

TABLA DE CONTENIDOS

EDITORIAL

ARTÍCULOS

Uso de inteligencia artificial por autoridades públicas para detección y prevención del ciberterrorismo

Carlos Ramírez Castañeda

Convergencia entre crimen organizado transnacional y terrorismo contemporáneo en América Latina: el caso ecuatoriano entre pragmatismo y utopía

Luis Miguel Hernández Flores, Cristian Fernando Hernández Flores, Carlos Eduardo Ortega Tapia y Miguel Iván Pazmiño Sotomayor

De la convergencia crimen terrorismo a la violencia híbrida: ataques con drones en América Latina

Mauricio Heise y Cristian Rodríguez

Radicalización a través de las imágenes: la propaganda extremista en la revista Dabiq

Jocelyn Vega Vargas y Dulce Sarai González González

RESEÑA

Islamic State, Media, and Propaganda: Performances of the 'Visual Caliphate'

Aarón Ferrando-Mkarbel

HISTORIA DEL TERRORISMO

Organizaciones terroristas: Provisional Irish Republican Army (PIRA)

El acontecimiento: El atentado de Marrakech, 24 de agosto de 1994

Efemérides

¿SABÍAS QUÉ?

EN MEMORIA DE LAS VÍCTIMAS

POLÍTICA EDITORIAL

CONSEJO EDITORIAL

CARLOS IGUALADA

Director

JAVIER YAGÜE

Editor Jefe

ANA AGUILERA

Editora Asociada

COMITÉ CIENTÍFICO

Carmen Aguilera

Centre for Analysis of the Radical Right

Sergio Altuna

Real Instituto Elcano

Ignacio Álvarez-Ossorio

Universidad Complutense de Madrid

Rubén Arcos

Universidad Rey Juan Carlos

Carlos Ardila

Escuela de Guerra de Colombia

Cristina Ariza

Tony Blair Institute of Global Change

Miguel Ángel Ballesteros

Departamento de Seguridad Nacional

Tamir Bar-On

Tec de Monterrey

Jose María Blanco

Universidad Autónoma de Madrid

Alessandro Boncio

European Foundation for Democracy

Moussa Bourekba

Barcelona Centre for International Affairs

Alberto Bueno

Universidad Pablo de Olavide

Pilar Cebrián

Periodista independiente

Álvaro Cremades

Universidad Complutense de Madrid

Luis de la Corte

Universidad Autónoma de Madrid

Gustavo Díaz

Universidad Complutense de Madrid

Jesús Díez

Departamento de Seguridad Nacional

Gaizka Fernández

Centro Memorial de las Víctimas del Terrorismo

Carola García-Calvo

Real Instituto Elcano

Alexandra Gil

Secretaría de Estado de Migraciones

Tore Hamming

International Centre for the Study of
Radicalisation

Thomas Hegghammer

Norwegian Defence Research Establishment

María Jiménez

Universidad de Navarra

Raúl López Romo

Centro Memorial de las Víctimas del Terrorismo

María Lozano

Oficina Antiterrorismo de Naciones Unidas

Francesco Marone

George Washington University

Manuel Moyano

Universidad de Córdoba

Diego Muro

Universidad de St. Andrews

Petter Nesser

Norwegian Defence Research Establishment

Matteo Re

Universidad Rey Juan Carlos

Jerónimo Ríos

Universidad Complutense de Madrid

Agata Serranò

Centro de Estudios Políticos y Constitucionales

Louie Dean Valencia

Universidad de Texas

Aaron Zelin

Washington Institute for Near East Policy

REVISTA INTERNACIONAL DE ESTUDIOS SOBRE TERRORISMO

Revista académica online de publicación cuatrimestral.

Observatorio Internacional de Estudios sobre Terrorismo (OIET).

Colectivo de Víctimas del Terrorismo, San Sebastián, España.

ISSN 2660-9673

 <https://rietjournal.org/>

 @RIET_revista



Este obra está bajo una [licencia de Creative Commons Reconocimiento 4.0 Internacional](#).



INDICE

PÁGINA

5	EDITORIAL
	ARTÍCULOS
7	Uso de inteligencia artificial por autoridades públicas para detección y prevención del ciberterrorismo Carlos Ramírez Castañeda
30	Convergencia entre crimen organizado transnacional y terrorismo contemporáneo en América Latina: el caso ecuatoriano entre pragmatismo y utopía Luis Miguel Hernández Flores, Cristian Fernando Hernández Flores, Carlos Eduardo Ortega Tapia y Miguel Iván Pazmiño Sotomayor
49	De la convergencia crimen terrorismo a la violencia híbrida: ataques con drones en América Latina Mauricio Heise y Cristian Rodríguez
69	Radicalización a través de las imágenes: la propaganda extremista en la revista Dabiq Jocelyn Vega Vargas y Dulce Sarai González González
	RESEÑA
88	<i>Islamic State, Media, and Propaganda: Performances of the 'Visual Caliphate'</i> Aarón Ferrando-Mkarbel
	HISTORIA DEL TERRORISMO
92	Organizaciones terroristas: Provisional Irish Republican Army (PIRA)
93	El acontecimiento: El atentado de Marrakech, 24 de agosto de 1994
100	Efemérides
101	¿SABÍAS QUÉ?
102	EN MEMORIA DE LAS VÍCTIMAS
110	POLÍTICA EDITORIAL

EDITORIAL

El pasado 11 de septiembre se cumplieron veinticinco años de los atentados que transformaron de forma irreversible la seguridad internacional contemporánea. Aquella fatídica mañana de 2001, diecinueve terroristas vinculados a Al Qaeda secuestraron cuatro aviones comerciales: dos fueron estrellados contra las Torres Gemelas del World Trade Center, un tercero contra el Pentágono y el cuarto cayó en Pensilvania después de que pasajeros y tripulantes se enfrentaran a los secuestradores. Los ataques causaron 2.977 víctimas mortales y situaron al terrorismo yihadista en el centro de la agenda internacional. Un cuarto de siglo después, el 11-S continúa constituyendo un punto de inflexión para comprender la evolución del terrorismo, la respuesta de los Estados y la transformación de las políticas de seguridad. Su legado se proyecta sobre la intervención en Afganistán, la expansión de la cooperación antiterrorista, el reforzamiento de los servicios de inteligencia y de los controles fronterizos, así como sobre debates todavía vigentes acerca del equilibrio entre seguridad y libertades. La conmemoración de este aniversario adquiere además una dimensión generacional: una parte creciente de la población mundial conoce ya el 11-S únicamente como un acontecimiento histórico, lo que refuerza la importancia de preservar su memoria y explicar sus consecuencias.

