

LA EVOLUCIÓN DE LA *MASKIROVKA*: LA INTELIGENCIA ARTIFICIAL GENERATIVA COMO CATALIZADORA DE ESTRATEGIAS DE ENGAÑO EN EL CONFLICTO RUSO-UCRANIANO (2014-2025).

Luiz Eugenio Cardoso Rangel Serra
Teniente Coronel de Artillería del Ejército de Tierra de Brasil

RESUMEN

En el conflicto ruso-ucraniano (2014-2025), Rusia ha transformado sus estrategias tradicionales de engaño, la *Maskirovka* y el *Control Reflexivo*, mediante la integración progresiva de inteligencia artificial generativa (IAG). Esta convergencia entre doctrinas soviéticas y tecnologías algorítmicas ha dado lugar a una nueva dimensión de guerra cognitiva, caracterizada por la manipulación perceptiva a través de narrativas falsas, contenidos sintéticos y desinformación automatizada. Durante la anexión de Crimea, Moscú empleó una *Maskirovka* tradicional basada en la ambigüedad operativa y la propaganda. Entre 2015 y 2022, amplió su capacidad informativa mediante redes de *trolls* y *bots*. Desde 2022, la IAG ha potenciado sus operaciones, permitiendo la creación masiva de *deepfakes*, portales falsos y campañas como *Doppelgänger* y *Pravda*. Estas operaciones han tenido impactos diferenciados: en Ucrania se ha desarrollado resiliencia social; en Rusia, la desinformación ha sido altamente eficaz; y en el Occidente, el resultado de la propaganda rusa ha sido mixto. Comprender esta evolución es crucial para anticipar las guerras cognitivas del futuro, donde el control de la percepción será el nuevo campo de batalla.

Palabras clave: *Control Reflexivo*; Desinformación; Engaño; Guerra cognitiva.

ABSTRACT

In the Russian-Ukrainian conflict (2014–2025), Russia has transformed its traditional deception strategies, *Maskirovka* and *Reflexive Control*, through the progressive integration of generative artificial intelligence (GAI). This convergence between Soviet doctrines and algorithmic technologies has given rise to a new dimension of cognitive warfare, characterized by perceptual manipulation through false narratives, synthetic content, and automated disinformation. During the annexation of Crimea, Moscow employed traditional *Maskirovka* based on operational ambiguity and propaganda. Between 2015 and 2022, it expanded its informational capabilities through networks of trolls and bots. Since 2022, GAI has significantly enhanced its operations, enabling the mass creation of deepfakes, fake portals, and campaigns such as *Doppelgänger* and *Pravda*. These operations have had differentiated impacts: in Ukraine, social resilience has developed; in Russia, disinformation has been highly effective; and in the West, the results of Russian propaganda have been mixed. Understanding this evolution is crucial to anticipating the cognitive wars of the future, where perception control will become the new battlefield.

Keywords: Cognitive Warfare; Deception; Disinformation; Reflexive Control.

INTRODUCCIÓN.

En la última década, los conflictos contemporáneos han experimentado una transformación profunda, impulsada por los avances tecnológicos, especialmente en el ámbito de la inteligencia artificial. Uno de los escenarios más emblemáticos de esta mutación ha sido el conflicto ruso-ucraniano (2014–2025), en el cual las herramientas digitales han desempeñado un papel destacado, complementando a los medios tradicionales de confrontación.

En este contexto, Rusia ha desplegado una estrategia de guerra informativa que fusiona doctrinas militares históricas, como la *Maskirovka* y el *Control Reflexivo*, con las capacidades operativas de la inteligencia artificial generativa (IAG). Esta convergencia ha propiciado una evolución doctrinal significativa que plantea nuevos desafíos a la seguridad internacional y al análisis académico del conflicto.

En los estudios sobre guerra informativa, la tradición rusa ha sido ampliamente analizada por su uso sistemático del engaño estratégico. La *Maskirovka*, entendida como un conjunto de medidas para desorientar al adversario en lo físico, psicológico e informacional, y el *Control Reflexivo*, desarrollado en la Unión Soviética por el científico Vladímir Lefebvre, y que se basa en inducir al adversario a tomar decisiones que, sin saberlo, favorecen los intereses de quien ejerce la influencia, constituyen un marco conceptual sólido para estudiar la manipulación perceptiva. En los últimos años, estos conceptos se han reformulado con la integración de tecnologías basadas en inteligencia artificial, especialmente la IAG, que ha transformado los métodos de producción y difusión de narrativas engañosas adaptadas a diversas audiencias.

Sin embargo, persisten vacíos académicos sobre cómo la IAG ha impulsado una transformación estructural en las prácticas rusas de desinformación. Aunque existen estudios sobre operaciones de influencia y sobre inteligencia artificial por separado, son escasos los que examinan esta fusión entre tradición doctrinal y disrupción tecnológica. Este trabajo busca contribuir a ese campo analizando la evolución de la *Maskirovka* en su fase cognitiva algorítmica y cómo la IAG ha potenciado las capacidades rusas de manipulación informativa en el conflicto ucraniano.

El objetivo de este artículo es, por tanto, analizar cómo la inteligencia artificial generativa ha modificado la aplicación de la doctrina *Maskirovka* en dicho conflicto, en términos de desinformación, manipulación cognitiva y guerra de información, evaluando su impacto en las audiencias ucraniana, rusa e internacional.

