Las amenazas híbridas: concepto, objetivos, elementos, medios y agentes

Hybrid Threats: Concept, Objectives, Elements, Means, and Actors

Carlos Galán Cordero
Doctor en Derecho – Máster en Relaciones Internacionales y Comunicación
Director del Máster en Análisis de Inteligencia y Ciberinteligencia
Departamento de Seguridad y Defensa
Universidad Nebrija
Director del Área de Amenazas Híbridas de la Agencia de Tecnología Legal, S.L.
ORCID: https://orcid.org/0009-0006-3858-1666

Fecha de recepción: 15.02.2026
Fecha de aceptación: 13.07.2026
Fecha de publicación en línea: octubre 2026

Resumen:
El presente artículo analiza el fenómeno de las amenazas híbridas como uno de los principales desafíos para la seguridad, la estabilidad institucional y el orden democrático. Partiendo de un enfoque jurídico-estratégico, se examinan su concepto, características, agentes y objetivos, así como los instrumentos empleados para su materialización, con especial atención a la desinformación, los ciberataques y el uso instrumental de marcos regulatorios, analizando el papel de la desinformación y su impacto sobre los procesos democráticos, la cohesión social y la confianza en las instituciones, y el papel de determinados actores estatales, subrayando las dificultades jurídicas derivadas de la atribución, la respuesta normativa y la protección de los derechos fundamentales. La aportación específica del trabajo consiste en ordenar las amenazas híbridas no solo como fenómeno de seguridad, sino como problema jurídico-regulatorio: identifica sus agentes, depura sus categorías funcionales, diferencia la guerra económica tradicional de la coerción económica híbrida y examina las consecuencias que tales operaciones proyectan sobre la atribución de responsabilidad, la respuesta estatal y la protección de derechos fundamentales[1].

Palabras clave:
Amenazas híbridas; desinformación; ciberseguridad; injerencia extranjera; seguridad democrática.

Abstract:
This article analyzes the phenomenon of hybrid threats as one of the main challenges to security, institutional stability, and democratic order. Taking a legal-strategic approach, it examines their concept, characteristics, agents, and objectives, as well as the instruments used to carry them out, with special attention to disinformation, cyberattacks, and the instrumental use of regulatory frameworks. It analyzes the role of disinformation and its impact on democratic processes, social cohesion, and trust in institutions, and the role of certain state actors, highlighting the legal difficulties arising from attribution, regulatory response, and the protection of fundamental rights. The specific contribution of the article is to frame hybrid threats not only as a security phenomenon but also as a legal-regulatory problem: it identifies the relevant agents, refines their functional categories, distinguishes traditional economic warfare from hybrid economic coercion, and examines the consequences of such operations for attribution of responsibility, state response, and the protection of fundamental rights.

Keywords:
Hybrid threats; disinformation; cybersecurity; foreign interference; democratic security.

[1] La elaboración de este artículo contó con el apoyo académico derivado de la estancia internacional del investigador en la Facultad de Derecho de la Universidad Estatal de Moldavia.

Sumario:

1. Las amenazas híbridas: concepto y agentes. **2.** Objetivos de las amenazas híbridas. **3.** Elementos de las amenazas híbridas. **3.1.** Elementos de naturaleza militar. **3.1.1.** Guerra irregular, operaciones encubiertas y empleo de fuerzas proxy. **3.2.** Elementos de naturaleza económica. **3.3.** Elementos de naturaleza política o diplomática. **3.4.** Elementos de naturaleza cibernética e informacional. **3.4.1.** Los ciberataques. **3.4.2.** Las campañas de desinformación. **4.** Los principales agentes estatales generadores de amenazas híbridas. **4.1.** Rusia. **4.2.** China. **4.3.** Irán. **4.4.** Corea del Norte. **5.** Consecuencias jurídico-regulatorias de las amenazas híbridas. **6.** Conclusiones. Bibliografía.

Summary:

1. *Hybrid threats: concept and actors.* ***2.*** *Objectives of hybrid threats.* ***3.*** *Elements of hybrid threats.* ***3.1.*** *Military elements.* ***3.1.1.*** *Irregular warfare, covert operations, and the use of proxy forces.* ***3.2.*** *Economic elements.* ***3.3.*** *Political or diplomatic elements.* ***3.4.*** *Cyber and informational elements.* ***3.4.1.*** *Cyberattacks.* ***3.4.2.*** *Disinformation campaigns.* ***4.*** *The main state actors generating hybrid threats.* ***4.1.*** *Russia.* ***4.2.*** *China.* ***4.3.*** *Iran.* ***4.4.*** *North Korea.* ***5.*** *Legal and regulatory consequences of hybrid threats.* ***6.*** *Conclusions. Bibliography.*

1. Las amenazas híbridas: concepto y agentes.

Las amenazas híbridas (también llamadas en ocasiones *estrategias híbridas*[2]) son acciones de naturaleza perturbadora que comprenden una combinación de tácticas militares y no militares que un adversario puede utilizar de forma simultánea y coordinada para alcanzar sus objetivos y pueden ser impulsadas por Estados, por actores patrocinados o tolerados por Estados, por grupos armados no estatales, por organizaciones criminales, por empresas privadas de influencia o desinformación, por comunidades hacktivistas e incluso por redes oportunistas que amplifican narrativas ajenas. La diferencia entre ellos no siempre es nítida: la eficacia de las estrategias híbridas reside precisamente en la utilización de intermediarios, proxies, empresas pantalla, cuentas coordinadas o infraestructuras técnicas situadas en terceros países, lo que dificulta la atribución jurídica y política de la operación.

Efectivamente, el concepto *amenazas híbridas* pretende sintetizar un fenómeno complejo y en evolución. En los últimos años, diversas instituciones, desde el Parlamento Europeo[3] hasta la OTAN[4], han aportado distintas definiciones. Sin embargo, la más completa, a nuestro juicio, es la ofrecida por el Hybrid CoE (Centro Europeo de Excelencia para la Lucha contra las Amenazas Híbridas)[5]. Según esta fuente, las características esenciales de las amenazas híbridas son las siguientes:

- Están coordinadas y sincronizadas;
- Apuntan deliberadamente a las vulnerabilidades sistémicas de los Estados y las instituciones democráticas;
- Utilizan una amplia gama de medios;
- Explotan los umbrales de detección y atribución, así como diferentes escenarios: guerra-paz, interno-externo, local-estatal, nacional-internacional, amigo-enemigo;
- Tratan de influir de diferentes formas en la toma de decisiones a nivel local, regional, estatal o institucional;
- Favorecen y/o permiten alcanzar los objetivos estratégicos del agente;

[2] Así lo hace la *Estrategia de Seguridad Nacional* de España. Consejo de Seguridad Nacional. (2021).

[3] *"Un fenómeno resultante de la convergencia e interconexión de diferentes elementos, que juntos forman una amenaza más compleja y multidimensional"*. European Parliamentary Research Service (EPRS). (2015). *At a Glance: Understanding Hybrid Threats*.

[4] Desde el punto de vista de la OTAN, las amenazas híbridas son *"Un tipo de amenaza que combina actividades convencionales, irregulares y asimétricas en el tiempo y en el espacio"*, destacando que se trata de una amenaza que debe su peligrosidad a las sinergias generadas por sus diversos componentes cuando se utilizan de forma combinada.

[5] The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). https://www.hybridcoe.fi/

- Perjudican y/o dañan al objetivo.

Aunque las amenazas híbridas pueden perseguir objetivos particulares vinculados a situaciones concretas relacionadas con la víctima como, por ejemplo, propiciar que un candidato concreto alcance la victoria en unas elecciones, interfiriendo en el proceso electoral a través de campañas de desinformación orquestadas, suelen asimismo perseguir objetivos más estratégicos y a largo plazo, tales como:

- Erosionar la confianza de los ciudadanos en sus instituciones.
- Generar desconfianza en el sistema democrático.
- Socavar la cohesión o los modelos sociales de los Estados, comunidades políticas (como la UE) u organizaciones internacionales (como la OTAN, por ejemplo).
- Debilitar el sistema de gobierno de sus víctimas.
- Convencer de la decadencia de un sistema político (tanto a la población de la víctima como a la suya propia).
- Desestabilización económica.
- Influir en la toma de decisiones políticas para favorecer la propia agenda del atacante.

Esta tipología de agentes suele utilizar las amenazas híbridas por su eficacia y, al mismo tiempo, por la dificultad que supone atribuir acciones a un actor en particular, especialmente en el ciberespacio.

Como se ha dicho, aunque las amenazas híbridas presentan desafíos únicos para la seguridad nacional y la defensa[6], puesto que requieren una respuesta flexible y multifacética que pueda abordar una variedad de tácticas simultáneamente, su alcance es mayor que aquel, ya que al ser ataques capilares pueden subvertir el orden político, social y económico, constituyendo un problema que debe abordarse desde la defensa nacional pero también para la seguridad ciudadana y el orden público, la política económica, etc.

2. Objetivos de las amenazas híbridas

Las amenazas híbridas, cuando se trata de acciones estatales, generalmente, tienen como objetivo desestabilizar, desmoralizar, o comprometer al adversario sin necesidad de un enfrentamiento militar directo, centrando los propósitos en objetivos políticos, militares, económicos o sociales.

Para ilustrar mejor esta cuestión, se señalan seguidamente algunos de los objetivos habituales de las amenazas híbridas, que se han evidenciado en acciones recientes.

Los ejemplos que siguen no deben interpretarse como compartimentos estancos. Un mismo episodio puede perseguir simultáneamente desestabilización política, polarización social, explotación de vulnerabilidades institucionales y erosión de la confianza pública. Por ello, en esta versión se utiliza cada caso solo como ilustración principal de una finalidad, evitando convertir el artículo en una mera acumulación reiterativa de supuestos.