En este contexto, el presente número de la Revista Internacional de Estudios sobre Terrorismo vuelve a aproximarse al fenómeno terrorista desde perspectivas diversas, combinando investigación académica, análisis histórico, estudio de nuevas amenazas y memoria de las víctimas. La pluralidad de enfoques que reúne la publicación permite observar tanto la evolución de las organizaciones terroristas y de sus repertorios de actuación como los cambios experimentados por las políticas de prevención y respuesta durante las últimas décadas.

En cuanto al contenido académico, en el primero de los artículos, Carlos Ramírez analiza el uso de la inteligencia artificial por parte de las autoridades públicas de cara a la detección y prevención del ciberterrorismo, prestando especial atención al equilibrio entre la eficacia de estas herramientas y las garantías jurídicas necesarias para proteger los derechos fundamentales. A continuación, cuatro autores ecuatorianos con amplia experiencia en las fuerzas de seguridad analizan la convergencia funcional entre crimen organizado transnacional y uso instrumental del terror en América Latina, tomando Ecuador como caso especialmente ilustrativo de la transformación de la violencia criminal, la gobernanza coercitiva y los límites de las respuestas estatales. Por su parte, Mauricio Heise y Cristian Rodríguez estudian el empleo de sistemas aéreos no tripulados por actores no estatales en Colombia, México y Brasil, mostrando cómo los drones se incorporan a repertorios de vigilancia, ataque y

control territorial dentro de escenarios de violencia híbrida. Por su parte, Jocelyn Vega y Dulce Sarai González analizan, mediante un análisis cualitativo de los marcos visuales, el papel de las imágenes en la propaganda de Estado Islámico a partir del estudio de los quince números de la revista *Dabiq*. El apartado académico se completa con la reseña elaborada por Aarón Ferrando-Mkarbel de *Islamic State, Media, and Propaganda: Performances of the 'Visual Caliphate'*, obra de Moign Khawaja y Christian Kaunert que analiza cómo Estado Islámico utilizó especialmente su producción audiovisual para proyectar ante distintas audiencias una imagen de estatalidad, capacidad de gobierno, control territorial y poder.

En lo que respecta a las secciones de carácter divulgativo, el acontecimiento histórico seleccionado es el atentado cometido el 24 de agosto de 1994 contra el hotel Atlas Asni de Marrakech. El ataque, en el que fueron asesinados dos turistas españoles, Salvador Torras y Antonia Cuevas, se convirtió en un episodio especialmente significativo en la evolución del terrorismo yihadista en el Magreb y anticipó la creciente dimensión transnacional de redes radicales conectadas con el contexto argelino de aquellos años. La organización terrorista abordada en este número es el Ejército Republicano Irlandés Provisional (PIRA), protagonista durante décadas de una campaña armada vinculada al conflicto de Irlanda del Norte y actor indispensable para comprender tanto la evolución del terrorismo etnonacionalista europeo como el complejo proceso que desembocó en los acuerdos de paz de finales de los años noventa. Por su parte, la sección «¿Sabías que...?» vuelve a reunir distintos episodios que permiten acercarse a la historia del terrorismo y del contraterrorismo a través de hechos concretos. Entre ellos se recuerda el intento de Richard Reid de hacer detonar en diciembre de 2001 explosivos ocultos en su calzado durante un vuelo entre París y Miami, episodio que acabaría influyendo en los procedimientos de control aeroportuario.

Siguiendo el cierre habitual de RIET, la sección dedicada a las víctimas del terrorismo, elaborada por Inés Gaviria y bajo el patrocinio del Centro Memorial para las Víctimas del Terrorismo, lleva por título «Los “traidores” de ETA». El texto recupera las historias de María Dolores González Katarain, Yoyes; Miguel Francisco Solaun Angulo, Mikel; Eduardo Moreno Bergaretxe, Pertur; y Juan María Jáuregui Apalategui, trayectorias diferentes unidas por haber conocido ETA desde dentro y haber representado, de distintas formas, la ruptura, la discrepancia o el rechazo de la violencia. Su recuerdo permite mostrar una dimensión especialmente reveladora de la lógica totalitaria de la organización: la conversión de antiguos integrantes o disidentes en enemigos a los que castigar, al tiempo que recuerda que reconocer su condición de víctimas no exige borrar ni simplificar sus responsabilidades o biografías anteriores.

Presentado brevemente el contenido de este nuevo número de la RIET, invitamos al lector a continuar con su lectura. Veinticinco años después del 11-S, estudiar el terrorismo continúa exigiendo combinar memoria, investigación rigurosa y capacidad para interpretar sus transformaciones. Agradecemos, como siempre, la contribución de autores, evaluadores y colaboradores que hacen posible la publicación de un nuevo ejemplar de la Revista Internacional de Estudios sobre Terrorismo.

Uso de inteligencia artificial por autoridades públicas para detección y prevención del ciberterrorismo

Use of Artificial Intelligence by Public Authorities for the Detection and Prevention of Cyberterrorism

Resumen

El uso de inteligencia artificial por autoridades para detectar y prevenir riesgos asociados al ciberterrorismo plantea una tensión central entre eficacia institucional y límites constitucionales. Estas herramientas permiten procesar grandes volúmenes de información, identificar anomalías y proteger infraestructuras críticas, pero su legitimidad no puede medirse únicamente por su utilidad operativa. En un Estado democrático de derecho, la prevención algorítmica exige base normativa suficiente, finalidad legítima, proporcionalidad, protección de datos personales, no discriminación, supervisión humana significativa, trazabilidad y control judicial. El artículo desarrolla un análisis jurídico-documental y comparado sobre el empleo de sistemas de inteligencia artificial en tareas de detección temprana, evaluación de riesgo y prevención del ciberterrorismo. Se examinan el Convenio de Budapest, las recomendaciones de la UNESCO y de la OCDE, el NIST AI Risk Management Framework y el Reglamento (UE) 2024/1689, junto con la experiencia de ENISA y CISA, los marcos de Naciones Unidas sobre inteligencia artificial y contrterrorismo y tres decisiones judiciales que han sometido a control sistemas algorítmicos de riesgo. Se concluye que la inteligencia artificial sólo puede emplearse legítimamente cuando se integra en una arquitectura garantista de legalidad, auditoría, responsabilidad y revisión efectiva.

