DEFENSA DE LA MENTE: ESPAÑA Y EL DESAFÍO DE LA GUERRA COGNITIVA

Defensa de la Mente: España y el Desafío de la Guerra Cognitiva

Resumen

La **guerra cognitiva** se ha consolidado en la práctica como un ámbito operativo mayor: no sólo compite por información sino por decisiones, voluntades y percepciones. El esfuerzo combina operaciones informativas, ciberoperaciones, IA generativa, técnicas de influencia psicológica y, emergentemente, el vector biológico/neurotecnológico. En el caso de España, se han dado pasos institucionales (legislación orgánica, inversiones en cibercapacidad, iniciativas en neurotecnología y marcos de resiliencia social) que muestran una respuesta **dual**:

a) desarrollar capacidades tecnológicas defensivas/ofensivas en el ciber-y-cognitivo
b) proteger derechos individuales y fortalecer la inmunidad social.

A continuación se presenta un análisis detallado, con evaluación crítica de las principales afirmaciones del documento aportado por usted y referencias a fuentes oficiales y académicas consultadas.

Palabras clave: guerra cognitiva; dominio cognitivo; seguridad nacional; amenazas híbridas; desinformación; inteligencia artificial generativa; ciberseguridad; resiliencia social; soberanía cognitiva; operaciones de influencia; conflicto multidominio; neurotecnología; comunicación estratégica; polarización social; geopolítica de la información.

1. ¿QUÉ ES LA GUERRA COGNITIVA?

1.1. Marco doctrinal y operacional

La **guerra cognitiva** se configura como una evolución de las operaciones de información y de influencia psicológica tradicionales hacia un **modelo sistémico orientado a la modificación deliberada de percepciones, marcos interpretativos y procesos de toma de decisión** en individuos, grupos y sociedades. A diferencia de los dominios operacionales clásicos —tierra, mar, aire, espacio y ciber—, el dominio cognitivo se sitúa en el **entorno neuropsicológico humano**, donde la información no solo se transmite sino que **se internaliza, se interpreta y se transforma en comportamiento político, social o estratégico**.

El concepto ha sido desarrollado y difundido en los últimos años por la estructura de transformación de la OTAN, particularmente por **NATO Allied Command Transformation**, que lo describe como un entorno donde **"la mente humana se convierte simultáneamente en objetivo y en vector operativo"**. En este marco, la guerra cognitiva busca **alcanzar superioridad cognitiva**, entendida como la capacidad de **influir, degradar o dirigir los procesos de percepción y decisión de un adversario o de una población objetivo** mediante una combinación sincronizada de herramientas informativas, tecnológicas, psicológicas y, en su fase emergente, neurocientíficas.

En términos doctrinales, la guerra cognitiva se inserta dentro del paradigma de **operaciones multidominio (MDO)** impulsado por la **OTAN**, donde la interacción entre los dominios físico, virtual y humano se concibe como un sistema integrado. El dominio cognitivo representa la **capa superior de este sistema**, ya que es en él donde finalmente se materializan los efectos estratégicos: decisiones políticas, legitimidad institucional, cohesión social o voluntad de combate.

Desde una perspectiva operacional, la guerra cognitiva no se limita a la manipulación de información. Su objetivo es **alterar la arquitectura cognitiva que estructura la interpretación de la realidad**, lo que implica intervenir en tres

niveles interrelacionados: el **nivel narrativo-social**, el **nivel psicológico individual** y el **nivel biológico-neurotecnológico emergente**.

1.2. Caracterización operacional del dominio cognitivo

A continuación se presenta una **síntesis analítica de los niveles operacionales** identificados en la literatura doctrinal y académica.

Nivel operativo	Descripción	Herramientas principales	Objetivo estratégico
Nivel social / narrativo	Intervención sobre el ecosistema informativo colectivo y los marcos narrativos que estructuran la opinión pública.	Desinformación, propaganda digital, manipulación algorítmica, amplificación de polarización emocional, bots y redes coordinadas.	Erosionar legitimidad institucional, fragmentar cohesión social, alterar percepciones de realidad política.
Nivel psicológico individual	Explotación sistemática de sesgos cognitivos y vulnerabilidades psicológicas mediante contenidos personalizados.	Microsegmentación de audiencias, IA generativa, análisis de datos masivos, psicometría conductual.	Influir en percepciones individuales y modificar patrones de decisión política o social.
Nivel biológico / neurotecnológico	Investigación sobre la interacción directa con procesos neurocognitivos o fisiológicos.	Interfaces cerebro-máquina, neuroestimulación, tecnologías de monitoreo cognitivo.	Comprensión avanzada del comportamiento humano y potencial manipulación directa de procesos cognitivos (fase emergente).

Estos niveles no operan de forma aislada; constituyen un **sistema escalonado de influencia**. Las campañas cognitivas contemporáneas combinan:

- **Infraestructura tecnológica** (IA, big data, redes sociales).
- **Modelos psicológicos del comportamiento humano**.
- **Estrategias narrativas adaptativas** capaces de evolucionar en tiempo real.

El resultado es un **entorno operativo híbrido** donde la frontera entre conflicto militar, competencia geopolítica e influencia sociopolítica se difumina progresivamente.

1.3. Arquitectura funcional de una operación cognitiva

La lógica operacional de una campaña de guerra cognitiva puede representarse en cinco fases secuenciales:

Fase	Función	Actividades típicas
1. Observación cognitiva	Obtención de datos sobre percepciones sociales y vulnerabilidades cognitivas.	Análisis de redes sociales, minería de datos, análisis semántico de narrativas.
2. Modelado de audiencia	Construcción de perfiles psicográficos y segmentación poblacional.	Modelos de comportamiento, análisis de emociones colectivas, inteligencia cultural.
3. Diseño narrativo	Creación de narrativas capaces de explotar sesgos y tensiones sociales.	Ingeniería de mensajes, manipulación semántica, storytelling político.
4. Amplificación tecnológica	Difusión masiva o selectiva de contenidos a través de ecosistemas digitales.	Bots, algoritmos de recomendación, plataformas sociales.
5. Efecto cognitivo	Interiorización del mensaje y traducción en comportamiento social o político.	Cambio de percepción, polarización, pérdida de confianza institucional.

Este modelo permite comprender por qué la guerra cognitiva es considerada por muchos analistas como una **forma avanzada de guerra híbrida**: los efectos buscados no son necesariamente territoriales o militares, sino **estratégicos en el plano de la legitimidad política y la cohesión social**.

1.4. Diferencias con las operaciones de información tradicionales

Aunque la guerra cognitiva deriva de las **Information Operations (IO)** y las **Psychological Operations (PSYOPS)**, introduce elementos cualitativamente distintos.

Característica	Operaciones de información clásicas	Guerra cognitiva
Escala	Campañas informativas limitadas	Ecosistema de influencia permanente
Tecnología	Medios tradicionales y propaganda	IA, análisis de datos, automatización algorítmica
Objetivo	Persuasión o propaganda	Reconfiguración de percepciones y decisiones
Temporalidad	Episódica	Continua y adaptativa
Nivel de intervención	Comunicación	Cognición humana

La transición hacia este paradigma se ha visto acelerada por tres factores estructurales:

1. **Digitalización del espacio informativo global.**
2. **Proliferación de IA generativa y herramientas de manipulación multimedia.**
3. **Disponibilidad masiva de datos conductuales de población civil.**

1.5. Dimensión emergente: neurotecnología y biopolítica cognitiva

Uno de los aspectos más debatidos en la literatura estratégica es el posible desarrollo de **capacidades neurotecnológicas aplicadas al conflicto cognitivo**. Aunque estas tecnologías se encuentran aún en fase experimental, su potencial dual —médico y militar— plantea interrogantes significativos.

Entre las áreas de investigación más relevantes se encuentran:

- Interfaces cerebro-computador (BCI).
- Sistemas de estimulación neuronal no invasiva.
- Monitorización neurofisiológica en tiempo real.
- Modelos computacionales del comportamiento cognitivo.

El interés estratégico reside en que estas tecnologías podrían permitir en el futuro **comprender o incluso influir directamente en procesos cognitivos humanos**, ampliando significativamente el espectro de herramientas disponibles en el dominio cognitivo.

No obstante, la mayoría de expertos coincide en que **la aplicación militar directa sigue siendo limitada**, y que los debates actuales se centran más en **implicaciones éticas, regulatorias y de seguridad tecnológica**.

2. DOCTRINA OTAN

La doctrina de la OTAN (2025–2026) reconoce el dominio cognitivo como un "sexto dominio" del conflicto y sostiene que **"el cerebro es tanto el objetivo como el arma"**.

Las publicaciones y materiales de investigación asociados a **NATO Allied Command Transformation** desarrollan el concepto de "*cognitive warfare"* dentro de programas de innovación doctrinal impulsados por la **OTAN**. En estos documentos se describe el conflicto cognitivo como una forma de confrontación donde **la mente humana constituye el espacio operativo principal**.

