



02/2026

9 de enero de 2026

Ángela Navarro Paredes *

La información en la guerra híbrida. Propuesta de un modelo predictivo temprano

La información en la guerra híbrida. Propuesta de un modelo predictivo temprano

Resumen:

En el marco de la guerra híbrida contemporánea, la información se convierte en un instrumento de poder y elemento desestabilizador. Este artículo reflexiona sobre el impacto de la desinformación y la manipulación narrativa en la seguridad y la confianza institucional, además de la necesidad de implementar un sistema que permita anticipar peligros informativos. A partir del análisis de narrativas y emociones en las redes sociales, se plantea la importancia de integrar herramientas tecnológicas y equipos de trabajo humanos para reforzar la resiliencia estratégica de los estados. De este modo, se resalta el uso de la información como arma de poder y elemento influyente del *status quo* internacional.

Palabras clave:

Información, Desinformación, Guerra híbrida, Redes sociales.

***NOTA:** Las ideas contenidas en los **Documentos de Opinión** son responsabilidad de sus autores, sin que reflejen necesariamente el pensamiento del IEEE o del Ministerio de Defensa.

Information in Hybrid Warfare. Early Predictive Model Proposal.

Abstract:

In the context of contemporary hybrid warfare, information becomes both an instrument of power and a destabilizing element. This article reflects on the impact of disinformation and narrative manipulation on security and institutional trust, as well as the need to implement a system capable of anticipating informational threats. Based on the analysis of narratives and emotions on social networks, the importance of integrating technological tools and human working groups to strengthen the strategic resilience of states is highlighted. In this way, the use of information as a weapon of power and an influential element in shaping the international status quo is underscored.

Keywords:

Information, Disinformation, Hybrid war, Social networks.

Cómo citar este documento:

NAVARRO PAREDES, Ángela. *La información en la guerra híbrida. Propuesta de un modelo predictivo temprano*. Documento de Opinión IEEE 02/2026. [enlace web IEEE](#) y/o [enlace bie³](#) (consultado día/mes/año)

Gracias a la creciente tendencia en el uso de las redes sociales, ya no solamente como medio de comunicación o interacción entre personas, sino también como medio de transmisión de información, en los últimos años se han experimentado nuevas mejoras en la optimización de los procesos y del trabajo. No obstante, con ello surgen nuevos riesgos que exponen tanto a las personas como a las instituciones e, incluso, a los estados, a situaciones complejas que pueden conllevar un perjuicio. De esta manera, cambia completamente el concepto de conflicto, tal y cómo antes se conocía, surgiendo nuevas modalidades como el concepto de guerra híbrida.

Así, los conflictos híbridos se convierten, a lo largo de las últimas décadas, en un problema real y difícil de solventar. Esto supone la insurgencia de nuevos retos para los gobiernos y de campos de batalla que son difíciles de controlar, con la información, entre otros, como territorio a conquistar o defender. Con esta casuística surge un nuevo orden mundial, en el que no es más poderoso aquél que posee los recursos más valiosos, tiene mayor peso militar o mayor influencia política, sino el que domina la información y la narrativa, tanto en los medios convencionales, como la televisión, la radio o la prensa, como en los digitales, como las redes sociales.

En este nuevo orden, por tanto, la información se convierte en fundamental, ya no solamente para mantener el principio democrático de información, a través del que se fomenta la participación ciudadana, sino también como arma. El control de lo que se transmite o, más bien, de cómo se transmite, se ha convertido en una manera de sembrar dudas y miedos, polarizar a la sociedad e, incluso, erosionar la confianza ciudadana en las instituciones. Todos estos factores hoy en día podrían considerarse igual o más efectivos incluso que la ocupación de un territorio y la violación de la soberanía nacional.

No obstante, la respuesta actual ante las campañas de guerra híbrida suele ser reactiva, es decir, se toma acción cuando los daños ya se han producido, cuando la información falsa ya ha surtido el efecto para el que se diseñó o cuando se han desestabilizado procesos democráticos tras generarse una desconfianza institucional. Así, sale a la luz una debilidad real, que es la falta de mecanismos de alerta temprana, capaces de detectar este tipo de operaciones híbridas en sus comienzos, antes de que sean capaces de infligir daño.