Palabras clave: inteligencia artificial, ciberterrorismo, autoridades públicas, derechos fundamentales, ciberseguridad, gobernanza algorítmica, infraestructuras críticas.

Abstract

The use of artificial intelligence by public authorities to detect and prevent risks associated with cyberterrorism raises a central tension between institutional effectiveness and constitutional limits. These tools make it possible to process large volumes of information, identify anomalies, and protect critical infrastructure, yet their legitimacy cannot be measured solely by their operational usefulness. In a democratic state governed by the rule of law, algorithmic prevention requires a sufficient legal basis, a legitimate aim, proportionality, personal data protection, non-discrimination, meaningful human oversight, traceability, and judicial control. This article develops a legal-documentary and comparative analysis of the use of artificial intelligence systems in early detection, risk assessment, and cyberterrorism prevention. It examines the Budapest Convention, the UNESCO and OECD recommendations, the NIST AI Risk Management Framework and Regulation (EU) 2024/1689, together with the experience of ENISA and CISA, the United Nations frameworks on artificial intelligence and counter-terrorism, and three judicial decisions that have subjected algorithmic risk systems to review. It concludes that artificial intelligence can only be legitimately employed when it is embedded in a guarantee-based architecture of legality, auditing, accountability, and effective review.

Keywords: artificial intelligence, cyberterrorism, public authorities, fundamental rights, cybersecurity, algorithmic governance, critical infrastructure

Carlos Ramírez Castañeda, Doctor en Administración y Políticas Públicas, Posdoctorado en Derecho. Universidad Nacional Abierta y a Distancia de México (UnADM).

Para citar este artículo: Ramírez Castañeda, C. (2026), Uso de inteligencia artificial por autoridades públicas para detección y prevención del ciberterrorismo, Revista Internacional de Estudios sobre Terrorismo, nº18, pp.7-29.

Recibido
18/05/2026

Aceptado
24/08/2026

1. Introducción

La inteligencia artificial se ha convertido en una de las herramientas más relevantes de la transformación digital del sector público. Su incorporación en funciones estatales ha generado expectativas de eficiencia, anticipación y optimización en ámbitos tan diversos como la salud, la administración, la justicia, la seguridad y la gestión de infraestructuras críticas. En materia de ciberseguridad, esas expectativas se intensifican, ya que la IA ofrece capacidades de procesamiento masivo, detección de anomalías, clasificación de incidentes y apoyo a la toma de decisiones en escenarios caracterizados por velocidad, complejidad e incertidumbre.

Cuando dichas capacidades se orientan a la detección y prevención del ciberterrorismo, el debate adquiere una densidad jurídica singular. La cuestión ya no es únicamente si la tecnología puede mejorar la respuesta del Estado, sino si su utilización por autoridades públicas resulta compatible con el principio de legalidad, los derechos fundamentales y los límites materiales del poder preventivo. En ese contexto, la IA se sitúa en el cruce entre dos exigencias constitucionales: por un lado, la obligación del Estado de proteger a la población y asegurar la continuidad de servicios esenciales; por otro, la necesidad de que toda intervención pública permanezca sometida al control democrático y a las garantías propias del Estado de derecho.

La dificultad aumenta debido a la propia inestabilidad conceptual del ciberterrorismo. Se trata de una categoría frecuentemente utilizada de forma expansiva, mezclando ataques a infraestructura crítica, sabotaje, propaganda extremista en línea, campañas coordinadas de intimidación digital y otras manifestaciones de criminalidad tecnológica. Como señalan Macdonald et al. (2022), la comunidad académica no ha alcanzado un consenso definitivo sobre los elementos constitutivos del ciberterrorismo, lo que dificulta su tratamiento normativo y su distinción de figuras conexas como el hacktivismo, el espionaje digital o la ciberguerra. Esa amplitud conceptual es jurídicamente problemática, pues puede conducir tanto a la banalización del término como a respuestas estatales excesivas. Por ello, un análisis serio del uso de IA por autoridades debe comenzar por una delimitación cuidadosa del objeto preventivo.

El estudio se inserta en un debate doctrinal que ha ganado densidad en los últimos años. La literatura sobre gobernanza algorítmica ha mostrado que los sistemas automatizados de gestión de riesgos no son meros instrumentos auxiliares, sino dispositivos que reconfiguran la forma misma en que el poder público define, mide y anticipa el peligro (Yeung, 2018). En paralelo, el derecho público europeo e iberoamericano ha comenzado a discutir la naturaleza jurídica de los algoritmos empleados por la administración y el estándar de habilitación legal que su uso reclama (Boix Palop, 2020; Cotino Hueso, 2023). A ello se suma una producción institucional específica sobre inteligencia artificial y contraterroismo, impulsada desde Naciones Unidas, que advierte sobre los riesgos de opacidad, sesgo y sobrevigilancia asociados a estas aplicaciones (UNOCT y UNICRI, 2021; ACNUDH, 2025). El presente trabajo dialoga con esa literatura y busca aportar una lectura situada en el ordenamiento mexicano.

El propósito del presente artículo es examinar bajo qué condiciones el uso de inteligencia artificial por autoridades para detectar y prevenir el ciberterrorismo puede considerarse jurídicamente legítimo. La tesis que se sostiene es que la validez de estas herramientas no deriva de su sola utilidad técnica. Su legitimidad depende de una arquitectura garantista basada en la legalidad, la finalidad legítima, la proporcionalidad, la protección de datos, la supervisión humana significativa, la trazabilidad, la auditoría independiente y la existencia de mecanismos efectivos de revisión y responsabilidad.

2. Metodología

La investigación es cualitativa, jurídico-documental y analítico-comparada. Se basa en la revisión de literatura académica especializada sobre ciberterrorismo, inteligencia artificial, función pública, gobernanza algorítmica, derechos fundamentales y gestión de riesgos tecnológicos. Asimismo, se examinan instrumentos jurídicos y marcos de referencia internacionales relevantes para valorar el uso de IA en contextos sensibles de prevención estatal.

En el plano nacional, se toman como referentes la Constitución Política de los Estados Unidos Mexicanos y el Código Penal Federal, con el fin de ubicar la discusión en el marco de los principios de legalidad, debido proceso, derechos humanos y persecución de amenazas graves. En el plano internacional y comparado, se revisan la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, el Convenio sobre la Ciberdelincuencia del Consejo de Europa, la Recomendación de la UNESCO sobre la Ética de la Inteligencia Artificial, la Recomendación del Consejo de la OCDE sobre Inteligencia Artificial, el NIST AI Risk Management Framework y el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo.

