La Inteligencia Artificial como herramienta de propaganda: un análisis de su uso por grupos terroristas en el escenario geopolítico actual.

Mayor (FAC) Jorge Hernando Gamboa Paternina

Artículo para optar al título profesional:

Magíster en Estrategia y Geopolítica

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

DATOS GENERALES		
Nombre del estudiante	**:**	Mayor (FAC) Jorge Hernando Gamboa Paternina
Identificación	**:**	80197244
Programa académico	**:**	Maestría en Estrategia y Geopolítica
Tutor metodológico	**:**	Juan Carlos Aristizábal Murillo
Tutor temático	**:**	Andrea Katherine Díaz Cante
Fecha de entrega	**:**	27/08/2025
Extensión	**:**	8.193 palabras

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

La Inteligencia Artificial como herramienta de propaganda: un análisis de su uso por grupos terroristas en el escenario geopolítico actual.

Artificial Intelligence as a propaganda tool: an analysis of its use by terrorist groups in the current geopolitical scenario.

Jorge Hernando Gamboa Paternina[1]

[1] Mayor de la Fuerza Aeroespacial Colombiana. Candidato a Magíster en Estrategia y Geopolítica, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Administración Aeronáutica, Escuela Militar de Aviación "Marco Fidel Suarez", Magíster Estudios Avanzados en Terrorismo, Universidad Internacional de la Rioja, España. Contacto: jorge.gamboa@esdeg.edu.co.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

Resumen: Este artículo analiza el uso de la Inteligencia Artificial (IA) por parte de grupos terroristas como herramienta para la producción y difusión de propaganda. Mediante un enfoque cualitativo y de revisión documental, se examinan las tecnologías utilizadas, sus efectos en la percepción pública, la radicalización y el reclutamiento, así como sus implicaciones geopolíticas. Se evidencia que la IA permite a estos grupos automatizar mensajes, manipular emociones y segmentar audiencias con alta precisión, intensificando la guerra cognitiva y los procesos de desinformación. Además, se identifican desafíos normativos y de gobernanza frente a esta amenaza, lo que plantea la necesidad de respuestas coordinadas entre Estados y organismos multilaterales para prevenir el uso malicioso de estas tecnologías emergentes.

Palabras clave: Ciberseguridad; desinformación; inteligencia artificial; propaganda; radicalización; terrorismo.

Abstract: This article analyses the use of artificial intelligence (AI) by terrorist groups as a tool for producing and disseminating propaganda. Through a qualitative approach and documentary review, it examines the technologies employed, their effects on public perception, radicalization, and recruitment, as well as their geopolitical implications. The findings show that AI enables these actors to automate messages, manipulate emotions and segment audiences with high precision, intensifying cognitive warfare and disinformation processes. Additionally, the study identifies regulatory and governance challenges in addressing this threat, highlighting the need for coordinated responses among states and multilateral organizations to prevent the malicious use of these emerging technologies.

Keywords: artificial intelligence; geopolitics; propaganda; radicalization; recruitment; terrorism.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

Introducción

La Inteligencia Artificial (IA) ha transformado numerosos sectores en la sociedad, desde la industria hasta la comunicación. Sin embargo, también se ha convertido en una herramienta clave para actores no estatales, incluidos grupos terroristas, quienes han aprovechado sus capacidades para amplificar la propaganda y manipular percepciones a nivel mundial. El uso de este tipo de tecnología por parte de los grupos terroristas plantea serios desafíos en el escenario político actual, lo que ha llevado a modificar estrategias de radicalización, reclutamiento y la percepción del público.

La relación entre la inteligencia artificial y el terrorismo ha cobrado importancia en el contexto geopolítico actual, donde la información y la guerra cognitiva juegan un papel significativo. El desarrollo y avances en la IA han permitido a los grupos terroristas desarrollar campañas de propaganda sofisticadas, empleando algoritmos que permiten personalizar mensajes, manipular imágenes y videos, difusión de información en las redes sociales y demás plataformas digitales a una velocidad y precisión sin precedentes. Este fenómeno no sólo amplifica la capacidad de influencia de estos grupos, sino que también plantea desafíos para los Estados y organismos internacionales en materia de seguridad y estabilidad global. (Weimann, 2004; Citron & Chesney, 2019)

El estudio de cómo los grupos terroristas emplean la IA en sus estrategias de propaganda es fundamental para comprender el impacto en cómo el público lo percibe, en la radicalización y el reclutamiento. En el panorama actual, de un mundo interconectado, en el cual la información fluye sin fronteras, resulta esencial para examinar cómo la inteligencia artificial influye en la creación y difusión de narrativas extremistas. Es

importante entender su capacidad de influir en la percepción y la respuesta emocional de las poblaciones objetivo. Un análisis de las dimensiones geopolíticas de este fenómeno permitirá prepararse para potenciales escenarios de riesgo y desarrollar mecanismos más efectivos tanto para prevenir y contener estas amenazas.

En este sentido, la pregunta central que guía el presente análisis es ¿cómo afecta el uso de la inteligencia artificial por parte de grupos terroristas el escenario geopolítico actual? Para poder dar respuesta a este interrogante, el presente artículo tiene como objetivo general analizar cómo los grupos terroristas emplean la IA como herramienta de propaganda y cómo esto influye en las relaciones geopolíticas hoy en día.

Para esto, se examinarán tres aspectos fundamentales. En un inicio, se identificarán las principales formas en que estos grupos utilizan la inteligencia artificial para generar contenido propagandístico y distribuirlo de manera eficaz. Posteriormente, se examinará la influencia de estas tecnologías en la percepción pública, la radicalización de individuos y el reclutamiento de nuevos integrantes, tanto a nivel regional como global. Por último, se establece el alcance y las implicaciones geopolíticas de la integración de la inteligencia artificial en las estrategias comunicativas de los grupos terroristas, considerando cómo esto afecta la seguridad internacional.

Teniendo en cuenta el avance tecnológico y la sofisticación en las estrategias de propaganda utilizadas por los grupos terroristas, es crucial comprender los desafíos emergentes en el ámbito de la seguridad y la estabilidad global. La combinación de tecnologías avanzadas con las estrategias terroristas, no solo desafía los marcos tradicionales de seguridad, sino que también redefine el papel de los Estados.

Metodología

Para realizar el análisis del impacto geopolítico del uso de la inteligencia artificial en la propaganda terrorista, este artículo adopta un método de investigación cualitativa, que según Taylor y Bogdan (1987) es un enfoque que implica el estudio directo de los escenarios y sujetos en su entorno natural, intentando comprender e interpretar los fenómenos de acuerdo con los significados que las personas le otorgan. Para este caso, se busca interpretar el uso de las herramientas de IA en la propaganda y su impacto en la geopolítica actual, a través de análisis documental como lo son informes gubernamentales, estudios académicos y publicaciones especializadas en terrorismo, propaganda digital e inteligencia artificial.