Para lograr este objetivo, además de esta introducción, el texto se estructura en tres apartados: un bloque de antecedentes, donde se justifica la relevancia del estudio; una exposición, que analiza la progresiva incorporación de la IAG

durante las distintas fases del conflicto y su efectividad según la audiencia; y una conclusión que sintetiza los hallazgos, valora la hipótesis y ofrece recomendaciones para fortalecer la resiliencia frente a futuras campañas de desinformación algorítmica.

Metodológicamente, se adopta un enfoque cualitativo-interpretativo, centrado en comprender la evolución doctrinal y operativa de la *Maskirovka cognitiva algorítmica*. Para ello, la investigación combina tres técnicas complementarias: análisis documental de doctrinas militares y marcos legales; estudio de casos emblemáticos como: Crimea (2014), el *deepfake* de Zelensky (2022), la campaña *Doppelgänger* y la explotación de inteligencia de fuentes abiertas (OSINT) para verificar y contextualizar rastros digitales.

Partiendo de este marco metodológico, se plantea como hipótesis central que la adopción progresiva de inteligencia artificial generativa ha multiplicado la eficacia de la *Maskirovka* y el *Control Reflexivo* rusos, al facilitar la producción, personalización y amplificación de narrativas de engaño mediante algoritmos.

El estudio se circunscribe al periodo comprendido entre 2014 y 2025, con especial atención a la fase final del conflicto, momento en que la Inteligencia Artificial Generativa (IAG) adquiere una relevancia operativa significativa. En términos geográficos, el análisis se centra en el espacio postsoviético, con énfasis en Ucrania, aunque también se consideran sus repercusiones cognitivas en la Unión Europea, Estados Unidos y el Sur Global.

En este contexto temporal y espacial, la convergencia entre doctrinas de engaño y tecnologías algorítmicas constituye un cambio cualitativo en la naturaleza del conflicto contemporáneo. Comprender esta transformación no solo permite interpretar con mayor profundidad el caso ruso-ucraniano, sino también anticipar los desafíos de una guerra cognitiva emergente, en la que la percepción se convierte en un objetivo estratégico y la IA en un multiplicador del engaño.

ANTECEDENTES.

El estudio de la *Maskirovka* y su interacción con la inteligencia artificial generativa (IAG) en el conflicto ruso-ucraniano resulta especialmente relevante por sus implicaciones teóricas, estratégicas y tecnológicas. Esta investigación examina cómo Rusia ha adaptado sus estrategias tradicionales de engaño al entorno digital, aprovechando los avances en IAG para reforzar sus campañas de desinformación.

Desde esta perspectiva, la convergencia entre la tradición rusa de engaño estratégico y la IAG ha dado lugar a una nueva dimensión del conflicto: la *Maskirovka* cognitiva algorítmica. Su evolución entre 2014 y 2025 merece

atención por tres motivos fundamentales.

En primer lugar, aporta un valor teórico-doctrinal al demostrar cómo un concepto originalmente concebido para el camuflaje físico se redefine en un entorno dominado por datos, algoritmos y redes sociales. Este fenómeno obliga a repensar categorías clásicas como la sorpresa o la disuasión, diferenciando entre la *Maskirovka* operacional y su versión cognitiva-algorítmica.

En segundo término, plantea un impacto estratégico: el dominio de estas técnicas permite influir en procesos electorales, fracturar sociedades y condicionar decisiones gubernamentales sin necesidad de recurrir a la fuerza militar. El caso ruso-ucraniano proporciona evidencia empírica valiosa, mediante el uso de *deepfakes*, perfiles sintéticos y campañas como *Doppelgänger* y la red *Pravda*, elementos clave para el diseño de políticas de resiliencia cognitiva.

Por último, pone de relieve un vacío académico y una necesidad práctica: pese a la abundancia de estudios sobre desinformación rusa, pocos abordan en profundidad la transformación estructural que implica integrar la IAG con doctrinas como la *Maskirovka* y el *Control Reflexivo*.

En suma, comprender esta convergencia entre tecnología avanzada y doctrinas clásicas no constituye únicamente un ejercicio teórico, sino una exigencia estratégica: quien controle los algoritmos que modelan la realidad percibida controlará el próximo campo de batalla: la mente.

EXPOSICIÓN.

APLICACIÓN TRADICIONAL DE LA MASKIROVKA (CRIMEA 2014).

En 2014, tras la anexión de Crimea y el estallido de la guerra en el Donbás, Rusia desplegó una intensa campaña de guerra informativa, manipulando datos con fines políticos y militares en el marco de una “guerra híbrida” (Golovchenko, 2020). Aprovechando el caos político tras el Euromaidán, Rusia ejecutó una operación relámpago basada en el engaño estratégico. Tropas rusas sin insignias, conocidas como los “hombrecitos verdes”, ocuparon puntos clave de Crimea sin identificarse como fuerzas rusas (Bouwmeester, 2021).

Esta ambigüedad deliberada evidenció la *Maskirovka* tradicional, orientada a generar confusión en Kiev y en la comunidad internacional. La reacción ucraniana y de la OTAN fue paralizada por la incertidumbre, lo que permitió a Moscú consolidar el control territorial sin grandes enfrentamientos (Bouwmeester, 2021). A la acción militar encubierta se sumó una ofensiva propagandística que legitimaba la anexión como autodeterminación, deslegitimando al gobierno ucraniano al tildarlo de “junta fascista” (Tipaldou y Casula). Esta narrativa engañosa ejemplifica el *Control Reflexivo*, orientado a

condicionar las decisiones del adversario (Tipaldou y Casula).