Partiendo de este problema, en este artículo se propone abordarlo a través de la elaboración de un modelo predictivo temprano basado en el análisis de patrones narrativos y emocionales en redes sociales. Por esto, se parte de la hipótesis de que las operaciones híbridas dejan evidencias detectables en el discurso en redes sociales antes de materializarse el efecto en la política, la economía o la sociedad. Estas evidencias pueden manifestarse en cambios radicales en cuanto a opiniones acerca de ciertos temas, en el incremento irregular de emociones polarizadoras, en la repetición del mismo mensaje por parte de cuentas falsas o *bots*, o en la distribución masiva de contenidos audiovisuales manipulados, conocidos como *deepfakes*¹.

Además, para completar este análisis se aborda el concepto de infoxicación, que hace referencia a la sobreinformación inyectada en la sociedad, mermando el pensamiento crítico de los ciudadanos². La saturación de información, ya sea veraz o no, favorece el afloramiento de un estado de desconcierto y hace que sea más fácil propagar información falsa. De este modo, la infoxicación no solamente puede ser vista como un producto del uso activo de los medios digitales, sino también como un vector real que potencia la eficacia de las campañas híbridas.

La guerra híbrida y la (des)información. La predicción de la guerra híbrida a través del cambio de patrones conductuales en redes sociales.

La guerra híbrida en la actualidad. Información y desinformación como armas.

En el concepto contemporáneo de guerra híbrida, la información ha pasado de ser un mero canal de transmisión de datos y hechos de actualidad a convertirse en una herramienta estratégica fundamental en el ámbito de la geopolítica. De este modo, las batallas ya no se libran solamente con el uso de carros de combate, buques de guerra o aviones, sino que también se utiliza lo simbólico, lo emocional y la percepción de la realidad como factor ofensivo. Muchos estados y actores no estatales han identificado el potencial de la información como elemento de desestabilización del orden mundial, de

¹ CHESNEY, Robert & CITRON, Danielle, *Deepfakes and the New Disinformation War*. Artículo Foreign Affairs <https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war> (consultado 22/05/2025).

² CORNELLA, Alfons, *Infoxicación. Buscando un orden en la información*. Libro (consultado 22/05/2025).

desgaste de las instituciones democráticas e, incluso, de debilitación de la sociedades desde dentro, sin recurrir al uso de la violencia directa o física³.

Una de las tácticas más recurridas en esta nueva forma de guerra es la manipulación y la lucha por el control de las narrativas a través de campañas de desinformación. Las campañas de desinformación se crean con el fin de confundir, polarizar y generar desconfianza hacia empresas, instituciones públicas, medios de comunicación, las fuerzas armadas y las fuerzas y cuerpos de seguridad de un estado o, incluso, entre los propios ciudadanos. En la actualidad, en vez de recurrir al silencio informativo, se persigue crear ruido. Esto es, inyectar una cantidad de mensajes excesiva, aunque se contradigan los unos a los otros, la falsificación de datos o la aportación de medias verdades, de tal manera que se confunda a las personas y no sean capaces de emitir un juicio crítico propio al no saber distinguir entre lo que es realidad y lo que es ficción dialéctica. De este modo, este fenómeno se ve amplificado en el entorno de la infoxicación, con el fin de impedir el conocimiento de la verdad, en vez de convencer de que un hecho es verídico⁴.

En contextos de conflictos, como el librado entre Rusia y Ucrania en los pasados años, este tipo de estrategias se ha desplegado con gran eficacia. Durante el conflicto, Moscú ha impulsado numerosas narrativas alternativas y contradictorias al discurso occidental, utilizando tanto medios afines, como redes sociales para justificar y convencer de que en realidad la intervención en suelo ucraniano era necesaria, además de para socavar el apoyo internacional al gobierno de dicho estado. Paralelamente, muchos estados europeos se han visto afectados por la difusión de algunas teorías conspirativas, imágenes manipuladas y noticias falsas que tenían como fin debilitar la cohesión social, generando dudas sobre las sanciones impuestas o alimentando corrientes y pensamientos prorrusos entre ciertos sectores de la población.

