



Revista Perspectivas en Inteligencia

(Revista Científica en Ciencias Sociales e Interdisciplinaria)

Volumen 18, Número 27, enero - junio de 2026

ISSN: 2145-194X (impreso), 2745-1690 (en línea)

Página Web: <https://revistaseditorialejc.org/index.php/pei>

Bogotá D.C., Colombia

Educación superior y resiliencia democrática: una propuesta para la formación en inteligencia sobre amenazas híbridas y manipulación informativa

Autor

Carlos Galán-Cordero

<https://orcid.org/0009-0006-3858-1666>

✉ cgalan@nebrija.es

Universidad Nebrija, España

Citación APA: Galán-Cordero, C. (2026). Educación superior y resiliencia democrática: una propuesta para la formación en inteligencia sobre amenazas híbridas y manipulación informativa. *Perspectivas en Inteligencia*, 18(27), 27-47. <http://doi.org/10.47961/2145194X.856>

Publicado en línea: 2026



Los artículos publicados por la Revista Científica Perspectivas en Inteligencia son de acceso abierto bajo una licencia **Creative Commons: Atribución - No Comercial – Sin Derivados**.

Para enviar un artículo:

<https://revistaseditorialejc.org/index.php/pei/about/submissions>



*Esta página queda
intencionalmente
en blanco*

Educación superior y resiliencia democrática: una propuesta para la formación en inteligencia sobre amenazas híbridas y manipulación informativa

Higher education and democratic resilience: a proposal for training in hybrid threat intelligence and information manipulation

Carlos Galán-Cordero¹

(1) Universidad Nebrija, Madrid, España,
✉ cgalan@nebrija.es

Resumen

Objetivo: diseñar y fundamentar una propuesta de formación universitaria de posgrado que permita responder al déficit de capacitación interdisciplinar existente en materia de amenazas híbridas, desinformación, injerencia extranjera y manipulación informativa en el ciberespacio, mediante el desarrollo de competencias analíticas, jurídicas, tecnológicas e institucionales orientadas al fortalecimiento de la resiliencia democrática. **Metodología:** se adopta un enfoque cualitativo, documental y propositivo, basado en el diseño curricular orientado a competencias y en los principios del aprendizaje activo. El estudio analiza e integra aportaciones procedentes de los estudios estratégicos, el derecho, la ciberseguridad, la comunicación, la psicología social y el análisis de inteligencia. A partir de esta revisión interdisciplinar se estructura un programa semestral de posgrado, de entre seis y ocho créditos ECTS (European Credit Transfer and Accumulation System), dirigido a profesionales de los ámbitos jurídico, periodístico, diplomático, militar, policial, académico y de la Administración pública. **Resultados:** se obtiene un modelo pedagógico organizado en cinco bloques progresivos: fundamentos de las amenazas híbridas; ciberespacio como dominio estratégico; psicología y sociología de la desinformación; marco jurídico e institucional; y prevención y resiliencia institucional. El modelo combina contenidos conceptuales con análisis de casos, verificación digital, inteligencia de fuentes abiertas, simulaciones de crisis y comunicación estratégica. **Conclusiones:** una formación interdisciplinar, aplicada y orientada a competencias puede reducir la fragmentación académica existente y mejorar la capacidad profesional para identificar, analizar y responder de manera jurídicamente legítima y operativamente eficaz a las operaciones de manipulación informativa, contribuyendo al fortalecimiento futuro de la resiliencia institucional y democrática.

Clasificación JEL: D83, I23

Palabras clave: amenazas híbridas; desinformación; ciberespacio; educación superior; resiliencia democrática.

Abstract

Objective: to design and substantiate a postgraduate higher education programme aimed at addressing the existing deficit in interdisciplinary training on hybrid threats, disinformation, foreign interference and information manipulation in cyberspace, through the development of analytical, legal, technological and institutional competencies intended to strengthen democratic resilience. **Methodology:** the study adopts a qualitative, documentary and proposal-oriented approach based on competency-based curriculum design and active learning principles. It analyses and integrates contributions from strategic studies, law, cybersecurity, communication, social psychology and intelligence analysis. On the basis of this interdisciplinary review, a semester-long postgraduate programme of six to eight (European Credit Transfer and Accumulation System) ECTS credits is structured for professionals working in legal, journalistic, diplomatic, military, law-enforcement, academic and public-administration settings. **Results:** the study produces a progressive pedagogical model organised into five modules: foundations of hybrid threats; cyberspace as a strategic domain; psychology and sociology of disinformation; legal and institutional framework; and prevention and institutional resilience. The model combines conceptual content with case analysis, digital verification, open-source intelligence, hybrid-crisis simulations and strategic communication. **Conclusions:** interdisciplinary, applied and competency-based education can reduce the current fragmentation of academic training and enhance professionals' ability to identify, analyse and respond to information-manipulation operations in a legally legitimate and operationally effective manner, thereby contributing to the future strengthening of institutional and democratic resilience.

Keywords: hybrid threats; disinformation; cyberspace; higher education; democratic resilience.

Introducción

El entorno estratégico internacional contemporáneo se caracteriza por una creciente complejidad derivada de la digitalización global, la interdependencia tecnológica y la intensificación de la competencia geopolítica entre Estados. En este contexto han adquirido una relevancia creciente las denominadas **amenazas híbridas**, entendidas como la combinación coordinada de instrumentos políticos, informativos, económicos, tecnológicos y, en ocasiones, militares con el objetivo de explotar vulnerabilidades estructurales de los Estados y de las sociedades abiertas (Humprecht et al., 2020; Sanz-Caballero, 2023).

Uno de los componentes centrales de estas estrategias es el uso sistemático de **operaciones de manipulación informativa**, en las que se incluyen las campañas de desinformación, las interferencias en procesos políticos y las operaciones de influencia desarrolladas a través del ciberespacio. Estas actividades persiguen influir en la percepción pública de determinados acontecimientos, erosionar la confianza en las instituciones democráticas, polarizar a la opinión pública o alterar procesos electorales (Freelon y Wells, 2020; Tuiñón-Navarro et al., 2019).

La expansión de las plataformas digitales y de las redes sociales ha facilitado el

desarrollo de nuevas técnicas de manipulación informativa basadas en el uso de automatización, análisis masivo de datos y microsegmentación de audiencias. Estas dinámicas han transformado profundamente el ecosistema informativo contemporáneo, generando nuevos desafíos para la gobernanza democrática y para la seguridad de los Estados (Arrese, 2024; Kozyreva et al., 2020; Salaverría et al., 2020).

A pesar de la creciente relevancia estratégica del fenómeno, la formación universitaria especializada en inteligencia para las amenazas híbridas y desinformación continúa siendo limitada y fragmentaria. Los programas académicos suelen abordar estas cuestiones desde perspectivas disciplinares aisladas -por ejemplo, desde la comunicación política, la seguridad internacional o la ciberseguridad- sin ofrecer una aproximación integrada que permita comprender la complejidad multidimensional del fenómeno (Huang et al., 2024; Wuyckens et al., 2022).

Esta carencia resulta especialmente significativa en la formación de profesionales que desempeñan funciones clave en la gestión de la información, la seguridad institucional y la protección de los procesos democráticos, como juristas, periodistas, diplomáticos, miembros de las fuerzas armadas o responsables de las administraciones públicas.