Tras la anexión, el conflicto se trasladó al este de Ucrania. En abril de 2014 se produjo el levantamiento prorruso en el Donbás, con toma de edificios públicos apoyada encubiertamente por agentes rusos. Entre 2014 y 2015, medios rusos difundieron narrativas falsas para deslegitimar al gobierno de Kiev y justificar a los separatistas (Polyakova, 2019), insistiendo en que Ucrania estaba gobernada por “nazis” y cometía “genocidio” contra la población rusoparlante (Alieva, Kloo y Carley, 2024).

Moscú mantuvo la ambigüedad sobre el conflicto, presentándolo como una guerra civil, lo que dificultó una respuesta internacional coordinada, objetivo característico del *Control Reflexivo*. Uno de los pilares de esta estrategia fue el uso masivo de *bots* y *trolls*. Poco después de la invasión, Yevgueni Prigozhin¹ fundó la Agencia de Investigación de Internet (IRA), encargada de difundir desinformación mediante múltiples perfiles falsos (Linvill y Warren, 2025; Seddon, 2014).

Estas granjas de *trolls* funcionaron como núcleos de guerra cognitiva. Operaban con lógica industrial: producción masiva de mensajes, rotación de identidades digitales, simulación de consenso y explotación de brechas sociopolíticas (Weiss y Pomerantsev, 2014). Constituyeron una forma temprana y eficaz de *Maskirovka* cognitiva. Aunque primitivas respecto a los sistemas actuales, demostraron el potencial de la desinformación algorítmica como vector fundamental de la guerra híbrida rusa.

Aunque los *deepfakes* aún no existían en este período, Rusia empleaba manipulaciones digitales básicas con fines propagandísticos. Como respuesta, surgieron iniciativas como *StopFake* (2014), orientada a verificar bulos en tiempo real, y el equipo *East StratCom* de la Unión Europea (2015), dedicado a monitorear la desinformación del Kremlin (Golovchenko, 2020).

Durante esta etapa, Rusia desplegó una primera generación de desinformación digital asistida por automatización básica: *trolls* humanos organizados, *bots* amplificadores, y manipulación de imágenes e identidades. Aunque sin inteligencia artificial generativa (IAG), estas operaciones sentaron las bases de una guerra cognitiva tecnológicamente mediada.

LA “PAUSA” HÍBRIDA (2015-2022).

Tras el Acuerdo de Minsk II, el conflicto armado en el Donbás disminuyó en intensidad; sin embargo, Moscú no abandonó sus objetivos estratégicos. En

¹ Mercenario ruso y líder del Grupo Wagner fallecido en agosto de 2023.

lugar de recurrir a ofensivas convencionales, Rusia intensificó sus operaciones en el ámbito informativo, político y cibernético con el fin de debilitar a Ucrania y mantener su influencia. Esta etapa marcó una evolución de la *Maskirovka* hacia el ámbito informacional, con un mayor grado de automatización y una proyección internacional más amplia (Bugayova, Kagan y Stepanenko, 2024).

Entre 2015 y 2022, el Kremlin llevó a cabo una auténtica “guerra de información permanente”, combinando el uso de medios tradicionales (RT, Sputnik) con la actividad de fábricas de *trolls* y redes de *bots* para difundir sus narrativas ante audiencias globales. La *Internet Research Agency* (IRA), activa desde 2014, consolidó su rol central en esta estrategia mediante acciones más sistemáticas y semiautomatizadas, como demuestra su implicación en las elecciones estadounidenses. Rusia también experimentó con la generación automatizada de noticias falsas. Un ejemplo paradigmático fue la campaña *Secondary Infektion* (2014–2020), una operación encubierta vinculada al Kremlin que difundió más de 2.500 historias falsas en al menos siete idiomas y en más de 300 plataformas digitales (Nimmo et al., 2020).

Aunque la campaña no empleó IAG avanzada en el sentido actual, sí recurrió a la automatización básica, especialmente en la traducción y la distribución multicanal. Con el avance de la tecnología, las operaciones rusas de influencia incorporaron IAG con el fin de sofisticar sus estrategias de engaño. Un caso emblemático fue *PeaceData* (2020), un sitio web ficticio creado por la IRA y dirigido a audiencias occidentales de izquierda (Carrie Wong, 2020).

En suma, el periodo 2015–2022 evidenció un salto cualitativo en las operaciones rusas de influencia. La *Maskirovka* dejó de ser una herramienta meramente táctica para consolidarse como estrategia informacional, sustentada en *trolls*, *bots*, *hackers* y técnicas incipientes de automatización, sentando las bases para una desinformación más sofisticada.

LA MASKIROVKA ALGORÍTMICA (2022-2025).

Desde el inicio de la invasión a gran escala en febrero de 2022, Rusia intensificó su ofensiva en el entorno informativo, aprovechando la proliferación de herramientas basadas en inteligencia artificial. En particular, la inteligencia artificial generativa (IAG) redujo notablemente las barreras de entrada para la creación masiva de contenido falso o manipulado, facilitando así nuevas formas de desinformación y propaganda (Osadchuk, 2024).