Por lo tanto, las redes sociales desempeñan un papel crucial en esta nueva dinámica. Debido a su capacidad de segmentar audiencias y viralizar contenidos, se han convertido en un campo de batalla privilegiado para las guerras cognitivas, definidas por Daniel Iriarte en su libro “Guerras cognitivas” como una manera de conseguir manipular el

³ HOFFMAN, Frank G., *Conflict in the 21st Century: the rise of hybrid wars*. Libro (consultado 24/05/2025).

⁴ PEIRANO, Marta, *El enemigo conoce el sistema: Manipulación de ideas, personas e influencias después de la economía de la atención*. Libro (consultado el 01/09/2025).

pensamiento y la manera de razonar y actuar a través de una sobreexposición a información fruto de una campaña psicológica⁵. En la actualidad, plataformas como X (anteriormente conocida como Twitter), TikTok, Instagram o Facebook permiten la rápida e indiscriminada propagación de mensajes que exploten las emociones de sus receptores, especialmente el miedo, la indignación, la frustración, la ansiedad o la confusión. A esta difusión de información falsa contribuyen los *bots* y las cuentas falsas, de manera completamente automatizada y sin necesidad de manipulación por parte de un humano⁶.

Como reacción ante este paradigma, algunos organismos internacionales han alertado sobre la necesidad de desarrollar estrategias de alfabetización mediática para hacer frente a la desinformación. Por ejemplo, la Unión Europea ha impulsado ciertas iniciativas como “EU vs. Disinfo” para rastrear y fulminar campañas de influencia extranjera, como las llevadas a cabo por Rusia⁷. No obstante, la rápida y constante evolución tecnológica y el desarrollo de *softwares* cada vez más sofisticados en el plano de la inteligencia artificial que contribuyen a la generación de desinformación con elementos como los *deepfakes*, hacen que este terreno se convierta en pantanoso, volátil y difícil de regular.

En definitiva, la guerra híbrida del siglo XXI encuentra en la información su arma más sutil y poderosa. No se trata solo de quién posee la verdad, sino de quién logra imponer su relato en el imaginario colectivo.

El problema actual: reacción tardía ante los ataques. Limitaciones de los modelos de respuesta actuales y riesgos de actuar tarde.

A lo largo de los años, las campañas híbridas basadas en la desinformación han revelado evidentes carencias en los modelos de respuesta presentes. De este modo, actuar con este retraso no solamente supone la pérdida del control del relato, sino también favorecer la erosión de la confianza de la sociedad en el gobierno, la polarización del debate y el

⁵ IRIARTE, Daniel. *Guerras cognitivas*. Libro (consultado 23/10/2025).

⁶ LÓPEZ GARAY, Miguel, *Las redes sociales como armas de influencia masiva y la necesidad de una doctrina informativa*. Documento de opinión IEEE núm. 68/2025. https://www.defensa.gob.es/ceseden/-/ieeee/las_redes_sociales_como_armas_de_influencia_masiva_y_la_necesidad_de_una_doctrina_informativa#A14 (consultado 23/10/2025).

⁷ EUvsDisinfo, *The architecture of Russia's FIMI operations*. <https://euvsdisinfo.eu/the-architecture-of-russias-fimi-operations/> (consultado 23/10/2025).

florecimiento de una sensación de confusión y duda generalizadas. En un mundo en el que la información se utiliza como arma, la demora ante una respuesta es una forma más de derrota en la batalla. Por esta razón, es de urgencia anticiparse a las narrativas falsas y reforzar la capacidad de respuesta en estas situaciones.

Es importante, por tanto, hablar acerca de las limitaciones de los modelos de respuesta actuales y, posteriormente, acerca de los riesgos de una actuación tardía. Por ende, las principales debilidades del modelo actual son la reacción tardía y fragmentada, la falta de coordinación entre los distintos actores, la insuficiencia de alfabetización mediática en las poblaciones modernas, la dependencia en medios privados y plataformas opacas y la debilidad ante tácticas híbridas sofisticadas.