Desestabilización Política:

Se trata de uno de los principales objetivos de las amenazas híbridas. Mediante la propagación de desinformación y propaganda, los actores maliciosos persiguen influir en la opinión pública, sembrar la discordia y la confusión, y desestabilizar los procesos políticos internos.

Como hemos podido constatar, las campañas de desinformación y propaganda para desestabilizar políticamente a un país han venido sucediéndose incesantemente en la historia reciente. Se señalan algunos ejemplos:

[6] Miguel Ángel Ballesteros Martín, (2022). *La lucha contra las campañas de desinformación en el ámbito de la Seguridad Nacional*. (Cuadernos de periodistas: revista de la Asociación de la Prensa de Madrid, Nº. 45, 2022)

- Injerencia en las elecciones presidenciales de Estados Unidos de 2016. Según informes de la comunidad de inteligencia de Estados Unidos, Rusia llevó a cabo una campaña de desinformación y ciberataques durante las elecciones presidenciales de 2016, con el objetivo de influir en el resultado. La campaña incluyó la propagación de noticias falsas y desinformación en las redes sociales, así como el hackeo de los correos electrónicos del Comité Nacional Demócrata[7] [8].

- Desestabilización en Ucrania. Durante el conflicto de 2014 en Ucrania, Rusia fue acusada de utilizar tácticas de guerra híbrida, incluyendo la desinformación y la propaganda, para fomentar la división y la inestabilidad. Por ejemplo, se llevaron a cabo campañas de desinformación para exagerar la amenaza de los grupos de extrema derecha en Ucrania y para minimizar el papel de Rusia en el conflicto.

- Brexit y desinformación. Durante el referéndum del Brexit en 2016 en el Reino Unido, se produjeron campañas de desinformación y manipulación de la opinión pública a través de las redes sociales. Aunque no se ha demostrado una interferencia estatal directa, el caso ilustra cómo la desinformación y la manipulación de la opinión pública pueden tener un gran impacto en los procesos políticos[9] [10].

- Campañas de desinformación en las redes sociales. Varias plataformas de redes sociales, incluyendo Facebook y X (antes, Twitter[11]), han eliminado cuentas falsas y redes de desinformación que se han venido utilizando para influir en la opinión pública y desestabilizar las políticas en diferentes regiones, incluyendo campañas dirigidas a América Latina, África[12] y el sudeste de Asia[13] [14].

- Desinformación en el conflicto Sirio. Durante la Guerra Civil siria de 2011, ambos bandos utilizaron tácticas de desinformación, incluyendo la difusión de noticias falsas y la manipulación de imágenes y vídeos para influir en la percepción pública del conflicto.

- Injerencia en las elecciones de Brasil en 2018. Durante las elecciones presidenciales en Brasil, se propagaron noticias falsas y desinformación a través de las redes sociales para influir en los votantes. Los informes sugirieron que este contenido falso podría haber influido significativamente en la opinión pública y en el resultado de las elecciones.

- Guerra de la información en el conflicto entre India y Pakistán. India y Pakistán se han acusado mutua y repetidamente de participar en campañas de desinformación y propaganda. Esto ha sido particularmente evidente durante los periodos de conflicto militar, donde ambos países han utilizado medios de comunicación y plataformas de redes sociales para difundir narrativas propicias a sus intereses.

- Injerencia en las elecciones de Taiwán. Antes de las elecciones presidenciales de Taiwán en 2020, se publicaron informes de campañas de desinformación dirigidas a influir en el resultado. Algunos de tales informes señalaron que estas campañas provenían de China y estaban destinadas a minar el apoyo al partido en el poder, visto como menos favorable a los intereses chinos.

---

[7] Raúl Magallón Rosa. *Desinformación y elecciones. La (des)confianza en el sistema*. En *Desinformación y Defensa*. (Dykinson, 2024).

[8] Joe Slocum. *Inmigración y campaña electoral en Estados Unidos: desinformación y promesas de deportaciones masivas*. (Notes internacionals CIDOB, Nº. 311, 2024)

[9] Juan Miguel Aguado Terrón, Ángel Gómez de Ágreda, Inmaculada Caravaca Barroso. *El ecosistema de la desinformación: actores, estrategias y redes de valor*. En *Desinformación y Defensa*. (Dykinson, 2024).

[10] Anna Sixma van Heemstra Fernández. *La desinformación como amenaza para la democracia: el caso del Brexit*. Boletín IEEE (Instituto Español de Estudios Estratégicos, Nº 30, 2023).

[11] Eva Campos-Dominguez, Marc Esteve del Valle, Cristina Renedo Farpón. *Retóricas de desinformación parlamentaria en Twitter*. Comunicar: Revista Científica de Comunicación y Educación, Nº 72, 2022).

[12] Carlos Galán Cordero. *Countering Foreign Information Manipulation and Interference in Africa*. Center For The Governance of Change. IE University – NATO, 2025).

[13] Gabriel Crespo-Carchi, David Villalba. *Libertad de expresión frente a la regulación en la difusión de contenidos en internet*. (593 Digital Publisher CEIT, Vol. 9, Nº. 5, 2024).

[14] Mariluz Congosto Martínez, Javier Barriuso Bernad. *Activismo, desinformación y campañas en redes. Estudio de Twitter, Telegram y TikTok*. En *Democracia y desinformación. Nuevas formas de polarización, discursos de odio y campañas en redes. Respuestas regulatorias de Europa y América Latina. (*Dykinson, 2024).

Interrupción Económica:

La *guerra económica*, como las sanciones, el espionaje económico, y la manipulación de la moneda, puede ser utilizada para debilitar la economía de un adversario y erosionar su estatus. Ahora bien, no toda sanción económica, embargo o arancel debe calificarse automáticamente como amenaza híbrida. La guerra económica tradicional opera, por regla general, mediante instrumentos declarados, jurídicamente formalizados y atribuibles a un sujeto estatal identificable. La estrategia económica híbrida aparece cuando esos instrumentos se combinan con opacidad, coerción encubierta, manipulación informativa, dependencia tecnológica, captura de infraestructuras críticas, financiación de actores políticos o presión comercial selectiva con la finalidad de condicionar decisiones soberanas sin activar los mecanismos ordinarios de respuesta. La diferencia no radica solo en el medio económico utilizado, sino en su integración coordinada en una operación más amplia de influencia, desestabilización o coerción.

Se señalan seguidamente algunos ejemplos de cómo la guerra económica ha sido utilizada en el pasado en el contexto de las amenazas híbridas:

- Sanciones económicas contra Irán. Las sanciones económicas impuestas por Estados Unidos y otros países occidentales han tenido un impacto significativo en la economía iraní. Estas sanciones, que incluyen restricciones a las exportaciones de petróleo y la exclusión de Irán del sistema financiero internacional, han sido utilizadas como herramienta para presionar a Irán sobre su programa nuclear.

- Guerra comercial entre Estados Unidos y China. Bajo la primera administración de Donald Trump, Estados Unidos impuso una serie de aranceles sobre los productos chinos como parte de una guerra comercial más amplia. Esto fue visto como un intento de debilitar la economía china y forzar cambios en sus prácticas comerciales. La realidad actual en la primavera de 2025 es todavía más evidente y peligrosa para el orden económico mundial.

- Sanciones económicas contra Rusia. Tras la anexión ilegal de Crimea por parte de Rusia en 2014, Estados Unidos y la Unión Europea impusieron una serie de sanciones económicas a Rusia. Estas sanciones, que incluyeron restricciones a los viajes y a las transacciones financieras, han tenido un impacto significativo en la economía rusa.

- Manipulación de la moneda por parte de China. Durante años, China ha sido acusada de manipular su moneda para obtener ventajas comerciales. Al mantener su moneda débil, China puede hacer que sus exportaciones sean más baratas, lo que claramente perjudica a los competidores extranjeros.

- Embargo económico a Cuba. Desde 1960, Estados Unidos ha mantenido un embargo económico contra Cuba -más o menos explícito y significativo- que ha tenido un efecto significativo en la economía cubana. Este embargo, que ha incluido restricciones comerciales y financieras, ha sido utilizado como una herramienta de presión política para impulsar cambios en el gobierno cubano.

- Sanciones económicas contra Venezuela. Desde 2014, Estados Unidos y varios otros países han impuesto sanciones económicas a Venezuela, acusada de violaciones de derechos humanos y corrupción. Las sanciones, que han incluido la congelación de activos y la prohibición de ciertas transacciones comerciales, han tenido un impacto significativo en la economía venezolana.

- Manipulación de precios de productos básicos. Algunos países, especialmente aquellos con grandes reservas de productos básicos como el petróleo, han podido utilizar el control de los precios de estos productos como una forma de guerra económica. Por ejemplo, durante los años 70, los países de la OPEP utilizaron su control sobre el suministro de petróleo para influir en los precios globales, lo que tuvo un impacto económico significativo en los países importadores.

- Guerra de divisas. Como hemos señalado para el caso de China, algunos países han sido acusados de manipular el valor de su moneda para obtener ventajas comerciales. Estas acciones pueden implicar devaluar la moneda para hacer que las exportaciones sean más baratas o para atraer inversión extranjera.

Desmoralización y/o Polarización Social:

A través de la desinformación y la propaganda, los actores pueden intentar exacerbar las tensiones sociales de sus víctimas y crear división, desmoralizando a la población y debilitando la cohesión social.