La formulación citada —"the brain is the battlefield" o expresiones equivalentes— aparece en informes y documentos de divulgación estratégica asociados a iniciativas de innovación de ACT. Dichos textos analizan cómo **la convergencia entre neurociencia, inteligencia artificial y ecosistemas digitales puede convertir el entorno cognitivo en un espacio central de competencia estratégica**.

No obstante, es importante realizar una **distinción metodológica**:

Elemento doctrinal	Evidencia pública	Evaluación
Reconocimiento del dominio cognitivo como ámbito estratégico	Documentos de investigación y publicaciones estratégicas de ACT	Confirmado
Concepto de la mente como objetivo y vector del conflicto	Material conceptual y académico vinculado a ACT	Confirmado
Existencia de manual operativo completo sobre guerra cognitiva	No existe documentación pública detallada	No confirmado públicamente
Integración formal como "sexto dominio doctrinal" equiparable a ciber o espacio	Uso frecuente en análisis y debates estratégicos, pero no siempre formalizado doctrinalmente	Parcial

2.1. Evaluación analítica

1. **La OTAN utiliza el concepto principalmente en un marco analítico y de investigación**, no necesariamente como doctrina operativa completamente codificada.
2. Gran parte de los desarrollos técnicos y operacionales relacionados con el dominio cognitivo **permanecen clasificados o restringidos**, por lo que la literatura pública es principalmente conceptual.
3. La narrativa sobre el "sexto dominio" debe entenderse más como **una herramienta conceptual para describir la centralidad de la dimensión humana del conflicto**, que como una categorización doctrinal rígida.

2.2. Valor crítico

La conceptualización amplia del dominio cognitivo promovida en entornos estratégicos aliados presenta **ventajas analíticas claras**, entre ellas:

- Permite comprender la convergencia entre **información, tecnología y comportamiento humano**.
- Facilita el diseño de **estrategias de resiliencia social y defensa informativa**.
- Integra la dimensión humana en la planificación de operaciones multidominio.

Sin embargo, esta amplitud conceptual también genera **desafíos normativos y políticos**:

1. **Ambigüedad entre defensa cognitiva e intervención sobre la opinión pública.**
2. **Necesidad de salvaguardas jurídicas y democráticas** para evitar abusos en la gestión de información.

3. Riesgo de **militarización excesiva del espacio informativo civil**.

Por ello, cualquier estrategia nacional en este ámbito debe combinar **capacidad operativa y garantías institucionales**, diferenciando claramente entre:

- **Medidas legítimas de resiliencia democrática** (alfabetización mediática, verificación de información, transparencia institucional)
- **Intervenciones potencialmente invasivas** que requieren supervisión legal, control parlamentario y evaluación ética.

Guerra Cognitiva: el nuevo campo de batalla del pensamiento. Fuente: Adaptado de NATO Science and Technology Organization (STO), *Cognitive Warfare Research Activities*, 2025.

3. ESPAÑA FRENTE A LA GUERRA COGNITIVA: CAPACIDADES ESTRATÉGICAS, RESILIENCIA Y SOBERANÍA COGNITIVA

España ha comenzado a integrar el **dominio cognitivo** dentro de su arquitectura de seguridad nacional mediante una combinación de reformas institucionales, inversión tecnológica, capacidades operativas en ciberdefensa y programas científicos orientados a la protección del cerebro humano y la resiliencia social.

Este enfoque se articula en torno a tres ejes estratégicos:

1. **Transformación institucional y tecnológica de la defensa.**
2. **Desarrollo de soberanía científica en neurotecnología y gobernanza ética.**
3. **Refuerzo de la resiliencia social frente a operaciones de manipulación informativa.**

La base conceptual de este enfoque ya estaba presente en la **Estrategia de Seguridad Nacional 2021**, que identificó la **protección del espacio informativo y cognitivo** como parte de la seguridad nacional frente a amenazas híbridas.

3.1. Transformación legislativa e institucional: Real Decreto 150/2026

La modernización institucional más relevante en 2026 se materializa en el **Real Decreto 150/2026**, publicado en el **Boletín Oficial del Estado**, que reorganiza estructuras del **Ministerio de Defensa de España** con especial énfasis en capacidades tecnológicas y sistemas digitales de defensa.

El decreto introduce modificaciones significativas en dos áreas clave:

- la **Dirección General de Armamento y Material**,
- el **Centro de Sistemas y Tecnologías de la Información y las Comunicaciones**.

➢ **Nuevas estructuras organizativas**

Unidad	Función estratégica	Impacto en guerra cognitiva
Subdirección General de Gestión Económica de Programas	Gestión de programas de I+D militar de alto impacto tecnológico	Permite acelerar el desarrollo de sistemas avanzados (IA, ciberinteligencia, sensores digitales)
Subdirección General de Contratación TIC (CESTIC)	Gestión centralizada de contratación de sistemas digitales críticos	Mejora la coordinación tecnológica y la seguridad de infraestructuras informáticas

El objetivo de esta reorganización es **centralizar la gestión de tecnologías disruptivas** dentro del ecosistema de defensa, facilitando la integración de:

- Inteligencia artificial aplicada a seguridad,
- Plataformas de ciberdefensa,
- Sistemas de información militares resilientes.

➢ **Evaluación estratégica**

Dimensión	Impacto
Coordinación tecnológica	Alto
Integración civil-militar	Moderado
Velocidad de adquisición tecnológica	Alto

La reforma pretende preparar la estructura defensiva española para **amenazas híbridas y cognitivas**, donde la tecnología digital y la inteligencia de datos se convierten en herramientas fundamentales.

3.2. Dominio ciber: Mando Conjunto del Ciberespacio y sistema SCOMCE

El principal instrumento operativo de España en el dominio digital es el **Mando Conjunto del Ciberespacio** (MCCE), dependiente del **Estado Mayor de la Defensa**.

Esta estructura militar es responsable de **planificar, dirigir y ejecutar operaciones militares en el ciberespacio**, garantizando la libertad de acción de las Fuerzas Armadas en el dominio digital.

El mando ha estado dirigido por el vicealmirante **Francisco Javier Roca Rivero** según diversas referencias públicas.

➢ **Funciones operativas del MCCE**

Función	Descripción
Ciberdefensa militar	Protección de redes e infraestructuras de defensa
Ciberinteligencia	Detección de amenazas y operaciones hostiles
Operaciones ofensivas	Neutralización de capacidades digitales adversarias
Coordinación interinstitucional	Cooperación con agencias nacionales e internacionales

➢ **Sistema de Combate del Ciberespacio (SCOMCE)**

Dentro del ecosistema del MCCE se está desarrollando el **SCOMCE (Sistema de Combate del Ciberespacio)**, concebido como una **plataforma integrada de planificación y ejecución de ciberoperaciones**.

Diversas fuentes del sector defensa sitúan su inversión aproximada en **80 millones de euros**.

➢ **Arquitectura funcional prevista**

Componente	Función
Sensores digitales	Monitorización de redes y detección de intrusiones
IA analítica	Identificación de patrones de ataque
Plataforma C2	Planificación y coordinación de operaciones
Herramientas de respuesta	Neutralización de amenazas cibernéticas

El SCOMCE pretende desempeñar en el ciberespacio un papel equivalente al de **sistemas de armas convencionales en dominios físicos**, proporcionando una infraestructura integrada para **anticipar, detectar y responder a amenazas digitales y cognitivas**.

3.3. Doctrina Defensa 5.0 y el concepto de "combatiente cognitivo"

España ha comenzado a adoptar el paradigma **Defensa 5.0**, un enfoque que sitúa **la interacción humano-máquina en el centro de la transformación militar**.

Este modelo enfatiza la ampliación de capacidades cognitivas del combatiente mediante tecnologías avanzadas.

➢ **Tecnologías clave**

Tecnología	Aplicación
Gemelos digitales cognitivos	Simulación de comportamiento humano en sistemas militares
IA explicable (XAI)	Sistemas de apoyo a decisión transparentes y auditables
Interfaces humano-máquina	Asistencia digital en operaciones complejas

Un ejemplo ilustrativo es la simulación de plataformas como la **Fragata F110**, donde los gemelos digitales pueden integrar variables psicológicas para evaluar el rendimiento humano bajo estrés.

➢ **Objetivos del modelo Defensa 5.0**

Objetivo	Resultado esperado
Optimizar toma de decisiones	Operadores con mayor conciencia situacional
Reducir errores humanos	Entrenamiento basado en simulación cognitiva
Mantener control humano	IA explicable con supervisión humana

Este enfoque reconoce que **el elemento decisivo del combate sigue siendo el ser humano**, aunque amplificado por sistemas tecnológicos.