En este contexto, el presente trabajo propone una **metodología docente para un curso de posgrado semestral** orientado a la formación interdisciplinar en materia de inteligencia para las amenazas híbridas, campañas de desinformación e injerencia extranjera en el ciberespacio. El objetivo de la propuesta es contribuir al desarrollo de programas formativos que permitan mejorar la comprensión de estos fenómenos y fortalecer las capacidades analíticas y estratégicas de los profesionales que deben enfrentarse a ellos.

Metodología

Diseño pedagógico de la propuesta formativa

La propuesta formativa presentada en este trabajo se basa en un proceso de **diseño curricular orientado a competencias**, inspirado en los principios del aprendizaje activo y en enfoques pedagógicos utilizados en programas de seguridad, inteligencia y estudios estratégicos (Wuyckens et al., 2022; Yang et al., 2021).

La propuesta se elaboró mediante una revisión narrativa e interdisciplinar de literatura científica reciente sobre amenazas híbridas, desinformación, alfabetización mediática, resiliencia democrática y metodologías activas de aprendizaje. La selección priorizó artículos publicados desde 2020 en revistas académicas indexadas, complementados con normas y documentos institucionales de la Unión Europea indispensables para el análisis jurídico y de gobernanza.

El diseño del programa se articula en torno a tres principios metodológicos fundamentales: **interdisciplinariedad, aprendizaje aplicado y enfoque institucional**.

Enfoque interdisciplinar

Las amenazas híbridas constituyen un fenómeno complejo que combina dimensiones políticas, tecnológicas, jurídicas, comunicativas y psicológicas. En consecuencia, el programa docente integra conocimientos procedentes de diversos campos del saber, entre ellos (Freelon y Wells, 2020; Sanz-Caballero, 2023):

- Relaciones internacionales y estudios estratégicos.
- Derecho internacional, constitucional y europeo.
- Ciberseguridad y gobernanza del ciberespacio.
- Comunicación política y periodismo.
- Psicología social y sociología de la información.
- Análisis de inteligencia.

Este enfoque interdisciplinar permite ofrecer una comprensión más completa de las dinámicas que caracterizan las operaciones híbridas y las campañas de manipulación informativa.

Aprendizaje aplicado y metodologías activas

El segundo eje metodológico del programa es la incorporación de **metodologías docentes** activas, orientadas al desarrollo de competencias analíticas y operativas (Guess et al., 2020; Huang et al., 2024; Moore y Hancock, 2022).

Entre las principales actividades formativas se incluyen:

- Análisis de casos reales de campañas de desinformación.
- Talleres de verificación digital y fact-checking.
- Ejercicios de inteligencia de fuentes abiertas (OSINT).
- Simulaciones de crisis híbridas.

Estas metodologías permiten que el alumnado desarrolle habilidades analíticas directamente aplicables a contextos profesionales reales (Basol et al., 2020; Yang et al., 2021; Zhang et al., 2022).

Enfoque institucional

La propuesta docente está diseñada para un alumnado compuesto por profesionales procedentes de distintos ámbitos institucionales. En consecuencia, el programa se orienta no solo a la comprensión teórica del fenómeno, sino también a la identificación de **estrategias institucionales de prevención, resiliencia y respuesta** frente a las amenazas híbridas.

Modelo pedagógico del curso

El modelo pedagógico propuesto se basa en una estructura progresiva que conecta **conocimiento conceptual, análisis aplicado y desarrollo de capacidades estratégicas**.

Tabla 1. Modelo pedagógico del programa formativo

Modelo pedagógico del programa formativo	
Módulo 1: Comprensión conceptual	• Fundamentos de las amenazas híbridas. • Geopolítica de la información. • Funcionamiento del ecosistema digital.
Módulo 2: Análisis del fenómeno	• Campañas de desinformación. • Herramientas de manipulación digital. • Factores psicológicos y sociales.
Módulo 3: Marco institucional	• Derecho internacional y europeo. • Gobernanza del ciberespacio. • Políticas públicas frente a la desinformación.
Módulo 4: Capacidades operativas	• Análisis de inteligencia. • Verificación digital. • Diseño de respuestas institucionales.
Resultado final: Profesionales capaces de identificar, analizar y responder a amenazas híbridas y campañas de manipulación informativa.	

Nota: El modelo integra y sistematiza la literatura interdisciplinar citada en el apartado metodológico.

Fuente: Elaboración propia

Resultados

Estructura del programa formativo

Los resultados del proceso de diseño curricular se concretan en la estructura, secuencia y contenidos del programa formativo que se exponen a continuación.

El curso se concibe como un **programa de posgrado de un semestre**, con una carga docente aproximada de entre seis y ocho créditos ECTS.

La estructura curricular se organiza en los siguientes cinco módulos o bloques temáticos.

Fundamentos de las amenazas híbridas

Este primer bloque resulta indispensable porque proporciona el **marco conceptual y estratégico básico** sin el cual no sería posible comprender adecuadamente el resto de los contenidos del programa. La noción de amenaza híbrida no se refiere simplemente a una suma de riesgos dispersos, sino a la articulación coordinada de instrumentos heterogéneos -políticos, económicos, informativos, tecnológicos, cibernéticos y, en ocasiones, militares- orientados a explotar vulnerabilidades institucionales y sociales de un Estado o de una sociedad abier-

ta. En consecuencia, antes de abordar manifestaciones concretas, como la desinformación, la manipulación algorítmica o la injerencia extranjera, resulta necesario dotar al alumnado de una comprensión rigurosa de la lógica estratégica que integra y da sentido a dichos fenómenos (Humprecht et al., 2020; Sanz-Caballero, 2023).

La inclusión de este bloque se justifica, además, porque una parte sustancial de la dificultad analítica que plantean las amenazas híbridas deriva precisamente de su **ambigüedad estructural**. No suelen manifestarse como ataques abiertos, formalmente declarados o jurídicamente fáciles de calificar, sino como actuaciones graduales, acumulativas y frecuentemente situadas en la denominada **zona gris**, esto es, en el espacio intermedio entre la paz y el conflicto armado tradicional. Esta característica exige formar al alumnado en categorías analíticas que permitan identificar dinámicas de hostigamiento, erosión o desestabilización que, consideradas aisladamente, podrían parecer hechos inconexos o carentes de relevancia estratégica (Sanz-Caballero, 2023).

Asimismo, el estudio de este bloque permite superar visiones reduccionistas que tienden a identificar la guerra híbrida exclusivamente con la dimensión militar o, en sentido inverso, a tratar la desinformación como un problema meramente comunicativo. Una de las aportaciones centrales de este módulo es mostrar que las campañas de influencia, la presión económica, las operaciones cibernéticas, la instrumentalización del derecho, la explotación de fracturas sociales o la manipulación del debate público pueden formar parte de una misma arquitectura de acción estratégica. De este modo, el alumnado comprende que las amenazas híbridas no deben analizarse como incidentes aislados, sino como **procesos sistémicos de competencia y coerción**.