Además, en octubre de 2024 Ucrania denunció que Rusia utilizaba IAG para multiplicar su propaganda en múltiples idiomas y formatos (Potkin y Lim, 2024). El uso combinado de medios estatales, redes de *trolls* humanos y herramientas automatizadas permitió desplegar una guerra informativa más dinámica,

adaptativa y de gran amplitud. A diferencia de conflictos previos, la IA generativa posibilitó la producción de falsificaciones más creíbles y rápidas, optimizando la generación de contenido engañoso (Osadchuk, 2024).

De hecho, Rusia logró imponer su propio relato tanto dentro de su población como en determinados sectores de la opinión pública internacional. Este fenómeno evidencia una nueva fase: la *Maskirovka* rusa ya no se limita al plano físico ni al psicológico tradicional, sino que opera en un nivel cognitivo-algorítmico. En esta dimensión, el Kremlin genera y propaga realidades simuladas a escala global, con una fidelidad y una velocidad sin precedentes.

En paralelo, la estrategia rusa incluyó intentos deliberados de quebrar la moral de la población civil y de las tropas ucranianas mediante información falsa, apoyándose en la IAG para aumentar la eficacia propagandística. Uno de los primeros usos intencionados de un *deepfake* en la guerra de Ucrania se registró el 16 de marzo de 2022, cuando un video manipulado mostró al presidente *Zelensky* anunciando falsamente su rendición y pidiendo a las fuerzas ucranianas que depusieran las armas (Pearson y Zinets, 2022). Pese a su baja calidad técnica, esta operación sirvió como prueba de concepto dentro de la lógica de la *Maskirovka cognitiva algorítmica*: recurrió a la tecnología de IAG para socavar la moral enemiga y sembrar confusión (Osadchuk, 2024).

Otro ejemplo ocurrió en noviembre de 2023, Rusia difundió *deepfakes* del general *Valerii Zaluzhny* criticando a *Zelensky* y sugiriendo la existencia de un grave conflicto interno en Ucrania. Aunque los videos seguían siendo imperfectos en las expresiones faciales y algunos detalles, representaron un salto cualitativo respecto al intento fallido de 2022, al mostrar una mayor verosimilitud (Osadchuk, 2024).

Por otra parte, la campaña *Doppelgänger*, activa desde mediados de 2022, constituyó una de las principales operaciones de manipulación e interferencia informativa (FIMI) atribuidas a Rusia. Según el Servicio Europeo de Acción Exterior (SEAE, 2025), esta campaña involucró 228 dominios y 25.000 redes de comportamiento inauténtico coordinado (CIB), operando en nueve idiomas. Impulsada por las empresas *Struktura* y *Social Design Agency*, ambas financiadas por el Estado ruso, su objetivo es erosionar el apoyo internacional a Ucrania mediante la suplantación digital de medios y autoridades oficiales (SEAE, 2025).

Asimismo, la red *Pravda*, activa desde 2023, representaba una nueva fase en la guerra híbrida rusa: su propósito no es únicamente desinformar al público humano, sino corromper desde dentro los modelos de lenguaje de IA generativa, sesgando sus respuestas mediante una estrategia conocida como adoctrinamiento de grandes modelos de lenguaje (LLM grooming) (American Sunlight Project, 2025, p.13; Newport y Jankowicz, 2025). No obstante, aunque

esta red constituye una evolución sofisticada de la guerra informativa al dirigir su contenido también hacia los modelos de lenguaje, es importante matizar su alcance real. Pese a su volumen sostenido de publicaciones y su estructura multilingüe, la escala de estas campañas sigue siendo relativamente reducida en comparación con la magnitud de los datos empleados para entrenar grandes modelos de lenguaje (LLMs).

En este sentido, la migración de la *Maskirovka* al entorno algorítmico marcó un punto de inflexión: el uso combinado de IAG, *deepfakes*, clonación de sitios web y redes *bot* permitió a Rusia fabricar identidades, testimonios y escenarios enteros con costos mínimos. De este modo, el camuflaje ya no se limitaba a soldados sin insignias en el terreno, sino que reviste la propia información, imitando voces, portales y fotografías “de campo” difíciles de distinguir del contenido real. En consecuencia, este camuflaje digital potenció las capacidades clásicas de sorpresa y ocultación, permitiendo a Moscú proyectar simultáneamente múltiples verdades alternativas en distintos contextos lingüísticos y mediáticos.

Del mismo modo, el *Control Reflexivo* se vio reforzado por herramientas algorítmicas: la personalización de narrativas, la dosificación emocional a escala y la fabricación de consensos artificiales mediante identidades sintéticas indujeron a actores externos a adoptar, por propia deducción, decisiones beneficiosas para Rusia. Asimismo, la inserción de contenidos sesgados en bucles de recomendación, junto con el adoctrinamiento de modelos LLM, configura una estrategia de influencia destinada a incrustar el sesgo prorruso en la propia arquitectura informativa global.

En efecto, la experiencia acumulada entre 2022 y 2025 revela cómo la convergencia entre la IAG y las doctrinas rusas de engaño ha potenciado el alcance del *Control Reflexivo*: *deepfakes* en tiempo real, identidades falsas creíbles y la manipulación de sistemas automatizados han creado un entorno en el que la verdad opera en clara desventaja.