3.4. Resiliencia nacional e inmunidad social

España ha reconocido que la guerra cognitiva no se limita al ámbito militar: **la sociedad en su conjunto constituye el objetivo principal de operaciones de influencia**.

Por ello, la seguridad cognitiva se ha integrado con políticas sociales, educativas y sanitarias.

Un ejemplo es la **Estrategia de Salud Mental 2022-2026**, que aunque no fue diseñada específicamente para seguridad nacional, contribuye a reforzar la resiliencia psicológica de la población.

➢ **Grupos vulnerables identificados**

Grupo	Vulnerabilidad
Jóvenes	Exposición intensa a redes sociales
Personas mayores	Baja alfabetización digital
Comunidades aisladas	Mayor exposición a desinformación

El **Real Instituto Elcano** y otros centros de análisis han señalado que estos colectivos pueden convertirse en **objetivos preferentes de campañas de manipulación informativa**.

➢ **Programas de resiliencia social**

Iniciativa	Objetivo
Alfabetización mediática en escuelas	Reducir vulnerabilidad a desinformación
Programas comunitarios	Reducir aislamiento social
Monitorización FIMI	Detectar interferencia informativa extranjera

El concepto FIMI (*Foreign Information Manipulation and Interference*) se refiere a sistemas de alerta temprana destinados a **identificar operaciones de manipulación informativa realizadas por actores extranjeros**.

3.5. Evaluación estratégica de capacidades y vulnerabilidades de España

➢ **Capacidades principales**

Área	Fortalezas
Gobernanza institucional	Reforma organizativa y centralización tecnológica
Ciberdefensa	MCCE y desarrollo del sistema SCOMCE
Ética tecnológica	Enfoque regulatorio y respeto a derechos fundamentales

➢ **Vulnerabilidades estructurales**

Vulnerabilidad	Impacto estratégico
Dependencia tecnológica externa	Riesgo en IA y servicios cloud
Dificultad de atribución	Complejidad para identificar actores hostiles
Fragmentación civil-militar	Coordinación limitada entre sectores
Brecha digital	Segmentos sociales vulnerables

España ha iniciado un **proceso significativo de adaptación al nuevo entorno de conflicto cognitivo**, caracterizado por la creciente competencia en el ámbito de la información, la percepción y la influencia social. Este proceso refleja una **toma de**

conciencia institucional sobre la ampliación del concepto tradicional de seguridad nacional, incorporando dimensiones tecnológicas, cognitivas y sociales. En este contexto, se observa un **desarrollo paralelo en varios ámbitos estratégicos**:

- **Capacidad militar en ciberespacio**, mediante la consolidación de unidades especializadas, el fortalecimiento de estructuras de ciberdefensa y la incorporación del **dominio cognitivo dentro de las operaciones multidominio**. Este avance permite a España no solo **proteger infraestructuras críticas**, sino también **mejorar la capacidad de detección, prevención y respuesta frente a amenazas híbridas y campañas de desinformación**.

- **Infraestructura científica en neurotecnología**, impulsada a través de universidades, centros de investigación y programas de innovación tecnológica. Este desarrollo contribuye a **posicionar a España en un campo emergente estratégico**, donde convergen **inteligencia artificial, neurociencia y seguridad**, con implicaciones directas tanto en el ámbito civil como en el estratégico.

- **Políticas públicas de resiliencia social**, orientadas a **fortalecer la capacidad de la ciudadanía y de las instituciones frente a la manipulación informativa**, la polarización social y las operaciones de influencia externa. Estas políticas incluyen **alfabetización mediática, cooperación institucional y mejora de los mecanismos de comunicación estratégica**.

Sin embargo, la **consolidación de una verdadera soberanía cognitiva nacional** dependerá de **tres factores críticos**:

1. **Integración operativa entre instituciones civiles y militares.** El desarrollo actual muestra **avances sectoriales, pero aún persiste una fragmentación institucional** entre defensa, seguridad, investigación y política pública. La creación de **marcos de cooperación estables y estructuras interinstitucionales** permitiría una **respuesta más eficaz frente a amenazas cognitivas complejas y multidimensionales**.

2. **Reducción de dependencias tecnológicas externas en IA y plataformas digitales.** España mantiene una **alta dependencia de tecnologías y plataformas desarrolladas fuera de su ámbito estratégico**, especialmente en **inteligencia artificial, redes sociales y servicios digitales críticos**. Esta situación **limita la autonomía estratégica nacional** y **aumenta la vulnerabilidad frente a posibles presiones o interferencias externas**.

3. **Fortalecimiento de la inmunidad social frente a manipulación informativa.** La **resiliencia social constituye un elemento central del dominio cognitivo**. Una ciudadanía con **mayor capacidad crítica, acceso a información fiable y confianza institucional** reduce significativamente el impacto de **campañas de desinformación y operaciones de influencia**, reforzando **la estabilidad democrática y la cohesión social**.

En el contexto de la **competencia geopolítica contemporánea**, la **defensa del dominio cognitivo se perfila como uno de los pilares estratégicos de la seguridad nacional española**. La capacidad de **proteger el espacio informativo, garantizar la autonomía tecnológica y fortalecer la resiliencia social** será **determinante para preservar la soberanía, la estabilidad institucional y la capacidad de actuación estratégica de España** en el nuevo entorno internacional.

4. ESCENARIOS FUTUROS DE GUERRA COGNITIVA CONTRA ESPAÑA (2026–2035)

La evolución de la competencia estratégica internacional sugiere que el **dominio cognitivo se consolidará como uno de los principales espacios de confrontación geopolítica durante la próxima década**. Para España, el riesgo principal no radica en conflictos militares directos, sino en **operaciones híbridas dirigidas a erosionar la cohesión política, la confianza institucional y la estabilidad social**.

Los escenarios prospectivos que se presentan a continuación se basan en tendencias observadas en conflictos recientes, capacidades tecnológicas emergentes y patrones de actuación documentados en operaciones de influencia estratégica.

4.1. Escenario 1 — Interferencia cognitiva en procesos electorales

Los procesos electorales constituyen uno de los objetivos más sensibles dentro del ámbito de la guerra cognitiva, ya que permiten incidir directamente sobre la **legitimidad política**, la **confianza ciudadana** y la **orientación estratégica** de un Estado sin necesidad de recurrir a una acción militar convencional. En el caso de España, este tipo de interferencia podría materializarse mediante campañas coordinadas de desinformación, manipulación emocional y amplificación de narrativas divisivas dirigidas a erosionar la percepción de imparcialidad, transparencia y credibilidad del sistema democrático.

Este escenario no tendría como finalidad exclusiva alterar el resultado formal de unas elecciones, sino más bien **debilitar el entorno cognitivo en el que se desarrolla la competencia política**. El objetivo principal sería introducir dudas persistentes sobre la legitimidad del proceso, aumentar la fragmentación social y favorecer una percepción de inestabilidad institucional. En este sentido, la eficacia de la operación no dependería tanto de la veracidad de los contenidos difundidos

como de su capacidad para instalar incertidumbre, indignación o sospecha en segmentos concretos de la población.

La creciente disponibilidad de plataformas digitales, herramientas de automatización, sistemas de segmentación de audiencias y contenidos generados mediante inteligencia artificial amplía notablemente la viabilidad de este tipo de operaciones. La intervención ya no requeriría grandes recursos materiales ni una estructura visible, sino una combinación de **baja atribución, alta difusión y elevada capacidad de adaptación al debate público**.

- **Lógica operativa del ataque**

La arquitectura de una campaña de interferencia cognitiva electoral puede entenderse como un proceso progresivo, diseñado para actuar sobre distintas fases del ecosistema informativo y psicológico de la ciudadanía.

1. Reconocimiento

En una primera fase, los actores hostiles analizarían el entorno digital y social para identificar **fracturas ideológicas, tensiones territoriales, clivajes generacionales, desconfianza institucional y comunidades especialmente vulnerables a mensajes polarizantes**. Este trabajo de observación permitiría localizar los puntos de mayor sensibilidad emocional y los temas con mayor capacidad de viralización.

En esta etapa resultan especialmente relevantes los datos procedentes de redes sociales, foros, medios digitales y patrones de interacción pública. El objetivo no sería únicamente conocer el debate electoral, sino comprender **qué temas generan reacción, qué grupos son más receptivos y qué narrativas tienen mayor potencial de desestabilización**.

2. Segmentación

Una vez identificadas las vulnerabilidades, la campaña podría recurrir a técnicas de **microtargeting** para adaptar los mensajes a perfiles concretos de usuarios o

comunidades. La lógica sería maximizar el impacto emocional mediante contenidos diseñados para cada audiencia: mensajes de indignación para unos grupos, de victimización para otros, o de alarma ante supuestas irregularidades para colectivos ya desconfiados del sistema.

