ISSN: 2981-3506 EN LÍNEA
BOLETÍN N° 17
BOGOTÁ D.C. ENERO 2026

ESICI
ESCUELA DE INTELIGENCIA Y CONTRAINTELIGENCIA
"BRIGADIER GENERAL RICARDO CHARRY SOLANO"
INSTITUCIÓN DE EDUCACIÓN SUPERIOR

BOLETÍN ESTRATÉGICO
MULTIDISCIPLINAR

Entre Datos y Desinformación: La Inteligencia Artificial como Multiplicador de Amenazas Híbridas en América Latina

Escrito por:
Mario Linares Vásquez
Profesor Asociado Universidad de los Andes
ST RVA. Fuerza Aeroespacial Colombiana

RESUMEN:

El avance de la inteligencia artificial (IA) está transformando profundamente el panorama de seguridad internacional, particularmente en el ámbito de las amenazas híbridas. Estas amenazas combinan instrumentos militares, cibernéticos, informacionales, económicos y políticos con el objetivo de influir o desestabilizar sociedades sin recurrir necesariamente al conflicto armado directo. En América Latina, la creciente digitalización, la dependencia de plataformas tecnológicas globales y la polarización política generan un entorno propicio para que actores estatales y no estatales utilicen herramientas basadas en IA para amplificar campañas de desinformación, manipulación de opinión pública y operaciones de influencia.

ANTECEDENTES

Las amenazas híbridas se definen como fenómenos resultantes de la convergencia de diversos elementos que constituyen una amenaza compleja y multidimensional, operando a menudo por debajo del umbral del conflicto armado tradicional. Históricamente, **Latinoamérica** ha sido un escenario de choques ideológicos, pero en la última década, la digitalización ha permitido que estas confrontaciones se trasladen al ciberespacio y a la mente de los ciudadanos.

Por ejemplo, durante octubre de 2019, **Ecuador** vivió un proceso insurreccional donde el levantamiento de masas fue potenciado por narrativas digitales coordinadas, obligando al traslado de la sede de gobierno. De manera similar, en **Chile (2019)** se evidenció cómo las tácticas híbridas explotaron la indignación social para sembrar el caos y canalizar frustraciones contra la institucionalidad.

En **Colombia**, actores no estatales como las extintas FARC-EP y el ELN han adoptado estrategias de "todas las formas de lucha", incluyendo la manipulación de la protesta social y la propaganda digital para destruir la legitimidad de la Fuerza Pública; durante las protestas de 2019 y 2020, el uso masivo de redes sociales y medios digitales permitió coordinar movilizaciones y la difusión de noticias falsas que derivaron en actos vandálicos y desmanes.

CONTEXTO: IA Y EL DOMINIO COGNITIVO

En los estudios contemporáneos de seguridad internacional ha emergido el concepto de **guerra cognitiva**, que describe la competencia estratégica por influir en la forma en que las sociedades y personas perciben la información, interpretan la realidad y toman decisiones políticas. A diferencia de los enfoques tradicionales de conflicto, centrados en el control territorial o militar, la guerra cognitiva plantea que el **objetivo principal del conflicto es la mente humana**, es decir, los procesos cognitivos que determinan creencias, emociones y comportamientos colectivos. Esto es en particular válido porque las sociedades contemporáneas, altamente interconectadas y dependientes de ecosistemas digitales, son particularmente vulnerables a operaciones que buscan manipular percepciones y erosionar la confianza social.

Dentro de este marco conceptual, las **operaciones psicológicas (PSYOPS)** constituyen uno de los instrumentos principales de la guerra cognitiva. Estas operaciones consisten en actividades planificadas y destinadas a influir en emociones, percepciones y comportamientos de audiencias específicas, con el fin de apoyar objetivos políticos o estratégicos. Históricamente, estas prácticas han incluido propaganda, campañas de información y manipulación narrativa en contextos de conflicto o competencia geopolítica.