Desde una perspectiva docente, este bloque también cumple una función de **homogeneización conceptual**, especialmente relevante, dado el perfil heterogéneo del alumnado al que va dirigido el curso. Juristas, periodistas, diplomáticos, miembros de fuerzas armadas, responsables públicos o profesionales de la seguridad parten de lenguajes técnicos y tradiciones disciplinares diferentes. Por ello, el curso necesita un módulo inicial que establezca una base común sobre conceptos como *guerra híbrida*, *operaciones de influencia*, *competencia estratégica*, *vulnerabilidad social*, *resiliencia democrática* o *confrontación en la zona gris*. Sin esa base compartida, la posterior aproximación interdisciplinar correría el riesgo de fragmentarse en discursos paralelos sin verdadera integración metodológica.

En coherencia con esta finalidad, los contenidos del bloque -evolución del concepto de guerra híbrida, competencia estratégica en la zona gris e instrumentos de influencia política y comunicativa- no deben entenderse como una mera introducción teórica, sino como el **andamiaje intelectual del programa entero**. Su estudio permite al alumnado identificar la racionalidad estratégica que conecta el empleo del ciberespacio, la instrumentalización de narrativas, la presión sobre procesos democráticos y la explotación de debilidades institucionales. En consecuencia, este módulo no solo introduce el objeto de estudio, sino que configura la matriz interpretativa necesaria para comprender todos los demás.

Síntesis del Módulo

- Las amenazas híbridas combinan instrumentos políticos, informativos, tecnológicos, económicos y, en ocasiones, militares para explotar vulnerabilidades institucionales y sociales.
- Su análisis exige comprender la lógica estratégica que integra fenómenos aparentemente diversos como desinformación, presión económica, ciberoperaciones o manipulación política.
- Estas dinámicas suelen desarrollarse en la denominada “**zona gris**”, situada entre la paz y el conflicto armado tradicional.
- El estudio del concepto permite superar visiones reduccionistas que separan artificialmente la dimensión militar, comunicativa o tecnológica del conflicto contemporáneo.
- Este bloque proporciona el **marco conceptual común** necesario para un alumnado procedente de disciplinas y ámbitos profesionales diversos.
- Constituye el **andamiaje interpretativo del programa**, al ofrecer las categorías analíticas que permiten comprender el resto de los contenidos del curso.

El ciberespacio como dominio estratégico

La inclusión de un bloque específicamente dedicado al ciberespacio se justifica por el hecho de que, en el contexto contemporáneo, este constituye el **entorno operativo privilegiado** para el desarrollo, amplificación y sincronización de múltiples formas de amenaza híbrida. El ciberespacio no es únicamente una infraestructura técnica o un canal de comunicación, sino un espacio de interacción política, social y económica en el que convergen actores públicos y privados, plataformas digitales, sistemas automatizados, comunidades de usuarios y flujos masivos de información. Por ello, cualquier programa formativo sobre amenazas híbridas que no incorpore un análisis específico de este dominio quedaría sustancialmente incompleto (Arrese, 2024; Kozyreva et al., 2020).

La relevancia de este bloque radica, en primer lugar, en que el ciberespacio facilita la **baja visibilidad, la alta velocidad y el reducido coste de las operaciones de influencia y manipulación**. Las campañas de desinformación, las operaciones coordinadas de amplificación, el uso de cuentas automatizadas, la difusión de contenidos sintéticos o la segmentación estratégica de audiencias encuentran en el entorno digital un medio especialmente eficaz para multiplicar su alcance y dificultar su atribución. A diferencia de los mecanismos tradicionales de propaganda, las plataformas digitales permiten modular mensajes para públicos específicos, explotar dinámicas virales y operar de forma transnacional, todo ello con un grado de escalabilidad sin precedentes (Hwang et al., 2021; Salaverría et al., 2020).

En segundo lugar, este bloque resulta esencial porque las plataformas digitales no

son meros intermediarios neutrales, sino **estructuras sociotécnicas que condicionan la visibilidad, circulación y jerarquización de la información**. El funcionamiento de los algoritmos de recomendación, los sistemas de publicidad dirigida, los mecanismos de priorización de contenidos o las lógicas de monetización basadas en la atención afectan directamente a la forma en que los mensajes se propagan y adquieren relevancia pública. Comprender esta arquitectura es imprescindible para analizar cómo determinadas narrativas manipulativas logran amplificación, persistencia e impacto político (Ecker et al., 2022; Pennycook y Rand, 2021).

Además, el estudio del ciberespacio como dominio estratégico permite al alumnado advertir que muchas amenazas híbridas no dependen exclusivamente de la falsedad del contenido difundido, sino de la **explotación de vulnerabilidades estructurales del ecosistema digital**, tales como: opacidad algorítmica, fragmentación de audiencias, asimetrías informativas, desintermediación del debate público, facilidad de anonimización, automatización del comportamiento en red y escasa trazabilidad de determinados procesos de difusión. Desde esta perspectiva, la enseñanza sobre plataformas, algoritmos y arquitectura digital no cumple una función meramente técnica, sino que permite comprender por qué el entorno digital favorece determinadas formas de coerción e injerencia.

Este bloque es también imprescindible para formar profesionales que, desde ámbitos distintos, deberán interactuar con realidades tecnológicas que condicionan sus respectivas funciones. Un jurista necesita entender las lógicas técnicas mínimas que subyacen a la regulación de plataformas; un periodista debe conocer los mecanismos de amplificación y coordinación digital que afectan a la circulación de contenidos; un diplomático o un analista de seguridad debe ser capaz de interpretar la dimensión geopolítica de la infraestructura digital y su utilización estratégica por actores estatales y no estatales. En todos estos casos, el conocimiento del ciberespacio actúa como una **competencia transversal de alfabetización estratégica**.

Por ello, los contenidos del bloque -arquitectura técnica del ciberespacio, funcionamiento de plataformas digitales, algoritmos y amplificación de contenidos- están plenamente justificados dentro del programa. No se trata de añadir un componente tecnológico accesorio, sino de situar al alumnado ante el dominio en el que hoy se despliegan gran parte de las dinámicas híbridas. El módulo permite comprender no solo dónde ocurren muchas de estas operaciones, sino también por qué el ciberespacio altera profundamente sus formas, ritmos, escalas y efectos.

Síntesis del Módulo

- El ciberespacio se ha convertido en el principal entorno operativo para la ejecución y amplificación de amenazas híbridas y operaciones de influencia.
- Las plataformas digitales permiten desarrollar campañas de manipulación informativa con bajo coste, alta velocidad y gran alcance transnacional.
- Los algoritmos de recomendación, la publicidad dirigida y la arquitectura de las plataformas influyen decisivamente en la visibilidad y difusión de con-

tenidos.

- Muchas campañas de desinformación explotan **vulnerabilidades estructurales del ecosistema digital**, como la opacidad algorítmica o la fragmentación de audiencias.
- Comprender el funcionamiento técnico y sociopolítico de las plataformas es una competencia transversal para profesionales de distintos ámbitos institucionales.
- El estudio del ciberespacio permite explicar cómo la digitalización transforma las formas, ritmos y escalas de las operaciones de influencia.

Psicología y sociología de la desinformación

Este bloque se justifica porque las amenazas híbridas no persiguen únicamente alterar sistemas técnicos o interferir en procesos institucionales, sino influir sobre la **percepción, las emociones, las creencias y los comportamientos colectivos**. En consecuencia, el estudio de la desinformación no puede agotarse en el análisis del mensaje o del canal tecnológico; requiere también comprender los mecanismos psicológicos y sociológicos que explican por qué determinados contenidos manipulan con eficacia, se difunden con rapidez y producen efectos políticos o sociales relevantes (Ecker et al., 2022; Pennycook y Rand, 2021).