Se mencionan seguidamente algunos ejemplos de ello:

- Desinformación sobre la crisis de los refugiados en Europa. Durante la crisis de los refugiados en 2015 y 2016, se difundieron noticias falsas y desinformación para exacerbar las tensiones y la polarización en torno a la cuestión de la inmigración, incluyendo rumores y falsedades sobre los propios refugiados, con el propósito de fomentar la xenofobia y la hostilidad.

- Campaña de desinformación en el conflicto de Rohingyas en Myanmar. En 2017, Facebook reconoció que su plataforma había sido utilizada para sembrar el odio y la desinformación contra la minoría Rohingya en Myanmar. Las noticias falsas y el discurso de odio que se difundió contribuyeron a la violencia y la desmoralización de la población Rohingya.

- Guerra de la información en Hong Kong. Durante las protestas en Hong Kong en 2019-2020, se desarrollaron campañas de desinformación en las redes sociales para sembrar la división y fomentar la desmoralización, incluyendo la difusión de teorías de la conspiración y desinformación sobre los manifestantes y sus motivos.

- Campañas de desinformación COVID-19. Durante la pandemia del COVID-19, hubo numerosas campañas de desinformación destinadas a sembrar la discordia y el miedo en las poblaciones. Las acciones oscilaron desde teorías de la conspiración sobre el origen del virus hasta falsedades sobre las vacunas y los tratamientos. Estas campañas de desinformación contribuyeron a la polarización en torno a la respuesta al virus y la administración de las vacunas[15].

- Desinformación y discordia social en la India. En la India, el uso de plataformas de mensajería como WhatsApp para difundir desinformación ha llevado a casos de violencia comunal y linchamientos en masa, propalando rumores y desinformación diseñados para incitar el odio y la violencia entre diferentes grupos religiosos y étnicos[16].

Compromiso de las Infraestructuras Críticas y de los sistemas de información de entidades esenciales o importantes:

Por su parte, como es sabido, los ciberataques -elementos muy efectivos de las amenazas híbridas-, pueden estar dirigidos a las infraestructuras críticas de un país, tales como las redes de energía, los sistemas de comunicación, los sistemas financieros o sanitarios, al objeto de causar daño físico o interrumpir los servicios esenciales.

Desde una perspectiva analítica, el compromiso de infraestructuras críticas constituye una modalidad especialmente grave de amenaza híbrida porque permite transformar una intrusión técnica en un efecto político o social. La interrupción de redes eléctricas, servicios sanitarios, comunicaciones, sistemas financieros, administraciones digitales o plataformas de servicios esenciales no solo produce daños operativos: genera percepción de vulnerabilidad estatal, erosiona la confianza ciudadana y puede ser utilizada para amplificar narrativas de incompetencia institucional. En este punto, la ciberseguridad deja de ser un problema meramente técnico y se convierte en una condición de continuidad democrática y de protección de derechos.

Son incesantes los ejemplos que pueden exponerse de este tipo de ataques. Véase, en este sentido los Informes de Ciberamenazas y Tendencias que anualmente viene publicando el CERT del Centro Criptológico Nacional (CNI).

Explotación de Brechas y Vulnerabilidades:

Las amenazas híbridas, frecuentemente, se diseñan para explotar las debilidades existentes en la sociedad o el país objetivo, lo que puede incluir la exacerbación de tensiones étnicas o religiosas, la corrupción o el mal gobierno, las vulnerabilidades en los sistemas de ciberseguridad, etc.

[15] Juan Miguel Evangelista Pintado. *La Unión Europea y la desinformación.* Revista general de marina, Octubre, 2021).

[16] Pablo Hernández Escayola. *Whatsapp y la desinformación que pasa desapercibida*. (Adcomunica, 2022).

La explotación de brechas y vulnerabilidades debe entenderse en sentido amplio. Incluye vulnerabilidades técnicas -sistemas no actualizados, ausencia de segmentación, cadenas de suministro débiles-, pero también vulnerabilidades sociales, jurídicas e institucionales: polarización previa, desconfianza en medios, desigualdad territorial, baja alfabetización mediática, fragmentación competencial o lentitud de la respuesta administrativa. La lógica híbrida consiste en identificar esos puntos de fricción y convertirlos en vectores de presión. Por ello, la resiliencia frente a amenazas híbridas requiere reducir vulnerabilidades estructurales, no solo reaccionar ante incidentes concretos.

Se señalan seguidamente algunos ejemplos -algunos de ellos previamente comentados bajo otros considerandos- sobre cómo los actores estatales o no estatales han utilizado tácticas híbridas para explotar las brechas y debilidades en las sociedades y los sistemas políticos de sus víctimas:

- Influencia de China en la política australiana. Durante los últimos años ha habido una creciente preocupación por la influencia de China en la política australiana, lo que incluye la supuesta infiltración en partidos políticos, la influencia en la Academia y la prensa, y el uso de inversiones y donaciones para ganar influencia.

- Operaciones de influencia de Irán en el Medio Oriente. Irán ha venido utilizando una variedad de tácticas híbridas para ampliar su influencia en Oriente Medio, incluyendo el apoyo a grupos de militantes y políticos, la desinformación, la propaganda, y la explotación de las divisiones sectarias y étnicas.

3. Elementos de las amenazas híbridas

Para superar la confusión entre medios digitales y no digitales, se adopta una clasificación funcional. Las amenazas híbridas se ordenan aquí según la función que cumple cada instrumento dentro de la estrategia: militar, económica, político-diplomática y cibernético-informacional. Esta clasificación no implica separación rígida; al contrario, lo característico de lo híbrido es que esas funciones se combinan y se refuerzan mutuamente.

Como hemos señalado, las amenazas híbridas son acciones coordinadas que comprenden una combinación de tácticas militares y no militares que un adversario utiliza de forma simultánea y coordinada para alcanzar sus objetivos. Veamos estos elementos por separado.

3.1. Elementos de naturaleza militar

3.1.1. Guerra irregular, operaciones encubiertas y empleo de fuerzas proxy

Las tácticas militares en el contexto de las amenazas híbridas suelen combinar elementos de guerra convencional y no convencional. He aquí hay algunas formas en que esto puede ocurrir:

Guerra irregular y de guerrillas:

Implica tácticas que no se consideran parte de la guerra tradicional o convencional, como el uso de fuerzas paramilitares, guerrillas, grupos insurgentes o mercenarios. Estos grupos, frecuentemente, se utilizan para desestabilizar a un enemigo sin implicar directamente a las fuerzas armadas regulares del país[17].

Se señalan seguidamente algunos ejemplos de acciones híbridas de naturaleza militar:

- Invasión de Crimea en 2014. Rusia utilizó una combinación de tácticas militares y no militares para anexarse la península de Crimea. Las fuerzas militares rusas, sin distintivos militares, conocidas como "pequeños hombres verdes", tomaron el control de las instalaciones gubernamentales y militares en Crimea. Mientras tanto, Rusia llevó a cabo una intensa campaña de desinformación para confundir a la comunidad internacional y a la población local sobre la realidad de lo que estaba ocurriendo.

[17] Ejemplo de esto fue la táctica de los llamados "*Little Green Men*", término que se originó durante la anexión de Crimea por parte de Rusia en 2014, cuando soldados sin distintivos militares, que más tarde resultaron ser rusos, tomaron el control de la región. Estos "*Little Green Men*" representan una táctica híbrida que perseguía sembrar la confusión y la incertidumbre sobre la identidad de los atacantes.

- Conflicto en el este de Ucrania. Desde 2014, Rusia ha estado apoyando a los separatistas en las regiones del este de Ucrania, Donetsk y Luhansk, incluyendo tanto el suministro de armas y el apoyo militar directo, como la realización de operaciones de desinformación y guerra cibernética.

- Operaciones de Irán en el Medio Oriente. Irán ha venido llevando a cabo una variedad de operaciones híbridas en toda la región del Oriente Medio, incluyendo el apoyo a grupos militantes y políticos en países como Siria, Irak, Yemen y Líbano, y el desarrollo de ataques encubiertos y operaciones cibernéticas.

- Infiltraciones de Hezbollah en Israel. Incluso antes del feroz ataque de Hamás del 7 de octubre de 2023, Hezbollah, un grupo militante libanés respaldado por Irán, ha llevado a cabo una serie de infiltraciones en territorio israelí. Estas operaciones han implicado una combinación de tácticas de guerra irregular, incluyendo el uso de túneles, cohetes y drones.

Estos ejemplos ilustran cómo las tácticas militares pueden ser combinadas con otros métodos en el contexto de una estrategia híbrida.

Guerra cibernética:

Los ataques cibernéticos son elementos muy importantes de las amenazas híbridas, puesto que pueden incluir ataques a las infraestructuras críticas de un país, tales como redes eléctricas, sistemas de transporte o sistemas de comunicaciones, y también puede incluir la infiltración en redes de ordenadores para sustraer información o interrumpir operaciones.

Desinformación y propaganda:

Se trata de tácticas clave en las amenazas híbridas, utilizadas para sembrar confusión, crear divisiones dentro de la sociedad de los países atacados y socavar la confianza en las instituciones.

3.2. Elementos de naturaleza económica

Es la denominada *Guerra Económica*, pudiendo implicar acciones tales como sanciones, embargos y otras medidas para dañar la economía de un país atacado.

Obviamente, las tácticas específicas utilizadas en una amenaza híbrida dependerán de una variedad de factores, incluyendo los objetivos del adversario, las capacidades y vulnerabilidades del objetivo, y el contexto estratégico.