Al analizar la evolución de la *Maskirovka* y el *Control Reflexivo* desde sus primeras manifestaciones digitales hasta las capacidades actuales de la IAG, se observa una progresión continua de sencillas campañas de *bots* y *trolls* hacia ecosistemas de engaño cada vez más sofisticados. Este recorrido culmina en el umbral psicológico que representa el denominado “valle inquietante”: el punto en que las falsificaciones sintéticas, imágenes, voces y rostros generados por IA, alcanzan un realismo tan elevado que ya no activan de manera inmediata la alerta cognitiva del receptor.

La superación de este umbral psicológico conlleva dos implicaciones operativas. En primer lugar, implica un mayor volumen efectivo de contenidos desinformativos, dado que la mayor parte del material sintético circula sin

levantar sospechas, multiplicando la relación coste/impacto. En segundo lugar, acorta la ventana de verificación, puesto que, si el adversario no percibe la falsedad a simple vista, los analistas disponen de mucho menos tiempo para desmontar la narración antes de que cristalice.

En suma, el avance de la inteligencia artificial generativa se aproxima cada vez más al cruce del “valle inquietante”, eliminando los indicios sutiles que antes delataban la falsedad de los *deepfakes*. Esta superación no solo incrementa el realismo visual y auditivo del contenido sintético, sino que aumenta exponencialmente su eficiencia operativa: circula con mayor credibilidad, evade la detección temprana y reduce significativamente la capacidad de respuesta del adversario.

LA EFECTIVIDAD DE LA MASKIROVKA Y DEL CONTROL REFLEXIVO POTENCIADOS POR LA IAG EN EL CONFLICTO RUSO-UCRANIANO.

La vulnerabilidad de la audiencia ucraniana ante la guerra informativa rusa potenciada por la Inteligencia Artificial Generativa (IAG) ha experimentado una evolución clara desde el inicio de la invasión de 2022. En las primeras etapas del enfrentamiento, la difusión del *deepfake* protagonizado por Volodymyr Zelensky evidenció cierta susceptibilidad de la sociedad ucraniana, pero tanto los medios de comunicación nacionales como el propio presidente reaccionaron rápidamente para desmentirlo.

Adicionalmente, la deficiente calidad técnica del video facilitó su identificación como un montaje, mientras que la experiencia directa de la población contradecía el mensaje difundido, restando credibilidad a la operación de desinformación. Cabe señalar que la ciudadanía ucraniana ya contaba con cierta preparación para enfrentar estas campañas manipulativas, gracias a su experiencia previa con las operaciones rusas de desinformación desde 2014 (Metz, 2022).

Ucrania desarrolló una resiliencia significativa ante esta guerra informativa. Esta adaptación se reflejó tanto en respuestas institucionales como sociales: el gobierno estableció unidades especializadas para contrarrestar las campañas de desinformación, y desde la sociedad civil se impulsó la alfabetización mediática entre la población. Más aún, la agresión rusa actuó como catalizador de un fortalecimiento de la identidad nacional ucraniana, factor que gradualmente redujo la efectividad de las narrativas originadas en Moscú (Helmus y Holynska, 2024).

En marcado contraste con la experiencia ucraniana, en Rusia la guerra informativa potenciada por IAG ha mantenido una alta efectividad en el ámbito doméstico. Desde 2014, el gobierno ruso ha ejercido un control casi total sobre el entorno mediático, lo que permitió la difusión de mensajes uniformes a través

de medios de comunicación estatales (Martín, 2025).

Además, la inteligencia artificial generativa posibilitó la producción masiva de contenidos alineados con las narrativas oficiales, dando una apariencia engañosa de pluralidad informativa. Al saturar deliberadamente el espacio mediático con versiones alternativas de los acontecimientos, se dificultó que los ciudadanos rusos accedieran a información objetiva sobre el conflicto (Martín, 2025).

Dentro de esta estrategia informativa, la anexión de Crimea y la posterior denominación de la invasión como “operación militar especial” fueron presentadas como correcciones históricas inevitables. Los medios estatales insistieron en el concepto de “retorno” de territorios considerados históricamente rusos y en la supuesta protección de los hablantes de ruso (Mahon y Walker, 2024). Esta narrativa, al apelar a la memoria histórica y a la política identitaria, generó un apoyo público abrumador: las encuestas registraban niveles de aprobación superiores al 80% para la anexión (Levada Center, 2025).

Este férreo control del entorno mediático por parte del gobierno ruso ha fomentado una atmósfera donde la narrativa dominante es el apoyo a la guerra. En consecuencia, las voces contrarias suelen guardar silencio, generando un ciclo autorreforzado en el que la disidencia resulta social y legalmente riesgosa (Gugushivili, 2025, p.4). En este contexto, la ausencia visible de protestas refuerza aún más la percepción de que la mayoría aprueba el conflicto, lo que desincentiva a quienes albergan opiniones contrarias a expresarlas abiertamente.

No obstante, la eficacia de la guerra informativa rusa a nivel nacional también se apoyó en la explotación de factores culturales y simbólicos. En particular, se echaron mano de narrativas históricas profundamente arraigadas, como la alusión a la Gran Guerra Patria (Núñez Seixas, 2023), así como de la construcción de amenazas externas, presentando por ejemplo la expansión de la OTAN como un peligro inminente (Hoyos, 2022).