Para complementar el análisis se toma un enfoque descriptivo, ya que permite explorar detalladamente este fenómeno sin necesidad de establecer relaciones de causa y efecto. El objetivo es describir de manera sistemática cómo se emplean herramientas de IA como bots, deepfakes y algoritmos en las campañas de propaganda terrorista, y entender cómo están moldeando la opinión pública y transformando las dinámicas de poder actual. Este tipo de enfoque es especialmente relevante en estudios sociales y políticos, como lo plantea Mejía Jiménez (2012), quien resalta que el enfoque descriptivo en las ciencias sociales permite evidenciar las condiciones institucionales y sociopolíticas que configuran los fenómenos públicos, lo que permite comprender mejor el contexto en el que estas prácticas aparecen y evolucionan.

La recolección y análisis de información documental se basa en una técnica de análisis documental. Este método recopila, selecciona e interpreta información proveniente

de fuentes secundarias relevantes como artículos académicos, informes especializados de seguridad, publicaciones de organismos internacionales y estudios de caso sobre propaganda terrorista digital. Esta técnica, enmarcada dentro del enfoque cualitativo y descriptivo, permite identificar patrones narrativos y estratégicos en el uso de la IA como herramienta propagandística. Como señalan Guevara et al. (2020), el análisis documental consiste en "revisar fuentes disponibles en la red, cuyo contenido sea actual, publicado en revistas de ciencia y ajustado al propósito del tema, con contenido oportuno y relevante desde el punto de vista científico" (p.166). Esta aproximación metodológica facilita la identificación de patrones narrativos y estratégicos en el uso de la IA como herramienta propagandística por parte de organizaciones terroristas. Así, se fortalece la validez interpretativa del estudio y se propicia un análisis riguroso del fenómeno observado.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

Sistemas de Inteligencia Artificial como catalizadores de propaganda terrorista

En este apartado se identifican las principales formas en que los grupos terroristas emplean herramientas de inteligencia artificial (IA) para la creación y difusión de propaganda. Para esto, se entiende que el terrorismo, como actividad ilegal y criminal, frecuentemente se justifica bajo argumentos ideológicos como la oposición al capitalismo global y motivaciones religiosas, entre otras. En muchos casos, los líderes de grupos terroristas suelen incitar a la violencia dirigida no solamente contra figuras estatales, sino también contra instituciones financieras y población que respaldan las políticas antiterroristas. Esta perspectiva extremista se ha potenciado con el aprovechamiento de las innovaciones tecnológicas, tanto en el campo armamentístico como en el digital, lo que incluye posibles ataques a centros nucleares o laboratorios biológicos con intenciones destructivas a gran escala.

La evidencia reciente recogida por investigaciones periodísticas indica que tanto ISIS como organizaciones de extrema derecha están adaptando con rapidez sus estructuras propagandistas al uso de IA generativa[2]. Los grupos extremistas han utilizado generadores de texto como ChatGPT para crear manifiestos, scripts de video y discursos de reclutamiento, mientras que plataformas de código abierto son empleadas para producir imágenes hiperrealistas. Esto reduce los costos logísticos de producción y diversifica los formatos

[2] La inteligencia artificial generativa es un tipo de IA que se centra en crear contenido nuevo a partir de datos existentes. Utiliza distintos modelos como las redes generativas adversariales (GANs) y los transformadores para generar textos, imágenes, música y otros tipos de contenido (Cortés, 2024)

comunicacionales, permitiendo una personalización más sofisticada del mensaje. Asimismo, estos grupos promueven guías para el uso de herramientas IA entre simpatizantes, con instrucciones claras para evadir la moderación automatizada de contenidos en plataformas como X (antes Twitter), Reddit o Telegram.

Igualmente, el análisis de la narrativa audiovisual empleada por el Estado Islámico revela un uso sofisticado de recursos visuales y simbólicos que hoy pueden ser amplificados por tecnologías de inteligencia artificial. Según Rodríguez (2017), la difusión de videos por parte de este grupo no solo representa actos de violencia, sino que estructuran una conceptualización del terror a través de la edición, el ritmo visual y el encuadre estético, diseñados para provocar fascinación y temor (p.109). La incorporación de la IA generativa en estos procesos permite automatizar y personalizar el contenido según la audiencia objetivo, lo que refuerza aún más el poder emocional de la propaganda extremista.

En particular, el ciberterrorismo ha generado gran preocupación en los últimos años, ya que ha emergido como una seria amenaza para la seguridad de los Estados, interfiriendo en el funcionamiento de instituciones estatales y financieras, además de poner en riesgo tanto a la sociedad en general como a personas específicas (Rakić, 2009). Los grupos terroristas han extendido su guerra también al ciberespacio, aprovechando las características de internet como un espacio de anonimato, poco regulado y de fácil acceso. Esta nueva dimensión ha sido documentada por Weimann (2006), quien identificó al menos ocho formas que los grupos terroristas utilizan en la red para avanzar en su causa, incluyendo entre ellas la guerra psicológica, el reclutamiento, establecimiento de redes de cooperación, recaudación de fondos y difusión de propaganda. (p. 52)

Los grupos terroristas administran miles de portales web dirigidos a diferentes públicos: desde sus actuales seguidores y posibles adeptos, hasta la opinión pública internacional y la población considerada como enemiga. Para evadir la vigilancia, estos sitios cambian frecuentemente de dirección electrónica o apariencia, lo que convierte la propaganda terrorista en línea en un fenómeno extremadamente dinámico. Si bien es fundamental proteger a las sociedades del ciberterrorismo, es importante considerar los riesgos que ciertas medidas, que, en nombre de la seguridad, pueden comprometer derechos fundamentales como las libertades civiles, la privacidad y el libro flujo de la información (Weimann G. , Terror on the internet : the new arena, the new challenges, 2006).

La incorporación de herramientas de IA por parte de grupos terroristas en sus estrategias comunicacionales para optimizar sus campañas de propaganda, se ha visto evidenciada tal y como ocurrió a mediados de 2023, cuando un grupo simpatizante del Estado Islámico difundió varios carteles con imágenes generadas por IA, así como grupos de extrema derecha produjeron una "guía para la guerra memética", en el cual se ofrecían consejos para la utilización de herramientas de IA generativa en la creación y difusión de memes extremistas (Nelu, 2024). El terrorismo ha encontrado en la comunicación digital y tecnologías emergentes un poderoso aliado. Se está presenciando una transformación preocupante en la naturaleza de los conflictos: los grupos violentos ya no solamente manipulan opiniones, sino que han incorporado el uso de algoritmos para distorsionar cómo las personas ven y entienden la realidad. En este sentido, la IA se ha convertido en una herramienta aliada de los grupos terroristas, que les permite dar mayor fuerza a su mensaje,

amplificar su alcance y, lo que es más inquietante, desarrollar técnicas cada vez más sofisticadas para influenciar psicológicamente en las audiencias objetivo.

Una de las estrategias más impactantes ha sido el uso de deepfakes, esta tecnología, basada en algoritmos de IA, permite crear contenido audiovisual sintético que reproduce de manera extremadamente convincente la apariencia física y vocal de personas reales. La capacidad de estos sistemas para generar imitaciones prácticamente indistinguibles de material auténtico ha transformado radicalmente el panorama de la manipulación informativa.

La propagación de estos contenidos falsificados se realiza principalmente a través de plataformas de redes sociales, donde se presentan como información periodística de última hora o comunicados oficiales. Esta estrategia de distribución aprovecha la velocidad de consumo informativo en el entorno digital, en el cual los usuarios frecuentemente comparten contenido sin verificar su autenticidad.