3.3. Elementos de naturaleza política o diplomática

Las acciones híbridas de naturaleza política o diplomática son también una parte importante de las amenazas híbridas. Las tácticas siguientes, de las que se señalan algunos ejemplos significativos, pueden ser utilizadas por los atacantes de manera individual o en combinación, y pueden ser empleadas tanto por estados como por actores no estatales.

Aunque estas tácticas no son nuevas, la proliferación de la tecnología digital y las redes sociales ha aumentado su alcance y eficacia[18].

La tabla siguiente ordena sintéticamente las principales técnicas político-diplomáticas, sus mecanismos de actuación y algunos ejemplos.

[18] Raúl Sampedro Oliver. *Redes sociales: desinformación, adicción y seguridad.* (Boletín IEEE-Instituto Español de Estudios Estratégicos, 2021).

Desinformación y propaganda	Se trata de una táctica clave en las estrategias híbridas. La desinformación y la propaganda pueden ser utilizadas para influir en la opinión pública, sembrar división y discordia, y debilitar la confianza en las instituciones. Por ejemplo, como hemos dicho, Rusia ha sido acusada de llevar a cabo campañas de desinformación en las elecciones en Estados Unidos y en Europa para tratar de influir en los resultados y debilitar la confianza en el proceso democrático. Algunos ejemplos son las elecciones presidenciales de Estados Unidos de 2016 o la campaña del referéndum del Brexit.
Diplomacia coercitiva	Los actores pueden utilizar la diplomacia como una herramienta de coacción, utilizando la amenaza de consecuencias negativas para influir en el comportamiento de otros países, incluyendo la posibilidad de sanciones económicas, el aislamiento diplomático, o incluso la intervención militar.
Apoyo a actores no estatales	Los estados pueden apoyar a grupos militantes, partidos políticos, o movimientos sociales en otros países para avanzar en sus propios intereses. Por ejemplo, Irán ha venido apoyando a una variedad de grupos militantes en Oriente Medio, incluyendo Hezbollah en el Líbano y varias milicias en Irak y Siria. Como decimos, algunos ejemplos son Hezbollah y el apoyo de Irán a los rebeldes Houthi en Yemen, proporcionándoles armas y apoyo financiero en su lucha contra el gobierno yemení y la coalición liderada por Arabia Saudita
Influencia económica y financiera	Los estados pueden utilizar su influencia económica y financiera para lograr objetivos políticos, lo que puede incluir la inversión en infraestructuras críticas, la compra de medios de comunicación, o la donación a partidos políticos. Algunos ejemplos son: ↘ Influencia china en África: China ha invertido grandes sumas de dinero en la infraestructura en muchos países africanos. Esta inversión ha dado a China una gran influencia en estos países y ha suscitado preocupaciones sobre la dependencia de estos países de China[19]. ↘ La construcción del gasoducto Nord Stream 2: Este proyecto, para el transporte de gas natural desde Rusia a Alemania, ha sido fuente de controversia. Algunos críticos argumentan que aumentará la dependencia de Europa del gas ruso, dando a Rusia una mayor influencia económica y política en la región.
Guerra cibernética	Los ataques cibernéticos pueden ser utilizados para lograr una variedad de objetivos políticos, desde el robo de información y la interrupción de infraestructuras críticas hasta la influencia en las elecciones y la opinión pública.
Injerencia en las elecciones	Un estado puede intentar influir en el resultado de las elecciones en otro país a través de una variedad de medios, desde la financiación de candidatos preferidos y la propagación de desinformación hasta el hackeo de los sistemas de votación, como hemos señalado en ejemplos precedentes.

3.4. Elementos de naturaleza cibernética e informacional

3.4.1. Los ciberataques

Según los Informes Anuales que viene publicando ENISA, las principales amenazas a la ciberseguridad son las siguientes[20]:

↘ Ransomware.

↘ Malware.

↘ Amenazas de ingeniería social.

[19] Carlos Galán Cordero. *Countering Foreign Information Manipulation and I*nterference in Africa. Center For The Governance of Change. IE University – NATO, 2025).

[20] ENISA (European Union Agency For Cybersecurity).

- Amenazas contra los datos.
- Amenazas contra la disponibilidad: Denegación de servicio.
- Amenazas contra la disponibilidad: Amenazas de Internet.
- Desinformación - información errónea.
- Ataques a la cadena de suministro.

Entender las tendencias asociadas a los agentes de las amenazas, junto con sus intenciones y metas, es crucial para diseñar estrategias de defensa y mitigación en ciberseguridad. Así, según el citado Informe de ENISA, los actores maliciosos que presentan más riesgo son: los actores estatales (Estados o agentes patrocinados por Estados), los ciberdelincuentes, los hackers a sueldo y los hacktivistas.

3.4.2. Las campañas de desinformación

Las plataformas digitales se han convertido en el medio mayoritariamente usado para acceder a las noticias, especialmente, entre la población más joven. Las redes sociales, los medios de comunicación digitales y hasta los motores de búsqueda constituyen en la actualidad la fuente de información principal para muchas personas. Debido a la forma de operar y a los intereses tales sitios, persiguiendo aumentar el número de usuarios y la generación de tráfico, la información que atrae a más espectadores suele ser la unilateralmente destacada, a veces sin la debida verificación. Temas actuales, como el conflicto entre Rusia y Ucrania, han generado numerosas narrativas que han captado mucha atención[21]. Las diferencias entre información incorrecta o intencionadamente falseada obedecen a diversos motivos. Es en este contexto donde cobran relevancia las definiciones de desinformación (*disinfomation*) y mala información (*misinformation)*[22] [23].

Por otro lado, la denominada *computación en la nube*, las herramientas y los algoritmos de inteligencia artificial facilitan a los actores de las amenazas la creación de información dañina. Esta eficacia tiene bases tanto técnicas como sociales y otorga a los actores estatales y no estatales potentes herramientas para fabricar y difundir desinformación. Además, estas plataformas y servicios también permiten a los agentes experimentar, supervisar, ajustar y mejorar el impacto de las campañas de desinformación.

Generalmente, estas campañas son el preludio de otros ataques, como el phishing, la ingeniería social o la propia infección por malware.

Como podemos apreciar, el caudal de desinformación generada por actores estatales y no estatales, que inunda las sociedades, tiene el objetivo de generar incertidumbre, indiferencia hacia la verdad, agotamiento al buscarla y miedo. Es cada vez más evidente que la desinformación es una amenaza significativa para la democracia -puesto que plantea tres tipos de riesgos: reputacional y de confianza, político-electoral y económico-financiero[24]-, que debe ser adecuadamente tratada -también desde el punto de vista jurídico-, en una sociedad libre y moderna. Como propondremos al final del presente trabajo, los encargados de formular políticas deberían incluir en sus agendas, como materia prioritaria, la desinformación, considerando también las implicaciones para la seguridad y la privacidad[25]. Esta situación ha sido amplificada y puesta en el foco de investigadores, gobiernos y la comunidad debido a la oleada de ataques de desinformación que precedieron y vienen acompañando la guerra entre Rusia y Ucrania[26]. En este marco, el Parlamento

[21] Pablo Hidalgo Cobo, Olga Serrano Villalobos, Belén Puebla Martínez. *Desinformación en la guerra de Ucrania: análisis de las agencias de verificación españolas en TikTok*. Doxa comunicación, nº. 40, 2025).

[22] La *misinformation* es un ataque involuntario, en el que se comparte información sin querer. La inexactitud que conlleva la información no es intencionada y puede ocurrir, por ejemplo, cuando un periodista transmite información errónea de buena fe o comunica información por error. European Union Agency for Cybersecurity. (2020). *Tendencias emergentes*.

[23] Como hemos señalado, el presente trabajo se centra en lo que se ha definido como "amenazas híbridas" y, especialmente las comprendidas en ellas: la "desinformación" y las "campañas de desinformación". No es nuestro propósito, por tanto, tratar aquí la significación e importancia de la denominada "misinformatión", que, por su carácter no deliberado, exigiría un análisis independiente.

[24] Juan David Abella Osorio, Vicente Torrijos Rivera. *Los riesgos de la desinformación para las democracias, un modelo de análisis*. (Cuadernos de la Guardia Civil: Revista de seguridad pública, Nº 69, 2023).

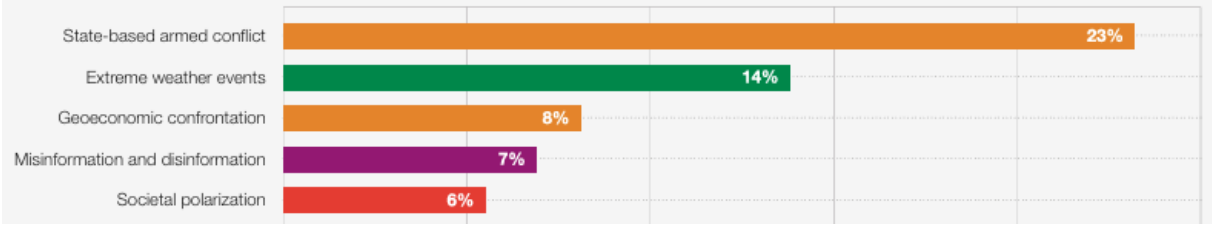
[25] The World Economic Forum. *The Global Risks Report 2021*.

[26] Aaron Schaffer. *Ukraine war is more about disinformation than cyberattacks*. (The Washington Post, 2022). / rachel Baig. *The deepfakes in the disinformation war*. (Deutsche Welle, 2022).

Europeo publicó una resolución el 9 de marzo de 2022 sobre la interferencia extranjera en todos los procesos democráticos de la Unión Europea, incluyendo la desinformación (2020/2268(INI))[27].