La aproximación comparada no persigue trasladar mecánicamente soluciones extranjeras al contexto mexicano. Más bien, busca identificar principios funcionales y estándares normativos que permitan evaluar la juridicidad del uso estatal de sistemas algorítmicos en tareas preventivas. Para ello, el análisis se organiza a partir de cinco variables: finalidad legítima, base normativa suficiente, intensidad de afectación a derechos fundamentales, nivel de autonomía del sistema y existencia de controles ex ante, concomitantes y ex post.

Junto al análisis normativo, el trabajo incorpora tres decisiones judiciales que han sometido a control sistemas algorítmicos de evaluación de riesgo desplegados por autoridades públicas. Su selección responde a tres criterios: que el sistema examinado hubiera sido operado por un poder público con finalidades preventivas o de seguridad, que la resolución hubiera abordado de manera expresa la suficiencia de la habilitación legal o las garantías frente al tratamiento automatizado, y que el pronunciamiento proviniera de un órgano jurisdiccional cuya doctrina resulte trasladable, como estándar argumentativo, al examen de constitucionalidad propio del ordenamiento mexicano. Estas resoluciones no operan como precedentes vinculantes, sino como casos que permiten observar cómo las cinco variables señaladas se aplican en escenarios reales de litigio.

Desde el punto de vista epistemológico, la investigación adopta un enfoque jurídico crítico que reconoce que el derecho no es neutral frente a la tecnología. Como apuntan Danaher et al. (2017), las instituciones jurídicas tienden a rezagarse respecto del desarrollo tecnológico, y esa brecha puede generar vacíos normativos con consecuencias directas sobre la tutela de derechos. Por esta razón, el análisis no se limita a describir el estado actual de la regulación, sino que evalúa su suficiencia y formula propuestas de mejora orientadas a garantizar el ejercicio legítimo del poder preventivo del Estado.

3. Ciberterrorismo y prevención algorítmica: precisiones necesarias

3.1. Definición y delimitación del ciberterrorismo

La categoría de ciberterrorismo exige una delimitación cuidadosa. No todo incidente informático de alto impacto puede calificarse como tal, ni toda actividad criminal en el ciberespacio comporta la finalidad de intimidación colectiva o desestabilización institucional propia del terrorismo. El criterio decisivo no se encuentra en el medio digital empleado, sino en la finalidad perseguida y en la naturaleza de los bienes afectados.

La literatura especializada ha insistido en que el ciberterrorismo supone el uso de medios digitales con el objetivo de infundir miedo, coaccionar a autoridades o alterar funciones esenciales del Estado o de la vida social (Denning, 2000; Conway, 2017; Mayer Lux, 2018). Denning (2000) definió el ciberterrorismo como ataques ilegales y amenazas de ataque contra computadoras, redes y la información almacenada en ellas cuando se realizan para intimidar o coaccionar a un gobierno o a su población en la persecución de objetivos políticos o sociales. Esta definición, pionera en el campo, continúa siendo referencia obligada en la literatura especializada, si bien ha sido objeto de refinamientos posteriores.

Macdonald et al. (2022) realizaron una encuesta a investigadores especialistas en terrorismo y encontraron que existe un amplio consenso en torno a la necesidad de distinguir el ciberterrorismo del cibercrimen común y del hacktivismo sobre la base del elemento intencional: mientras el primero busca generar terror o desestabilización política, el segundo persigue ganancias económicas o la interrupción temporal de servicios, y el tercero tiene motivaciones protestatarias sin necesariamente producir daños de la magnitud propia del terrorismo. Esta distinción tiene implicaciones jurídicas de primer orden, pues determina el régimen aplicable, las garantías procesales exigibles y la proporcionalidad de las medidas preventivas.

Por su parte, Venkatachary et al. (2024) analizan los desafíos específicos que plantea el ciberterrorismo para las infraestructuras críticas del sector energético, identificando vectores de ataque diferenciados, marcos de ciberseguridad aplicables y dimensiones económicas del problema. Su análisis confirma que los ataques a infraestructuras esenciales pueden producir efectos en cadena

con consecuencias para la seguridad pública, la salud y la continuidad del Estado, lo que justifica una respuesta preventiva de alta intensidad, aunque sujeta a condiciones jurídicas estrictas.

La UNODC, en su módulo educativo sobre ciberdelincuencia (s. f.), distingue entre hacktivismo, terrorismo, espionaje, desinformación y ciberguerra como categorías analíticamente separadas, cada una con características propias respecto a actores, motivaciones, blancos y consecuencias jurídicas. Esta taxonomía es útil porque evidencia que la prevención algorítmica no puede operar con categorías indiferenciadas: el sistema debe estar diseñado para detectar conductas jurídicamente tipificadas, no para rastrear genéricamente “actividades sospechosas” sin contornos normativos precisos.

3.2. Prevención algorítmica: caracterización técnica y jurídica

En paralelo, la prevención algorítmica puede entenderse como el uso de sistemas computacionales capaces de identificar patrones, inferir riesgos, clasificar eventos o priorizar alertas para orientar la respuesta institucional. En contextos de ciberseguridad pública, esa prevención puede manifestarse en sistemas de detección de anomalías en redes, herramientas de correlación de incidentes, análisis automatizado de indicadores de compromiso o procesamiento de lenguaje en fuentes abiertas.

Desde una perspectiva técnica, los sistemas de IA aplicados a la ciberseguridad pueden clasificarse en diversas categorías según su función: sistemas de detección de intrusiones basados en aprendizaje automático (ML-IDS), plataformas de inteligencia de amenazas (Threat Intelligence Platforms, TIP), herramientas de análisis de comportamiento de entidades y usuarios (UEBA), sistemas de correlación de eventos de seguridad (SIEM potenciados con IA), y modelos de lenguaje natural para análisis de contenido en fuentes abiertas (OSINT). Cada tipo de sistema plantea condicionantes jurídicos distintos en términos de datos procesados, nivel de autonomía y potencial de afectación a derechos (European Union Agency for Cybersecurity, 2023; National Institute of Standards and Technology, 2023).

Conviene precisar, además, qué tipo de regulación algorítmica se pone en juego. Yeung (2018) propone distinguir entre sistemas reactivos, que responden a comportamientos ya verificados, y sistemas preventivos o anticipatorios, que actúan sobre inferencias acerca de conductas futuras, y advierte que estos últimos concentran los problemas de legitimidad más serios, pues intervienen antes de que exista un hecho jurídicamente relevante. La detección del ciberterrorismo se sitúa precisamente en ese segundo grupo. De ahí que el examen no pueda limitarse a la fiabilidad estadística del modelo: lo que está en discusión es la licitud de anticipar consecuencias jurídicas sobre la base de una probabilidad calculada.