Esta fase incrementa la eficacia del ataque porque evita la difusión genérica y permite modular el discurso en función de la predisposición del receptor. En la práctica, esto convierte la interferencia en una operación altamente personalizada, más difícil de detectar y neutralizar.

3. Amplificación

La siguiente etapa consistiría en aumentar artificialmente la visibilidad de los mensajes mediante **bots, cuentas coordinadas, perfiles aparentemente orgánicos, influencers afines o canales de mensajería cerrada**. El objetivo es simular consenso, urgencia o volumen social para que una narrativa marginal parezca ampliamente compartida.

La amplificación no se limita a difundir contenido falso; también puede consistir en exagerar hechos reales, descontextualizar declaraciones, sacar de contexto datos electorales o presentar rumores como indicios de fraude. En esta fase, la velocidad de propagación es más importante que la precisión del mensaje.

4. Crisis de confianza

La fase final buscaría erosionar la credibilidad del proceso electoral mediante la difusión de supuestas irregularidades, denuncias de fraude o narrativas sobre manipulación institucional. Incluso en ausencia de pruebas, la repetición sostenida de estas ideas puede generar en parte del electorado la percepción de que el sistema no es fiable.

El efecto estratégico no sería necesariamente la deslegitimación total del resultado, sino la instalación de una **duda estructural**: que una parte significativa de la población considere que las elecciones no reflejan realmente la voluntad

popular. Esa percepción, una vez extendida, puede ser difícil de revertir y tiene efectos duraderos sobre la estabilidad democrática.

➢ **Arquitectura de ataque probable**

Fase	Método	Objetivo
Reconocimiento	Análisis de redes sociales, tendencias y perfiles electorales	Identificar fracturas sociales y temas sensibles
Segmentación	Microtargeting mediante datos de comportamiento	Dirigir mensajes a públicos vulnerables
Amplificación	Bots, cuentas coordinadas, influencers y contenido viral	Inflar artificialmente narrativas conflictivas
Crisis de confianza	Difusión de supuestas irregularidades y acusaciones de fraude	Deslegitimar el proceso electoral y sus resultados

➢ **Actores potenciales**

En este escenario podrían intervenir distintos tipos de actores, con motivaciones que no siempre serían idénticas, pero sí convergentes en su efecto desestabilizador.

1. **Estados competidores**

Pueden buscar debilitar la cohesión interna de España o de sus aliados, fomentar la división política y reducir la capacidad de respuesta colectiva frente a intereses externos. En este caso, la interferencia electoral se convertiría en una herramienta de presión geopolítica indirecta.

2. **Redes híbridas**

Incluyen estructuras no necesariamente estatales, sino mixtas o informales, capaces de operar en el espacio digital con fines de inestabilidad política,

influencia ideológica o desorden informativo. Su ventaja radica en la flexibilidad, la opacidad y la posibilidad de actuar desde múltiples jurisdicciones.

3. **Plataformas de desinformación**

Pueden responder a motivaciones económicas, ideológicas o de visibilidad, explotando la polarización como mecanismo de captación de audiencia y rentabilidad. Aunque no siempre actúen con una intención estratégica de alto nivel, sus dinámicas pueden ser funcionales a campañas más amplias de manipulación cognitiva.

Actor	Motivación estratégica
Estados competidores	Debilitar cohesión política e institucional
Redes híbridas	Generar inestabilidad y amplificar conflicto
Plataformas de desinformación	Influencia ideológica, económica o de audiencia

➢ **Impacto estratégico estimado**

El impacto de un escenario de este tipo no debe medirse únicamente en términos de voto o resultado electoral. Su verdadero alcance radica en la afectación de variables estructurales del sistema político y social.

1. **Confianza institucional: impacto alto**

La desconfianza en la limpieza del proceso electoral puede deteriorar la legitimidad de las instituciones representativas, afectar la aceptación de los resultados y dificultar la gobernabilidad posterior.

2. **Polarización social: impacto alto**

La campaña podría intensificar las dinámicas de confrontación entre bloques políticos y sociales, reforzando la lógica de antagonismo y reduciendo los espacios de consenso.

3. Estabilidad política: impacto moderado

Aunque no necesariamente produciría un colapso institucional, sí podría generar un clima de tensión prolongada, protestas, contestación de resultados y debilitamiento del debate público.

Dimensión	Impacto estimado
Confianza institucional	Alto
Polarización social	Alto
Estabilidad política	Moderado

➢ **Valoración analítica**

Este escenario es especialmente relevante porque combina tres factores de alta peligrosidad: **baja atribución, alta escalabilidad y fuerte impacto psicológico**. A diferencia de otras amenazas más visibles, la interferencia cognitiva electoral opera de manera gradual, aprovecha vulnerabilidades preexistentes y actúa sobre percepciones más que sobre estructuras físicas. Por ello, su detección temprana resulta compleja y su neutralización requiere capacidades que van más allá de la respuesta técnica: demanda coordinación institucional, comunicación estratégica, alfabetización mediática y una narrativa pública sólida.

Desde una perspectiva de seguridad nacional, este tipo de amenaza debe entenderse como una forma de agresión indirecta contra la soberanía democrática. El objetivo no es solo influir en un resultado concreto, sino **debilitar la confianza en el mecanismo mismo de representación política**. En consecuencia, la defensa frente a este escenario exige proteger tanto la integridad del proceso electoral como el ecosistema cognitivo que lo rodea.

➢ **Indicadores de alerta temprana**

Para completar el análisis, pueden considerarse como señales de alerta:

- aparición súbita de narrativas uniformes sobre fraude o manipulación;
- incremento artificial del tráfico sobre contenidos electorales polarizantes;
- coordinación temporal entre cuentas, canales y actores aparentemente inconexos;
- uso intensivo de contenidos sintéticos o generados por IA;
- ataques a la credibilidad de organismos electorales, medios o autoridades de supervisión;
- desplazamiento del debate desde propuestas políticas hacia sospechas de ilegitimidad.

➢ **Conclusión del escenario**

La interferencia cognitiva en procesos electorales representa una amenaza de primera magnitud para la democracia española, no tanto por su capacidad de alterar formalmente la votación, sino por su potencial para **erosionar la confianza pública, amplificar la polarización y deslegitimar las instituciones**. En un entorno digital cada vez más automatizado y emocionalizado, la protección del proceso electoral debe concebirse como una tarea integral de seguridad, comunicación y resiliencia democrática.

4.2 Escenario 2 — Crisis informativa durante conflictos internacionales

España mantiene una participación activa en **misiones internacionales bajo mandato de la OTAN** y de la **UE**, contribuyendo a operaciones de mantenimiento de la paz, estabilización regional y seguridad colectiva. Estas misiones son, sin embargo, **objetivos potenciales de campañas cognitivas** por parte de adversarios estratégicos, especialmente en contextos de escalada militar en Europa oriental o en el Mediterráneo.

En un escenario de tensión internacional, un actor hostil podría buscar **erosionar el apoyo interno español** a estas operaciones mediante la manipulación de información, amplificación de narrativas emocionales y difusión de contenidos audiovisuales diseñados para generar indignación o desconfianza. La estrategia no busca confrontar militarmente a España, sino **desestabilizar la percepción pública y política sobre la utilidad, legitimidad y ética de sus misiones internacionales**.

El objetivo principal de estas operaciones cognitivas sería **alterar la narrativa interna**, generar presión sobre los decisores políticos y debilitar la cohesión del Estado y de la opinión pública respecto a compromisos internacionales. La eficacia de la intervención se basa en el **uso de herramientas digitales avanzadas, automatización de contenidos y explotación de emociones colectivas**, combinando técnicas de desinformación, amplificación artificial y manipulación emocional.

➢ **Técnicas de influencia previstas**

La campaña de desestabilización podría estructurarse en torno a **tres líneas tácticas principales**, complementarias entre sí:

Técnica	Descripción	Objetivo operativo
Manipulación audiovisual	Uso de deepfakes, montaje de imágenes o videos sobre supuestos abusos militares o errores de tropas españolas	Provocar indignación y dudas sobre la ética de las operaciones
Narrativas emocionales	Amplificación de relatos sobre víctimas civiles, exageración de daños colaterales y difusión de testimonios sesgados	Activar emociones de miedo, culpa o indignación en la sociedad
Campañas pacifistas artificiales	Movilización digital coordinada a través de redes sociales, hashtags y perfiles automatizados	Generar sensación de consenso público contra las misiones y presionar decisiones políticas

Estas técnicas, utilizadas de manera combinada, permiten **afectar simultáneamente la percepción pública, la agenda mediática y el debate político**, generando un impacto más profundo que la difusión aislada de noticias falsas.