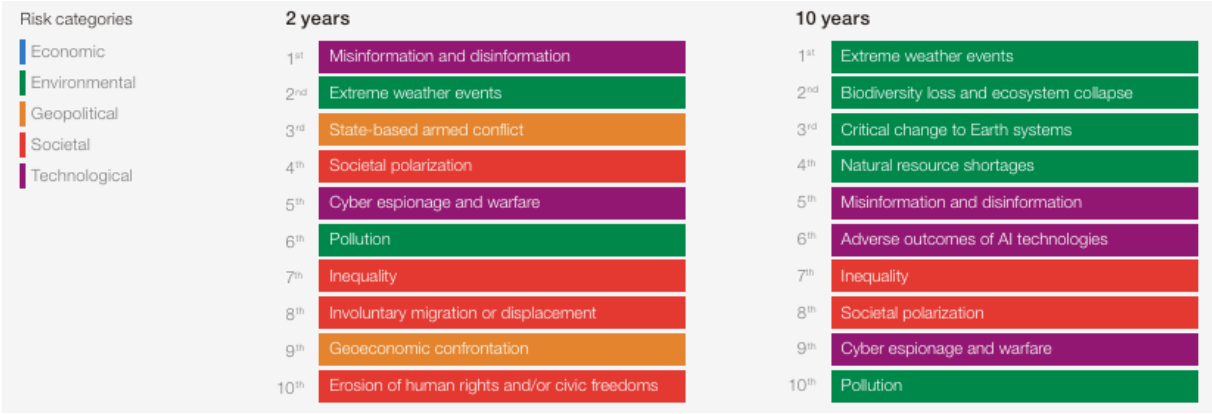
Al igual que en 2021, los Informes de Riesgos Globales de 2022, 2023, 2024 y 2025 del Foro Económico Mundial han señalado que la interacción entre la digitalización y el crecimiento de las ciberamenazas también tiene consecuencias intangibles. El auge de los denominados *deepfakes* y la "desinformación bajo demanda" intensificará la desconfianza entre sociedades, empresas y gobiernos. Todo ello podría emplearse, por ejemplo, para influir en campañas electorales u otro tipo de iniciativas políticas[28]. Además, la desinformación es una de las dimensiones que más impacta negativamente en la confianza pública hacia los sistemas digitales, que también está afectando la colaboración entre estados, ya que la ciberseguridad se convierte en un punto de desacuerdo en lugar de cooperación.

La figura siguiente muestra el panorama de riesgos globales definido por el WEF en su informe de 2025. Obsérvese la presencia de la problemática señalada, encuarto y quinto lugar.



Current Global Risk Landscape. (Fuente: WEF. Global Risk Report 2025)

Y en relación con el resto de los riesgos globales y su proyección a dos años (donde la desinformación ocupa el primer lugar) y a diez años.



Global riks ranked by severity over the short and long term. (Fuente: WEF. Global Risks Report 2025)

Según el antedicho documento, los ciberataques transfronterizos y la desinformación se identifican como áreas en las que los esfuerzos actuales para mitigar riesgos están o "no iniciados" o en un "desarrollo temprano".

Hay que señalar, además, que las falsificaciones, la propaganda y la desinformación, según el proyecto CONCORDIA de la UE[29], están muy extendidas y su objetivo es siempre inducir a error a los usuarios, lo que impacta en la vida cotidiana de las personas y la sociedad, que se ven directamente afectadas por estas campañas.

Por otro lado, como hemos dicho, la lucha contra la desinformación también tiene lugar en ambiente militar.

Efectivamente, durante las operaciones, las Fuerzas Armadas recopilan, procesan, analizan y utilizan datos e información para comprender situaciones, tomar decisiones y emitir órdenes que desembocan en acciones, negando a las amenazas el acceso a datos e información amiga,

[27] Resolución del Parlamento Europeo, de 9 de marzo de 2022, sobre las injerencias extranjeras en todos los procesos democráticos de la Unión Europea, incluida la desinformación (2020/2268(INI)).

[28] Óscar Sánchez Muñoz. *La regulación de las campañas electorales en la era digital. Desinformación y microsegmentación en las redes sociales con fines electorales*. (Centro de Estudios Políticos y Constitucionales. Mº de la Presidencia, 2020).

[29] Servicio de Información Comunitario sobre Investigación y Desarrollo (CORDIS). (2018)

protegiendo las decisiones y defendiendo las redes para garantizar las comunicaciones y permitir el mando y control. Además, es misión de las FAS comunicar información para informar a las audiencias relevantes, corregir la desinformación y contrarrestar la desinformación de las amenazas, empleando la información en combinación con la acción física para influir en la toma de decisiones y el comportamiento de las amenazas[30].

La desinformación, entendida como un elemento o componente de las amenazas híbridas, se remonta a la Guerra Fría y experimentó un resurgimiento en Estados Unidos tras las elecciones de 2016, cuando, como hemo señalado previamente, se denunció que Rusia había interferido en el proceso electoral. El conflicto entre Rusia y Ucrania, en el que el foco de la ciberguerra pasó de los ciberataques a la desinformación, ha dejado claro el papel crucial que desempeña la desinformación en este tipo de conflictos armados.

Efectivamente, incluso antes de que comenzara la guerra "física", ya se estaba utilizando la desinformación como preludio de la invasión rusa de Ucrania. Antes de la invasión, se dirigieron contra Ucrania acciones masivas de desinformación, que se agravaron durante la misma[31]. A modo de ejemplo, Euronews presentó un informe de la Asociación Europea de Expertos sobre diversas acusaciones infundadas utilizadas como justificación de la acción militar de Rusia, como esa noticia que afirmaba que Ucrania estaba preparando un ataque en el Donbás, que fue evaluada recientemente de forma independiente por el Índice Global de Desinformación. Según la ucraniana Maria Avdeeva, fundadora y directora de investigación de la Asociación Europea de Expertos, la estrategia utilizada para combatir la desinformación en esta situación fue priorizar la cantidad sobre la calidad, en un esfuerzo por reducir la capacidad de las personas para distinguir las noticias falsas de las verdaderas.

Todas las partes involucradas en la guerra, de un modo u otro, emplearon la desinformación. La desinformación rusa se centró en las motivaciones de la invasión (como la *desnazificación* o la *liberación* de Ucrania)[32], la agresión ucraniana y la de la OTAN[33], o la provisión de armas biológicas por parte de los Estados Unidos[34]. La desinformación de Ucrania, por su parte, se enfocó en motivar a los soldados y en destacar las pérdidas militares rusas. También hubo otras naciones que contribuyeron a la difusión de desinformación. Por ejemplo, la relativa al uso de armas químicas en Ucrania o la ayuda militar de China[35].

Además de ello, la desinformación mediante IA basada en deepfakes desempeñó un papel importante en el origen del conflicto, generándose imágenes de Vladimir Putin y de Volodymyr Zelenskyy con mensajes que respaldaban los puntos de vista de los enemigos. A pesar de ser falsos, los vídeos se hicieron virales en Internet. Como respuesta, grandes empresas, como Meta, YouTube y Twitter anunciaron nuevas medidas de respuesta a las crecientes peticiones del gobierno ucraniano, de los líderes mundiales y de los propios ciudadanos.

Efectivamente, la desinformación generada por la IA desempeña un papel cada vez más importante en su producción y difusión, y tiene el potencial de proporcionar un flujo incesante de desinformación. Al saturar las agencias gubernamentales con comentarios falsos, el desarrollo de bots que imitan identidades puede perturbar fácilmente el modelo habitual de "noticia y comentario", así como la participación de la comunidad, haciendo que las plataformas de medios sociales impulsadas por IA estén en el centro de la problemática de la desinformación, facilitando que la tecnología de las falsificaciones profundas se desarrolle rápidamente, sabiendo que los deepfakes pueden crearse más fácilmente gracias a estas tecnologías y que no pueden contrarrestarse totalmente[36] [37].

Desde hace décadas, el contenido creado o difundido por los líderes políticos ha venido siendo

[30] USA. Department of the Army. *ADP 3-13 Information*. (Noviembre, 2023).

[31] Ian Smith. *The Disinformation War: The falsehoods about the Ukraine invasion and how to stop them spreading*. (Euronews, 2022).

[32] Zack Beauchamp. *Putin's "Nazi" rhetoric reveals his terrifying war aims in Ukraine*. (Vox-Times of Israel, 2022)./Robert Farley. *The Facts on 'De-Nazifying' Ukraine*. (FactCheck.org, 2022)

[33] Cain Burdeau. *Putin blames NATO for pushing Russia into invasion*. (Courthouse News Service, 2022).

[34] Kari Paul. *'Game of Whac-a-Mole': why Russian disinformation is still running amok on social media*. (The Guardian, 2022) / Justin Ling. *False Claims of U.S. Biowarfare Labs in Ukraine Grip QAnon*. (Foreign Policy, 2022) / Olga Robinson, Shayan Sardarizadeh, Jake Horton. *Ukraine war: Fact-checking Russia's biological weapons claims*. (BBC, 2022).

[35] Ken Dilanian, Courtney Kube, Carol Lee, Dan De Luce. *In a break with the past, U.S. is using intel to fight an info war with Russia, even when the intel isn't rock solid*. (NBC News, 2022) / Branco Marcetic. *The Biden Administration Fed the Press Dubious Intelligence About Russia*. (Jacobin, 2022).