La inclusión de este módulo responde, en primer lugar, a la necesidad de superar una visión excesivamente instrumental o tecnocéntrica de la desinformación. Las campañas de manipulación informativa triunfan no solo por el uso de bots, plataformas o algoritmos, sino porque logran activar disposiciones cognitivas y emocionales preexistentes en los públicos destinatarios. Sesgos como el de confirmación, la heurística de disponibilidad, la percepción selectiva o la tendencia a aceptar información congruente con las propias creencias desempeñan un papel determinante en la recepción y circulación de mensajes manipulativos. Sin el estudio de estas dimensiones, el alumnado difícilmente podrá comprender por qué la mera rectificación factual suele resultar insuficiente frente a determinados procesos de polarización o radicalización narrativa (Kim et al., 2020; Sultan et al., 2024).

En segundo lugar, este bloque permite analizar la dimensión **colectiva y estructural** de la desinformación. Los contenidos manipulativos no operan en el vacío, sino en entornos sociales caracterizados por fragmentación del espacio público, crisis de confianza institucional, polarización afectiva, debilitamiento de autoridades epistémicas y transformación de las pautas de consumo informativo. Desde esta perspectiva, la sociología de la información y de la comunicación ofrece herramientas indispensables para comprender cómo se conforman comunidades interpretativas cerradas, cómo se consolidan las cámaras de eco o cómo determinadas narrativas se insertan en identidades políticas y culturales preexistentes (Arrese, 2024; Humprecht et al., 2020).

La justificación de este bloque se refuerza además por el hecho de que muchas amenazas híbridas explotan deliberadamente **fracturas sociales latentes**: tensiones territoriales, escisiones ideológicas, desconfianza hacia las élites, inseguridades culturales o agravios

percibidos. Las operaciones de influencia no necesitan inventar desde cero esas divisiones; les basta con intensificarlas, reencuadrarlas o utilizarlas para erosionar la cohesión democrática. Por ello, la formación en psicología y sociología de la desinformación resulta esencial para que el alumnado comprenda que la resiliencia frente a estas amenazas depende también de variables sociales profundas y no solo de mecanismos tecnológicos o regulatorios.

Desde el punto de vista profesional, este bloque tiene un valor añadido evidente para todos los perfiles destinatarios del curso. Para periodistas, permite entender mejor la dinámica de circulación y recepción de narrativas falsas o manipuladas. Para juristas y responsables públicos, ayuda a calibrar los límites y potencialidades de la regulación cuando el problema afecta a procesos sociales complejos y no solo a contenidos individualizables. Para fuerzas de seguridad, diplomáticos o analistas, facilita la comprensión del componente cognitivo de las operaciones híbridas. Para psicólogos y politólogos, ofrece un marco directamente conectado con sus respectivas áreas de especialización.

Los contenidos del bloque -sesgos cognitivos, polarización política y viralidad emocional de los contenidos digitales- se justifican porque permiten comprender la **dimensión antropológica y social de la amenaza híbrida**. Su función en el programa no es complementaria, sino central: explicar por qué ciertas narrativas encuentran terreno fértil, cómo se transforman en vectores de división y de influencia, y por qué la defensa frente a la desinformación exige actuar también sobre los factores de vulnerabilidad cognitiva y social que la hacen efectiva (Huang et al., 2024; Lewandowsky y Van der-Linden, 2021).

Síntesis del Módulo

- Las amenazas híbridas buscan influir sobre percepciones, creencias y emociones colectivas, por lo que requieren un análisis psicológico y sociológico.
- Los sesgos cognitivos y las heurísticas influyen decisivamente en la recepción y difusión de contenidos desinformativos.
- La polarización política y la fragmentación del espacio público favorecen la formación de **cámaras de eco y comunidades interpretativas cerradas**.
- Las campañas de manipulación informativa suelen explotar divisiones sociales preexistentes para intensificar tensiones políticas o identitarias.
- La comprensión de estos factores permite explicar por qué la refutación factual resulta a menudo insuficiente frente a determinadas narrativas manipulativas.
- Este bloque aporta una perspectiva interdisciplinar esencial para comprender la **dimensión cognitiva y social de las amenazas híbridas**.

Marco jurídico e institucional

La inclusión de un bloque dedicado al marco jurídico e institucional es imprescindible

porque las amenazas híbridas y las campañas de desinformación plantean problemas que no son solo estratégicos o tecnológicos, sino también profundamente **normativos, competenciales y de gobernanza democrática**. Cualquier programa formativo dirigido a juristas, responsables públicos, periodistas, diplomáticos o profesionales de la seguridad debe abordar necesariamente las preguntas relativas a qué instrumentos jurídicos son aplicables, qué competencias corresponden a cada nivel institucional, cuáles son los límites impuestos por los derechos fundamentales y cómo puede articularse una respuesta pública legítima y eficaz (Sanz-Caballero, 2023).

La necesidad de este bloque deriva, en primer lugar, de la propia naturaleza ambigua de las amenazas híbridas puesto que muchas de sus manifestaciones no encajan con facilidad en las categorías jurídicas tradicionales del uso de la fuerza, la agresión armada o incluso la injerencia clásica. Las operaciones de desinformación, las campañas de influencia, la manipulación de procesos electorales o ciertas ciberoperaciones de carácter no destructivo se sitúan frecuentemente en zonas de indeterminación normativa, lo que genera problemas de calificación, atribución de responsabilidad y activación de respuestas institucionales. Por ello, el alumnado debe familiarizarse con los debates contemporáneos sobre soberanía digital, responsabilidad internacional, atribución en el ciberespacio y protección de la integridad democrática.

En segundo lugar, este bloque resulta esencial porque la respuesta a la desinformación y a la manipulación informativa se encuentra atravesada por una tensión estructural entre, de un lado, la defensa de la seguridad, la integridad electoral y el orden democrático y, de otro, la garantía de la **libertad de expresión, el pluralismo informativo y otros derechos fundamentales**. Esta tensión convierte el análisis jurídico en una pieza central del programa: no basta con identificar riesgos, sino que es preciso determinar qué respuestas son compatibles con un Estado democrático de Derecho. En este sentido, la formación debe capacitar al alumnado para evitar tanto la infrarregulación ingenua como la sobrereacción normativa incompatible con los principios constitucionales y europeos (Parlamento Europeo y Consejo de la Unión Europea, 2022; Sanz-Caballero, 2023).

Además, la dimensión institucional del bloque se justifica porque la gobernanza de estas amenazas es necesariamente **multinivel y multisectorial**. La regulación y la respuesta frente a la desinformación involucran a instituciones nacionales, a la Unión Europea, a plataformas digitales, a autoridades reguladoras, a organismos de supervisión electoral, a estructuras de ciberseguridad y a actores de la sociedad civil. Comprender esta arquitectura institucional resulta decisivo para formar profesionales capaces de moverse en entornos complejos de cooperación, coordinación y reparto competencial. De lo contrario, el análisis quedaría reducido a una abstracción académica desconectada de los marcos reales de toma de decisiones.