Asimismo, el acceso restringido a fuentes informativas independientes (Human Rights Watch, 2022) y las conexiones culturales con Ucrania fueron empleadas para justificar la intervención militar (Tipaldou y Casula, 2018). En conjunto, estos elementos contribuyeron a que, para 2025, las encuestas siguieran reflejando un apoyo mayoritario a lo que las autoridades continuaban denominando “operación militar especial” (Levada Center, 2025).

La efectividad de la guerra informativa rusa no puede concebirse como el resultado de acciones aisladas, sino como el fruto de un esfuerzo propagandístico prolongado y acumulativo. Desde al menos 2014, e incluso en periodos anteriores, el Estado ruso ha cultivado sistemáticamente una narrativa fundamentada en el victimismo histórico, la percepción de amenaza occidental y la glorificación del sacrificio patriótico. Estos elementos centrales han sido

reforzados en el sistema educativo, en los medios estatales y en las plataformas digitales bajo control gubernamental.

A escala internacional, la respuesta a la guerra informativa rusa potenciada por IAG ha sido notablemente heterogénea, observándose diferencias significativas entre las potencias occidentales y las regiones del Sur Global. En los países occidentales (la Unión Europea y Estados Unidos), los esfuerzos rusos de manipulación informativa registraron resultados mixtos. En las fases iniciales del conflicto, como durante la anexión de Crimea y la aparición de los primeros *deepfakes*, las tácticas de *Maskirovka* rusas generaron confusión y dudas sobre la realidad de los sucesos. No obstante, a partir de 2014 aumentó la conciencia en Occidente sobre estas técnicas de guerra informativa, lo que impulsó la creación de unidades especializadas dedicadas a contrarrestar la desinformación proveniente de Moscú (Giles, 2023).

Para 2022 estas operaciones informativas rusas mostraron un éxito limitado en cuanto a influir en las sanciones occidentales o en reducir el apoyo militar a Ucrania. Sin embargo, siguieron explotando la polarización interna de las sociedades occidentales para amplificar narrativas divisivas. A su vez, la eficacia del denominado *Control Reflexivo* disminuyó a medida que los gobiernos occidentales reforzaron su vigilancia frente a los intentos de manipulación rusa (Szyszczak, 2025; Secrétariat général de la défense et de la sécurité nationale, 2025).

En marcado contraste, la ofensiva informativa rusa potenciada por IAG ha tenido un éxito notable en el Sur Global. En regiones de África, Oriente Medio y América Latina, Rusia ha capitalizado el sentimiento anticolonial y antioccidental para presentarse como una alternativa a la influencia de Occidente. Las inversiones significativas en medios orientados a estos mercados, incluyendo *RT Arabic* y *RT en Español*, han producido resultados tangibles en términos de expansión de su influencia (Presl, 2024). En particular, América Latina ha demostrado ser un terreno especialmente fértil para la expansión de esta propaganda, situándola como una de las regiones donde Rusia ha alcanzado mayor impacto, junto con África Occidental y Central.

CONCLUSIÓN.

El conflicto ruso-ucraniano (2014-2025) ha evidenciado de manera clara cómo la inteligencia artificial generativa ha transformado las doctrinas tradicionales de engaño militar de Rusia, en particular la *Maskirovka* y el *Control Reflexivo*. La hipótesis de partida, que la incorporación progresiva de la IAG ha multiplicado la eficacia de las campañas rusas de manipulación informativa, se confirma ampliamente tras analizar las distintas fases del conflicto y su impacto en las audiencias ucraniana, rusa e internacional.

Durante la anexión de Crimea y el inicio del conflicto en el Donbás, Rusia aplicó una *Maskirovka* tradicional, basada en la ambigüedad operativa, la negación plausible y el uso intensivo de desinformación manual. Estas acciones ya mostraban un notable impacto estratégico, pero aún sin la escala que luego aportaría la automatización algorítmica.

Entre 2015 y 2022, en la denominada “pausa híbrida”, se registró una evolución relevante: Moscú incorporó sistemas automatizados de generación y distribución de contenidos, marcando la transición hacia un plano cognitivo, donde la percepción y el sentido común de las audiencias se convirtieron en objetivos operativos.

A partir de 2022, la invasión a gran escala consolidó esta transformación. La IAG permitió escalar masivamente las campañas de desinformación, generando contenidos falsos con rapidez y realismo, desde *deepfakes* hasta webs clonadas. Casos como *Doppelgänger* y la red *Pravda* muestran una integración avanzada entre doctrina y tecnología, orientada no solo a manipular audiencias humanas, sino también a contaminar sistemas automatizados como los grandes modelos de lenguaje.

Los efectos fueron desiguales según el público objetivo. En Ucrania, una experiencia acumulada desde 2014, combinada con respuestas institucionales y ciudadanas, favoreció una resiliencia significativa. En cambio, en el entorno mediático ruso, la eficacia de la desinformación generada con IAG fue elevada, debido al control estatal, la represión de la disidencia y la explotación de narrativas identitarias.

A escala internacional, los resultados han sido mixtos. En Occidente, una mayor preparación institucional redujo el impacto directo en lo político, aunque las campañas rusas lograron explotar fracturas sociales. En el Sur Global, la narrativa rusa tuvo mayor eco, apoyándose en discursos anticoloniales para posicionarse como contrapeso a las potencias occidentales.