➢ **Efecto buscado**

El **resultado estratégico esperado** de una crisis informativa de este tipo puede desglosarse en tres niveles:

Objetivo	Resultado esperado	Impacto
Reducir apoyo público	Disminución de la aceptación social de la participación en misiones internacionales	Presión política para retirar tropas o limitar operaciones
Generar crisis parlamentaria	Amplificación de debates internos, cuestionamiento del consenso y polarización política	Fragmentación del consenso político y debilitamiento de la capacidad de decisión
Deslegitimar misiones internacionales	Percepción de falta de transparencia o eficacia de las operaciones	Reducción de la credibilidad estratégica de España ante aliados y adversarios

Estos efectos se retroalimentan: la **desconfianza social** alimenta la **presión política**, que a su vez puede **minar la credibilidad internacional**, creando un círculo de vulnerabilidad cognitiva difícil de revertir sin una respuesta coordinada y temprana.

➢ **Arquitectura de ataque probable**

El proceso de intervención cognitiva podría estructurarse en **cuatro fases secuenciales**:

1. **Reconocimiento y recopilación de información**

   Análisis de medios, redes sociales y opinión pública para identificar narrativas sensibles y puntos de vulnerabilidad sobre las misiones españolas.

2. **Producción de contenidos manipulativos**

   Creación de deepfakes, videos descontextualizados, testimonios sesgados y narrativas emocionales con alta capacidad de viralización.

3. **Amplificación digital**

   Difusión coordinada mediante bots, perfiles automatizados, influencers y redes temáticas, simulando consenso ciudadano y legitimando la narrativa hostil.

4. **Erosión de confianza y presión política**

   Exposición repetida de supuestos abusos, exageración de víctimas y movilización social artificial para **inducir cuestionamientos internos y debates parlamentarios** sobre la continuidad de las operaciones.

➢ **Actores potenciales**

Los responsables de este tipo de campaña podrían ser diversos, con motivaciones convergentes:

- **Estados competidores:** buscan debilitar la cohesión política de España y de sus aliados, disminuir el compromiso militar y crear un precedente de desconfianza hacia intervenciones internacionales.
- **Redes híbridas y no estatales:** aprovechan la situación para generar inestabilidad, visibilidad mediática o influencia ideológica sin exposición directa.
- **Medios y plataformas de desinformación:** pueden colaborar de forma activa o indirecta, motivados por intereses económicos o políticos, amplificando mensajes falsos o manipulados.

➢ Impacto estratégico estimado

El impacto de este escenario se manifiesta principalmente en tres dimensiones críticas:

Dimensión	Impacto estimado
Opinión pública	Alto: disminuye la confianza y la percepción de legitimidad de las misiones
Cohesión política	Moderado-alto: aumenta la polarización interna y genera debates parlamentarios intensos
Credibilidad internacional	Moderado: debilita la posición estratégica de España ante aliados y socios de la OTAN y la UE

➢ Valoración analítica

Este escenario refleja cómo la **guerra cognitiva internacional puede operar sin conflicto militar directo**, utilizando únicamente el **control de narrativas, emociones y percepciones**. La capacidad de manipulación digital, combinada con la amplificación emocional de contenidos, permite a actores hostiles generar **impactos estratégicos significativos** sobre decisiones políticas, apoyo social y reputación internacional.

La defensa frente a este tipo de amenaza requiere un enfoque integral: **monitoreo activo de información, comunicación estratégica proactiva, alfabetización mediática de la ciudadanía y coordinación institucional**, tanto a nivel nacional como con aliados internacionales. La anticipación y neutralización temprana de campañas de desinformación será determinante para preservar el **consenso político, la credibilidad de las misiones y la estabilidad institucional** de España.

4.3 Escenario 3 — Ataques cognitivos combinados con ciberataques

Uno de los escenarios más plausibles en el actual entorno de amenazas es la **convergencia entre ciberataques y operaciones de manipulación cognitiva**. A diferencia de los ataques puramente técnicos, esta modalidad híbrida no se limita a interrumpir sistemas o comprometer datos, sino que busca **provocar una reacción psicológica y social desproporcionada** respecto al impacto material inicial. En este contexto, el daño no se mide únicamente por la afectación operativa de una infraestructura, sino también por la capacidad del ataque para generar **miedo, incertidumbre, desconfianza institucional y conductas de pánico**.

España, por su nivel de digitalización y la interdependencia creciente de sus servicios esenciales, presenta una superficie de exposición significativa frente a este tipo de operaciones. Un ciberataque contra una infraestructura crítica podría ser acompañado, de manera simultánea o casi inmediata, por campañas de desinformación diseñadas para **amplificar la percepción de colapso**, exagerar las consecuencias del incidente o atribuirle motivaciones políticas, militares o terroristas. La finalidad no sería únicamente interrumpir un servicio, sino **desestabilizar el entorno cognitivo de la población y de los decisores públicos**.

Este tipo de operación se apoya en una lógica de **sincronización entre la acción técnica y la manipulación narrativa**. Cuanto más coordinadas estén ambas dimensiones, mayor será la probabilidad de que el incidente provoque un efecto sistémico, afectando no solo al sector atacado, sino también a la confianza general en la capacidad del Estado para proteger a la ciudadanía y mantener la continuidad de los servicios esenciales.

➢ Infraestructuras potencialmente afectadas

Las infraestructuras críticas constituyen objetivos prioritarios porque su interrupción tiene un efecto directo sobre la vida cotidiana, la actividad económica y la percepción de seguridad colectiva. Entre los sectores más vulnerables se encuentran los siguientes:

Sector	Vulnerabilidad
Energía	Redes eléctricas, sistemas industriales y control automatizado de suministro
Transporte	Aeropuertos, redes ferroviarias, sistemas logísticos y de señalización
Sanidad	Sistemas hospitalarios digitalizados, historiales clínicos y dispositivos conectados
Telecomunicaciones	Redes de comunicación estratégicas, conectividad móvil y servicios esenciales

La afectación de cualquiera de estos sectores puede generar una reacción social inmediata, especialmente si el servicio interrumpido es percibido como indispensable para la seguridad o la vida cotidiana. Por ello, estos sectores no solo son relevantes desde una perspectiva técnica, sino también **desde el punto de vista psicológico y político**.

➢ Sincronización cognitiva

El rasgo distintivo de este escenario es la **coordinación entre el evento técnico y su amplificación informativa**. La eficacia del ataque aumenta cuando la narrativa hostil logra adelantarse a la verificación oficial o llenar el vacío informativo dejado por la interrupción del servicio.

Acción técnica	Amplificación cognitiva
Interrupción eléctrica	Difusión de rumores sobre sabotaje masivo, colapso prolongado o fallo generalizado del sistema
Caída de telecomunicaciones	Narrativas sobre pérdida de control estatal, aislamiento del país o ruptura de la cadena de mando
Ataque a hospitales	Explotación emocional del incidente mediante imágenes, testimonios y mensajes de alarma en redes sociales

En todos estos casos, la clave está en que la población no solo perciba el fallo, sino que lo interprete como síntoma de un **colapso estructural mayor**. La desinformación actúa, por tanto, como un multiplicador de daños. Un incidente que en condiciones normales sería gestionable puede transformarse en una crisis de confianza si se combina con mensajes virales, contenidos manipulados o supuestas filtraciones sobre una situación más grave de la que realmente existe.

La velocidad de difusión juega aquí un papel decisivo. En los primeros minutos u horas tras el incidente, las narrativas no verificadas suelen tener una ventaja comunicativa sobre las fuentes oficiales. Ese margen temporal es suficiente para instalar interpretaciones erróneas, generar comportamiento de pánico y erosionar la credibilidad de la respuesta institucional.

- **Lógica operativa del escenario**

Este tipo de ataque híbrido suele seguir una secuencia relativamente coherente:

1. Preparación del terreno

Antes del ataque técnico, los actores hostiles pueden haber desplegado previamente narrativas sobre debilidad institucional, vulnerabilidad tecnológica o incapacidad estatal para responder a emergencias. Esto facilita que, cuando se produce la interrupción real, la población ya esté predispuesta a interpretar el incidente como parte de una crisis mayor.

2. Ejecución del ciberataque

La acción técnica afecta a una infraestructura crítica, interrumpiendo un servicio visible y socialmente relevante. El impacto inicial no tiene por qué ser catastrófico para que el efecto cognitivo sea profundo; basta con que el fallo resulte llamativo, inesperado o prolongado.

3. Amplificación informativa

De forma casi simultánea, se difunden rumores, vídeos manipulados, mensajes alarmistas o supuestas explicaciones sobre el origen del ataque. Esta fase busca llenar el vacío informativo y moldear la percepción pública antes de que las autoridades puedan establecer un relato sólido y verificable.

4. Escalada emocional

A medida que la incertidumbre crece, pueden intensificarse las reacciones de miedo, indignación o desconfianza. En este punto, la crisis deja de ser solo técnica y pasa a convertirse en una **crisis de legitimidad y percepción**.