En el contexto europeo, además, la evolución normativa reciente ha convertido este bloque en particularmente necesario. La regulación de servicios digitales, la transparencia de la publicidad política, las políticas europeas frente a la manipulación informativa, las obligaciones de plataformas y las disposiciones relativas a contenidos sintéticos generados por inteligencia artificial son ya parte del entorno regulatorio en el que operan instituciones y profesionales. No incorporar estas materias supondría ofrecer una formación incompleta y poco adaptada a la realidad jurídica contemporánea (Comisión Europea, 2022; Parlamento

Europeo y Consejo de la Unión Europea, 2022, 2024a, 2024b).

Por ello, los contenidos del bloque -regulación internacional de las ciberoperaciones, políticas europeas frente a la desinformación y protección de los procesos democráticos- están plenamente justificados. Su función es dotar al alumnado de una **capacidad de encuadramiento jurídico e institucional** sin la cual no sería posible traducir el diagnóstico de las amenazas en propuestas de respuesta compatibles con el ordenamiento jurídico y con las exigencias de legitimidad propias de una democracia constitucional.

Síntesis del Módulo

- Las amenazas híbridas plantean desafíos jurídicos complejos relacionados con la atribución de responsabilidades y la calificación normativa de determinadas acciones.
- Muchas de estas actividades se sitúan en zonas de ambigüedad jurídica que dificultan la activación de mecanismos tradicionales de respuesta.
- La regulación frente a la desinformación debe equilibrar la protección de la seguridad democrática con el respeto a derechos fundamentales, como la libertad de expresión.
- La gobernanza de estas amenazas implica una arquitectura institucional multinivel y multisectorial, que incluye Estados, Unión Europea, plataformas digitales y sociedad civil.
- Las recientes iniciativas regulatorias europeas han reforzado la importancia del marco jurídico en la gestión de la manipulación informativa digital.
- Este bloque proporciona al alumnado herramientas para comprender las posibilidades y límites de la respuesta normativa frente a las amenazas híbridas.

Prevención y resiliencia institucional

Este bloque final se justifica porque un programa docente sobre amenazas híbridas no puede limitarse a la descripción del problema; debe orientarse también a la **acción preventiva, la preparación institucional y la construcción de resiliencia**. Las amenazas híbridas se caracterizan precisamente por explotar debilidades previas de los sistemas políticos y sociales. Por ello, una formación verdaderamente útil para profesionales debe capacitar no solo para identificar campañas de influencia o manipulación, sino para diseñar respuestas proporcionales, coordinadas y sostenibles (Lewandowsky y Van der-Linden, 2021; Roozenbeek et al., 2022).

La necesidad de este bloque deriva, en primer lugar, de que la mera detección de una campaña de desinformación o de una operación de injerencia no garantiza por sí sola una respuesta eficaz. Las instituciones necesitan capacidades de anticipación, mecanismos de alerta temprana, procedimientos de análisis, coordinación interinstitucional y estrategias

de comunicación pública capaces de reducir la vulnerabilidad del sistema. En este sentido, la prevención y la resiliencia no son complementos opcionales, sino el núcleo práctico de cualquier política seria frente a amenazas híbridas (Amazeen et al., 2022; Bertolotti y Cattellani, 2023).

En segundo lugar, este bloque permite trasladar al plano operativo todo lo aprendido en los módulos anteriores. Si el alumnado ha adquirido un marco conceptual sobre amenazas híbridas, ha comprendido la centralidad del ciberespacio, ha analizado los factores psicológicos y sociales de la desinformación y conoce ya el marco jurídico e institucional aplicable, el siguiente paso lógico consiste en desarrollar capacidades para **transformar ese conocimiento en procedimientos de respuesta**. De ahí la importancia de incluir contenidos como análisis de inteligencia, OSINT y comunicación estratégica, que actúan como puentes entre la comprensión académica del fenómeno y su gestión práctica (Guess et al., 2020; Moore y Hancock, 2022).

La inclusión del **análisis de inteligencia** se justifica porque las amenazas híbridas suelen manifestarse a través de señales fragmentarias, ambiguas o aparentemente inconexas. Su detección exige metodologías sistemáticas de recogida, evaluación e interpretación de información. A su vez, la formación en OSINT resulta particularmente pertinente en el entorno digital actual, en el que una parte significativa de los indicios relevantes se encuentra en fuentes abiertas, redes sociales, bases de datos públicas, repositorios digitales o trazas accesibles en línea. Capacitar al alumnado en estas herramientas incrementa su autonomía analítica y su capacidad para contrastar, contextualizar y evaluar evidencias.

Por otra parte, el énfasis en la comunicación estratégica está plenamente justificado porque muchas respuestas institucionales fracasan no por ausencia de información, sino por incapacidad para **comunicar de forma creíble, oportuna y coherente**. En contextos de manipulación informativa, el silencio institucional, la reacción improvisada o la contradicción entre actores públicos pueden agravar el impacto de la campaña hostil. En consecuencia, este bloque debe enseñar que la resiliencia no depende únicamente de la capacidad de refutar falsedades, sino también de la construcción de confianza, la coherencia narrativa, la transparencia y la preparación comunicativa de las organizaciones (DiResta, 2024; Van der-Linden, 2023).

Finalmente, este módulo resulta esencial porque orienta el programa hacia su objetivo último: la formación de profesionales capaces de contribuir al fortalecimiento de la **resiliencia democrática e institucional**. La resiliencia, en este contexto, no debe entenderse como mera resistencia pasiva, sino como la capacidad de anticipar, absorber, adaptarse y responder a presiones híbridas sin comprometer los principios constitucionales ni la funcionalidad de las instituciones. Por ello, los contenidos del bloque no solo tienen una dimensión técnica, sino también una clara proyección cívica e institucional.

En suma, la presencia de este apartado en el programa se justifica porque convierte la propuesta formativa en una herramienta orientada a capacidades reales de prevención y respuesta. Los contenidos incluidos -análisis de inteligencia, OSINT y diseño de estrategias de comunicación estratégica- permiten cerrar coherentemente el itinerario formativo, integrando conocimiento conceptual, análisis crítico y aplicación profesional.

Síntesis del Módulo

- La respuesta eficaz a las amenazas híbridas requiere no solo capacidad de detección, sino también estrategias de prevención y fortalecimiento institucional.
- Las políticas de resiliencia buscan reducir vulnerabilidades estructurales y mejorar la capacidad de anticipación frente a campañas de influencia.
- El análisis de inteligencia permite interpretar señales fragmentarias y detectar patrones asociados a operaciones híbridas.
- Las herramientas de **OSINT** resultan especialmente relevantes en el entorno digital para el análisis de información procedente de fuentes abiertas.
- La comunicación estratégica es un elemento clave para contrarrestar narrativas manipulativas y preservar la confianza pública.
- Este bloque orienta el programa hacia su objetivo final: formar profesionales capaces de contribuir al fortalecimiento de la **resiliencia democrática e institucional**.

En conjunto, los cinco bloques temáticos responden a una lógica de progresión pedagógica que va desde la comprensión conceptual del fenómeno hasta la adquisición de capacidades aplicadas de análisis y respuesta. Esta secuencia permite evitar aproximaciones fragmentarias y dota al programa de una coherencia interna especialmente adecuada para un alumnado profesional y multidisciplinar, que necesita integrar marcos teóricos, comprensión normativa y herramientas operativas en un único itinerario formativo.