[36] Chuck Brooks. *Alarming Cybersecurity Stats: What You Need To Know For 2021*. (Forbes, 2021)

[37] EUROPOL. *Serious And Organised Crime Threat Assessment*. (2021)

alterado o sacado de contexto, y la tendencia va en aumento. Los deepfakes, por su parte, elevan esta técnica a un nuevo nivel al proporcionar a los actores maliciosos herramientas fáciles de usar para crear contenidos falsos (audio, vídeo, imágenes y texto) que apenas pueden distinguirse de los auténticos. Gracias a la capacidad de la IA, los agentes hostiles -estatales o no- pueden desarrollar ataques a medida que combinen perfiles de usuarios e individuos con desinformación personalizada. Los deepfakes y el engaño basado en IA están haciendo que los medios, el periodismo y la información pierdan credibilidad. No cabe duda de que cuando una campaña de desinformación consigue suprimir la verdad más que difundir noticias falsas, está logrando los mejores resultados para los agentes de las amenazas[38].

Con el auge de la desinformación por encargo, estas campañas son cada vez más fáciles de gestionar y ejecutar. Cuando estos servicios se combinan con falsificaciones profundas, lo más probable es que aumente el escepticismo de la sociedad. La desinformación por encargo es un sector floreciente en el que se paga a agencias privadas de marketing, comunicación y relaciones públicas para crear conflictos mediante la difusión de información falsa y la manipulación de contenidos en línea. Según el *Centre for International Media Assessment (CIMA),* desde 2009 se han invertido, al menos, 60 millones de dólares en servicios de propaganda de este tipo[39].

Además de ello, diversos gobiernos están utilizando la IA para generar noticias, imágenes e incluso videos para manipular la opinión pública a su favor y/o censurar automáticamente contenido crítico en línea[40]. Correlativamente, pocos gobiernos poseen el conocimiento técnico y el marco regulatorio necesarios para crear normativas sólidas que guíen la introducción de las herramientas de IA. Si bien los gobiernos, desde Indonesia hasta los Emiratos Árabes Unidos, han comenzado a introducir marcos o estrategias de alto nivel con respecto a la IA en general, muchos aún no han convertido estas declaraciones en leyes. Los legisladores pueden referirse a los primeros modelos legislativos de China, la UE y los EE. UU. a medida que las ventajas y desventajas de la tecnología se vuelven más evidentes. Por ejemplo, China ha realizado importantes inversiones en el sector de la inteligencia artificial, al tiempo que se ha asegurado de que las empresas involucradas mantuvieran sus objetivos. La importante agencia reguladora de China, la Administración del Ciberespacio de China (CAC), ha estado trabajando durante años para incorporar los objetivos de censura del PCC (Partido Comunista de China) en las herramientas de inteligencia artificial generativa y los algoritmos de recomendación de contenido del país. En junio de 2023, por ejemplo, la CAC aprobó 41 proveedores de servicios de IA generativa y, en agosto del mismo año, cinco chatbots se pusieron a disposición del público en general, sabiendo que las solicitudes de este tipo deben defender o promover los "principios socialistas fundamentales" y omitir cualquier información que el Partido Comunista considere objetable[41].

Por último, no debemos olvidar que la desinformación constituye una de las principales bazas de los regímenes autoritarios para acallar, dividir o sembrar la confrontación entre movimientos reivindicativos de derechos y libertades.

4. Los principales agentes estatales generadores de amenazas híbridas

Es habitual que los informes de seguridad y estudios de inteligencia citen a determinados países como especialmente generadores de tácticas híbridas y desinformación a gran escala, entre ellos, Rusia, China, Irán y Corea del Norte.

Se repasan sumariamente sus acciones más destacadas.

4.1. Rusia

Rusia es frecuentemente referenciada como uno de los principales actores en el uso de amenazas híbridas y tácticas de desinformación. Los ejemplos que se citan incluyen la intervención en Crimea y el este de Ucrania, las campañas de desinformación en las redes sociales dirigidas a interferir en

[38] Joao Franca. *Wolf, wolf! Alarm over disinformation and the liar's dividend.* (CCCBLAB, 2022).

[39] Ann Lewandowski. *Disinformation-for-hire: the pollution of news ecosystems and erosion of public trust*. (Center for International Media Assistance, 2021)

[40] Tate Ryan-Mosley. *How generative AI is boosting the spread of disinformation and propaganda.* (MIT Technology Review, 2023).

[41] Allie Funk, Adrian Shahbaz, Kian Vesteinsson. *Freedom on the net 2023: The repressive power of artificial intelligence.* (Freedom House, 2023)

las elecciones de terceros países, y el patrocinio de piratas informáticos para realizar ciberataques.

Algunos ejemplos concretos de amenazas híbridas y campañas de desinformación dirigidas a la Unión Europea han sido las siguientes:

- Influencia en las Elecciones: las agencias de inteligencia europeas y norteamericanas han venido acusado a Rusia de interferir en las elecciones de varios países de la UE. Por ejemplo, durante las elecciones presidenciales de Francia en 2017, el candidato Emmanuel Macron fue blanco de ciberataques y desinformación, supuestamente vinculados a actores rusos.

- Propaganda y Desinformación: las plataformas de medios de comunicación respaldadas por el estado ruso, como RT y Sputnik, han sido acusadas de difundir información engañosa y de polarización en toda la UE, persiguiendo exacerbar las divisiones sociopolíticas y debilitar la confianza en las instituciones de la UE.

- Ciberataques: Rusia ha sido acusada de una serie de ciberataques de alto perfil contra objetivos de la UE. Por ejemplo, en 2015, el Bundestag alemán fue objeto de un ciberataque que se atribuyó a un grupo de hackers rusos conocido como APT28/Fancy Bear[42].

Consciente de esta problemática, el 8 de febrero de 2024, el Parlamento Europeo publicó su Resolución sobre el *Rusiagate*: acusaciones de injerencia rusa en los procesos democráticos de la Unión Europea[43].

Esta Resolución, muy significativa por su contenido, poniendo de manifiesto que la injerencia extranjera, la manipulación informativa y la desinformación constituyen una grave violación de los valores y principios universales en los que se basa la Unión, como la dignidad humana, la libertad, la igualdad, la solidaridad, el respeto de los derechos humanos y las libertades fundamentales, la democracia y el Estado de Derecho, y considerando que la confianza en la integridad del Parlamento y en el Estado de Derecho es primordial para el funcionamiento de la democracia europea, señala explícitamente que existen pruebas de la injerencia y manipulación rusas en muchas democracias, así como de su apoyo práctico a fuerzas extremistas y entidades de mentalidad radical para promover la desestabilización de la Unión.

La Resolución señala igualmente la significativa variedad de tácticas de guerra híbrida que viene utilizando Rusia para lograr sus objetivos, aplicadas como parte de una estrategia más amplia para socavar el buen funcionamiento de los procesos democráticos europeos; recordando que el uso de la injerencia extranjera y la manipulación de la información, como medio para dividir a las sociedades democráticas, fue el precursor de la guerra de agresión no provocada de Rusia contra Ucrania, afirmando que la difusión de desinformación por parte de Rusia a través de los medios de comunicación tradicionales y las plataformas de medios sociales, la captura de élites, su piratería de candidatos electorales y los ciberataques han aumentado a un nivel sin precedentes.

La Resolución, tras exponer los motivos que la inspiran, finaliza con 27 expresiones y decisiones, entre las que destacamos las siguientes:

- Expresa la total indignación del Parlamento Europeo y su grave preocupación por los continuos esfuerzos de Rusia por socavar la democracia europea;

- Condena inequívocamente los actuales esfuerzos rusos por abusar y falsificar el recuerdo histórico de los periodos más trágicos de Europa, incluidas las consecuencias del Pacto Molotov-Ribbentrop y el terror que siguió para los territorios conquistados por la Alemania nazi y la Rusia comunista, para tratar de justificar su actual agresión brutal, ilegal e inhumana y su política expansionista;

- Expresa su profunda preocupación por las informaciones según las cuales la diputada al Parlamento Europeo Tatjana Ždanoka podría haber actuado como informante para el Quinto

[42] APT28, también conocido como *Fancy Bear,* es un grupo de amenazas persistentes avanzadas (APT) que se cree que tiene vínculos con el gobierno ruso, específicamente con la GRU, la agencia de inteligencia militar de Rusia. Este grupo ha estado activo desde al menos 2008 y ha sido vinculado con una serie de ciberataques de alto perfil. APT28 se especializa en operaciones de ciberespionaje dirigidas principalmente contra objetivos gubernamentales y militares, así como contra organizaciones internacionales, medios de comunicación y activistas políticos, especialmente aquellos situados o centrados en países de la OTAN, el Cáucaso, Europa Central y Europa del Este.

[43] *Rusiagate*: acusaciones de injerencia rusa en los procesos democráticos de la Unión Europea. Resolución del Parlamento Europeo, de 8 de febrero de 2024, sobre el Rusiagate: acusaciones de injerencia rusa en los procesos democráticos de la Unión Europea (2024/2548(RSP)).