5. Efecto político y social

Si la campaña tiene éxito, puede producirse presión mediática, cuestionamiento de la capacidad del Gobierno, tensión social y deterioro de la confianza en el Estado. El atacante no necesita destruir completamente el sistema; basta con **debilitar la percepción de control y resiliencia**.

➢ Impacto estratégico

El impacto de este escenario debe evaluarse en tres planos: seguridad nacional, economía y cohesión social.

Área	Consecuencia
Seguridad nacional	Crisis de confianza en las instituciones y percepción de vulnerabilidad del Estado
Economía	Pérdida de estabilidad financiera, interrupciones logísticas y costes de recuperación elevados
Cohesión social	Reacciones emocionales masivas, difusión de rumores y aumento de la ansiedad colectiva

Seguridad nacional: Estatal de proteger infraestructuras y garantizar la continuidad de los servicios esenciales. Si el ataque se percibe como una demostración de impotencia institucional, su impacto puede extenderse mucho más allá del ámbito técnico.

Economía: La interrupción de servicios estratégicos puede afectar a la actividad productiva, al transporte de mercancías, a las operaciones financieras y a la confianza de los mercados. Además, la incertidumbre informativa incrementa el coste de la respuesta, tanto en términos operativos como reputacionales.

Cohesión social: La población puede reaccionar con comportamientos de acumulación, saturación de servicios, difusión de rumores o desconfianza hacia los comunicados oficiales. En situaciones de alta ansiedad, la esfera digital actúa como acelerador del conflicto cognitivo.

➢ **Valoración analítica**

Este escenario es especialmente grave porque combina dos tipos de vulnerabilidad que se refuerzan mutuamente: la **vulnerabilidad técnica de los sistemas críticos** y la **vulnerabilidad perceptiva de la opinión pública**. La interacción entre ambas permite a un adversario generar efectos desproporcionados con recursos relativamente limitados.

A diferencia de un ciberataque aislado, la operación híbrida persigue que el daño material sea acompañado por una **crisis narrativa**. El objetivo final no es solo interrumpir un servicio, sino producir una sensación generalizada de descontrol, fragilidad institucional y pérdida de seguridad. En términos estratégicos, esto puede traducirse en una forma de presión indirecta sobre el Estado, sus instituciones y su capacidad de respuesta.

Por ello, la defensa frente a este escenario no puede limitarse a la ciberseguridad tradicional. Requiere una **arquitectura integrada de resiliencia**, que combine protección técnica, comunicación estratégica, gestión de crisis y capacidades de detección temprana de desinformación. Cuanto más coordinada sea la respuesta institucional, menor será la capacidad del atacante para convertir un incidente técnico en una crisis nacional.

➢ **Indicadores de alerta temprana**

Algunos signos que podrían anticipar este tipo de operación son:

- aumento de rumores coordinados tras incidentes técnicos menores;
- aparición simultánea de contenidos alarmistas en múltiples plataformas;
- uso de imágenes o vídeos reutilizados para magnificar el alcance del ataque;
- atribución inmediata del incidente a causas políticas o militares sin evidencia;
- incremento artificial del tráfico sobre palabras clave asociadas al fallo;

- narrativa insistente sobre “colapso”, “caos” o “pérdida de control” antes de la verificación oficial.

➢ **Conclusión del escenario**

Los ataques cognitivos combinados con ciberataques representan una de las formas más peligrosas de amenaza híbrida, porque explotan la interdependencia entre sistemas digitales, infraestructura crítica y percepción social. Su eficacia radica en la capacidad de convertir un incidente técnico en una **crisis de confianza, legitimidad y cohesión**. Para España, este escenario exige una respuesta que no sea solo reactiva, sino también preventiva, coordinada y orientada a reforzar la resiliencia institucional y social frente a operaciones de manipulación multifactorial.

4.4 Escenario 4 — Manipulación cognitiva mediante IA generativa

La rápida evolución de los sistemas de **inteligencia artificial generativa** está transformando profundamente el ecosistema informativo global. Estas tecnologías permiten crear **contenido sintético altamente realista** en formatos audiovisuales, textuales y conversacionales, reduciendo significativamente las barreras técnicas y económicas para la manipulación informativa a gran escala. Como consecuencia, la **guerra cognitiva adquiere una nueva dimensión**, caracterizada por la capacidad de generar narrativas falsas creíbles, amplificarlas rápidamente y adaptarlas a públicos específicos.

En el caso de España, la proliferación de estas herramientas podría facilitar operaciones destinadas a **influir en la opinión pública, desacreditar actores políticos o generar confusión informativa**. A diferencia de las campañas tradicionales de desinformación, la inteligencia artificial generativa permite producir contenido de forma automatizada, masiva y personalizada, incrementando la sofisticación y el alcance de las operaciones cognitivas.

Entre las aplicaciones más relevantes de este escenario se encuentran la creación de **vídeos falsos hiperrealistas**, la generación de **discursos políticos falsificados** y la construcción de **identidades digitales artificiales** capaces de interactuar con usuarios reales y participar en debates públicos. Estas capacidades reducen la capacidad de verificación tradicional y dificultan la distinción entre contenido auténtico y manipulado.

➢ **Modalidades de manipulación mediante IA generativa**

Las operaciones cognitivas basadas en inteligencia artificial pueden adoptar diversas formas, con efectos complementarios:

- **Vídeos falsos hiperrealistas**: creación de contenidos audiovisuales en los que figuras políticas, militares o institucionales aparecen realizando declaraciones o acciones que nunca ocurrieron. Este tipo de contenido puede difundirse rápidamente y generar reacciones emocionales inmediatas antes de ser verificado.
- **Discursos políticos falsificados**: generación de mensajes, comunicados o entrevistas simuladas atribuidas a líderes políticos o institucionales. Estas falsificaciones pueden introducir narrativas divisivas o provocar crisis políticas.
- **Identidades digitales artificiales**: creación de perfiles automatizados que simulan ser ciudadanos reales, periodistas o expertos, capaces de interactuar en redes sociales y contribuir a la amplificación de narrativas manipuladas.

Estas modalidades permiten a los actores hostiles **combinar volumen, realismo y segmentación**, generando una capacidad de influencia sin precedentes en el espacio informativo.

➢ Capacidades tecnológicas emergentes

El desarrollo de estas herramientas introduce nuevos riesgos cognitivos, especialmente cuando se combinan con técnicas de amplificación digital y microsegmentación.

Tecnología	Riesgo cognitivo
Deepfakes hiperrealistas	Desinformación audiovisual difícil de verificar
Bots conversacionales	Manipulación del debate público mediante interacción automatizada
Generación masiva de contenido	Saturación informativa y dificultad para distinguir fuentes fiables

Deepfakes hiperrealistas: Los avances en generación audiovisual permiten producir vídeos con un alto nivel de realismo, en los que resulta complejo detectar la manipulación. Estos contenidos pueden difundirse rápidamente, especialmente en momentos de crisis política o social, generando reacciones inmediatas y difíciles de revertir.

Bots conversacionales: Los sistemas de inteligencia artificial permiten crear perfiles que simulan comportamiento humano, participan en debates y responden en tiempo real. Esto puede generar la **percepción artificial de consenso social**, influyendo en la opinión pública y amplificando determinadas narrativas.

Generación masiva de contenido: La capacidad de producir grandes volúmenes de texto, imágenes y vídeos permite saturar el entorno informativo. Esta saturación dificulta la verificación y aumenta la probabilidad de que contenidos manipulados circulen sin ser cuestionados.

➢ **Lógica operativa del escenario**

La manipulación cognitiva mediante inteligencia artificial generativa podría desarrollarse en varias fases:

1. Preparación narrativa

Identificación de temas sensibles en el debate público español, como polarización política, tensiones territoriales, crisis económicas o conflictos internacionales.

2. Producción automatizada de contenido

Generación masiva de vídeos, textos y perfiles digitales artificiales adaptados a distintos segmentos de la población.

3. Amplificación coordinada

Difusión del contenido mediante redes sociales, plataformas digitales y cuentas automatizadas, simulando consenso social o urgencia informativa.

4. Confusión informativa

Dificultad para distinguir entre contenido real y manipulado, generando incertidumbre y debilitando la credibilidad de las fuentes tradicionales.

5. Impacto político y social

Desconfianza generalizada, polarización y debilitamiento de la capacidad institucional de comunicación.

➢ **Impacto potencial**

El impacto de este escenario afecta a múltiples dimensiones del sistema informativo y democrático:

Área	Nivel de riesgo
Credibilidad mediática	Alto
Confianza pública	Alto
Procesos democráticos	Moderado–alto

Credibilidad mediática (Riesgo alto): La proliferación de contenido sintético puede erosionar la confianza en los medios de comunicación, dificultando la verificación de información y generando un entorno informativo más incierto.