El impacto psicológico y social de este material digital fabricado es considerable. Al simular declaraciones de figuras políticas, militares o de autoridad, los deepfakes logran múltiples objetivos desestabilizadores: la generación de estados de alarma en la población, la polarización de la opinión pública y el deterioro sistemático de la confianza ciudadana hacia las instituciones y sus representantes (Citron & Chesney, 2019; Weimann, 2006).

La aplicación práctica de esta tecnología por parte de grupos terroristas ha quedado en evidencia en diversos incidentes. Durante 2024, la organización terrorista ISIS desarrolló una campaña de desinformación basada en la creación de material audiovisual que imitaba

características visuales y de producción de medios reconocidos internacionalmente como CNN y Al Jazeera. Estos contenidos fabricados difundieron narrativas falsas sobre supuestas expansiones territoriales del grupo en el continente africano, incorporando elementos gráficos oficiales y estándares de producción que los hacían virtualmente indistinguibles de las transmisiones legítimas (Ayad, 2014).

Un segundo caso ilustrativo se registró después del atentado perpetrado en el complejo de entretenimiento Crocus City Hall en Moscú. En este contexto, circuló un video deepfake que presentaba al secretario del Consejo de Seguridad de Ucrania, Oleksiy Danilov, aparentemente confesando la autoría del ataque terrorista. La sofisticación técnica del material resultaba particularmente preocupante, ya que había sido construido utilizando fragmentos de intervenciones televisivas previas del funcionario en el canal ucraniano 1+1, lo que le otorgaba una apariencia de autenticidad considerable. (Perelló, 2014).

Otra práctica habitual es el uso de bots automatizados, que son como ejércitos invisibles de cuentas falsas que inundan las redes sociales. Estos bots están programados para interactuar en redes sociales, responder comentarios e incluso mantener conversaciones que parecen totalmente naturales, en ocasiones, su intervención es tan natural que los usuarios no perciben que están interactuando con un algoritmo lo que permite reforzar ideas propagandísticas y manipular el flujo de la información y así generar la idea de consenso entre el público. Este fenómeno ha sido documentado en campañas de radicalización en línea y resulta especialmente peligroso por su capacidad de viralizar contenido extremista sin la intervención humana de manera directa (Weimann G. , Terror on the internet : the new arena, the new challenges, 2006). Por ejemplo, el Estado Islámico ha implementado redes

automatizadas en plataformas como Twitter y Telegram para diseminar masivamente contenido propagandístico, incluyendo enlaces a material audiovisual, particularmente durante operaciones militares en Siria, con el propósito de preservar su huella digital frente a los intentos de bloquear sus cuentas (Berger & Morgan, 2015).

De acuerdo con el informe *The ISIS Twitter Census* desarrollado por Berger y Morgan, al menos 6,216 cuentas de apoyo a ISIS fueron identificadas empleando tecnología de bots o spam para la difusión de contenido, y aproximadamente el 20% del total de tuits analizados se generaron usando aplicaciones automatizadas (p. 9). El informe también evidencia que ISIS organizó a sus usuarios más activos, conocidos como *mujtahidum,* quienes tuitearon en ráfagas cortas y masivas para posicionar hashtags y amplificar su mensaje (Berger & Morgan, 2015, pág. 25). De igual manera, ISIS implementó una campaña digital conocida como "Salil al-Sawarim" (El choque de espadas), la cual se caracterizó por la difusión de videos e imágenes en extremo violentos con mensajes religiosos a través de redes sociales, esta campaña estaba específicamente dirigida al reclutamiento de jóvenes de origen musulmán residentes en occidente, mediante la romantización del sacrificio personal y la participación en conflictos bajo la retórica del deber religioso. (Greenberg, 2016)

La IA también ha acelerado y optimizado los procesos de radicalización. Chatbots como Asharq al-Awsat, utilizados por ISIS, emplean procesamiento de lenguaje natural (PLN) para identificar vulnerabilidades psicológicas en tiempo real, reduciendo el ciclo de radicalización de meses a apenas 72 horas en casos documentados Weimann et al. (2024) . La IA también ha acelerado y optimizado los procesos de radicalización. Estudios recientes demuestran que grupos terroristas como ISIS han implementado chatbots y plataformas de

IA generativa para diseminar propaganda y realizar reclutamiento (Weimann et al., 2024). El sentiment analysis, también denominado minería de opiniones, constituye una aplicación del PLN que integra algoritmos de aprendizaje automático para examinar contenido textual y establecer la orientación emocional manifestada por el autor. Esta tecnología permite a los grupos extremistas identificar vulnerabilidades psicológicas en las audiencias objetivo y sincronizar el envío de contenidos en momentos de máxima receptividad (Alotaibi, 2019). Como señala la investigación del National Institute of Justice sobre trayectorias de radicalización (Jayasumana & Klausen), estos desarrollos representan una transformación en los técnicas de reclutamiento, donde la escalabilidad y precisión superan considerablemente los técnicas (Alotabi, 2019) (Klausen, 2020) tradicionales.

La evolución de las capacidades de IA ha permitido a las organizaciones terroristas sofisticar considerablemente sus estrategias comunicativas y de reclutamiento a través de técnicas avanzadas de personalización y segmentación de audiencias. Como lo documenta Gomes-Gonçalves (2022), estos grupos han desarrollado una capacidad sin precedentes para procesar y analizar volúmenes masivos de datos provenientes de múltiples fuentes digitales, incluyendo plataformas de redes sociales, historiales de navegación, patrones de interacción en línea y metadatos comportamentales.

Esta capacidad analítica les permite identificar con precisión algorítmica patrones complejos de comportamiento, preferencias personales, estados emocionales, vulnerabilidades psicológicas y predisposiciones ideológicas de diferentes segmentos de la población digital. La aplicación de técnicas de machine learning y procesamiento de lenguaje natural facilita la construcción de perfiles psicográficos detallados que van más allá de las

características demográficas tradicionales, incorporando elementos como la receptividad a ciertos tipos de narrativas, momentos de mayor vulnerabilidad emocional, y factores contextuales que aumentan la susceptibilidad a mensajes extremistas.

La implementación de estas técnicas trasciende a la mera eficiencia comunicativa, transformando fundamentalmente la naturaleza de los procesos de radicalización. La personalización algorítmica permite crear ecosistemas informativos cerrados que refuerzan progresivamente las predisposiciones extremistas, utilizando técnicas de refuerzo positivo y validación social artificial. Además, la capacidad de optimización continua de estos sistemas, mediante el análisis de métricas de engagement y conversión, permite a los grupos terroristas refinar constantemente sus estrategias de reclutamiento, aumentando exponencialmente su efectividad operacional y expandiendo su alcance geográfico y demográfico de una manera sin precedentes en la historia del terrorismo contemporáneo.