Sin embargo, la complejidad jurídica aumenta cuando estos sistemas dejan de ser simples apoyos técnicos y comienzan a influir en decisiones institucionales sobre vigilancia, priorización de riesgos o apertura de líneas de investigación. La diferencia entre apoyo operativo y estructuración del juicio preventivo es central. En el primer caso, el sistema puede servir para fortalecer la resiliencia

de redes o infraestructuras. En el segundo, la IA empieza a incidir directamente sobre derechos, expectativas de privacidad, patrones de monitoreo o procesos administrativos y penales.

El Reglamento (UE) 2024/1689, conocido como Ley de Inteligencia Artificial, establece precisamente esta distinción como criterio de clasificación de riesgos. Los sistemas de IA utilizados por autoridades para la aplicación de la ley, la evaluación de riesgos o la identificación de sospechosos son considerados de alto riesgo y quedan sujetos a obligaciones reforzadas de transparencia, documentación, supervisión humana y evaluación de conformidad antes de su despliegue. Esta categorización normativa confirma que el derecho europeo ya reconoce que no todos los usos de IA en el ámbito público son equivalentes y que la intensidad regulatoria debe graduarse en función del impacto potencial sobre derechos fundamentales.

De ahí que la discusión jurídica no deba centrarse sólo en la sofisticación técnica del modelo, sino en el lugar institucional que ocupa dentro de la actuación estatal.

4. Riesgos jurídicos del uso de IA por autoridades públicas

4.1. Insuficiencia de base normativa

El primer riesgo jurídico es la insuficiencia de base normativa. Ninguna autoridad pública puede justificar el uso intensivo de IA en funciones preventivas sobre la base de cláusulas genéricas de seguridad o modernización administrativa. El principio de legalidad exige una habilitación clara respecto de finalidades, autoridades competentes, categorías de datos, límites temporales, supuestos de activación y mecanismos de supervisión. Sin una base normativa suficiente, la herramienta tecnológica termina sustituyendo a la norma y desdibujando la garantía de previsibilidad.

La doctrina administrativista ha ofrecido una vía para precisar esta exigencia. Boix Palop (2020) sostiene que los algoritmos empleados por la administración para adoptar decisiones cumplen una función materialmente equivalente a la de un reglamento, en tanto reglan y predeterminan la actuación del poder público, por lo que deberían quedar sujetos a las garantías de publicidad, participación y control ya previstas para las normas reglamentarias. Cotino Hueso (2023), al examinar los sistemas de identificación biométrica, subraya que la superposición entre la regulación de inteligencia artificial y la de protección de datos no dispensa de una habilitación legal específica y de calidad, y que los estándares exigidos por diversos tribunales constitucionales europeos rara vez se satisfacen en la práctica administrativa. Ambas aproximaciones convergen en un punto relevante para este trabajo: la reserva de ley no se agota en la existencia de una norma que mencione la tecnología, sino que reclama densidad normativa sobre su diseño, sus límites y sus controles.

El Tribunal Europeo de Derechos Humanos ha desarrollado en su jurisprudencia la doctrina de la “calidad de la ley” como condición para que las injerencias en derechos fundamentales sean compatibles con el Convenio Europeo. Según esta doctrina, la ley habilitante no sólo debe existir,

sino ser accesible, previsible y estar dotada de garantías adecuadas contra el abuso. Aunque esta jurisprudencia no es directamente vinculante para México, ofrece un estándar útil para evaluar la suficiencia de las habilitaciones normativas en materia de vigilancia y prevención algorítmica.

En el contexto latinoamericano, la Relatoría Especial para la Libertad de Expresión de la CIDH ha alertado sobre los riesgos de la vigilancia digital sin habilitación legal clara, señalando que la interceptación de comunicaciones y el procesamiento masivo de datos por parte del Estado requieren marcos normativos específicos que establezcan con precisión los supuestos, las autoridades competentes y los mecanismos de control. Aunque sus pronunciamientos se refieren principalmente a la vigilancia de comunicaciones, los principios que desarrollan son plenamente aplicables a los sistemas de detección algorítmica del ciberterrorismo.

4.2. Protección de datos personales

Un segundo riesgo radica en la protección de datos personales. La lógica preventiva tiende a favorecer la acumulación de información bajo la premisa de que más datos mejoran la capacidad de detección. Sin embargo, ese supuesto debe someterse a los principios de minimización, finalidad específica, proporcionalidad, exactitud y seguridad. La recolección masiva e indiscriminada no sólo es jurídicamente problemática, sino también técnicamente cuestionable, pues puede aumentar el ruido informacional y producir inferencias erróneas o excesivas.

En México, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados establece principios rectores aplicables al tratamiento de datos por autoridades públicas, incluyendo licitud, finalidad, lealtad, proporcionalidad y responsabilidad. No obstante, la ley no contiene disposiciones específicas sobre el tratamiento de datos en sistemas algorítmicos de seguridad pública, lo que mantiene una zona de insuficiencia normativa que la regulación futura deberá atender.

La UNESCO (2021), en su Recomendación sobre la Ética de la IA, dedica especial atención a la protección de la privacidad y de los datos personales como condición necesaria para el desarrollo y despliegue ético de sistemas de IA. La Recomendación establece que los sistemas de IA no deben utilizarse para infringir el derecho a la privacidad, que incluye el control sobre los datos personales y la protección contra la vigilancia arbitraria o ilegal. Estos principios resultan directamente aplicables al diseño de sistemas de detección algorítmica del ciberterrorismo por parte de autoridades públicas.

4.3. Sesgo, discriminación y validez epistémica

En tercer lugar, debe considerarse el problema del sesgo y la discriminación. Los sistemas algorítmicos aprenden a partir de datos, decisiones de diseño y contextos institucionales. Si esos elementos están marcados por asimetrías, errores o lógicas de sobre-vigilancia, la herramienta puede reproducir o amplificar tales distorsiones. En materia de prevención del ciberterrorismo, ello

es especialmente grave, ya que una clasificación errónea puede activar vigilancia reforzada, afectar reputaciones o generar tratamientos desproporcionados antes de que exista un control judicial efectivo.