La evolución del entorno digital ha ampliado significativamente el alcance de las operaciones psicológicas. La automatización, los algoritmos, redes sociales, y el análisis masivo de datos permiten manipular conversaciones públicas mediante *bots*, redes coordinadas y segmentación de audiencias. Por lo tanto, la guerra cognitiva representa una evolución de las operaciones informacionales tradicionales, ahora potenciadas por tecnologías digitales que incrementan su escala y efectividad de influencia.

ESICI
ESCUELA DE INTELIGENCIA Y CONTRAINTELIGENCIA "BRIGADIER GENERAL RICARDO CHARRY SOLANO" INSTITUCIÓN DE EDUCACIÓN SUPERIOR

Entre Datos y Desinformación: La Inteligencia Artificial como Multiplicador de Amenazas Híbridas en América Latina

La incorporación de IA en el ecosistema informacional ha ampliado significativamente las capacidades asociadas a las amenazas híbridas. Los sistemas basados en IA permiten automatizar la producción de contenido persuasivo, analizar grandes volúmenes de datos sociales y optimizar mensajes de influencia en tiempo real. Gracias a los recientes avances de la **IA generativa** cualquier persona puede crear rápidamente textos, imágenes, audios, voz y videos sintéticos que pueden emplearse en campañas de desinformación.

La IA no solo amplía la escala de las operaciones sicológicas, también introduce nuevas capacidades asociadas al concepto de **guerra inteligente**. Mediante el análisis masivo de datos, se puede realizar **microsegmentación conductual** para identificar vulnerabilidades emocionales y dirigir ataques cognitivos de precisión (personalizados); por otro lado, a partir del análisis de datos de interacción digital, es posible identificar perfiles psicológicos de usuarios y diseñar mensajes adaptados a sus emociones, creencias o predisposiciones políticas.

A esto se suma la **amplificación algorítmica** mediante *bots/agentes* y redes coordinadas que generan percepciones artificiales de consenso y refuerzan "cámaras de eco" en plataformas digitales. Los sistemas basados en IA pueden ejecutar ciclos de retroalimentación en tiempo real para descubrir y escalar nuevas formas de lucha, optimizando las estrategias de desinformación más rápido de lo que los analistas humanos pueden detectar o contrarrestar.

Por otro lado, usando IA se puede **optimizar estrategias de influencia en tiempo real y de forma adaptativa/personalizada,** así como automatizar técnicas de ingeniería social mediante ataques de *phishing* a gran escala (de calidad humana), o con agentes de IA conversacionales capaces de interactuar con usuarios para influir gradualmente en sus percepciones y comportamientos. La falsificación de identidades mediante contenido multimedia de alta calidad y realismo (p. ej., *deepfakes*) ya es una posibilidad al alcance de todos.

En consecuencia, las amenazas híbridas contemporáneas ya no se limitan a acciones militares o cibernéticas, sino que incluyen la manipulación sistemática del entorno informacional y cognitivo de las sociedades.

IMPLICACIONES Y RIESGOS

La integración de inteligencia artificial en operaciones psicológicas y de información genera varias implicaciones estratégicas relevantes. En primer lugar, **reduce significativamente los costos operativos** asociados a campañas de influencia. Actores estatales y no estatales pueden producir grandes volúmenes de contenido persuasivo mediante sistemas automatizados, lo que facilita la ejecución prolongada de campañas de desinformación.

En segundo lugar, la IA incrementa la **precisión de las operaciones psicológicas**. La segmentación algorítmica permite dirigir mensajes a audiencias específicas con base en variables demográficas, ideológicas o emocionales. Esto aumenta la efectividad de las narrativas diseñadas para polarizar sociedades, erosionar la confianza institucional o influir en procesos electorales.