En primer lugar, en cuanto a la reacción tardía y fragmentada, es notorio cómo los sistemas de detección actuales no tienden a anticiparse con una respuesta, sino que responden una vez la desinformación ya está diseminada. En segundo lugar, la falta de coordinación entre las distintas partes, es decir, gobiernos, medios, sociedad y redes sociales, provoca que las respuestas sean descoordinadas y desiguales, lo que reduce su efectividad. En tercer lugar, la falta de alfabetización mediática que impide a la población acceder a herramientas para distinguir información fiable de información falsa. Esto hace que la eficacia de las campañas institucionales se vea limitada y, por ende, la ciudadanía se vea expuesta a bulos virales, deepfakes y otras herramientas de campañas de desinformación que forman parte de posibles operaciones híbridas en redes sociales.

En cuarto lugar, los estados dependen altamente de plataformas como X, Telegram, Instagram o Facebook para contrarrestar la desinformación. No obstante, estas redes sociales no siempre son completamente transparentes ni ofrecen la rapidez necesaria, ya que sus algoritmos suelen favorecer la visualización de contenidos de carácter emocional y extremo. Por último, la combinación del uso de herramientas como los bots o los deepfakes, además de los ataques a la reputación institucional o el desempeño de campañas coordinadas, superan las capacidades de los gobiernos y de los mecanismos de verificación a la hora de hacer frente a una campaña híbrida estructurada, ya que están diseñados únicamente para combatir casos de desinformación aislados y cuando ésta ya ha surtido sus efectos nocivos.

En otro orden de ideas, una actuación tardía conlleva una serie de riesgos, como la pérdida del control de la narrativa y la generación de un escenario contrario a los intereses nacionales, la creación de una situación de desconfianza social e institucional generalizada, la posibilidad de aprovechamiento de las debilidades por parte de potencias enemigas, la consecución de un estado de alteración emocional y psicológica, o la propia legitimación de los agresores. Así, en cuanto a la pérdida del control de la narrativa, cuando la respuesta con información veraz llega tarde, se permite la penetración de la falsa en la opinión pública. De este modo, resulta más difícil que la verdad recupere terreno, con respecto a la reticencia de ciertos sectores de la población a creer las versiones oficiales de los hechos y sus recomendaciones en situaciones de crisis.

En el caso de la creciente desconfianza social institucional, la constante desinformación expuesta al público puede llegar a generar cierto escepticismo respecto a la narrativa oficial de gobiernos, medios de comunicación o, incluso, académicos y científicos. Como resultado de esta desconfianza pueden surgir conductas desobedientes, la polarización de la sociedad y, por ende, la debilitación de la estructura institucional. De este modo, con estos sentimientos se puede generar en un estado una situación de debilidad y caos que puede ser utilizada por potencias extranjeras para debilitar los regímenes democráticos desde su interior, como sucedió en Ucrania, donde la información ha tenido mayor peso a la hora a incidir en el pensamiento colectivo, que la propia ofensiva militar.

Además, debido a una saturación informativa (o infodemia), que va de la mano con la confusión y el miedo generados por la desinformación, se puede llegar a producir una desestabilización emocional y psicológica que suponga una reducción en la capacidad de respuesta o reacción por parte de los ciudadanos frente emergencias o situaciones críticas reales. Si se permite que la desinformación se imponga frente a la información veraz, el enemigo puede llegar a aparecer retratado como una víctima o defensor de una causa justa.

Es evidente, por tanto, que la desinformación no es solamente un problema de comunicación, sino una amenaza estratégica que exige respuestas coordinadas anticipadas y bien estructuradas. Así, una actuación tardía es una forma más de perder una guerra sin haber llegado a pisar el campo de batalla.

Propuesta de un modelo predictivo temprano de guerra híbrida a través del análisis de narrativas y comportamientos en redes sociales.

Tomando como punto de partida los efectos negativos de la imprevisión de las campañas relacionadas con la información que formen parte de una operación híbrida en las redes sociales, surge la necesidad de formular un modelo de predicción temprana a través del análisis tanto de las narrativas como de los comportamientos de los usuarios en estas plataformas. De este modo, con este modelo se pretende abandonar la forma de actuar presente hasta ahora, que consiste en actuar después de que la operación informativa haya surtido efecto y haya conseguido los objetivos para la que fue diseñada. Esto es fácilmente identificable si se presta la suficiente atención, ya que las narrativas se instauran antes de los propios ataques⁸.