La literatura especializada ha documentado extensamente los riesgos de sesgo en sistemas de IA utilizados en contextos de seguridad. Estudios como los de Obermeyer et al. (2019) han demostrado que algoritmos utilizados en la toma de decisiones públicas pueden codificar y amplificar sesgos raciales, socioeconómicos o de género presentes en los datos de entrenamiento. En el ámbito específico de la seguridad, los sesgos pueden traducirse en sobre-vigilancia de determinadas comunidades, generando un impacto desproporcionado sobre personas y grupos que ya se encuentran en situación de vulnerabilidad. Esta dinámica es incompatible con el principio de igualdad y no discriminación, consagrado en los artículos 1º de la Constitución Política de los Estados Unidos Mexicanos y 24 de la Convención Americana sobre Derechos Humanos.

El NIST AI Risk Management Framework (2023) aborda el problema del sesgo como un riesgo sistémico que debe gestionarse en todas las etapas del ciclo de vida del sistema: diseño, desarrollo, validación, despliegue y monitoreo continuo. El marco propone mecanismos de evaluación de equidad, pruebas adversariales y mecanismos de retroalimentación para detectar y corregir sesgos, subrayando que la gestión del sesgo no es un evento único sino un proceso permanente. Esta perspectiva es especialmente relevante para los sistemas de detección del ciberterrorismo, donde la dinámica de las amenazas cambia constantemente y los datos de entrenamiento pueden volverse rápidamente obsoletos o sesgados.

4.4. Opacidad y exigencia de explicabilidad

Un cuarto riesgo es la opacidad. Cuando la autoridad no puede explicar suficientemente cómo operó el sistema, qué datos fueron relevantes o cómo se integró la recomendación algorítmica en la decisión final, la exigencia de motivación se debilita y el control judicial se vuelve precario. Por ello, la trazabilidad y la explicabilidad no son atributos deseables en abstracto, sino condiciones de juridicidad.

La OCDE (2023), en su Recomendación revisada sobre IA, establece que los sistemas de IA deben ser transparentes y que los operadores deben ser capaces de explicar sus decisiones y predicciones en la medida en que sea razonablemente posible. Asimismo, señala que los agentes de IA deberían poder proporcionar información suficiente para ayudar a las partes interesadas a comprender las capacidades y limitaciones de los sistemas y a responder a los resultados que producen. Estas exigencias de explicabilidad son especialmente relevantes en el contexto del uso estatal de IA, donde las decisiones tomadas con base en sistemas algorítmicos pueden afectar derechos fundamentales y deben poder ser objeto de revisión judicial efectiva.

El Reglamento (UE) 2024/1689 operacionaliza estas exigencias a través de obligaciones concretas para los sistemas de alto riesgo, incluyendo la llevanza de registros automáticos (logs),

la documentación técnica detallada, la provisión de instrucciones de uso, y la obligación de diseñar el sistema de manera que las salidas sean interpretables por las personas físicas responsables de su supervisión. Estas obligaciones no sólo tienen un valor instrumental para el control judicial, sino que contribuyen a construir la confianza institucional necesaria para el despliegue legítimo de la IA en contextos sensibles.

La doctrina ha señalado, sin embargo, los límites de este modelo. Veale y Zuiderveen Borgesius (2021) advierten que buena parte de las obligaciones de transparencia del régimen europeo descansa en mecanismos de autoevaluación de conformidad, de modo que el cumplimiento queda en manos del propio proveedor o del organismo implantador, con una supervisión externa limitada. Esta observación resulta especialmente pertinente en el ámbito de la seguridad, donde las exigencias de reserva pueden invocarse para restringir el acceso a la documentación técnica. Si la explicación se reduce a un expediente interno inaccesible para el afectado y para el juez, la garantía se vuelve nominal.

4.5. Responsabilidad pública y riesgo de tecnocracia

Finalmente, existe el riesgo de debilitamiento de la responsabilidad pública. La administración no puede escudarse en la complejidad técnica del sistema ni en el prestigio del proveedor para diluir su responsabilidad. Si la tecnología influye en una actuación estatal, la imputación jurídica sigue correspondiendo a la autoridad. La supervisión humana significativa, en este sentido, es también una exigencia de responsabilidad democrática.

El riesgo de tecnocracia se manifiesta cuando la complejidad técnica de los sistemas algorítmicos genera una asimetría informacional entre los operadores tecnológicos y los decisores políticos y judiciales. Esta asimetría puede producir lo que la doctrina denomina “deferencia algorítmica”: la tendencia de los funcionarios a aceptar sin cuestionamiento las recomendaciones de los sistemas automatizados, delegando efectivamente la decisión en el algoritmo. En contextos de ciberseguridad y prevención del terrorismo, donde la urgencia operativa es elevada, este riesgo se intensifica.

La Recomendación de la OCDE sobre IA (2023) aborda este problema exigiendo que los sistemas de IA sean diseñados de manera que permitan la supervisión, el reemplazo o la reversión por parte de operadores humanos. La UNESCO (2021) va más lejos al establecer que las decisiones que afecten significativamente a los derechos y libertades de las personas deben poder ser revisadas y, si fuera necesario, corregidas por seres humanos.

5. Referentes internacionales y comparados

5.1. *Convención de Naciones Unidas contra la Delincuencia Organizada Transnacional*

La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional no regula directamente la inteligencia artificial ni el ciberterrorismo, pero aporta una arquitectura valiosa para la cooperación internacional frente a fenómenos complejos y transfronterizos. Su principal enseñanza es que la respuesta estatal frente a riesgos organizados no puede descansar únicamente en herramientas técnicas, sino en coordinación institucional, intercambio de información y fortalecimiento de capacidades. La Convención establece, en su artículo 29, la obligación de los Estados parte de adoptar, desarrollar o mejorar programas de capacitación para su personal, incluyendo la capacitación en técnicas de investigación compatibles con los derechos humanos. Esta disposición es relevante para el uso de IA en la prevención del ciberterrorismo, ya que implica que cualquier herramienta tecnológica debe ser acompañada por formación adecuada que garantice su uso dentro de los parámetros del Estado de derecho.

5.2. *Convenio de Budapest sobre Ciberdelincuencia*

El Convenio de Budapest ofrece, por su parte, un marco esencial en materia de cooperación penal y preservación de evidencia digital. Su relevancia en este estudio reside en recordar que la detección tecnológica no sustituye la juridicidad de la investigación. La IA puede contribuir a identificar señales tempranas o patrones de amenaza, pero cualquier actuación posterior debe quedar integrada en procedimientos compatibles con el debido proceso y con las reglas de obtención y preservación de evidencia. El Convenio de Budapest, en su Capítulo II, establece disposiciones específicas sobre medidas procesales que los Estados deben adoptar para la investigación de delitos informáticos, incluyendo la conservación expedita de datos almacenados, la divulgación expedita de datos de tráfico conservados y la interceptación de datos de contenido. Estas disposiciones deben entenderse como un piso mínimo de garantías que los sistemas de IA utilizados en la detección del ciberterrorismo no pueden ignorar.