Este análisis de la *Maskirovka* cognitiva algorítmica revela una mutación profunda de la guerra informativa. Ya no se trata solo de ocultar tropas o inducir confusión táctica, sino de construir entornos informativos diseñados para moldear percepciones, inducir decisiones erróneas y tomar el control narrativo del conflicto. La capacidad de producir realidades simuladas verosímiles con IA representa una ventaja estratégica que redefine el poder, incluso antes de un enfrentamiento físico.

Comprender esta evolución no es un ejercicio académico menor, sino una prioridad de seguridad. Las democracias deben prepararse ante amenazas que no destruyen infraestructuras, pero que alteran percepciones, socavan la confianza pública y condicionan decisiones políticas. Esta preparación requiere reforzar la alfabetización mediática y cognitiva, desarrollar tecnologías de detección de desinformación sintética y establecer marcos regulatorios

adecuados para el uso dual de la IAG.

En suma, este trabajo demuestra que la *Maskirovka*, lejos de quedar relegada al pasado soviético, se ha reinventado como herramienta estratégica clave en la guerra del siglo XXI. Su convergencia con la IAG marca una nueva era del engaño, donde controlar los algoritmos equivale a controlar el campo de batalla más decisivo: la mente.

Por fin, este análisis abre diversas líneas de investigación futuras. Una de ellas es el estudio comparado del uso de IAG en operaciones informativas por parte de otras potencias como China, Irán o EE. UU. Otra línea relevante es la evaluación de las contramedidas aplicadas por Ucrania, la UE o la OTAN, identificando buenas prácticas y factores de éxito. El estudio de la *Maskirovka* cognitiva algorítmica apenas ha comenzado. Comprenderla, medirla y anticiparla será fundamental para proteger la integridad informativa de las democracias y la autonomía crítica de las personas en un entorno crecientemente mediado por algoritmos opacos.

(4491)

BIBLIOGRAFÍA.

Alieva, I., Kloo, I. y Carley, K.M. (2024) "Analyzing Russia's propaganda tactics on Twitter using mixed methods network analysis and natural language processing: a case study of the 2022 invasion of Ukraine", *EPJ Data Science*, 13(42). Disponible en: <https://doi.org/10.1140/epjds/s13688-024-00479-w> [Consulta: 2-3-2025].

American Sunlight Project. (2025) *A Pro-Russia Content Network Foreshadows the Automated Future of Info Ops*. Disponible en: <https://static1.squarespace.com/static/6612cbdfd9a9ce56ef931004/t/67fd396818196f3d1666bc23/1744648558879/PK+Report.pdf> [Consulta: 2-3-2025].

Bouwmeester, A. J. H. (2021) "The Art of Deception Revisited – Part 2: The Unexpected Annexation of Crimea in 2014". *Militaire Spectator*, 15 de octubre. Disponible en: <https://militairespectator.nl/artikelen/art-deception-revisited-part-2-unexpected-annexation-crimea-2014> [Consulta: 2-3-2025].

Bugayova, N., Kagan, F.W. y Stepanenko, K. (2024) *Denying Russia's Only Strategy for Success*. Disponible en: <https://www.understandingwar.org/backgrounder/denying-russia%E2%80%99s-only-strategy-success#:~:text=lengths%20to%20which%20we%20are,pervasive%20in%20US%20discussions%20about> [Consulta: 2-3-2025].

Carrie Wong, J. (2020) "Russian agency created fake leftwing news outlet with fictional editors, Facebook says". *The Guardian*, 2 September. Disponible en: <https://www.theguardian.com/technology/2020/sep/01/facebook-russia-internet-research-agency-fake-news> [Consulta: 2-1-2025].

Giles, K. (2023) *Russian Cyber and Information Warfare in Practice: Lessons Observed from the War on Ukraine*. Disponible en: <https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice> [Consulta: 2-3-2025].

Golovchenko, Y. (2020) "Measuring the scope of pro-Kremlin disinformation on Twitter". *Humanities and Social Sciences Communications*, 7(176). Disponible en: <https://www.nature.com/articles/s41599-020-00659-9> [Consulta: 15-3-2025].

Gugushvili, A. (2025) "Russian public perceptions of the war in Ukraine: a paradox of optimism amid crisis". *Journal of Contemporary European Studies*. Disponible en: <https://www.tandfonline.com/doi/epdf/10.1080/14782804.2025.2472635?needAccess=true> [Consulta: 24-2-2025].

Helmus, T.C. y Holynska, K. (2024) *Ukrainian Resistance to Russian Disinformation: Lessons for Future Conflict*. Disponible en: https://www.rand.org/pubs/research_reports/RRA2771-1.html [Consulta: 2-3-2025].

Hoyos, A. (2023) "Rusia: El conflicto con Ucrania y la expansión de la OTAN. Una breve revisión histórica". *Tiempo y Espacio*, 41(79), pp. 95–120. Centro de Investigaciones Históricas Mario Briceño Iragorry. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=9545733> [Consulta: 11-3-2025].

Human Rights Watch (2022) *Rusia: Con la guerra, la censura alcanza nuevos niveles*. Disponible en: <https://www.hrw.org/es/news/2022/03/01/rusia-con-la-guerra-la-censura-alcanza-nuevos-niveles> [Consulta: 17-2-2025].

Levada Center (2025) *The conflict with Ukraine: attention, support, attitude to negotiations and possible concessions, opinion on the various terms of a peace agreement in February 2025*. Disponible en: <https://www.levada.ru/en/2025/03/10/the-conflict-with-ukraine-attention-support-attitude-to-negotiations-and-possible-concessions-opinion-on-the-various-terms-of-a-peace-agreement-in-february-2025/> [Consulta: 14-3-2025].