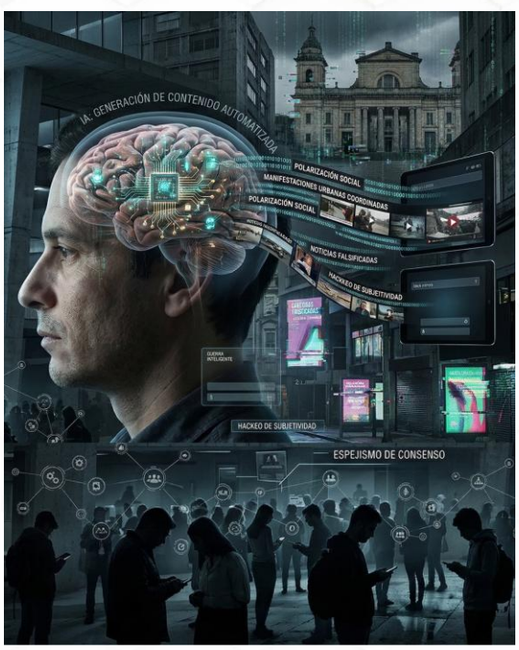

Imagen generada con IA

Gracias a la **amplificación coordinada de narrativas** mediante redes de bots y cuentas falsas, se pueden manipular tendencias en redes sociales, crear percepciones artificiales de consenso o intensificar conflictos discursivos en espacios digitales. La IA también contribuye a aumentar la **opacidad y dificultad de atribución** de las operaciones sicológicas; las campañas de influencia pueden ejecutarse mediante infraestructuras distribuidas que dificultan identificar a los actores responsables y el lugar de origen, lo que complica las respuestas diplomáticas o legales.

La integración de la IA en las amenazas híbridas y la guerra cognitiva trasciende los métodos convencionales de desestabilización, planteando riesgos sistémicos que afectan desde la integridad biológica del individuo hasta la estabilidad misma de los estados democráticos Al combinar menores costos de las operaciones de información, con mayor precisión en la segmentación sicológica, amplificación coordinada de narrativas, y mayor dificultad de atribución, aparecen desafíos para la gobernanza democrática, la integridad electoral y la confianza institucional.

El riesgo más profundo a nivel macro es la **fragmentación de la sociedad y la ruptura del contrato social**. La guerra cognitiva no busca necesariamente la derrota militar física, sino lograr que el adversario se destruya a sí mismo, desde adentro, mediante el colapso interno por la inercia de sus organizaciones, sin recurrir a la fuerza física. En este escenario, la IA permite una **militarización de la opinión pública** que socava la unidad social y daña la confianza en el sistema político.

BOLETÍN ESTRATÉGICO MULTIDISCIPLINAR
BOGOTÁ D.C. ENERO 2026
BOLETÍN N° 17
ISSN: 2981-3506 EN LÍNEA

Otro riesgo es la proliferación de contenido manipulado por IA, como los *deepfakes*, que genera un estado de sospecha constante donde los ciudadanos pueden terminar **desconfiando incluso de la información verídica**; a este fenómeno se le conoce como el **"dividendo del mentiroso"**. Esta sobrecarga informativa de contenido falso agota psicológicamente a los receptores y anula su capacidad de discernimiento.

La IA potencia la explotación de las **vulnerabilidades biológicas y psicológicas** del cerebro humano. Mediante el uso de datos masivos, se pueden ejecutar ataques de precisión que aprovechan **sesgos cognitivos**, como el de confirmación, para manipular percepciones y forzar decisiones irracionales que pueden llevar a una escalada de conflictos no deseada. Por otro lado, la IA potencia la creación de dispositivos y plataformas "inteligentes" diseñados para ser adictivos, con el fin de asegurar que la vida y la realidad del individuo permanezcan dentro de ellos (incluso mundos digitales) para ser controladas con mayor facilidad. Los riesgos asociados incluyen un aumento dramático de la **adicción a las redes sociales, ansiedad y depresión**, especialmente en jóvenes. A largo plazo, esto puede resultar en la **desensibilización de la población**, erosionando la voluntad y disposición de los ciudadanos para defender su nación ante una emergencia nacional.

En resumen, la IA aplicada a las amenazas híbridas no solo busca ganar una batalla informativa, sino **hackear la subjetividad humana** para provocar parálisis institucional y desorden social crónico, desafiando las estructuras de seguridad tradicionales que no están preparadas para operar en este nuevo campo de batalla invisible.