El auge de la IA generativa ha abierto una nueva etapa en la difusión de propaganda extremista. Herramientas que permiten generar imágenes, videos y voz facilitan la rápida creación de escenarios con alta carga emocional y narrativa detallada. Según señala (Nelu, 2024), organizaciones como Al-Qaeda, ISIS y Hezbolla ya están implementando la IA generativa para producir contenido falso, incluyendo imágenes manipuladas de víctimas infantiles que buscan provocar indignación y odio, así como videos que presentan versiones distorsionadas de conflictos armados. Este tipo de material se difunde y circula con facilidad en redes sociales, llegando de manera masiva a diferentes audiencias lo que les permite amplificar su efecto e impacto emocional.

Finalmente, los grupos terroristas implementan la IA para ocultar su identidad y evitar los mecanismos de control de contenido. A través del uso de redes neuronales que transforman palabras clave o reformulan los contenidos textuales, logran eludir los sistemas de filtros automatizados que implementan las plataformas digitales. Así mismo, desarrollan operaciones para la creación masiva de cuentas falsas para reemplazar aquellas que son bloqueadas, manteniendo así activa la continuidad en la difusión de su propaganda (Castells, 2009; Weimann, 2006).

Estas formas de intervención demuestran cómo la IA ha expandido significativamente el repertorio de capacidades comunicacionales a disposición de los grupos terroristas, proporcionándoles herramientas que integran altos niveles de anonimato, eficacia operativa y complejidad técnica. De igual manera su empleo constituye un desafío para los sistemas de seguridad nacional y los sistemas democráticos modernos, obligando a reconsiderar los mecanismos de control y defensa en el ciberespacio.

Grupo Terrorista	Tipo de Inteligencia Artificial Usada	Descripción de las Acciones Realizadas con la Inteligencia Artificial
Estado Islámico (IS/ISIS/Daesh)	Bots/Cuentas Automatizadas	Se utilizan en Telegram para facilitar y potenciar las actividades de influencia, facilitando la amplificación de contenido y el cultivo de comunidades
		En Telegram, estos bots desempeñan tres funciones clave: publicar contenido, moderar discusiones y actuar como guardianes (gatekeepers).
		Se emplearon redes automatizadas en Twitter y Telegram para diseminar masivamente contenido propagandístico y enlaces a material audiovisual, especialmente durante operaciones militares en Siria, buscando preservar su huella digital frente a los bloqueos de cuentas.
	IA Generativa / Imágenes (general)	Hay evidencia de experimentación temprana con servicios de IA generativa. Un grupo simpatizante del IS difundió varios carteles con imágenes generadas por IA.

	IA Generativa / Generador de contenido	Un grupo de apoyo técnico pro-IS compartió una guía en árabe aconsejando a las redes del IS sobre el uso seguro de un generador de contenido de IA.
	IA Generativa / LLMs (Modelos de Lenguaje Largo)	Han usado generadores de texto (como ChatGPT) para crear manifiestos, scripts de video y discursos de reclutamiento.
	Deepfakes / Medios Sintéticos	Se ha documentado que el 67% de la propaganda yihadista recopilada en plataformas alternativas entre 2022 y 2023 empleaba deepfakes o imágenes para simular apoyos masivos o atrocidades inexistentes.
		En 2024, desarrollaron una campaña de desinformación creando material audiovisual que imitaba la producción de medios reconocidos (como CNN y Al Jazeera) para difundir narrativas falsas sobre supuestas expansiones territoriales en África.
	Procesamiento de Lenguaje Natural (PLN) / Chatbots	Chatbots como *Asharq al-Awsat* utilizan PLN para identificar vulnerabilidades psicológicas en tiempo real, lo que acelera el ciclo de radicalización.
	Reconocimiento Automático de Voz (ASR) / Transcripción	Un usuario pro-IS afirmó haber usado una herramienta de transcripción de IA para transcribir y traducir un mensaje de liderazgo central de IS del árabe a otros idiomas (indonesio e inglés), facilitando la difusión de propaganda a una audiencia internacional más amplia.
	Redes Neuronales	Se implementa la IA para ocultar la identidad y eludir los sistemas de filtros automatizados de las plataformas digitales mediante redes neuronales que transforman o reformulan palabras clave y contenidos textuales.
Al-Qaeda (AQ)	IA Generativa / Imágenes	Una entidad de medios alineada con Al-Qaeda ha publicado varios carteles cuyas imágenes son altamente probables de haber sido creadas usando IA generativa, incluyendo inconsistencias en sistemas de armas, distorsiones anómalas en equipos y ropa.
	Deepfakes de audio	Han utilizado deepfakes de audio extremistas con personajes animados y personalidades de internet para integrar narrativas extremistas en contenido de entretenimiento popular.
Hamás / Brigadas Al Qassam	IA Generativa / Deepfakes de audio e imágenes	Amplificó la narrativa de la "Fuerza Israelí de los Pañales" mediante contenido generado por IA, incluyendo videos de TikTok con imágenes GenAI de soldados de las FDI con pañales y un clon de voz de un comandante israelí, transformando narrativas complejas en memes sintéticos atractivos.
	IA Generativa / Imágenes	Han difundido carteles generados por IA con imágenes simbólicas durante conflictos armados para moldear narrativas de victimización y resistencia. Los canales

		oficiales han compartido carteles de propaganda que son probablemente generados o mejorados por IA, con imágenes de sus combatientes y ataques a objetivos militares israelíes.
Al-Shabaab	Sistemas basados en IA / Machine Learning	Ha implementado sistemas que cruzan datos de redes sociales con variables geopolíticas locales para adaptar mensajes a conflictos específicos, lo que aumenta la efectividad reclutadora en un 40%.
Extremistas de extrema derecha / Neonazis	IA Generativa / Imágenes	Produjeron una "guía para la guerra memética" que aconsejaba usar herramientas de IA generativa para la creación y difusión de memes extremistas. Esto incluye el uso de la edición humana posterior para maximizar el efecto y evadir bloqueos.
		Se identificó un canal dedicado a compartir imágenes racistas, antisemitas y pro-nazis generadas por una aplicación de arte de IA disponible en una tienda de aplicaciones, incluyendo representaciones de estatuas de Hitler y caricaturas antisemitas.

Fuente: Elaboración propia con base en Weinmann (2006), Berger & Morgan (2015), Perelló (2014), Ayad (2014) y Citron & Chesney (2019).

Influencia de la Inteligencia Artificial en la percepción pública.

Para este apartado se examina la influencia de estas tecnologías en la percepción pública, la radicalización de individuos y el reclutamiento de nuevos integrantes, tanto a nivel regional como global. La incorporación de IA por parte de los grupos terroristas no solo ha mejorado la calidad de sus mensajes, sino que también ha amplificado su capacidad de impacto en la percepción pública y los procesos de radicalización, tanto en contextos regionales como globales. La automatización de contenidos, el uso de algoritmos para segmentar audiencias y la manipulación de emociones a través de imágenes y narrativas generadas por IA han transformado significativamente las dinámicas de influencia psicológica.

Como señala Weimann (2004), los terroristas han identificado en el internet un terreno propicio para desarrollar campañas de guerra psicológica, difundir propaganda, reclutar adeptos y recaudar fondos (p.5). Con la llegada de la IA generativa, esta capacidad se ha multiplicado. Los modelos de lenguaje como ChatGPT y generadores de imágenes permiten ahora diseñar mensajes específicos dirigidos a públicos vulnerables, como jóvenes en riesgo de exclusión, utilizando lenguaje emocionalmente cargado y con un contenido visual impactante (Weimann et al., 2024).