Linvill, D. y Warren, P. (2025) *Ukraine: The Past, Present, and Future of Russian Disinformation*. Disponible en: <https://www.lawfaremedia.org/article/ukraine--the-past--present--and-future-of-russian-disinformation> [Consulta: 13-1-2025].

Mahon, A. y Walker, S. (2024) "Russia's Digital Repression Landscape: Unraveling the Kremlin's Digital Repression Tactics". *The Journal of Illiberalism Studies*, 4(3), pp. 29–50. Disponible en: <https://www.illiberalism.org/russias-digital-repression-landscape-unraveling-the-kremlins-digital-repression-tactics/> [Consulta: 13-1-2025].

Martín, C. (2025) *Russian Propaganda Machine: Mechanics of Success*. Disponible en: <https://daviscenter.fas.harvard.edu/russian-propaganda-machine-mechanics-success> [Consulta: 2-3-2025].

Metz, R. (2022) "Facebook and YouTube say they removed Zelensky deepfake". *CNN*, 16 de marzo. Disponible en: <https://edition.cnn.com/2022/03/16/tech/deepfake-zelensky-facebook-meta/index.html> [Consulta: 2-3-2025].

Newport, A. y Jankowicz, N. (2025) *Russian networks flood the Internet with propaganda, aiming to corrupt AI chatbots*. Disponible en: <https://thebulletin.org/2025/03/russian-networks-flood-the-internet-with-propaganda-aiming-to-corrupt-ai-chatbots/> [Consulta: 11-1-2025].

Nimmo, B. et al. (2020) *Exposing Secondary Infektion: Forgeries, Interference, and Attacks on Kremlin Critics Across Six Years and 300 Sites and Platforms*. Graphika. Disponible en: <https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf> [Consulta: 17-2-2025].

Núñez Seixas, X.M. (2023) "Las fragmentadas memorias públicas de la Gran Guerra Patria en Ucrania (1991–2022)". *Política y Sociedad*, 60(3), pp. 1–12. Disponible en:

<https://revistas.ucm.es/index.php/POSO/article/view/84417/4564456567882>
[Consulta: 12-4-2025].

Osadchuk, R. (2024) *AI tools usage for disinformation in the war in Ukraine*. Disponible en: <https://dfrlab.org/2024/07/09/ai-tools-usage-for-disinformation-in-the-war-in-ukraine/> [Consulta: 11-1-2025].

Pearson, J. y Zinets, N. (2022) “Deepfake footage purports to show Ukrainian president capitulating”. *Reuters*, 17 de marzo. Disponible en: <https://www.reuters.com/world/europe/deepfake-footage-purports-show-ukrainian-president-capitulating-2022-03-16/> [Consulta: 2-3-2025].

Polyakova, A. (2019) *Five Years after the Revolution of Dignity: Ukraine's Progress / Russia's Malign Activities*. Disponible en: https://www.foreign.senate.gov/imo/media/doc/061819_Polyakova_Testimony.pdf [Consulta: 17-2-2025].

Potkin, F. y Lim, P. (2024) “Russia using generative AI to ramp up disinformation, says Ukraine minister”. *Reuters*, 16 de octubre. Disponible en: <https://www.reuters.com/technology/artificial-intelligence/russia-using-generative-ai-ramp-up-disinformation-says-ukraine-minister-2024-10-16/> [Consulta: 2-3-2025].

Presl, D. (2024) *Rusia está ganando la guerra de información global*. Disponible en: <https://www.rusi.org/explore-our-research/publications/commentary/russia-winning-global-information-war> [Consulta: 17-2-2025].

Seddon, M. (2014) “Documents Show How Russia's Troll Army Hit America”. *BuzzFeed News*, 2 June. Disponible en: <https://www.buzzfeednews.com/article/maxseddon/documents-show-how-russias-troll-army-hit-america> [Consulta: 29-1-2025].

Servicio Europeo de Acción Exterior (EEAS) (2025) *3rd EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats: Exposing the architecture of FIMI operations*. Disponible en: <https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf> [Consulta: 7-1-2025].

StopFake (2017) *Fakes Debunked by the StopFake Project Between 2014-2017: Narratives and Sources*. Disponible en: <https://www.stopfake.org/en/fakes-debunked-by-the-stopfake-project-between-2014-2017-narratives-and-sources/> [Consulta: 7-1-2025].

Szyszczyk, E. (2025) *Sanctions effectiveness: What lessons three years into the war on Ukraine?* Disponible en: <https://www.economicsobservatory.com/sanctions-effectiveness-what-lessons-three-years-into-the-war-on-ukraine> [Consulta: 17-2-2025].

Tipaldou, S. y Casula, P. (2018) “¿Justificaciones populistas de la guerra? La intervención rusa en el este de Ucrania”. *Revista CIDOB*, nº 119, pp. 135–160.

Disponible en: <https://www.cidob.org/publicaciones/justificaciones-populistas-de-la-guerra-la-intervencion-rusa-en-el-este-de-ucrania> [Consulta: 2-3-2025].

Weiss, M. y Pomerantsev, P. (2014) *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. Institute of Modern Russia. Disponible en: https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev__The_Menace_of_Unreality.pdf [Consulta: 9-5-2025].