Servicio del FSB mientras ejercía también como diputada al Parlamento Europeo;

- Señala otros casos de diputados al Parlamento Europeo que sirven deliberadamente a los intereses de Rusia;

- Expresa su especial preocupación por las recientes informaciones según las cuales las autoridades rusas están proporcionando narrativas específicas a partidos y actores políticos de extrema derecha en distintos países de la UE, sobre todo en Alemania y Francia, con el objetivo de subvertir el apoyo público a Ucrania;

- Reitera su indignación por las revelaciones periódicas de financiación rusa a gran escala de partidos políticos, políticos, funcionarios y movimientos en varios países democráticos en un intento de interferir y ganar influencia en sus procesos internos;

- Condena enérgicamente el reciente incidente ocurrido en Eslovaquia, en el que el Servicio Ruso de Inteligencia Exterior, en una maniobra de provocación, hizo pública una declaración durante el periodo preelectoral moratoria que cuestiona la integridad del proceso electoral de la República Eslovaca;

- Condena enérgicamente la campaña de desinformación a gran escala destapada por el Ministerio de Asuntos Exteriores alemán, supuestamente orquestada por Rusia en la plataforma X, con la intención de manipular la opinión pública en Alemania;

- Observa con preocupación que X ha dejado de seguir el Código Voluntario de Buenas Prácticas sobre Desinformación, y la consiguiente desinformación generalizada y los contenidos ilegales en la plataforma;

- Pide a la Secretaría del Registro de Transparencia de la UE que prohíba toda entidad que mantenga relaciones directas o indirectas con el Gobierno de Rusia, de conformidad con la Decisión del Consejo de 3 de junio de 2022 relativa a la adopción de medidas restrictivas;

De entre todas ellas, por su importancia para nuestro país, reproducimos la número 11, que dice:

> *Expresa su extrema preocupación por las supuestas relaciones entre los secesionistas catalanes y la administración rusa; señala que la injerencia rusa en Cataluña, de confirmarse, formaría parte de una estrategia rusa más amplia para promover la desestabilización interna y la desunión de la UE; expresa su profunda preocupación por las campañas de desinformación a gran escala que Rusia ha llevado a cabo en Cataluña, así como por los supuestos contactos intensos y el número de reuniones entre los agentes responsables de la injerencia rusa con el movimiento independentista y el Gobierno regional de la Comunidad Autónoma de Cataluña; pide a las autoridades judiciales competentes que investiguen efectivamente las conexiones de los diputados al Parlamento Europeo supuestamente asociados con el Kremlin y los intentos de desestabilización e injerencia de Rusia en la UE y sus Estados miembros; deplora todos los ataques contra los jueces que investigan cualquier actividad de injerencia; pide que los casos de los diputados catalanes afectados se remitan al Comité Consultivo sobre la Conducta de los Diputados;*

4.2. China

China también ha sido acusada de utilizar tácticas híbridas, particularmente en el ámbito de la guerra cibernética y la influencia económica. Además, ha habido acusaciones de campañas de desinformación, especialmente en relación con la disputa territorial en el Mar de China Meridional y la situación en Hong Kong y Xinjiang.

Algunos ejemplos concretos de amenazas híbridas y campañas de desinformación dirigidas a la Unión Europea han sido las siguientes:

- Influencia Económica y Política: China ha sido acusada de utilizar su influencia económica para coaccionar a los países de la UE, tratando de dividir su unidad. Un ejemplo de esto es el "17+1", un formato de diálogo iniciado por China con 17 países de Europa Central y Oriental, que algunos ven como un intento de dividir la UE[44].

[44] El así llamado "17+1" es un formato de cooperación iniciado por China que involucra a diecisiete países de Europa Central y Oriental (ECE), incluyendo once países de la Unión Europea (Bulgaria, Croacia, República Checa, Estonia, Hungría, Letonia, Lituania, Polonia, Rumania, Eslovaquia, Eslovenia) y cinco países de los Balcanes (Albania, Bosnia y Herzegovina, Macedonia

- Ciberespionaje: China ha sido acusada de realizar acciones de ciberespionaje contra empresas y gobiernos de la UE. Por ejemplo, el grupo APT10, pretendidamente vinculado al gobierno chino, ha sido acusado de llevar a cabo una serie de ciberataques contra entidades en Europa[45].

- Desinformación sobre el COVID-19: durante la pandemia de COVID-19 se ha acusado a China de llevar a cabo campañas de desinformación en la UE, incluyendo la difusión de teorías de la conspiración y la exageración de la ayuda proporcionada por China a los países de la UE.

4.3. Irán

Irán ha sido acusado de utilizar tácticas híbridas, incluyendo la utilización de milicias proxy en conflictos regionales, la realización de ciberataques, y la ejecución de campañas de desinformación.

En el caso iraní, la dimensión híbrida se manifiesta en la combinación de influencia regional, apoyo a actores proxy, operaciones de información y actividad cibernética. Su estrategia no se limita al empleo de milicias aliadas, sino que integra presión diplomática, narrativas de legitimación regional, campañas de propaganda, espionaje digital y acciones de represalia en el ciberespacio. Este modelo permite a Teherán proyectar poder más allá de sus capacidades convencionales y mantener un margen de negación plausible respecto de determinados incidentes, especialmente cuando actúan grupos interpuestos o infraestructuras técnicas no directamente atribuibles al Estado.

4.4. Corea del Norte

Conocida por su aislamiento y secretismo, Corea del Norte ha sido acusada de utilizar tácticas híbridas, incluyendo ciberataques a gran escala, como el famoso ataque a Sony Pictures en 2014[46].

Corea del Norte representa un perfil distinto. Su uso de tácticas híbridas se concentra de forma especial en el ciberespacio, donde combina espionaje, obtención ilícita de recursos económicos, sabotaje y operaciones de presión política. Los ciberataques atribuidos a grupos vinculados al régimen muestran cómo un Estado con limitadas capacidades económicas puede obtener efectos estratégicos relevantes mediante herramientas digitales relativamente baratas, escalables y difíciles de atribuir. La dimensión híbrida aparece, precisamente, en la conexión entre cibercriminalidad, financiación del régimen, coerción internacional y propaganda interna.

Como hemos dicho, estos cuatro países son frecuentemente señalados en los informes de inteligencia y estudios de seguridad por su uso de tácticas híbridas, pero es importante tener en cuenta que estas tácticas pueden ser empleadas por cualquier actor, estatal o no estatal, y que las acusaciones específicas deben basarse en evidencias sólidas, recordando en cualquier caso que las tácticas híbridas y de desinformación son a menudo difíciles de atribuir con certeza debido a su naturaleza encubierta.

del Norte, Montenegro, Serbia). La iniciativa, también conocida como la Cooperación China-Europa Central y Oriental (CEEC), fue lanzada en 2012 y tiene como objetivo promover la inversión y la cooperación entre China y los países de la región ECE en una variedad de áreas, incluyendo comercio, inversión, infraestructuras, finanzas, cultura y educación. "17+1" es parte de la iniciativa más amplia de la Franja y la Ruta (también conocida como la Nueva Ruta de la Seda) de China, que busca conectar a China con Europa, África y otras partes de Asia a través de una red de infraestructuras de comercio y transporte. Ha habido críticas y preocupaciones respecto al "17+1", incluyendo la percepción de que puede ser un intento de China de dividir a Europa y debilitar la unidad de la UE. Algunos países participantes también han expresado insatisfacción con la falta de inversiones concretas de China, lo que ha llevado a algunos a cuestionar el valor de la iniciativa.

[45] APT10, también conocido como Menupass, es un grupo de amenazas persistentes avanzadas (APT) que se cree que opera desde China. Este grupo ha estado activo desde al menos 2009 y ha lanzado una serie de campañas de ciberespionaje altamente sofisticadas y a gran escala contra organizaciones en todo el mundo. Los objetivos de APT10 han sido amplios y variados, y han incluido organizaciones en sectores como la defensa, las finanzas, la salud, las telecomunicaciones, la aeroespacial, y la manufactura, entre otros. Las víctimas han sido principalmente ubicadas en países como Estados Unidos, Japón, Canadá y varios países europeos. Las técnicas de APT10 son variadas, pero a menudo implican el uso de spear phishing (correo electrónico de phishing dirigido) y malware personalizado para ganar acceso a las redes de las organizaciones objetivo. Una vez dentro, el grupo busca exfiltrar datos valiosos, que pueden incluir información comercial sensible, datos personales, y secretos de estado. Algunas campañas notables atribuidas a APT10 incluyen Operation Cloud Hopper, una operación de ciberespionaje a gran escala dirigida a proveedores de servicios gestionados (MSP) con el fin de acceder a las redes de sus clientes, y Operation Red Apollo, que se centró en organizaciones japonesas y globales en varias industrias.

[46] El ciberataque a Sony Pictures Entertainment en 2014 fue uno de los ciberataques más notorios de la década. Los atacantes, que se identificaron a sí mismos como el "Guardians of Peace" (GOP), filtraron información confidencial de Sony, incluyendo datos personales de empleados y exempleados, correos electrónicos internos, copias de películas inéditas y otros materiales sensibles.

5. Consecuencias jurídico-regulatorias de las amenazas híbridas

Desde la perspectiva de una revista centrada en privacidad, innovación y tecnología, las amenazas híbridas plantean cuatro problemas jurídicos especialmente relevantes. El primero es la atribución: las operaciones se diseñan para ocultar la autoría mediante proxies, infraestructura distribuida, cuentas coordinadas o empresas privadas de influencia, lo que dificulta la imputación estatal y la activación de contramedidas. El segundo es la proporcionalidad de la respuesta: la protección de la seguridad democrática no puede justificar medidas indiscriminadas de vigilancia, bloqueo o retirada de contenidos que afecten de forma desproporcionada a la libertad de expresión, al pluralismo informativo o a la protección de datos personales.

El tercer problema se refiere a la responsabilidad de las plataformas digitales. Las campañas híbridas se aprovechan de arquitecturas de recomendación, publicidad segmentada, automatización de cuentas y opacidad algorítmica. Por ello, instrumentos como el Reglamento de Servicios Digitales de la Unión Europea, el Código de Buenas Prácticas en materia de Desinformación, el Reglamento de Inteligencia Artificial y la normativa de protección de datos deben interpretarse de forma coordinada, no como compartimentos estancos. El objetivo no es convertir a las plataformas en árbitros generales de la verdad, sino exigir diligencia reforzada frente a riesgos sistémicos, manipulación coordinada e interferencia extranjera.