Uno de los aspectos más preocupantes es la capacidad de la IA generativa para crear y propagar contenidos de naturaleza hiperrealista, específicamente diseñados con el propósito de manipular sesgos cognitivos y respuestas emocionales en el público receptor. Investigaciones recientes documentan que el 67% de la propaganda yihadista recopilada en plataformas alternativas entre 2022 y 2023 empleaba Deepfakes o imágenes para simular apoyos masivos o atrocidades inexistentes (Berger, 2023).

Además, los sistemas de recomendación basados en IA amplifican exponencialmente estos contenidos. Un estudio sobre 10,000 usuarios de TikTok demostró que la exposición a narrativas extremistas se incrementó en un 320% cuando los algoritmos identificaban perfiles con predisposición a la radicalización (Al-Rawi et al., 2024). Este fenómeno ha creado un ecosistema desinformativo donde la distinción entre la realidad y la ficción se difumina progresivamente, socavando los consensos sociales básicos (UNOCT, 2023).

Paralelamente, la IA ha permitido la creación de sistemas autónomos de reclutamiento altamente eficaces. Bots conversacionales en Telegram y RocketChat simulan

interacciones humanas mediante modelos de lenguaje avanzados, logrando tasas de conversión tres veces superiores a las de reclutadores humanos (Klausen, 2023). En regiones como el Cuerno de África, Al-Shabaab ha implementado sistemas que cruzan datos de redes sociales con variables geopolíticas locales, permitiendo adaptar mensajes a conflictos específicos y aumentando la efectividad reclutadora en un 40% (Hussain, 2023).

Las dinámicas de radicalización online han sido descritas como procesos de manipulación ideológica que explotan la vulnerabilidad emocional y cognitiva de los usuarios. Jiménez y Rivera (2020) identifican patrones de engaño, acoso y presión psicológica en redes sociales, los cuales se ven hoy en día amplificados por herramientas de IA que permiten micro segmentar el público objetivo, generar respuestas automatizadas para mantener la atención del usuario a través de contenidos hiper públicos y emotivos. Estas tácticas, combinadas con el uso de bots y algoritmos de predicción emocional, aumenta significativamente la probabilidad de éxito en los procesos de radicalización digital.

El caso de Al-Shabaab, documentado por Georgia Gilroy (2024), revela cómo estos grupos han diseñado estrategias de comunicación adaptativas, donde la IA es usada para medir el impacto de las campañas, reconfigurar contenidos y automatizar respuestas. Este enfoque ha fortalecido su capacidad para sobrevivir a operaciones de contrainsurgencia, manteniendo la moral de sus seguidores y atrayendo nuevos simpatizantes.

Además, la literatura especializada ha identificado cómo los grupos radicales islamistas dirigen sus estrategias de comunicación hacia jóvenes musulmanes en Europa, aprovechando factores de exclusión, identidad y pertenencia. Según Delgado y Reinares

(2019), estas organizaciones emplean tácticas adaptativas que hoy, con la ayuda de la IA, pueden multiplicar su efectividad, automatizando mensajes y seleccionando objetivos con mayor precisión. Estas campañas se articulan con narrativas de victimización, glorificación del martirio y demonización del "otro", todo lo cual se ve reforzado por tecnologías de IA que validan emocionalmente estos discursos.

La versatilidad de la IA no solo ha optimizado la propaganda, sino que ha facilitado la creación de auténticos entornos de instrucción digital. Según Stenersen (2008), los espacios en línea han evolucionado hacia verdaderos "campamentos de entrenamiento virtual", donde los individuos acceden a manuales de adoctrinamiento, simulaciones de combate y contenidos motivacionales sin necesidad de contacto directo con las organizaciones. Con la llegada de sistemas de IA capaces de adaptar los contenidos al nivel de radicalización del usuario, este tipo de formación informal se ha vuelto más eficiente, discreta y personalizada, permitiendo incluso la evaluación de la predisposición a actuar con base en variables psicológicas y comportamentales extraídas de la actividad digital del recluta.

Así mismo, campañas como Salil al-Sawarim del Estado Islámico no solo utilizaron imágenes crudas de violencia, sino que combinaron elementos religiosos, estéticos y simbólicos generados por IA para exaltar el martirio y fomentar la emulación entre jóvenes musulmanes en Europa (Greenberg, 2016). Esto genera que la percepción pública se vea afectada, generando desconcierto entre la realidad y las representaciones artificiales, lo que genera temor, confusión o incluso simpatía hacia los grupos extremistas.

Un estudio del Combating Terrorism Center resalta que estas tecnologías permiten a los grupos extremistas operar con mayor precisión y rapidez, creando contenidos propagandísticos en varios idiomas y formatos adaptados a varias plataformas digitales. Este informe, señala particularmente que herramientas como modelos de lenguaje generativo pueden ser empleadas por los extremistas para redactar manifiestos, discursos, respuestas automáticas y materiales formativos ideológicos sin la intervención directa del hombre.

De igual manera el informe del United Nations Counter-Terrorism Centre (UNCCT, 2023) subraya el aumento de las capacidades de los grupos terroristas para explotar nuevas tecnologías en campañas de radicalización. A través del Global Programme on Cybersecurity and New Technologies, se ha evidenciado que la manipulación algorítmica favorece procesos de reclutamiento orientados a población joven, mediante segmentación emocional y microtargeting (UNCCT, 2023).

Datos tomados de Profiles Of Individual Radicalization in the United States (PIRUS), que es una base de datos que recopila información sobre 1.867 individuos en los Estados Unidos, vinculados al islamismo, a la extrema izquierda, extrema derecha y a causas específicas, que adoptaron posturas extremistas, tanto violentas como no violentas entre los años 1948 y 2016, señalan que el uso de las redes sociales por extremistas en EE.UU. pasó de ser marginal en 2005 a tener un papel central en el 86.67% de los casos en 2016. Particularmente, un 45.4% de los extremistas islamistas emplearon estas plataformas como principal vía de radicalización (START, 2018).

Esta capacidad incrementa significativamente la velocidad de producción y reduce la necesidad de expertos en comunicación al interior de las organizaciones terroristas. Además, se ha documentado que estas tecnologías pueden simular conversaciones con reclutas, automatizar el contenido propagandístico en chats privados y facilitar la difusión estratégica en momentos de crisis o ataques (Weinmann et al., 2024). Esta versatilidad facilita la difusión viral, especialmente en regiones con alta penetración de redes sociales y limitada alfabetización mediática, como algunos países del Sahel, Medio Oriente y sudeste asiático.

Además, como advierte Wagner (2021), la inteligencia artificial ofrece a los grupos terroristas una ventaja operativa significativa al permitirles analizar patrones de comunicación y reacciones emocionales en línea. Esta capacidad de Inteligencia de Código Abierto (OSINT) se potencia con algoritmos de minería de datos, que identifican objetivos vulnerables y momentos críticos para influir en la narrativa pública. El uso de estas herramientas para seleccionar blancos discursivos o diseminar campañas emocionales específicas convierte a la IA en una extensión del aparato de inteligencia terrorista, con la diferencia de que actúa a escala global y con un grado de anonimato sin precedentes.