Con el fin de sintetizar la lógica pedagógica del programa y la relación entre los distintos bloques formativos, la tabla siguiente presenta la estructura del curso, su justificación y las competencias que se pretenden desarrollar en cada uno de los módulos.

Tabla 2. Estructura del curso, justificación, competencias y contenidos

Bloque formativo	Justificación pedagógica	Competencias que desarrolla	Contenidos principales
1. Fundamentos de las amenazas híbridas	Proporciona el marco conceptual necesario para comprender la lógica estratégica que integra fenómenos como la desinformación, las operaciones de influencia o las ciberacciones dentro de dinámicas de confrontación en la “zona gris”. Permite además establecer una base conceptual común para un alumnado interdisciplinar.	Comprensión estratégica del fenómeno; capacidad de identificar dinámicas de amenaza híbrida; análisis de vulnerabilidades institucionales.	Evolución del concepto de guerra híbrida; competencia estratégica en la zona gris; instrumentos de influencia política, informativa y económica.

Bloque formativo	Justificación pedagógica	Competencias que desarrolla	Contenidos principales
2. El ciberespacio como dominio estratégico	Analiza el papel central del entorno digital como espacio operativo para la amplificación y coordinación de campañas de desinformación y manipulación informativa. Permite comprender cómo la arquitectura tecnológica condiciona la difusión de contenidos y las dinámicas de influencia.	Alfabetización estratégica en el entorno digital; análisis del funcionamiento de plataformas; comprensión de dinámicas de amplificación algorítmica.	Arquitectura técnica del ciberespacio; funcionamiento de plataformas digitales; algoritmos y sistemas de recomendación; difusión y viralización de contenidos.
3. Psicología y sociología de la desinformación	Permite comprender los mecanismos cognitivos y sociales que facilitan la eficacia de las campañas de manipulación informativa. Analiza cómo sesgos cognitivos, polarización política y fragmentación del espacio público influyen en la circulación de narrativas manipulativas.	Análisis crítico del impacto social de la desinformación; comprensión de procesos de polarización y viralidad emocional; interpretación de dinámicas sociopolíticas del ecosistema informativo.	Sesgos cognitivos; formación de cámaras de eco; polarización política; factores emocionales en la viralización de contenidos digitales.
4. Marco jurídico e institucional	Aborda los desafíos normativos y de gobernanza asociados a las amenazas híbridas y a la manipulación informativa. Permite analizar las posibilidades y límites de la respuesta jurídica en contextos en los que confluyen seguridad democrática y derechos fundamentales.	Interpretación del marco normativo aplicable; comprensión de la gobernanza multinivel; análisis jurídico de políticas públicas frente a la desinformación.	Regulación internacional de ciberoperaciones; políticas europeas frente a la desinformación; protección de procesos democráticos; responsabilidades de plataformas digitales.
5. Prevención y resiliencia institucional	Orienta el programa hacia la dimensión aplicada del problema, proporcionando herramientas para la detección temprana y la respuesta institucional frente a campañas de manipulación informativa y operaciones híbridas.	Análisis estratégico; uso de herramientas OSINT; diseño de estrategias de comunicación institucional; elaboración de informes de riesgo.	Metodologías de análisis de inteligencia; OSINT; sistemas de alerta temprana; comunicación estratégica y gestión institucional de crisis informativas.

Fuente: Elaboración propia

Discusión

Beneficios esperados de la implementación del programa

La implementación de un programa formativo como el propuesto puede generar diversos beneficios en el ámbito académico, institucional y social.

En primer lugar, contribuye a **reducir el déficit formativo existente en relación con las amenazas híbridas y la desinformación**, proporcionando a los profesionales herramientas analíticas para comprender fenómenos complejos que afectan al funcionamiento de los sistemas democráticos (Apuke et al., 2023; Huang et al., 2024).

En segundo lugar, el carácter interdisciplinar del programa favorece el desarrollo de **espacios de aprendizaje compartido entre profesionales de distintos sectores**, lo que resulta especialmente relevante en el ámbito de la seguridad y de la gobernanza democrática.

En tercer lugar, la utilización de metodologías activas, como las simulaciones de crisis híbridas o el análisis de campañas reales, facilita la **transferencia de conocimientos entre el ámbito académico y el profesional**, reforzando la utilidad práctica de la formación (Yang et al., 2021; Zhang et al., 2022).

Finalmente, este tipo de programas puede contribuir a fortalecer la **resiliencia institucional frente a operaciones de manipulación informativa**, al promover una comprensión crítica del ecosistema informativo digital y de los mecanismos utilizados para influir en la opinión pública (Basol et al., 2021; Hwang et al., 2021).

Conclusiones

La naturaleza multidimensional de las amenazas exige una formación interdisciplinar. Las amenazas híbridas, las campañas de desinformación, las operaciones de influencia y las distintas formas de manipulación informativa constituyen fenómenos complejos, transnacionales y tecnológicamente mediados que pueden afectar a la estabilidad institucional, la cohesión social y el funcionamiento de los sistemas democráticos. Su análisis no puede realizarse adecuadamente desde una única disciplina, puesto que en estas dinámicas confluyen factores estratégicos, tecnológicos, jurídicos, comunicativos, psicológicos, sociales y políticos. En consecuencia, su tratamiento formativo requiere integrar conocimientos y métodos procedentes de diferentes áreas académicas y profesionales.

La formación universitaria existente presenta una fragmentación que dificulta la comprensión integral del fenómeno. Las amenazas híbridas y la desinformación suelen abordarse separadamente desde ámbitos como la seguridad internacional, la comunicación política, la ciberseguridad, el derecho o la psicología social. Esta compartimentación puede impedir que el alumnado comprenda que las campañas de manipulación informativa forman parte, en determinados casos, de estrategias más amplias en las que se combinan instrumentos políticos, informativos, tecnológicos, económicos y psicológicos. Resulta necesario, por tanto, avanzar hacia modelos docentes capaces de relacionar estas dimensiones dentro de un marco analítico común.

El modelo propuesto responde a esa necesidad mediante la combinación de interdisciplinariedad, aprendizaje aplicado y orientación institucional. La interdisciplinariedad permite integrar aportaciones de los estudios estratégicos, el derecho, la ciberseguridad, la comunicación, la psicología social y el análisis de inteligencia. El aprendizaje aplicado

facilita la transferencia de los conocimientos teóricos a contextos profesionales mediante estudios de caso, actividades de verificación digital, ejercicios de inteligencia de fuentes abiertas, simulaciones de crisis y prácticas de comunicación estratégica. La orientación institucional vincula la formación con las capacidades de prevención, detección, coordinación y respuesta que requieren las organizaciones públicas y privadas.

La principal aportación del trabajo es la formulación de un itinerario pedagógico progresivo y coherente. Los cinco bloques propuestos -fundamentos de las amenazas híbridas; ciberespacio como dominio estratégico; psicología y sociología de la desinformación; marco jurídico e institucional; y prevención y resiliencia institucional- articulan una secuencia que parte de la comprensión conceptual del fenómeno y culmina con el desarrollo de capacidades aplicadas. Esta organización permite relacionar el conocimiento estratégico con el análisis tecnológico, social y jurídico, evitando una acumulación de contenidos desconectados entre sí.