El cuarto problema es la protección de derechos fundamentales. La respuesta frente a amenazas híbridas debe preservar el núcleo de los derechos que los actores hostiles intentan erosionar: libertad de expresión e información, privacidad, protección de datos, participación política y acceso a información plural. De ahí que las políticas públicas deban combinar prevención, transparencia, alfabetización mediática, cooperación institucional, trazabilidad de campañas y control judicial o independiente de las medidas restrictivas. La seguridad democrática solo es jurídicamente sostenible si se articula como defensa del Estado de Derecho, no como excepción permanente a sus garantías.

6. Conclusiones

El análisis desarrollado a lo largo de este trabajo permite afirmar que las amenazas híbridas constituyen hoy uno de los principales vectores de inestabilidad política, social y jurídica a escala global. Su carácter multidimensional, su capacidad de adaptación y su bajo umbral de atribución las convierten en instrumentos especialmente eficaces para erosionar la cohesión social, debilitar las instituciones democráticas y condicionar los procesos de toma de decisiones sin recurrir necesariamente al uso directo de la fuerza militar.

La conclusión principal no es simplemente que las amenazas híbridas sean relevantes, sino que su tratamiento exige desplazar el análisis desde la mera enumeración de medios hacia la identificación de funciones estratégicas, agentes, vulnerabilidades explotadas y consecuencias jurídico-regulatorias. Esa es la aportación central del artículo.

Como se ha puesto de manifiesto, estas amenazas no se limitan a acciones aisladas, sino que responden a estrategias complejas que combinan de forma coordinada elementos militares, económicos, informativos, tecnológicos y normativos. En este contexto, la desinformación emerge como uno de los instrumentos más eficaces, al permitir la manipulación de percepciones, la polarización social y la degradación del debate público, afectando directamente a la confianza en las instituciones democráticas y al funcionamiento del Estado de Derecho.

El estudio evidencia, asimismo, que los marcos jurídicos nacionales e internacionales presentan importantes limitaciones para hacer frente a este tipo de amenazas. La dificultad de atribuir responsabilidades, la explotación de vacíos normativos y la tensión permanente entre seguridad y derechos fundamentales dificultan la adopción de respuestas eficaces. En particular, la protección de la libertad de expresión y de información, pilares esenciales de las sociedades democráticas, puede ser instrumentalizada por actores hostiles para legitimar campañas de manipulación y desinformación.

En este escenario, resulta imprescindible avanzar hacia un enfoque integral que combine herramientas jurídicas, tecnológicas, institucionales y sociales. La respuesta frente a las amenazas híbridas no puede limitarse al ámbito de la seguridad o la defensa, sino que debe incorporar políticas de prevención, educación mediática, cooperación público-privada y fortalecimiento de la resiliencia social. Del mismo modo, es necesario reforzar los mecanismos de cooperación internacional y, en particular, el papel de la Unión Europea como actor normativo y estratégico frente a este tipo de riesgos.

En definitiva, las amenazas híbridas constituyen un fenómeno estructural del entorno geopolítico contemporáneo. Afrontarlas eficazmente exige una comprensión profunda de su naturaleza, una adaptación continua de los marcos jurídicos y una firme defensa de los valores democráticos. Solo mediante una respuesta coordinada, proporcional y respetuosa con el Estado de Derecho será posible preservar la estabilidad institucional y la confianza ciudadana frente a unas amenazas cada vez más sofisticadas y persistentes.

De forma más concreta, el análisis permite sostener cinco resultados:

- La categoría de amenaza híbrida solo resulta útil si se vincula a coordinación, intencionalidad estratégica, explotación de vulnerabilidades y dificultad de atribución.
- Los agentes no se reducen a Estados: incluyen proxies, empresas de influencia, grupos criminales y redes coordinadas que operan en zonas grises.
- La dimensión económica debe distinguir entre presión económica tradicional y coerción económica híbrida integrada en operaciones de influencia.
- La desinformación y la IA generativa no son un añadido tecnológico, sino un acelerador de escala, personalización y plausibilidad del engaño.
- La respuesta jurídica debe articularse desde la proporcionalidad, la trazabilidad, la responsabilidad de plataformas y la protección de derechos fundamentales.

Bibliografía

Abella Osorio, J. D., y V. Torrijos R. "Los riesgos de la desinformación para las democracias: un modelo de análisis." *Cuadernos de la Guardia Civil: Revista de Seguridad Pública* 69 (2023): 7–29.

Aguado, J. M., Á. Gómez de Ágreda, e I. Caravaca. "El ecosistema de la desinformación: actores, estrategias y redes de valor." En *Desinformación y Defensa*. Madrid: Dykinson, 2024.

Alegría Continente, P. "Desinformación y democracia." *Temas para el Debate* 356–357 (2024): 15–18.

Arteaga Martín, F. "La desinformación y las grandes plataformas." *Análisis del Real Instituto Elcano* 23 (2020).

Ballesteros Martín, M. A. "La lucha contra las campañas de desinformación en el ámbito de la Seguridad Nacional." *Cuadernos de Periodistas* 45 (2022): 79–81.

Beauchamp, Zack. "Putin's 'Nazi' Rhetoric Reveals His Terrifying War Aims in Ukraine." *Vox*, 2022.

Brooks, Chad. "Alarming Cybersecurity Stats: What You Need to Know for 2021." *Forbes*, 2021.

Burdeau, Cain. "Putin Blames NATO for Pushing Russia into Invasion." *Courthouse News Service*, 2022.

Campos-Domínguez, Eva, Marc Esteve del Valle, y Carmen Renedo Farpón. "Retóricas de desinformación parlamentaria en Twitter." *Comunicar* 72 (2022): 47–58.

Congosto Martínez, María Luz, y Javier Barriuso Bernad. "Activismo, desinformación y campañas en redes. Estudio de Twitter, Telegram y TikTok." En *Democracia y Desinformación: Nuevas Formas de Polarización, Discursos de Odio y Campañas en Redes*. Madrid: Dykinson, 2024.

Crespo Carchi, G., y D. Villalva. "Libertad de expresión frente a la regulación en la difusión de contenidos en internet." *593 Digital Publisher CEIT* 9, no. 5 (2024): 339–352.

DiResta, Renée. "The Supply of Disinformation Will Soon Be Infinite." *The Atlantic*, 2020.

Evangelista Pintado, J. M. "La Unión Europea y la desinformación." *Revista General de Marina* 281 (2021): 543–562.

Galán Cordero, Carlos. "Countering Foreign Information Manipulation and Interference in Africa." Center for the Governance of Change, IE University–NATO, 2025.

———. "Las campañas de desinformación y la responsabilidad de las redes y plataformas de comunicación: el caso de Telegram." Real Instituto Elcano, 2021.

Greenberg, Andy. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York: Doubleday, 2020.

Harding, Luke. *Collusion: Secret Meetings, Dirty Money, and How Russia Helped Donald Trump Win*. New York: Vintage, 2017.

Helmus, Todd C., y William Marcellino. "Lies, Misinformation Play Key Role in Israel-Hamas Fight." RAND Corporation, 2023.

Herasimenka, Aliaksandr, Jonathan Bright, Ariadna Knuutila, y Philip N. Howard. "Misinformation and Professional News on Largely Unmoderated Platforms: The Case of Telegram." *Journal of Information Technology & Politics* (2022).

Hernández Escayola, P. "WhatsApp y la desinformación que pasa desapercibida." *AdComunica* 23 (2022): 335–337.

Hidalgo Cobo, P., O. Serrano Villalobos, y B. Puebla Martínez. "Desinformación en la guerra de Ucrania: análisis de las agencias de verificación españolas en TikTok." *Doxa Comunicación* 40 (2025): 19–41.

Lewandowski, Adam. *Disinformation-for-Hire: The Pollution of News Ecosystems and Erosion of Public Trust*. Washington, DC: Center for International Media Assistance, 2021.

Ling, Justin. "False Claims of U.S. Biowarfare Labs in Ukraine Grip QAnon." *Foreign Policy*, 2022.

Llorens, M. P. *Los desafíos del uso de la fuerza en el ciberespacio*. Barcelona: Elsevier, 2017.

López Martín, A., y A. Córdoba Cabús. "Desinformación sobre la guerra de Israel-Hamás: análisis de las fake news identificadas por las plataformas de verificación españolas." *Estudios sobre el Mensaje Periodístico* 30, no. 2 (2024): 311–322.

Magallón Rosa, Raúl. "Desinformación y elecciones. La (des)confianza en el sistema." En *Desinformación y Defensa*. Madrid: Dykinson, 2024.

Marcetic, Branko. "The Biden Administration Fed the Press Dubious Intelligence About Russia." *Jacobin*, 2022.

Romaniuk, Anastasiia. "Freedom of Speech in Russian Hands: How Russia Uses Telegram for Informational Occupation." OPORA, 2023.

Ryan-Mosley, Tate. "How Generative AI Is Boosting the Spread of Disinformation and Propaganda." *MIT Technology Review*, 2023.

Sánchez Muñoz, Óscar. *La regulación de las campañas electorales en la era digital: desinformación y microsegmentación en las redes sociales con fines electorales*. Madrid: Centro de Estudios Políticos y Constitucionales, 2020.

Sixma van Heemstra Fernández, A. "La desinformación como amenaza para la democracia: el caso del Brexit." *Boletín IEEE* 30 (2023): 835–848.

Slocum, J. "Inmigración y campaña electoral en Estados Unidos: desinformación y promesas de deportaciones masivas." *Notes Internacionals CIDOB* 311 (2024): 1–7.