Por tanto, los impactos de la IA en el ámbito del terrorismo trascienden lo técnico: configuran nuevas formas de guerra cognitiva donde la percepción, la emoción y la desinformación son armas clave. Esta guerra perceptiva erosiona la confianza en las instituciones, polariza a la sociedad y transforma los espacios digitales en escenarios de confrontación simbólica (UNICRI & UNOCT, 2021). La escalabilidad, eficiencia y anonimato operativo de la IA convierten esta tecnología en un recurso estratégico de primer orden para las organizaciones terroristas en la actualidad.

Como se advierte en el Handbook on Disinformation, AI and Synthetic Media (Commonwealth Parliamentary Association, 2023), el uso de bots, deepfakes y algoritmos de amplificación no solo afecta la calidad del discurso público, sino que puede socavar elecciones democráticas, polarizar sociedades y legitimar discursos extremistas con apariencia de legitimidad técnica.

De manera complementaria, Cano Paños (2019) sostiene que el yihadismo ha profesionalizado su comunicación audiovisual como forma de espectáculo violento, usando recursos estéticos y simbólicos que estimulan la fascinación por la violencia. Este enfoque refuerza la propaganda mediante la teatralización de ejecuciones o ataques, capturando la atención de audiencias globales e intensificando procesos de radicalización a través del impacto sensorial que la IA puede hoy en día amplificar exponencialmente.

Desde una perspectiva sociológica, la propaganda extremista alimentada por IA no solo influye en las emociones individuales, sino que también reconstruye el imaginario colectivo de ciertas comunidades propensas a la radicalización. Slinko et al. (2023) argumentan que el terrorismo moderno se ha adaptado a las transformaciones sociales impulsadas por las tecnologías digitales, lo que permite que los discursos violentos se inserten en el tejido simbólico cotidiano a través de memes, videos cortos y narrativas de victimización, reforzando el sentido de pertinencia entre los potenciales reclutas. Así, los procesos de radicalización ya no solo son verticales, es decir desde líderes hacia simpatizantes, sino también horizontales, entre pares conectados a través de algoritmos de recomendación y afinidad ideológica.

Finalmente, Roberts e Ingleson (2023) destacan que la relación entre desinformación automatizada y radicalización no es meramente técnica, sino profundamente estructural. En un ecosistema donde las audiencias confían cada vez más en fuentes digitales y algoritmos de personalización, la capacidad de insertar mensajes polarizantes o conspirativos con apariencia de neutralidad, incrementa la credibilidad del contenido de la propaganda terrorista. Esta percepción de "legitimidad tecnológica" es explotada por grupos terroristas para debilitar el discurso democrático y amplificar la resonancia de sus narrativas, incluso en contextos socio políticos ajenos a sus conflictos originales

El análisis permitió examinar de manera integral el impacto del uso de la IA por parte de grupos terroristas en tres frentes claves como lo son la percepción pública, los procesos de radicalización y las estrategias de reclutamiento. Se evidenció que estas tecnologías no solo han transformado los métodos de persuasión y adoctrinamiento, sino que han permitido a las organizaciones extremistas adaptar sus mensajes a perfiles psicológicos específicos, automatizar interacciones y amplificar sus narrativas a nivel regional y global. La IA ha potenciado la capacidad de los grupos terroristas para moldear el imaginario colectivo, reclutar nuevos miembros con una mayor eficiencia y erosionar la confianza social, convirtiéndose en un recurso estratégico central en los medios y métodos comunicacionales del extremismo violento contemporáneo.

Implicaciones geopolíticas del uso de la Inteligencia Artificial en la propaganda terrorista.

En este apartado se establece el alcance y las implicaciones geopolíticas de la integración de la inteligencia artificial en las estrategias comunicativas de los grupos terroristas, considerando cómo esto afecta la seguridad internacional. El fenómeno analizado en esta investigación se enmarca en lo que la teoría contemporánea de conflictos denomina Guerra de Quinta Generación (5GW). Lind et al. (1989) establecieron las bases teóricas para comprender la evolución de los conflictos modernos, identificando cómo la guerra ha transitado desde confrontaciones convencionales entre Estados hacia formas asimétricas donde actores no estatales desafían el monopolio estatal de la violencia mediante operaciones en el dominio informacional.

Hammes (2006) profundiza este análisis señalando que la 5GW se caracteriza por tres elementos fundamentales que se manifiestan claramente en el uso de IA por grupos terroristas:

Primero, la difuminación deliberada de las fronteras entre guerra y paz, donde las operaciones de propaganda digital mediante IA operan en una zona gris que dificulta la aplicación de marcos legales tradicionales del derecho internacional humanitario. Como evidencian los casos documentados de ISIS y Al-Shabaab, la propaganda generada por IA no constituye un acto de guerra en sentido convencional, pero produce efectos estratégicos equivalentes al minar la cohesión social y erosionar la confianza institucional.

Segundo, la convergencia entre combatientes y población civil como actores operacionales. Los sistemas de IA permiten que simpatizantes dispersos globalmente contribuyan a campañas de propaganda sin estructura jerárquica formal, transformando a usuarios individuales en nodos de una red distribuida de influencia. Los datos del estudio PIRUS (START, 2018) que documentan que el 45.4% de extremistas islamistas en EE.UU.

emplearon redes sociales como principal vía de radicalización, confirman esta transformación estructural del conflicto.

Tercero, el desplazamiento del centro de gravedad estratégico desde la capacidad militar hacia la voluntad política de las sociedades objetivo. Como señala Hammes (2006, p. 208), "el objetivo no es destruir las fuerzas enemigas, sino erosionar su determinación política mediante la manipulación de percepciones". Los hallazgos de esta investigación sobre el incremento del 320% en exposición a narrativas extremistas mediante algoritmos de recomendación (Al-Rawi et al., 2024) demuestran precisamente esta mecánica operacional. Para esto la adopción de tecnologías de IA por parte de grupos terroristas no sólo redefine las estrategias de influencia, a su vez configura un fenómeno de alcance sistémico que interpela los fundamentos de la gobernanza global y reconfigurar las dinámicas de poder en el sistema internacional contemporáneo. Esta transformación opera a través de tres dimensiones analíticas diferenciadas: la táctica, la estratégica y la narrativa.

La primera dimensión evidencia cómo las plataformas digitales han evolucionado hacia espacios de extensión directa del conflicto armado. Según Singer y Brooking (2018), ISIS desarrolló una campaña propagandística altamente profesionalizada durante la toma de Mosul en 2014, en la cual integró sistemas automatizados de difusión en Twitter, deepfakes y aplicaciones móviles para viralizar el hashtag #AllEyesOnISIS. Esta estrategia de guerra psicológica digital precedió y acompañó la fase cinética del conflicto, generando efectos desestabilizadores en la moral y cohesión de las fuerzas defensoras antes de que el ataque físico ocurriera. Este tipo de guerra cognitiva basada en algoritmos sienta un precedente del potencial disruptivo de la IA en escenarios híbridos.