5.3. *Marco ético de UNESCO y OCDE*

La Recomendación de la UNESCO sobre la Ética de la Inteligencia Artificial y la Recomendación de la OCDE sobre Inteligencia Artificial aportan principios directamente útiles para la evaluación del uso estatal de IA: respeto a los derechos humanos, privacidad, transparencia, explicabilidad, responsabilidad, seguridad, robustez y supervisión humana. Ambos instrumentos muestran que el sector público, especialmente en ámbitos sensibles como seguridad y justicia, debe operar con estándares más exigentes que los contextos puramente privados o experimentales.

La UNESCO (2021) introduce el concepto de “evaluación del impacto ético” como herramienta prospectiva para identificar los posibles efectos de los sistemas de IA sobre los derechos humanos antes de su despliegue. Esta herramienta es especialmente relevante para los sistemas de detección del ciberterrorismo, dado que la anticipación de los efectos sobre la privacidad, la igualdad y el debido proceso puede contribuir a diseñar sistemas más respetuosos con los derechos desde el origen, incorporando lo que la doctrina denomina “privacidad por diseño” (*privacy by design*).

La OCDE (2023), por su parte, ha actualizado su Recomendación sobre IA para reforzar los principios de rendición de cuentas y responsabilidad, señalando que los agentes de IA deberían ser responsables de la aplicación correcta de los principios relacionados con la IA. En el ámbito del sector público, esta responsabilidad adquiere una dimensión constitucional, puesto que el Estado no actúa como un agente privado más, sino como titular del poder público cuya actuación está sometida a los principios de legalidad, eficacia y servicio al interés general.

5.4. NIST AI Risk Management Framework

El NIST AI Risk Management Framework añade un enfoque operativo especialmente valioso: la gestión continua del riesgo. La gobernanza de la IA no debe concebirse como una autorización única, sino como un proceso permanente de identificación, evaluación, mitigación, monitoreo y revisión. En contextos preventivos, donde el riesgo y la incertidumbre cambian constantemente, esta lógica resulta indispensable.

El AI RMF 1.0 del NIST (2023) estructura la gestión del riesgo en cuatro funciones principales: Gobernar (Govern), Mapear (Map), Medir (Measure) y Gestionar (Manage). La función de Gobernar establece las políticas, procesos, procedimientos y prácticas para la gobernanza del riesgo de IA. La función de Mapear contextualiza los riesgos identificados en función del propósito y las partes interesadas. La función de Medir analiza, evalúa y monitorea los riesgos. Y la función de Gestionar ordena las respuestas de riesgo y aplica las medidas apropiadas. Este marco es aplicable directamente al diseño de sistemas de detección del ciberterrorismo por autoridades.

5.5. Reglamento (UE) 2024/1689 y la experiencia de ENISA

El Reglamento (UE) 2024/1689 confirma que, cuanto mayor es la sensibilidad del entorno de uso y mayor la posibilidad de afectación a derechos fundamentales, más densas deben ser las obligaciones regulatorias. Su valor comparado para el caso mexicano no está en la traslación automática de su contenido, sino en la racionalidad que lo inspira: la innovación pública sólo es legítima cuando va acompañada de obligaciones reforzadas de documentación, supervisión, evaluación y responsabilidad.

El Reglamento (UE) 2024/1689 clasifica como sistemas de alto riesgo, entre otros, los sistemas de IA utilizados por autoridades competentes para realizar evaluaciones individuales del riesgo de

delincuencia y terrorismo (Anexo III). Para estos sistemas, el Reglamento exige: establecimiento de sistemas de gestión de riesgos, gobernanza de datos y gestión de datos de entrenamiento, documentación técnica, registro de eventos automático, transparencia e información a los usuarios, supervisión humana, y niveles de exactitud, solidez y ciberseguridad. Este conjunto de obligaciones constituye el estándar más avanzado actualmente disponible para el uso legítimo de IA en contextos preventivos de seguridad pública.

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) ha publicado directrices específicas sobre el uso de IA en ciberseguridad, subrayando tanto las oportunidades que ofrecen estas tecnologías para la detección y respuesta a incidentes como los riesgos propios de la IA, incluyendo vulnerabilidades específicas como los ataques adversariales, el envenenamiento de datos (*data poisoning*) y la evasión de modelos. Estos riesgos técnicos tienen una dimensión jurídica directa: un sistema de detección vulnerado o manipulado puede producir falsos negativos, dejando pasar amenazas reales, o falsos positivos, generando intervenciones estatales injustificadas sobre personas inocentes.

5.6. *La experiencia de CISA en los Estados Unidos*

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) de los Estados Unidos ha desarrollado un enfoque integral para el uso de IA en la protección de infraestructuras críticas que ofrece enseñanzas relevantes desde una perspectiva comparada. CISA ha publicado directrices sobre el uso responsable de IA en el ámbito de la ciberseguridad que establecen principios de transparencia, supervisión humana, privacidad y rendición de cuentas.

La experiencia de CISA ilustra la importancia de distinguir entre los usos defensivos de la IA (protección de sistemas propios, detección de intrusiones, respuesta a incidentes) y los usos ofensivos o de vigilancia (identificación de actores, seguimiento de individuos, análisis de comunicaciones). Mientras los primeros son menos controvertidos desde el punto de vista de los derechos fundamentales, los segundos requieren garantías jurídicas adicionales y mecanismos de supervisión más robustos.

5.7. *Los marcos de Naciones Unidas sobre inteligencia artificial y contraterrorismo*

El sistema de Naciones Unidas ha producido en los últimos años un cuerpo de trabajo específicamente orientado a la relación entre inteligencia artificial y prevención del terrorismo, que resulta directamente aplicable al objeto de este estudio. La Oficina de las Naciones Unidas contra el Terrorismo y el UNICRI (2021) documentaron tanto el uso malicioso de estas tecnologías por actores terroristas como su empleo por agencias estatales para la detección de contenidos y el análisis de redes, y concluyeron que la capacidad técnica avanza con mayor rapidez que los marcos de garantía que deberían acompañarla.