De esta manera, el diseño de este modelo predictivo temprano se basa en la observación de algunos patrones de actividad, cambios en la popularidad o viralización de ciertas narrativas y alteraciones de comportamientos en las redes sociales, que pudiesen preceder a acciones más evidentes. Este análisis del comportamiento en las redes sociales se consigue optimizar a través del empleo de la inteligencia artificial y herramientas de análisis de datos como Pulsar, CrowdTangle o Meltwater, que permiten identificar patrones de comportamiento o de cambios en la narrativa. No obstante, estas herramientas han de coordinarse con el factor humano, que sería el encargado de analizar los datos extraídos de las mismas e identificar si, efectivamente, existe una amenaza informativa o no, detectar su origen, su inicio y su posible impacto.

Las características que poseen las aplicaciones mencionadas anteriormente son las siguientes. En primer lugar, Pulsar tiene como fin analizar cómo piensan y hablan los usuarios en las plataformas de Internet. Esto lo hace a través de una inteligencia artificial que estudia las opiniones, emociones y los temas que se comentan en las redes sociales y en los medios de comunicación. Esta aplicación es especialmente útil para entender lo que las comunidades o grupos comentan. En segundo lugar, la aplicación CrowdTangle permite ver qué publicaciones se están haciendo virales en algunas redes sociales como Facebook o Instagram. Es decir, no analiza personas ni su comportamiento, sino el

⁸ POMERANTSEV, Peter, *This is not propaganda: Adventures in the war against reality*. Libro (consultado 11/06/2025).

contenido que más se comparte, lo que es útil para detectar noticias falsas o temas tendencia en las redes sociales en cada momento. Finalmente, MeltWater combina la posibilidad de vigilancia tanto redes sociales como otros medios con formato de blog, noticia o podcast, entre otros. Esta aplicación, por tanto, se utiliza para conocer qué se está diciendo acerca de una institución o un tema y cómo se percibe.

Adicionalmente, para optimizar la extracción de datos sería necesario codificar las narrativas, es decir, establecer categorías temáticas y emocionales con el fin de detectar esos posibles cambios en ellas. Además, este modelo predictivo temprano estaría basado en sistemas de alerta basados en umbrales cuantitativos. Esto es, que en el caso de que ciertas señales superen ciertos niveles, entraría a actuar el análisis humano. Por ilustrarlo con un ejemplo, en el caso de que aumentase en un treinta por ciento la presencia de narrativas que incluyen un tema polarizador o sensible, entraría a actuar el factor humano de análisis, que determinaría la existencia o no de una amenaza. En caso de detectarse de manera anticipada una posible operación o campaña informativa, se activaría un protocolo de aviso a las autoridades en el ámbito de la comunicación en el ministerio de defensa o se lanzarían mensajes correctivos.

Por lo tanto, se consideran indicadores de riesgo los siguientes escenarios. En primer lugar, las alteraciones en el discurso emocional y en el léxico, que implicarían cambios en el uso de las palabras, sustituyendo unas por otras que tengan un significado más contundente, como “guerra” o “conflicto” por “invasión”, o “afectado” por “víctima”. En segundo lugar, es importante prestar atención a los cambios en los temas de conversación, sobre todo si son de entidad polarizadora o sensible, como la inmigración, la identidad nacional, las fuerzas armadas, el sistema sanitario nacional o la educación pública. En tercer lugar, el incremento atípico de actividad en cuentas bot o cuentas falsas en redes sociales, que difunden de manera masiva noticias falsas, convierten en tendencia ciertos hashtags, o comparten casi de manera simultánea el mismo argumento acerca de un asunto muy concreto.

En cuarto lugar, la identificación de discursos que ataquen directa o indirectamente a los garantes institucionales de la democracia y la constitución, como las fuerzas armadas, los medios de comunicación o los jueces es importante para detectar agentes que pretendan desestabilizar la sociedad. Por último, la distribución de deepfakes, vídeos

manipulados y memes, en contraposición de vídeos reales, textos largos y

elaborados, además del aumento en redes sociales de presencia de vídeos con contenido impactante o extremo en relación a un tema concreto.