Confianza pública (Riesgo alto): Cuando la ciudadanía percibe que no puede distinguir entre contenido real y manipulado, aumenta la desconfianza generalizada, tanto hacia las instituciones como hacia el debate público.

Procesos democráticos (Riesgo moderado-alto): La manipulación mediante inteligencia artificial puede influir en campañas electorales, debates políticos y percepción de actores institucionales, afectando indirectamente a la calidad del proceso democrático.

➢ **Actores potenciales**

Este tipo de operaciones puede ser llevado a cabo por distintos actores:

- **Estados competidores**, interesados en debilitar la cohesión interna y la estabilidad política;
- **Redes híbridas o grupos organizados**, que buscan generar polarización o inestabilidad;
- **Actores privados o ideológicos**, que utilizan la tecnología para amplificar narrativas o influir en el debate público.

La accesibilidad creciente de estas herramientas incrementa el número de actores con capacidad de ejecutar este tipo de campañas, reduciendo el umbral técnico necesario.

➢ **Valoración analítica**

La manipulación cognitiva mediante inteligencia artificial generativa representa una **evolución cualitativa de la desinformación**, ya que combina automatización, personalización y realismo. A diferencia de campañas tradicionales, estas operaciones pueden desarrollarse con mayor rapidez, menor coste y mayor dificultad de atribución.

El principal riesgo no reside únicamente en la difusión de contenidos falsos, sino en la **erosión progresiva de la confianza en el propio ecosistema informativo**. Cuando cualquier contenido puede ser manipulado, se debilita la capacidad de la sociedad para construir consensos basados en hechos verificables.

Desde una perspectiva estratégica, este escenario exige fortalecer las capacidades de **detección de contenido sintético, comunicación institucional rápida, cooperación con plataformas digitales y alfabetización mediática de la ciudadanía**. La resiliencia cognitiva frente a inteligencia artificial generativa será un elemento clave para preservar la estabilidad democrática y la seguridad nacional.

➢ **Indicadores de alerta temprana**

Entre los posibles indicadores de este escenario se incluyen:

- aparición repentina de vídeos altamente realistas con contenido controvertido;
- incremento de perfiles digitales con comportamiento automatizado;
- aumento masivo de contenido similar difundido simultáneamente;
- mensajes políticos atribuidos a figuras públicas sin confirmación oficial;
- viralización acelerada de contenido audiovisual antes de su verificación;

- incremento de narrativas que cuestionan la autenticidad de fuentes informativas.

➢ **Conclusión del escenario**

La manipulación cognitiva mediante inteligencia artificial generativa constituye una de las amenazas emergentes más relevantes para España, debido a su capacidad para **alterar percepciones, erosionar la confianza y amplificar la polarización social**. En un entorno donde la producción de contenido sintético es cada vez más accesible, la protección del espacio informativo se convierte en un elemento esencial de la seguridad nacional. La anticipación, la detección temprana y la resiliencia social serán factores determinantes para mitigar el impacto de estas operaciones cognitivas avanzadas.

5. MATRIZ DE RIESGO ESTRATÉGICO PARA ESPAÑA (2026–2035)

La evolución del entorno estratégico internacional durante el periodo 2026–2035 apunta hacia un **incremento sostenido de amenazas cognitivas e híbridas**, caracterizadas por su bajo coste, alta escalabilidad y dificultad de atribución. Estas amenazas no buscan necesariamente la confrontación directa, sino la **erosión progresiva de la estabilidad institucional, la cohesión social y la autonomía estratégica** de los Estados.

En este contexto, España presenta un conjunto de **vulnerabilidades estructurales y oportunidades de resiliencia** derivadas de su grado de digitalización, su pertenencia a alianzas internacionales, su exposición mediática y su creciente relevancia geopolítica en el entorno europeo y mediterráneo. La siguiente matriz sintetiza los principales escenarios identificados, evaluando su **probabilidad de ocurrencia**, **impacto estratégico potencial** y **nivel global de riesgo**.

➢ **Matriz de riesgo estratégico (2026–2035)**

Escenario	Probabilidad	Impacto	Nivel de riesgo
Interferencia electoral	Alta	Alto	**Muy alto**
Crisis narrativa en conflictos internacionales	Media	Alto	**Alto**
Ataques híbridos ciber-cognitivos	Media	Muy alto	**Muy alto**
Desinformación mediante IA generativa	Alta	Alto	**Muy alto**

➢ **Análisis por escenarios**

1. Interferencia electoral (Riesgo muy alto)

La **interferencia cognitiva en procesos electorales** presenta una probabilidad elevada debido a varios factores estructurales: la polarización política creciente, la digitalización del debate público y la facilidad de acceso a herramientas de manipulación informativa. Estos elementos convierten los procesos electorales en **objetivos prioritarios para actores hostiles**, tanto estatales como no estatales.

El impacto potencial de este escenario es alto, ya que puede afectar directamente a la **legitimidad institucional, la estabilidad política y la confianza ciudadana**. Incluso sin alterar formalmente el resultado electoral, la introducción de dudas persistentes sobre la transparencia del proceso puede generar efectos prolongados en el funcionamiento democrático.

Entre los factores que incrementan el riesgo destacan:

- Alta dependencia del debate político en redes sociales;
- Creciente fragmentación del ecosistema mediático;
- Velocidad de difusión de narrativas polarizantes;

- Uso de inteligencia artificial para generación de contenido manipulado.

Por estos motivos, este escenario se clasifica como **riesgo muy alto**, especialmente en periodos electorales nacionales, autonómicos o europeos.

2. Crisis narrativa en conflictos internacionales (Riesgo alto)

La participación de España en **misiones internacionales y estructuras de seguridad colectiva** la convierte en objetivo potencial de campañas cognitivas destinadas a **erosionar el apoyo interno a estas operaciones**. En contextos de escalada militar, actores hostiles pueden intentar explotar la sensibilidad social hacia conflictos armados y víctimas civiles.

La probabilidad de este escenario se considera media, ya que depende de la evolución del contexto geopolítico internacional. Sin embargo, su impacto es elevado, dado que puede afectar a:

- la cohesión política interna;
- la credibilidad internacional de España;
- la continuidad de misiones estratégicas;
- el consenso parlamentario sobre política exterior.

Este escenario se caracteriza por el uso de **narrativas emocionales, manipulación audiovisual y campañas de movilización digital**, diseñadas para influir en la percepción pública y generar presión política.

Aunque el riesgo global se evalúa como alto, su materialización dependerá en gran medida del **grado de implicación española en escenarios de tensión internacional** durante el periodo analizado.

3. Ataques híbridos ciber-cognitivos (Riesgo muy alto)

Los **ataques híbridos que combinan ciberataques con manipulación informativa** representan uno de los escenarios más complejos y potencialmente disruptivos. La probabilidad de este tipo de operaciones es media, pero su impacto es **muy alto**, debido a la posibilidad de generar **efectos sistémicos simultáneos** en infraestructuras críticas y percepción social.

España presenta una exposición relevante a este tipo de amenazas debido a:

- alta digitalización de servicios esenciales;
- dependencia tecnológica de infraestructuras conectadas;
- interdependencia entre sectores críticos;
- rapidez de propagación de información en redes sociales.

La combinación de un incidente técnico con una campaña de desinformación puede provocar:

- crisis de confianza institucional;
- reacciones de pánico social;
- impacto económico inmediato;
- presión política y mediática.

Este escenario se clasifica como **riesgo muy alto** porque permite a un adversario generar **impactos estratégicos significativos con recursos relativamente limitados**, amplificando el daño mediante la dimensión cognitiva.

4. Desinformación mediante IA (Riesgo muy alto)

La expansión de la **inteligencia artificial generativa** incrementa notablemente la probabilidad de campañas de desinformación avanzadas. La facilidad para crear **deepfakes, identidades digitales artificiales y contenido masivo automatizado** convierte este escenario en uno de los más probables durante el periodo 2026–2035.

El impacto potencial es alto debido a su capacidad para:

- erosionar la credibilidad mediática;
- aumentar la polarización política;
- debilitar la confianza institucional;
- influir en procesos democráticos.

Además, este escenario presenta una **tendencia creciente**, ya que la accesibilidad tecnológica continuará aumentando y reduciendo el coste de las operaciones cognitivas.

Entre los factores que intensifican el riesgo se incluyen:

- democratización de herramientas de IA generativa;
- dificultad de verificación audiovisual;
- automatización del debate digital;
- saturación informativa del ecosistema mediático.

La combinación de alta probabilidad e impacto elevado sitúa este escenario dentro de la categoría de **riesgo muy alto** para la seguridad cognitiva nacional.