Imagen generada con IA

AFECTACIONES PARA COLOMBIA

Colombia se encuentra en una posición de vulnerabilidad crítica frente a la guerra cognitiva potenciada por IA. Nuestro país tiene características que pueden ser explotadas dentro de este entorno de amenazas híbridas. Entre ellas se destacan la alta penetración de redes sociales, la persistente polarización política/social y la presencia de actores armados ilegales que utilizan plataformas digitales para propaganda o reclutamiento.

El uso de tecnologías de manipulación informacional podría afectar procesos electorales, exacerbar tensiones sociales o debilitar la confianza pública en instituciones del Estado. La persistente polarización política y social genera un entorno en el cual las operaciones psicológicas pueden explotar tensiones existentes para amplificar divisiones internas. Narrativas diseñadas para desacreditar instituciones, manipular percepciones sobre procesos electorales o exacerbar conflictos sociales podrían difundirse con rapidez en ecosistemas digitales altamente interconectados. Además, actores armados ilegales y organizaciones criminales han demostrado capacidad para utilizar plataformas digitales con fines propagandísticos o de reclutamiento. La incorporación de herramientas de IA podría fortalecer estas capacidades mediante la automatización de mensajes, la segmentación de audiencias vulnerables o la creación de contenido manipulativo.

En este contexto, el **fortalecimiento de la resiliencia cognitiva** se vuelve una prioridad estratégica. Esto implica desarrollar capacidades institucionales de monitoreo de desinformación, promover alfabetización digital crítica en la ciudadanía y establecer marcos regulatorios que fomenten mayor transparencia/trazabilidad algorítmica en plataformas digitales. La construcción de resiliencia cognitiva en Colombia exige una transición desde el enfoque tradicional de seguridad hacia uno que priorice la **soberanía mental** de sus ciudadanos y la robustez de sus instituciones frente a la manipulación algorítmica y la guerra psicológica, reconociendo que la defensa ya no es puramente militar, sino también psicológica, social y digital.

REFERENCIAS

1. Beauchamp-Mustafaga, N. (2024). *Exploring the Implications of Generative AI for Chinese Military Cyber-Enabled Influence Operations*. RAND Corporation.
2. Bernal, A., et al. (2020). *Fall 2020 Cognitive Warfare: An Attack on Truth and Thought*. Johns Hopkins University & NATO Innovation Hub.
3. Bradshaw, S. & Howard, P. N. (2018). *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation*. Oxford Internet Institute.
4. du Cluzel, F. (2021). *Cognitive Warfare*. NATO Innovation Hub.
5. Fonseca-Ortiz, T. L., Sierra-Zamora, P. A. & Luque-Ochoa, C. E. (2022). *Guerras irrestricta e híbrida en los desafíos a la seguridad y defensa nacionales*. Sello Editorial ESDEG.
6. Hernández Vargas, J. R. & Freitas de Souza Lima, L. (2023). *La guerra cognitiva y nuevas formas de amenazas a la paz y a la seguridad y la defensa nacionales*. KAS / ESDEG.
7. Luque Juárez, J. M. (2019). *Las amenazas híbridas contra las democracias abiertas*. Estudios en Seguridad y Defensa, **14**(27), 115-137.
8. Howard, P.N., Woolley, S.C. (2018). *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. Oxford Academic.
9. Blatny, J.M., Søndergaard S. (2025). *Cognitive Warfare NATO - Chief Scientist Research Report*. NATO Science and Technology Organization.
10. European Centre of Excellence for Countering Hybrid Threats. (2020). *The Landscape of Hybrid Threats: A Conceptual Model.*
11. Aral, S. (2020). *The Hype Machine: How Social Media Disrupts Our Elections, Our Economy, and Our Health—and How We Must Adapt*. Crown Currency.

BOLETÍN ESTRATÉGICO MULTIDISCIPLINAR
BOLETÍN N° 17
BOGOTÁ D.C. ENERO 2026
ISSN: 2981-3506 EN LÍNEA