Una de las principales preocupaciones es la incorporación de la IA en estrategias de desestabilización híbrida. Según el informe de la Oficina de las Naciones Unidas contra el Terrorismo y el UNICRI (2021), actores no estatales podrían utilizar drones autónomos, bots de ataque y otros dispositivos potenciados por IA para llevar a cabo operaciones terroristas sin intervención humana directa. Este tipo de amenazas redefine el concepto de guerra asimétrica y plantea serios desafíos a la seguridad nacional y regional.

La incorporación de tecnologías de IA por parte de actores no estatales violentos representa un cambio estructural en la naturaleza de la guerra asimétrica. Como indica Cano Paños (2020), la tecnología se ha convertido en una fuerza niveladora que permite a grupos terroristas disputar narrativas globales, interferir en los procesos políticos y erosionar la hegemonía comunicacional de los Estados. La capacidad de simular ataques, difundir contenidos coordinados y manipular percepciones a través de IA configura un nuevo teatro de confrontación estrategia en el ciberespacio.

En paralelo, la sofisticación de las estrategias de influencia mediante deepfakes, bots y algoritmos de amplificación ha permitido a los grupos extremistas erosionar la confianza en las instituciones democráticas, alterar procesos electorales y generar caos social. Organizaciones como Hamas, por ejemplo, han difundido posters generados por IA con imágenes simbólicas durante conflictos armados para moldear narrativas de victimización y resistencia (Georgetown Security Studies Review, 2024).

Estas acciones se enmarcan en una lógica de guerra cognitiva, donde los algoritmos se convierten en herramientas de manipulación emocional y desinformación. Como lo argumenta Fonseca (2024), esto representa una amenaza directa a la soberanía nacional,

pues dificulta el control estatal sobre la circulación de narrativas hostiles y la protección de sus ciudadanos frente a campañas de radicalización transnacional.

Walker y Ludwig (2017) introducen el concepto de "sharp power" para distinguir las estrategias de manipulación informativa de actores autoritarios del tradicional "soft power" de Nye. Mientras el soft power busca atraer mediante cultura y valores, el sharp power opera mediante "la penetración y manipulación de entornos informativos" (Walker & Ludwig, 2017, p. 3).

Esta distinción teórica es crucial para comprender el fenómeno analizado. Los grupos terroristas no buscan generar admiración por sus valores (soft power), sino penetrar, distorsionar y manipular el ecosistema informativo para generar confusión, polarización y erosión de consensos democráticos. Como documentan los casos de Hamas y Al-Shabaab en esta investigación, el uso de IA para crear contenido sintético que explota narrativas de victimización constituye precisamente esta forma de "sharp power no estatal".

Singer y Brooking (2018) lo conceptualizan como "soft power destructivo" – la capacidad de actores no estatales para erosionar legitimidad institucional y cohesión social mediante operaciones informacionales sistemáticas. Los hallazgos sobre la campaña "Salil al-Sawarim" de ISIS, que combinó elementos religiosos, estéticos y simbólicos generados por IA para fomentar emulación entre jóvenes musulmanes europeos (Greenberg, 2016), ilustran esta dinámica. (Walker, 2017)

A nivel institucional, la proliferación de la IA plantea interrogantes urgentes sobre la gobernanza global de estas tecnologías. La ausencia de un marco normativo común para controlar el uso de la IA por actores violentos dificulta la respuesta coordinada entre Estados y organizaciones multilaterales. En este sentido, iniciativas como el programa AI

Shield de la Unión Europea buscan desarrollar algoritmos que detecte y bloquee contenidos extremistas de manera preventiva (Commonwealth Parliamentary Association, 2023), aunque enfrentan dilemas éticos relacionados con la privacidad y la libertad de expresión.

Así mismo, le informo de la ONU (2023) alerta sobre el riesgo de que vehículos autónomos y sistemas urbanos inteligentes sean convertidos en "slaughterbots" por parte de grupos terroristas, aumentando la letalidad de sus ataques. Estas amenazas exigen una respuesta integrada que combine ciberdefensa, diplomacia tecnológica y cooperación fronteriza.

La IA trasciende su dimensión puramente tecnológica para configurarse como un elemento determinante en las dinámicas de poder contemporáneas. Como señala De la Torre (2022), esta tecnología opera como un vector político fundamental que redefine las capacidades y la influencia relativa tanto de actores estatales como de entidades no gubernamentales en el sistema internacional. Esta transformación se manifiesta particularmente en la capacidad de la IA para alterar los equilibrios de poder tradicionales, otorgando ventajas estratégicas significativas a aquellos actores que logran dominar su desarrollo y aplicación.

La apropiación de tecnologías de inteligencia artificial por parte de organizaciones extremistas y actores no estatales con agendas desestabilizadoras ha generado una presión normativa sin precedentes en el ámbito internacional. Esta problemática impulsa de manera urgente la necesidad de establecer marcos regulatorios comprehensivos que incluyan instrumentos legales vinculantes, directrices éticas robustas y mecanismos de cooperación multilateral efectivos. Sin embargo, la complejidad inherente a la regulación de tecnologías emergentes, combinada con las divergencias en los intereses nacionales y las diferentes

percepciones sobre los riesgos asociados a la IA, ha resultado en la persistencia de significativos vacíos normativos.

En el panorama actual de amenazas globales, la integración de tecnologías de inteligencia artificial en estrategias de propaganda terrorista ha generado consecuencias particularmente preocupantes por su capacidad de diseminar desinformación a escala transnacional. Según Roberts e Ingleson (2023), este fenómeno trasciende la mera radicalización individual, constituyendo un mecanismo sistemático que debilita el consenso democrático e incrementa la inestabilidad política, afectando tanto a regiones en conflicto como a democracias consolidadas. Los movimientos extremistas han desarrollado estrategias sofisticadas que aprovechan las capacidades de la IA para crear contenido propagandístico con una alta carga de emoción, diseñado particularmente para activar respuestas psicológicas basadas en estados emocionales como la ansiedad, el resentimiento y la ira. Esta producción de contenido no solo fortalece las ideologías violentas existentes, sino que facilita la creación de ecosistemas digitales donde se produce una validación recíproca entre individuos radicalizados.

En el plano geopolítico, el uso de IA generativa por parte de actores terroristas plantea una amenaza asimétrica de carácter transnacional. El riesgo de que las campañas de desinformación con contenido creado por IA sean utilizadas para interferir en procesos democráticos o exacerbar tensiones interétnicas en contextos ya polarizados. Esta manipulación dirigida socava la legitimidad de las instituciones y obstaculiza los esfuerzos de estabilización en regiones vulnerables. En este escenario, el ciberespacio adquiere una dimensión estratégica sin precedentes. Como sostiene Gómez de Ágreda (2012), ya no es necesario ocupar físicamente un territorio para ejercer poder: basta con manipular redes,

sistemas informáticos y flujos de información. Esta lógica ha sido rápidamente adoptada por organizaciones extremistas, que explotan el entorno digital como campo de batalla simbólico, mediático y operacional. La naturaleza descentralizada y transnacional del ciberespacio, unida a la dificultad de poder atribuir los ataques, convierte a la IA en un multiplicador de poder para actores violentos, erosionando las bases de la gobernanza global y socavando la seguridad colectiva.