➢ Evaluación comparativa del riesgo

Del análisis conjunto de los escenarios se desprenden varias conclusiones estratégicas:

- **Tres de los cuatro escenarios presentan un nivel de riesgo muy alto**, lo que indica una creciente centralidad del dominio cognitivo en la seguridad nacional.
- Las amenazas cognitivas presentan **alta probabilidad y bajo umbral de entrada**, lo que incrementa el número potencial de actores hostiles.
- La convergencia entre tecnologías emergentes y manipulación informativa **aumentará la complejidad del entorno estratégico** en la próxima década.
- Los escenarios más peligrosos son aquellos que **combinan impacto técnico y percepción social**, como los ataques híbridos ciber-cognitivos.

➢ Conclusión de la matriz de riesgo

La matriz de riesgo estratégico para España durante el periodo 2026–2035 evidencia que las **amenazas cognitivas e híbridas se consolidarán como uno de los principales desafíos para la seguridad nacional**. La alta probabilidad de interferencia electoral y desinformación mediante inteligencia artificial, junto con el elevado impacto de ataques híbridos, configura un entorno en el que la **resiliencia cognitiva, tecnológica e institucional** será determinante.

En este contexto, España deberá reforzar su capacidad de **detección temprana, coordinación interinstitucional, comunicación estratégica y protección del espacio informativo**, con el objetivo de mitigar riesgos y preservar la estabilidad democrática en un entorno cada vez más competitivo y complejo.

6. CONCLUSIONES Y RECOMENDACIONES ESTRATÉGICAS

6.1 Conclusiones estratégicas

El análisis prospectivo realizado pone de manifiesto que **España se enfrentará durante el periodo 2026–2035 a un incremento sostenido de la presión cognitiva como dimensión estructural del conflicto contemporáneo**. La evolución del entorno geopolítico y tecnológico sugiere que la competencia estratégica entre actores estatales y no estatales se desplazará progresivamente hacia **operaciones de influencia persistentes, de baja intensidad y alta continuidad**, orientadas a modificar percepciones sociales, erosionar la confianza institucional y condicionar la toma de decisiones políticas.

A diferencia de los conflictos tradicionales, estas dinámicas no requieren confrontación directa ni generan necesariamente crisis abiertas. Por el contrario, se caracterizan por su **gradualidad, ambigüedad y dificultad de atribución**, lo que las convierte en herramientas especialmente eficaces para la erosión progresiva de la cohesión social y la estabilidad institucional. En este contexto, la guerra cognitiva se consolida como un instrumento central de la competencia geopolítica, donde la influencia sobre percepciones y narrativas adquiere un valor estratégico comparable al poder militar convencional.

Tres tendencias estructurales destacan en la evolución del entorno estratégico:

1. **Consolidación de la guerra cognitiva como conflicto permanente de baja intensidad**

La presión cognitiva tenderá a manifestarse mediante campañas continuadas, adaptativas y segmentadas, orientadas a explotar vulnerabilidades sociales, políticas o económicas. Estas operaciones buscarán influir en la percepción pública más que provocar disrupciones inmediatas, generando efectos acumulativos a medio y largo plazo.

2. **Expansión de la inteligencia artificial como multiplicador de manipulación informativa**

La proliferación de herramientas de inteligencia artificial generativa permitirá producir contenido manipulado de forma masiva, hiperrealista y personalizada. Este fenómeno reducirá los costes operativos de las campañas de desinformación, ampliará el número de actores con capacidad de influencia y dificultará la verificación de la información.

3. **Convergencia entre ciberespacio, información y neurotecnología**

El campo de batalla cognitivo se ampliará progresivamente hacia nuevas dimensiones tecnológicas, donde la manipulación informativa, la explotación de datos y las capacidades emergentes en neurotecnología generarán un entorno de competencia más complejo y multidimensional.

Estas tendencias indican que el conflicto estratégico del siglo XXI se desarrollará cada vez más en el ámbito de la **percepción, la legitimidad y la confianza social**, transformando el concepto tradicional de seguridad nacional.

6.2 Juicio analítico

La guerra cognitiva representa una **transformación estructural del conflicto estratégico contemporáneo**, en la que la superioridad militar convencional deja de ser el único factor determinante. En este nuevo paradigma, la capacidad de un Estado para **preservar la integridad cognitiva de su sociedad** y mantener la autonomía de sus decisiones políticas adquiere una relevancia estratégica creciente.

España ha iniciado un proceso relevante de adaptación institucional, científica y tecnológica orientado a fortalecer su resiliencia frente a amenazas cognitivas. Sin embargo, el análisis realizado evidencia que este proceso aún presenta

limitaciones estructurales, particularmente en términos de coordinación interinstitucional, autonomía tecnológica y resiliencia social.

La consolidación de una verdadera soberanía cognitiva nacional requerirá avanzar en tres áreas críticas:

1. Integración efectiva entre inteligencia, defensa, ciencia y sociedad civil
La naturaleza transversal de las amenazas cognitivas exige una respuesta igualmente transversal. La coordinación entre organismos de inteligencia, estructuras de defensa, centros de investigación, administraciones públicas y actores sociales resulta esencial para anticipar y mitigar campañas de influencia.

2. Reducción de dependencias tecnológicas externas en infraestructuras digitales estratégicas

La autonomía cognitiva está estrechamente vinculada al control sobre plataformas digitales, sistemas de inteligencia artificial y servicios tecnológicos críticos. La dependencia excesiva de proveedores externos puede limitar la capacidad de respuesta ante operaciones de manipulación informativa.

3. Refuerzo sistemático de la resiliencia social frente a manipulación informativa
La capacidad de una sociedad para identificar y resistir la desinformación constituye un elemento fundamental de la seguridad cognitiva. La alfabetización mediática, la confianza institucional y la cultura democrática son factores clave para reducir la vulnerabilidad frente a operaciones de influencia.

En este sentido, la defensa del dominio cognitivo no debe interpretarse exclusivamente como un desafío tecnológico o de seguridad, sino como un **reto estructural que afecta al funcionamiento democrático, la cohesión social y la autonomía estratégica del Estado**.

6.3 Recomendaciones estratégicas

A partir del análisis realizado, se identifican varias líneas prioritarias de actuación estratégica:

- **Fortalecimiento institucional**
  - **Desarrollar una arquitectura nacional de defensa cognitiva** que integre inteligencia, defensa, ciberseguridad y comunicación estratégica.
  - **Establecer mecanismos permanentes de coordinación interinstitucional** para la detección y respuesta ante amenazas híbridas.
  - **Incorporar el dominio cognitivo en la planificación de seguridad nacional** y en la doctrina estratégica del Estado.
- **Autonomía tecnológica**
  - **Reducir la dependencia de plataformas digitales y tecnologías externas** en ámbitos críticos.
  - **Impulsar el desarrollo nacional y europeo de inteligencia artificial y capacidades de detección de desinformación**.
  - **Fortalecer la protección de infraestructuras digitales estratégicas** frente a ataques híbridos.
- **Resiliencia social**
  - **Promover la alfabetización mediática y digital** como elemento de seguridad nacional.
  - **Reforzar la comunicación institucional estratégica** para contrarrestar campañas de desinformación.
  - **Fomentar la confianza social e institucional** como mecanismo de mitigación de amenazas cognitivas.

➢ **Cooperación internacional**

- **Fortalecer la cooperación con aliados europeos y atlánticos** en materia de defensa cognitiva.
- **Compartir inteligencia y buenas prácticas** sobre detección de campañas de influencia.
- **Participar en iniciativas multilaterales de protección del espacio informativo democrático**.

6.4 Prioridades estratégicas para el periodo 2026–2035

El análisis comparativo de escenarios permite identificar las siguientes prioridades estratégicas:

- **Protección de procesos electorales frente a interferencias cognitivas**
- **Defensa de infraestructuras críticas frente a ataques híbridos**
- **Mitigación del impacto de inteligencia artificial generativa en el ecosistema informativo**
- **Fortalecimiento de la confianza institucional y cohesión social**
- **Desarrollo de capacidades nacionales de análisis y anticipación cognitiva**

Estas prioridades reflejan la necesidad de adoptar un enfoque integral que combine **tecnología, gobernanza, comunicación estratégica y resiliencia social**.

CONCLUSION

La defensa del dominio cognitivo no consiste únicamente en proteger infraestructuras digitales o sistemas tecnológicos, sino en **preservar la capacidad de una sociedad para deliberar, decidir y actuar de forma autónoma**. En un entorno estratégico donde la percepción y la información se han convertido en instrumentos de poder, la seguridad nacional depende tanto de la fortaleza tecnológica como de la **solidez democrática e intelectual de la sociedad**.

España dispone de las bases institucionales y tecnológicas necesarias para avanzar hacia una mayor soberanía cognitiva. Sin embargo, el carácter dinámico de las amenazas exige una adaptación continua, anticipatoria y coordinada. La capacidad de proteger el espacio cognitivo nacional será, en este contexto, un **factor determinante para la estabilidad política, la autonomía estratégica y la seguridad nacional española en la próxima década**.