. Se suele utilizar información antigua o descontextualizada para crear confusión o manipular la información. Se debe comprobar la fecha de publicación y si se ha actualizado o modificado y verificar si la información se refiere al contexto actual o a otro diferente.
- El contenido de la información. Publican mensajes mayoritariamente sobre temas políticos, utilizando un lenguaje sensacionalista, emotivo y alarmista proporcionando datos poco verificables y contrastables. En otras ocasiones no crean propio contenido, sino que sólo reenvía información publicada por otros. Asimismo, minimizan el mensaje, sustituyendo la complejidad de un conflicto, y sus consecuencias, por una trama simple que no tiene en cuenta ni antecedentes

[11] Consejo de Europa (2021). Horizontal Task Force on Strengthening Resilience and Countering Hybrid Threats. https://www.coe.int/en/web/counter-terrorism/-/horizontal-task-force-on-strengthening-resilience-and-countering-hybrid-threats

históricos ni el contexto en el que se desarrolla. Se busca además una historia conmovedora, que simplifique todo el conflicto reduciéndolo a una simple historia de buenos y malos [12].

Estos contenidos se suelen acompañar de temas de actualidad que tienen un gran consenso entre la población o que, al contrario, generan polarización social. En el primer caso, la campaña desinformativa se encubre con temas como cambio climático, lucha por la igualdad, fin de la violencia…. para vestir a la desinformación con la capa de la justica. En el segundo, el agente desinformativo no pretende crear nuevos escenarios de polarización, sino que explota los ya existentes apelando a emociones fuertes, como el miedo, la ira o la indignación. En definitiva, si el contenido es incoherente, con errores, exagerado, subjetivo o infundado, hay que dudar de su veracidad.

- La intención de la información. Hay que preguntarse cuál es el propósito de la información, si busca influir en la opinión pública o desacreditar a una persona, grupo, partido político o institución, y quién se beneficia de ella. Si la intención es persuadir, influir, favorecer, perjudicar, dividir o provocar, hay que sospechar de una posible campaña desinformativa. Saber el objetivo que buscan ayudará a conocer a los actores.
- La difusión de la información. Para su difusión se usan todos los medios digitales, como RRSS, plataformas de mensajería, blogs o sitios web. Principalmente utilizan las redes sociales clásicas (Facebook, X, TikTok o Instagram) ya que pueden crear avalanchas de opinión en tiempo récord, pero el uso de redes sociales alternativas significa mayor anonimato, libertad y privacidad de discurso. De esta manera, los actores de la desinformación aprovechan las plataformas que proporcionan menos seguridad a los usuarios, donde las políticas de control no son muy estrictas y los controles para eliminación de contenido y cuentas falsas son menores.

  Hay que resaltar la difusión utilizando servicios automatizados a través de *bots*, diseñados para imitar o sustituir el accionar humano que amplifican las campañas de desinformación. De esta forma, difunden, de manera sistemática y recurrente

[12] HARARI, Y. N. (2018). *21 lecciones para el siglo XXI.* Madrid: Debate.

narrativas que contribuyen a polarizar a la opinión pública, explotando vulnerabilidades políticas sociales o de un Estado.

Según un estudio publicado en la revista *Science*, las informaciones falsas consiguen difundirse más rápido y llegar más lejos que las veraces: tienen hasta un 70% más de retuits que las noticias verdaderas. Uno de los problemas a destacar de las noticias falsas es que son mucho más virales cuando se producen que cuando se realiza el desmentido de la misma.

- Actividad de la información. Presentan una tasa de actividad elevada de manera sostenida en el tiempo. Por ejemplo, que se publiquen más de 50 mensajes diarios indica algo incompatible con un estilo de vida normal. Otro indicador de que detrás puede haber cuentas automatizadas es que las publicaciones son las veinticuatro horas del día. Incluso se publican a la misma hora, la misma información en medios digitales distintos y en diferentes idiomas.

  También se debe destacar la manipulación de algoritmos diseñados para que el usuario reciba e interactúe, únicamente, con mensajes en función de sus preferencias políticas, gustos o aficiones.

- El origen de la información. Dificultad para establecer una atribución directa de la fuente originaria de la información y su trazabilidad. Los que realizan estas campañas utilizan: perfiles digitales anónimos, software de ocultación de direcciones IP, VPN (Red Privada Virtual), servidores proxy, VPS (servidores privados virtuales) de diferentes países. De esta manera el anonimato les dará impunidad. Hacer la atribución de donde viene la desinformación es clave para atajarla.

Los puntos anteriores son algunos de los indicadores que pueden ayudarnos a detectar una campaña desinformativa en medios digitales, pero no son los únicos. Hoy en día los procedimientos denominados *"fact-checking"* son fundamentales para combatir y eliminar las noticias falsas y deben ser usados, no solo por instituciones y periodistas para evitar campañas de desinformación, sino también, por los lectores que buscan saber que la información que leen es realmente cierta.

Conclusiones

La lucha contra la desinformación representa un desafío crucial y multifacético que requiere una respuesta coordinada y en constante evolución. A nivel nacional, España ha establecido un marco jurídico y operativo sólido, que involucra a diversas entidades gubernamentales y actores de la sociedad. No obstante, la efectividad de estas medidas depende de la capacidad de adaptarse rápidamente a las cambiantes tácticas de desinformación, lo cual implica una necesidad constante de innovación en herramientas y estrategias. La incorporación activa y representativa de profesionales de medios de comunicación y asociaciones periodísticas, así como la implicación más directa de entidades de ciberseguridad, podrían fortalecer significativamente este enfoque.

En el ámbito internacional, la colaboración de España con entidades europeas y transatlánticas como la UE y la OTAN es fundamental para abordar la desinformación, que no conoce fronteras y afecta a la seguridad y estabilidad globales. Estas alianzas permiten compartir experiencias, metodologías y recursos, lo cual es esencial para combatir una amenaza que es inherentemente transnacional. Además, la participación en iniciativas internacionales demuestra el compromiso de España con un enfoque unificado y coherente, reforzando así su posición como un actor clave en la lucha contra la desinformación a nivel global.

En conclusión, existen instrumentos jurídicos y procedimentales que sientan las bases para la defensa activa frente a la desinformación, con una estructura de coordinación interministerial, internacional y multi-actor. Sin embargo, se requiere reforzar capacidades, cerrar vacíos legales, fomentar la coordinación entre instituciones públicas y privadas incluyendo a compañías tecnológicas, medios de comunicación y organismos o unidades específicamente dedicados a la ciberseguridad.

Un enfoque integral que incluya educación, transparencia y colaboración con múltiples actores puede proporcionar la base para una sociedad más resiliente y preparada para enfrentar los desafíos que plantea la desinformación en el siglo XXI.

Jaime Alastuey Rivas, María Isabel García López, Francisca García Vizcaíno, Adolfo Garrido López, Fernando Mora Moret, Jesús Mª Pedrazo Majarrez, Sofía Pérez-Tejada García