Con el fin de ilustrar el funcionamiento del modelo predictivo temprano frente a operaciones relacionadas con la información en redes sociales, se plantea un escenario hipotético en el contexto de un estado que denominaremos “X”. De esta forma y a escasas semanas de unas elecciones generales, un sistema de monitoreo semántico y emocional aplicado a redes sociales detecta una actividad anómala con respecto al papel que las fuerzas armadas de este estado pueden jugar en el proceso electoral. Surgen así, nuevas cuentas anónimas y coordinadas en plataformas como Telegram, TikTok y X que, de forma coordinada, difunden mensajes que apelan al miedo hablando acerca de una supuesta intervención militar encubierta para alterar el resultado electoral. Así, estos contenidos compartidos consiguen un alcance masivo en menos de 48 horas gracias a vídeos, fotografías y publicaciones de alto carácter emocional.

Por ende, a través del modelo propuesto de predicción temprana se identifican varios indicadores, como el aumento del 30% en publicaciones que contienen las palabras “fraude electoral” y “golpe de Estado encubierto”, el uso de los mismos hashtags por perfiles de reciente creación y la utilización de un lenguaje en el que predominan las emociones negativas, como el miedo o la ira. Al haberse superado el umbral establecido del 30% en la cantidad de veces que se emplean palabras que se considera que pueden favorecer la polarización de la opinión pública, se emite una alerta automáticamente al centro de coordinación de ciberdefensa informativa, compuesto por técnicos del gobierno, analistas de inteligencia, agencias de verificación y especialistas en comunicación estratégica.

Tras haberse recibido esta alerta, se activa el protocolo y se inicia un análisis cualitativo que confirma que, efectivamente, la narrativa difundida es parte de un ataque llevado a cabo por una potencia extranjera. Así, la respuesta institucional se va a centrar en atacar tres frentes. En relación al primer frente, el ministerio de defensa emite un comunicado público en el que se desmienten las acusaciones. En segundo lugar, hay una colaboración con ciertas agencias de verificación como Newtral o Agencia EFE con el objetivo de desacreditar esas publicaciones dañinas que se hicieron virales. Por último, el Gobierno del estado “X” tendría que contactar con Telegram, TikTok y X para exponer

esas dialécticas y denunciar aquellas cuentas que infringen las políticas de estas plataformas y el riesgo que suponen.

Además, el gobierno lanza una campaña informativa con el fin de reforzar, por un lado, el principal papel de las fuerzas armadas de defensoras del ordenamiento constitucional y, por otro, la garantía de transparencia en los procesos electorales nacionales. De esta manera, gracias a estas medidas preventivas, la campaña informativa perdería alcance y credibilidad antes de ser consolidada la narrativa diseminada en el imaginario colectivo, preservándose la confianza ciudadana y garantizando el desarrollo normal de las elecciones generales en este estado “X”.

Finalmente, se propone un análisis de las debilidades, amenazas, fortalezas y oportunidades (en adelante, análisis DAFO), del modelo predictivo propuesto para evaluar los elementos que afectarían al desarrollo y aplicación del mismo.