Conclusiones

El presente análisis evidencia que la inteligencia artificial (IA) ha emergido como una herramienta estratégica de alto impacto en las operaciones propagandísticas de los grupos terroristas, transformando radicalmente la naturaleza, el alcance y la efectividad de sus mensajes. La integración de tecnologías como la IA generativa, los algoritmos de segmentación y los bots conversacionales ha permitido a estos actores producir contenidos persuasivos, hiper personalizados y de rápida distribución, adaptados a las vulnerabilidades emocionales y culturales de públicos específicos (Weinmann, 2004; Berger, 2023).

En el ámbito comunicativo, la IA ha multiplicado la capacidad de los grupos extremistas para manipular percepciones públicas y moldear narrativas a su favor. Deepfakes, imágenes generadas por IA y vídeos alterados constituyen recursos capaces de erosionar la frontera entre realidad y ficción, socavando la confianza social y alimentando procesos de polarización (Commonwealth Parliamentary Association, 2023; Roberts & Ingleson, 2023). El uso de sistemas de recomendación en plataformas como TikTok y YouTube refuerza cámaras de eco digitales, intensificando la exposición de individuos

predispuestos a la radicalización y acelerando la conversión ideológica (Al-Rawi et al., 2024).

En el plano de la radicalización y el reclutamiento, las capacidades de la IA han permitido desarrollar procesos más automatizados, continuos y difíciles de detectar. Ejemplos como el de Al-Shabaab, que combina datos de redes sociales con variables geopolíticas locales para optimizar mensajes, demuestran la eficacia de estas estrategias (Hussain, 2023). A su vez, campañas como Salil al-Sawarim del Estado Islámico integraron elementos estéticos, religiosos y simbólicos, ahora potenciados por herramientas generativas, para provocar impacto emocional y fomentar la emulación (Greenberg, 2016; Cano Paños, 2019).

En términos geopolíticos, el uso de IA por parte de grupos terroristas introduce un desafío sistémico que trasciende la dimensión militar. La manipulación algorítmica, la creación de entornos informativos artificiales y el empleo de ciberataques híbridos con tecnologías autónomas alteran la estabilidad de regiones enteras y pueden incidir en procesos democráticos y de gobernanza (Singer & Brooking, 2018; UNOCT, 2023). Estas acciones, al operar en un espacio sin fronteras físicas, obligan a replantear los marcos de cooperación internacional y las normativas de control tecnológico, dado que las capacidades ofensivas están ahora al alcance de actores no estatales con recursos limitados (La inteligencia artificial en la geopolítica y los conflictos, 2022).

Asimismo, la ausencia de una regulación global coherente en materia de IA aplicada a la seguridad genera vacíos legales que facilitan su explotación maliciosa. Aunque

iniciativas como AI Shield de la Unión Europea buscan prevenir la difusión de contenidos extremistas, subsisten dilemas éticos en torno a la privacidad, la libertad de expresión y la gobernanza tecnológica (Commonwealth Parliamentary Association, 2023).

En suma, los hallazgos de este estudio confirman que la IA no solo amplifica la capacidad operativa de los grupos terroristas, sino que redefine la naturaleza misma de la propaganda extremista, proyectando su influencia a escala transnacional y con consecuencias directas sobre la seguridad internacional. En este sentido, se hace indispensable fortalecer los marcos regulatorios, fomentar la cooperación interinstitucional e internacional, y desarrollar tecnologías defensivas capaces de identificar y neutralizar estas amenazas antes de que se materialicen.

El futuro de la lucha contra el terrorismo no se decidirá únicamente en el terreno físico, sino también en el dominio cognitivo y digital, donde la IA se erige como un campo de batalla central. Ignorar este frente implicaría dejar a las sociedades expuestas a formas cada vez más sofisticadas de manipulación, radicalización y violencia política.

Bibliografía

Alotabi, F. (2019). Detection and classification of social media-based extremist affiliations using sentiment analysis techniques. *Human-centric Computing and Information Sciences*, 24.

Ayad, M. (18 de junio de 2014). *Institute for strategic Dialogue*. Obtenido de https://www.isdglobal.org/digital_dispatches/cnn-the-caliphate-news-network-is-support-groups-hiding-behind-faux-media-giant-social-accounts/

Berger, J., & Morgan, J. (2015). *The ISIS Twitter Census Defining and describing the population of ISIS supporters on Twitter.* The Brookings Institution. Washington, D.C.: Center for Middle East Policy at Brookings.

Castells, M. (2009). *Comunicación y Poder.* Madrid: Alianza Editorial.

Citron, D. &. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*(107), 1753-1819.

Citron, D. y. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*(107), 1753-1819.

Cortés, A. H. (2024). La Inteligencia Artificial Generativa como un Asistente Estratégico en la Era del Aprendizaje Digital. *Ciencia Latina Revista Científica Multidisciplinar, 8*(4), 2159-2178.

Gomes-Gonçalves, S. (2022). Los deepfakes como una nueva forma de desinformación corporativa – una revisión de la literatura. *IROCAMM, 5*(2), 22-38.

Greenberg, A. (2016). *Wired*. Obtenido de https://www.wired.com/2016/06/isis-facebook-for-jihad-recruiting-tool/

Guevara, G. V. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas y de investigación acción). *Recimundo, 4*(3), 163-173.

Klausen, J. L. (2020). Radicalization Trajectories: An Evidence-Based Computational Approach to Dynamic Risk Assessment of 'Homegrown' Jihadists. *Studies in Conflict & Terrorism*, 615.

Lind, W. S. (1989). The Changing Face of War: Into the Fourth Generation. *Marine Corps Gazette*, 73.

Mejía, J. (2012). Modelos de implementación de las políticas públicas en Colombia y su impacto en el bienestar social. *Analecta Política, 2*(3), 141–163.

Nelu, C. (10 de junio de 2024). *ICCT.* Obtenido de The International Centre for Counter-Terrorism: https://icct.nl/publication/exploitation-generative-ai-terrorist-groups

Perelló, B. e. (23 de marzo de 2014). *newtral.es*. Obtenido de https://www.newtral.es/bulos-ataque-moscu/20240323/

Rakić, B. (2009). Terrorism and political violence. (M. M. (Ed.), Ed.) *Contemporary Political Violence and Terrorism*, 20-21.

Rodríguez, A. (2017). Narrativa audiovisual, ontología y terrorismo: paradojas comunicativas en los videos del Estado Islámico. *Palabra Clave, 20*(1), 96-115.

Taylor, S. J. (1987). *Introducción a los métodos cualitativos de investigación: La búsqueda de significados.* Editorial Paidós.

Walker, C. &. (2017). The Meaning of Sharp Power: How Authoritarian States Project Influence. *Foreign Affairs.*, 11-16.

Weimann, G. (2004). *www.terror.net. How Modern Terrorism Uses the Internet.* Special Report, United States Institute of Peace, Washington, DC.,.

Weimann, G. (2006). *Terror on the internet : the new arena, the new challenges.* Washington, D.C., Estados Unidos: United States Institute of Peace.

Weimann, G. A., & Diaz, D. (enero de 2024). Generating Terror: The Risks of Generative AI Exploitation. *CTC Sentinel, 17*(1), 17-24.

Weimann, G. P. (2024). Generating terror: The risks of generative AI exploitation. *CTC Sentinel, 17*(1), 17-24.