El programa resulta especialmente adecuado para un alumnado profesional y multidisciplinar. Juristas, periodistas, diplomáticos, miembros de las fuerzas armadas y de seguridad, analistas, responsables públicos, politólogos, psicólogos o especialistas en comunicación parten de lenguajes técnicos y tradiciones metodológicas diferentes. La creación de una base conceptual común y la realización de actividades compartidas pueden favorecer una cultura de cooperación interdisciplinar e interinstitucional, necesaria para hacer frente a amenazas que atraviesan sectores, competencias y niveles territoriales distintos.

La formación debe incorporar los límites jurídicos y democráticos de la respuesta frente a la desinformación. La protección de la integridad institucional y de los procesos democráticos no puede justificar medidas indiscriminadas que restrinjan desproporcionadamente la libertad de expresión, el pluralismo informativo u otros derechos fundamentales. La formación especializada debe capacitar para distinguir entre información falsa o engañosa, propaganda, opinión legítima, error, discurso protegido y operaciones coordinadas de manipulación. Asimismo, debe proporcionar criterios para valorar la legalidad, necesidad y proporcionalidad de las actuaciones de los poderes públicos, las plataformas digitales y los demás actores implicados.

La prevención y la resiliencia institucional deben ocupar una posición central en el proceso formativo. La respuesta frente a la manipulación informativa no puede limitarse a la refutación posterior de contenidos falsos. Las organizaciones necesitan desarrollar sistemas de alerta temprana, metodologías de análisis de inteligencia, capacidades de verificación, protocolos de coordinación y estrategias de comunicación previamente definidas. La formación puede contribuir a sustituir una actuación exclusivamente reactiva por una política de preparación institucional orientada a anticipar riesgos, reducir vulnerabilidades y preservar la confianza pública.

La propuesta puede contribuir al fortalecimiento de la resiliencia democrática, aunque no permite todavía acreditar empíricamente dicho efecto. El programa está diseñado para mejorar la capacidad de los profesionales para identificar señales relevantes, contextualizar campañas informativas, analizar actores, objetivos y técnicas, valorar las implicaciones jurídicas y formular respuestas institucionales proporcionadas. Sin embargo, la

relación entre formación especializada y aumento efectivo de la resiliencia democrática deberá verificarse mediante la implementación y evaluación del programa en contextos académicos y profesionales concretos.

El carácter conceptual y propositivo del estudio constituye su principal limitación metodológica. El modelo curricular no ha sido todavía aplicado de forma completa a una cohorte determinada ni se han medido empíricamente los resultados de aprendizaje obtenidos. Por esta razón, el trabajo no pretende establecer relaciones causales entre la participación en el programa y la mejora de las capacidades institucionales. Su aportación se sitúa en el diseño fundamentado de una propuesta formativa susceptible de implantación, evaluación y revisión posterior.

Las futuras investigaciones deberán centrarse en la validación empírica y en la adaptación del modelo. Resultaría conveniente desarrollar experiencias piloto, definir indicadores de aprendizaje y comparar las competencias del alumnado antes y después de la formación. También sería pertinente evaluar la eficacia relativa de metodologías como las simulaciones, los estudios de caso, los laboratorios de verificación o los ejercicios de inteligencia de fuentes abiertas. El modelo podría, además, adaptarse a perfiles profesionales específicos, diferentes contextos nacionales y modalidades de formación continua.

La educación superior debe considerarse una capacidad estratégica frente a la manipulación informativa. Su función no consiste únicamente en transmitir conocimientos sobre amenazas emergentes, sino en formar profesionales capaces de integrar información fragmentaria, evaluar críticamente narrativas y evidencias, aplicar el marco jurídico correspondiente y diseñar respuestas institucionales legítimas y eficaces. La incorporación de programas especializados de esta naturaleza puede contribuir al fortalecimiento de la autonomía analítica, la anticipación, la cooperación interinstitucional y la resiliencia democrática frente a las formas contemporáneas de injerencia y competencia estratégica en el entorno digital.

Declaración obligatoria de uso de IAGen

El autor declara que no se utilizaron herramientas de inteligencia artificial generativa en la elaboración de este manuscrito.

Referencias

- Amazeen, M. A., Krishna, A. y Eschmann, R. (2022). Cutting the bunk: Comparing the solo and aggregate effects of prebunking and debunking COVID-19 vaccine misinformation. *Science Communication*, 44(4), 387-417. <https://doi.org/10.1177/10755470221111558>
- Apuke, O. D., Omar, B. y Tunca, E. A. (2023). Literacy concepts as an intervention strategy for improving fake news knowledge, detection skills, and curtailing the tendency to share fake news in Nigeria. *Child & Youth Services*, 44(1), 88-103. <https://doi.org/10.1080/0145935X.2021.2024758>

- Arrese, Á. (2024). Cultural dimensions of fake news exposure: A cross-national analysis among European Union countries. *Mass Communication and Society*, 27(5), 827-850. <https://doi.org/10.1080/15205436.2022.2123278>
- Basol, M., Roozenbeek, J., Berriche, M., Uenal, F., McClanahan, W. P. y Van der-Linden, S. (2021). Towards psychological herd immunity: Cross-cultural evidence for two prebunking interventions against COVID-19 misinformation. *Big Data & Society*, 8(1), 1-18. <https://doi.org/10.1177/205395172111013868>
- Basol, M., Roozenbeek, J. y Van der-Linden, S. (2020). Good news about bad news: Gamified inoculation boosts confidence and cognitive immunity against fake news. *Journal of Cognition*, 3(1), 1-9. <https://doi.org/10.5334/joc.91> PMID:31934684 PMCID:PMC6952868
- Bertolotti, M. y Catellani, P. (2023). Counterfactual thinking as a prebunking strategy to contrast misinformation on COVID-19. *Journal of Experimental Social Psychology*, 104. <https://doi.org/10.1016/j.jesp.2022.104404>
- Comisión Europea. (16 de junio de 2022). *The strengthened code of practice on disinformation*. digital-strategy.ec.europa.eu. <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation>
- DiResta, R. (2024). *Invisible rulers: The people who turn lies into reality*. PublicAffairs.
- Ecker, U. K. H., Lewandowsky, S., Cook, J., Schmid, P., Fazio, L. K., Brashier, N., Kendeou, P., Vraga, E. K. y Amazeen, M. A. (2022). The psychological drivers of misinformation belief and its resistance to correction. *Nature Reviews Psychology*, 1, 13-29. <https://doi.org/10.1038/s44159-021-00006-y> PMCID:PMC9049321
- Freelon, D. y Wells, C. (2020). Disinformation as political communication. *Political Communication*, 37(2), 145-156. <https://doi.org/10.1080/10584609.2020.1723755>
- Guess, A. M., Lerner, M., Lyons, B., Montgomery, J. M., Nyhan, B., Reifler, J. y Sircar, N. (2020). A digital media literacy intervention increases discernment between mainstream and false news in the United States and India. *Proceedings of the National Academy of Sciences*, 117(27), 15536-15545. <https://doi.org/10.1073/pnas.1920498117> PMID:32571950 PMCID:PMC7355018
- Huang, G., Jia, W. y Yu, W. (2024). Media literacy interventions improve resilience to misinformation: A meta-analytic investigation of overall effect and moderating factors. *Communication Research*. <https://doi.org/10.1177/00936502241288103>
- Humprecht, E., Esser, F. y Van Aelst, P. (2020). Resilience to online disinformation: A framework for cross-national comparative research. *The International Journal of Press/Politics*, 25(3), 493-516. <https://doi.org/10.1177/1940161219900126>
- Hwang, Y., Ryu, J. Y. y Jeong, S.-H. (2021). Effects of disinformation using deepfake:

- The protective effect of media literacy education. *Cyberpsychology, Behavior, and Social Networking*, 24(3), 188-193. <https://doi.org/10.1089/cyber.2020.0174> PMID:33646021
- Kim, H. K., Ahn, J., Atkinson, L. y Kahlor, L. A. (2020). Effects of COVID-19 misinformation on information seeking, avoidance, and processing: *A multi-country comparative study*. *Science Communication*, 42(5), 586-615. <https://doi.org/10.1177/1075547020959670> PMID:38603002 PMCID:PMC7492825
- Kozyreva, A., Lewandowsky, S. y Hertwig, R. (2020). Citizens versus the Internet: Confronting digital challenges with cognitive tools. *Psychological Science in the Public Interest*, 21(3), 103-156. <https://doi.org/10.1177/1529100620946707> PMID:33325331 PMCID:PMC7745618
- Lewandowsky, S. y Van der-Linden, S. (2021). Countering misinformation and fake news through inoculation and prebunking. *European Review of Social Psychology*, 32(2), 348-384. <https://doi.org/10.1080/10463283.2021.1876983>
- Moore, R. C. y Hancock, J. T. (2022). A digital media literacy intervention for older adults improves resilience to fake news. *Scientific Reports*, 12. <https://doi.org/10.1038/s41598-022-08437-0> PMID:35397631 PMCID:PMC8994776
- Parlamento Europeo y Consejo de la Unión Europea. (19 de octubre de 2022). *Reglamento (UE) 2022/2065, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales)*. Diario Oficial de la Unión Europea, L 277, 1-102. eur-lex.europa.eu/eli/reg/2022/2065/oj
- Parlamento Europeo y Consejo de la Unión Europea. (13 de marzo de 2024a). *Reglamento (UE) 2024/900, sobre transparencia y segmentación en la publicidad política*. Diario Oficial de la Unión Europea. eur-lex.europa.eu/eli/reg/2024/900/oj
- Parlamento Europeo y Consejo de la Unión Europea. (13 de junio de 2024b). *Reglamento (UE) 2024/1689, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828*. Diario Oficial de la Unión Europea. eur-lex.europa.eu/eli/reg/2024/1689/oj
- Pennycook, G. y Rand, D. G. (2021). The psychology of fake news. *Trends in Cognitive Sciences*, 25(5), 388-402. <https://doi.org/10.1016/j.tics.2021.02.007> PMID:33736957 PMCID:PMC11135712
- Roozenbeek, J., Van der-Linden, S., Goldberg, B., Rathje, S. y Lewandowsky, S. (2022). Psychological inoculation improves resilience against misinformation on

- social media. *Science Advances*, 8(34), eabo6254. <https://doi.org/10.1126/sciadv.abo6254> PMID:36001675 PMCID:PMC9401631
- Salaverría, R., Buslón, N., López-Pan, F., León, B., López-Goñi, I. y Erviti, M. C. (2020). Desinformación en tiempos de pandemia: tipología de los bulos sobre la COVID-19. *El profesional de la información*, 29(3), e290315. <https://doi.org/10.3145/epi.2020.may.15>
- Sanz-Caballero, S. (2023). The concepts and laws applicable to hybrid threats, with a special focus on Europe. *Humanities and Social Sciences Communications*, 10. <https://doi.org/10.1057/s41599-023-01864-y>
- Sultan, M., Tump, A. N., Ehmann, N., Lorenz-Spreen, P., Hertwig, R., Gollwitzer, A. y Kurvers R. H. J. M. (2024). Susceptibility to online misinformation: A systematic meta-analysis of demographic and psychological factors. *Proceedings of the National Academy of Sciences*, 121(47), e2409329121. <https://doi.org/10.1073/pnas.2409329121> PMID:39531500 PMCID:PMC11588074
- Tuñón-Navarro, J., Oleart, A. y Bouza-García, L. (2019). Actores europeos y desinformación la disputa entre el factchecking, las agendas alternativas y la geopolítica. *Revista de comunicación*, 18(2), 245-260. <https://dialnet.unirioja.es/servlet/articulo?codigo=7039215> <https://doi.org/10.26441/RC18.2-2019-A12>
- Van der-Linden, S. (2023). *Foolproof: Why misinformation infects our minds and how to build immunity*. W. W. Norton & Company.
- Wuyckens, G., Landry, N. y Fastrez, P. (2022). Untangling media literacy, information literacy, and digital literacy: A systematic meta-review of core concepts in media education. *Journal of Media Literacy Education*, 14(1), 168-182. <https://doi.org/10.23860/JMLE-2022-14-1-12>
- Yang, S., Lee, J. W., Kim, H.-J., Kang, M., Chong, E. y Kim, E.-M. (2021). Can an online educational game contribute to developing information literate citizens? *Computers & Education*, 161, 104057. <https://doi.org/10.1016/j.compedu.2020.104057>
- Zhang, L., Iyendo, T. O., Apuke, O. D. y Gever, V. C. (2022). Experimenting the effect of using visual multimedia intervention to inculcate social media literacy skills to tackle fake news. *Journal of Information Science*. 51(1), 135-145. <https://doi.org/10.1177/01655515221131797>



Revista Perspectivas en Inteligencia

(Revista Científica en Ciencias Sociales e Interdisciplinaria)

Volumen 18, Número 27, enero - junio de 2026

ISSN: 2145-194X (impreso), 2745-1690 (en línea)

Página Web: <https://revistaseditorialejc.org/index.php/pei>

Bogotá D.C., Colombia

Educación superior y resiliencia democrática: una propuesta para la formación en inteligencia sobre amenazas híbridas y manipulación informativa

Declaración de divulgación

Los autores declaran que no existe ningún potencial conflicto de interés relacionado con el artículo.

Financiamiento

Los autores no declaran fuente de financiamiento para la realización de este artículo.

Sobre el/los autor(es)

Carlos Galán-Cordero es Doctor en Derecho de la Universidad Carlos III de Madrid (España), Magíster en Relaciones Internacionales y Comunicación de la Universidad Camilo Jose Cela (España), Licenciado en Derecho de la Universidad Autónoma de Madrid (España), es profesor de la Universidad Carlos III de Madrid, de la Universidad Oberta de Catalunya y de la Universidad Internacional de la Rioja (España), es experto en Ciberamenazas y Ciberinteligencia por la Universidad Pablo de Olavide de Sevilla (España), es Director de la Maestría en Análisis de Inteligencia y Ciberinteligencia de la Universidad Nebrija (España), es Director del Área de Amenazas Híbridas de la Agencia de Tecnología Legal y miembro del Grupo de Trabajo sobre Desinformación del Departamento de Seguridad Nacional de la Presidencia del Gobierno de España.

<https://orcid.org/0009-0006-3858-1666> - Contacto: cgalan@nebrija.es