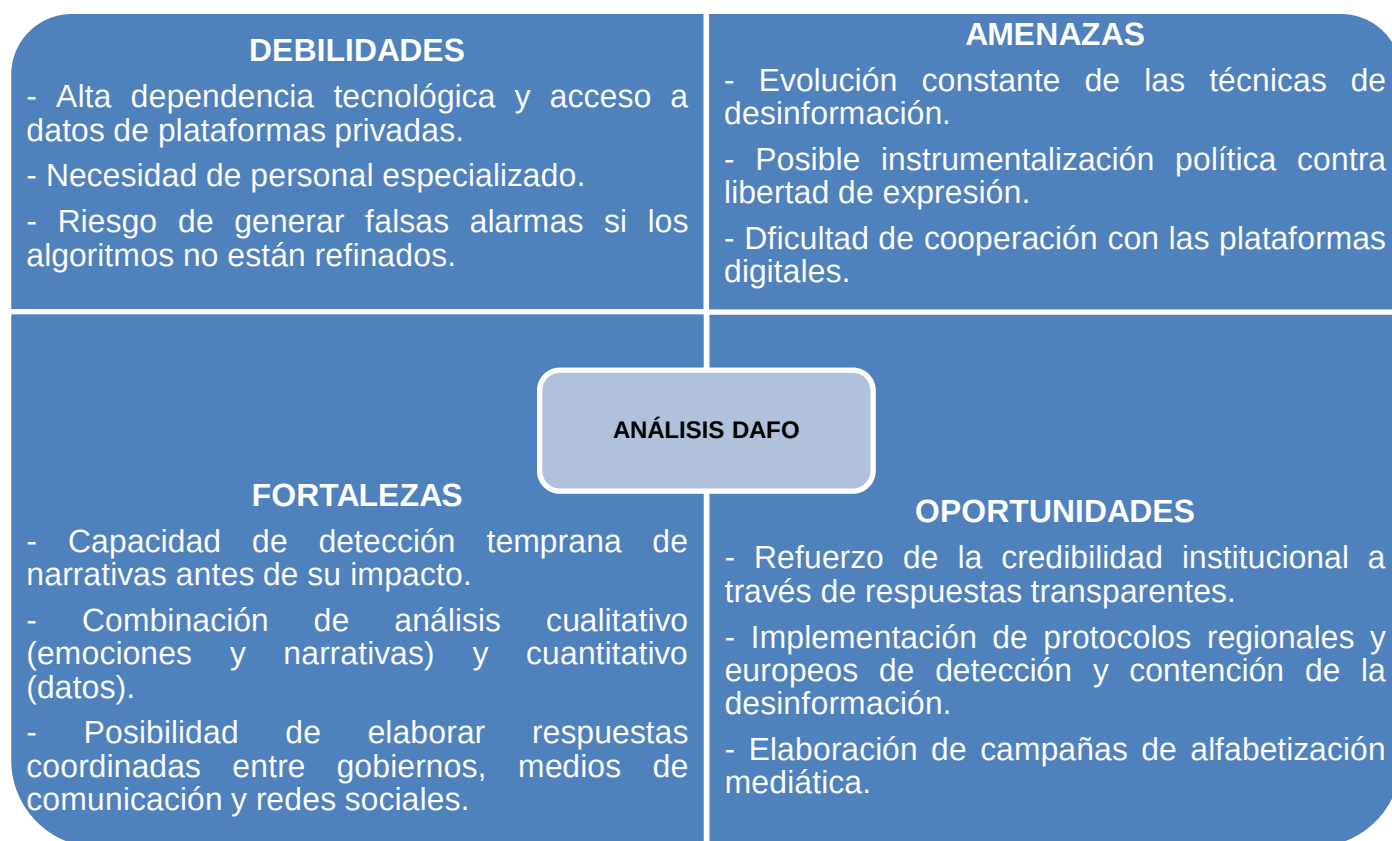


Figura 1: Análisis DAFO del modelo predictivo temprano de campañas híbridas basadas en la información (elaboración propia).

A lo largo de este artículo se ha puesto de manifiesto cómo el desarrollo de campañas híbridas a través del empleo de la información y la desinformación representa una amenaza real tanto para la seguridad como para la estabilidad de las sociedades democráticas contemporáneas. De este modo, al analizar el impacto de la información en los usuarios, se ha evidenciado de manera sólida que las respuestas actuales tienden a ser reactivas y tardías.

Considerando esta limitación como punto de partida, se pone de manifiesto la necesidad y eficacia potencial de un modelo predictivo temprano como herramienta efectiva de prevención de los posibles efectos de las operaciones que emplean la información como arma. De esta manera, partiendo del análisis narrativo y emocional en redes sociales, se ha comprobado que es posible identificar señales débiles que preceden al despliegue de este tipo de campañas. Implementar este modelo, por tanto, no solo mejora la resiliencia informativa, sino que constituye una estrategia imprescindible para salvaguardar el derecho a la información veraz, la estabilidad institucional y democrática y la seguridad nacional en el contexto actual.

Ángela Navarro Paredes

Teniente del Cuerpo de Intendencia de la Armada, graduada en Relaciones Internacionales y Administración y Dirección de Empresas.