Con mayor densidad jurídica, el documento de posición del Relator Especial sobre la promoción y protección de los derechos humanos en la lucha contra el terrorismo (ACNUDH, 2025) examina los riesgos que estos sistemas proyectan sobre la igualdad y la no discriminación, la privacidad, la libertad de expresión, el debido proceso y el derecho a un recurso efectivo. El documento subraya que las obligaciones internacionales en materia de derechos humanos vinculan a los Estados con independencia del grado de automatización de la decisión, y que la delegación de funciones en proveedores privados no desplaza esa responsabilidad. Se trata de un referente relevante para México, en tanto proviene de un mecanismo del propio sistema universal cuya doctrina interpretativa incide sobre el cumplimiento de las obligaciones convencionales asumidas por el Estado.

6. Estudios de caso: el control jurisdiccional de la prevención algorítmica

Los marcos normativos revisados enuncian principios, pero es en sede jurisdiccional donde se observa cómo esos principios operan frente a sistemas concretos. Los tres casos que se examinan a continuación comparten un rasgo: en todos ellos una autoridad pública desplegó un sistema de evaluación algorítmica de riesgo y un tribunal verificó si la habilitación normativa y las garantías asociadas resultaban suficientes. Su interés para el objeto de este trabajo no reside en la identidad del fenómeno regulado, sino en la estructura del razonamiento judicial aplicado.

6.1. *El caso SyRI (Países Bajos, 2020)*

El Tribunal de Distrito de La Haya resolvió, el 5 de febrero de 2020, la impugnación del *Systeem Risico Indicatie* (SyRI), una herramienta estatal que cruzaba bases de datos de distintas administraciones para generar informes de riesgo sobre personas presuntamente vinculadas a fraude en materia de seguridad social. El tribunal declaró que la legislación habilitante era incompatible con el artículo 8.2 del Convenio Europeo de Derechos Humanos, al no superar el juicio de necesidad en una sociedad democrática ni el equilibrio exigible entre finalidad perseguida e injerencia en la vida privada (Rechtbank Den Haag, 2020).

Tres elementos del razonamiento resultan trasladables. El primero es que la legitimidad del fin, la lucha contra el fraude no bastó para validar el medio. El segundo es que la opacidad del modelo de riesgo, cuyos indicadores no fueron divulgados, impidió tanto el escrutinio público como la defensa individual, lo que el tribunal valoró como una insuficiencia de garantías y no como una decisión técnica discrecional. El tercero es que las personas incluidas en los registros de riesgo no eran notificadas, de modo que no podían conocer ni impugnar su clasificación. Trasladado al ámbito del ciberterrorismo, donde las exigencias de reserva son todavía más intensas, este último punto anticipa el problema central: si la afectación permanece invisible para el afectado, el derecho al recurso se vacía de contenido.

6.2. *El caso Ligue des droits humains (Tribunal de Justicia de la Unión Europea, 2022)*

Este pronunciamiento es el más directamente pertinente, pues examina un sistema de tratamiento automatizado diseñado precisamente para prevenir delitos de terrorismo. En su sentencia de 21 de junio de 2022, la Gran Sala del Tribunal de Justicia analizó la validez de la Directiva (UE) 2016/681, relativa al uso de los datos del registro de nombres de los pasajeros, y admitió su compatibilidad con la Carta de los Derechos Fundamentales únicamente bajo una interpretación estricta, reconociendo que el régimen entraña injerencias serias en los derechos a la vida privada y a la protección de datos (Tribunal de Justicia de la Unión Europea, 2022).

Dos precisiones del fallo tienen valor de estándar. La primera es la exclusión de los sistemas de aprendizaje automático capaces de modificar sin intervención ni revisión humana los criterios de evaluación: el tribunal razonó que tal capacidad de autoadaptación impide que el revisor humano y la persona afectada conozcan las razones de una coincidencia positiva, lo que priva de contenido a la supervisión y al control judicial. La segunda es la exigencia de que los criterios preestablecidos de evaluación sean específicos, fiables y no discriminatorios, y que toda coincidencia sea objeto de revisión individual por medios no automatizados antes de producir efecto alguno.

Para el objeto de este trabajo, la enseñanza es doble. Por una parte, confirma que la finalidad antiterrorista, aun siendo un objetivo de interés general de primer orden, no funciona como habilitación abierta para el tratamiento masivo ni para la autonomía técnica del sistema. Por otra, ofrece un criterio operativo poco frecuente en los instrumentos de *soft law*: la opacidad derivada del autoaprendizaje no es un inconveniente que deba mitigarse, sino una razón para excluir esa arquitectura del ámbito preventivo estatal.

6.3. *El caso Bridges (Reino Unido, 2020)*

El Tribunal de Apelación de Inglaterra y Gales declaró ilícito el uso de reconocimiento facial automatizado en vivo por la policía de Gales del Sur, por tres motivos convergentes: la ausencia de una base legal suficiente que delimitara a quién podía incluirse en las listas de vigilancia y dónde podía desplegarse el sistema, la insuficiencia de la evaluación de impacto en materia de protección de datos, y el incumplimiento del deber de valorar si el software presentaba sesgos por razón de sexo o de origen étnico (Court of Appeal of England and Wales, 2020).

El fallo es útil porque muestra que el déficit de habilitación normativa no se localiza en la ausencia de norma, sino en su indeterminación: existían códigos de práctica y procedimientos internos, pero ninguno resolvía las preguntas sobre el quién y el dónde. Esa exigencia de precisión coincide con lo sostenido en el apartado 4.1 y refuerza la conclusión de que las cláusulas genéricas de seguridad no satisfacen el principio de legalidad. El tercer motivo añade un elemento procedimental relevante: la evaluación del sesgo no fue tratada como una buena práctica técnica, sino como una obligación jurídica cuyo incumplimiento vició el despliegue.

6.4. Lecciones transversales para el diseño de la prevención algorítmica

Leídos en conjunto, los tres casos revelan un patrón argumentativo estable. Los tribunales no cuestionan la legitimidad del fin preventivo ni la utilidad de la herramienta; lo que examinan es la densidad de la habilitación legal, la posibilidad efectiva de reconstruir el funcionamiento del sistema en un caso concreto, la existencia de una revisión humana con capacidad real de contradicción y la disponibilidad de un recurso para la persona clasificada. Cuando alguno de estos elementos falta, la ilicitud se declara con independencia del rendimiento técnico del sistema.

Este patrón permite formular una advertencia para el debate mexicano. La discusión pública sobre inteligencia artificial en seguridad tiende a plantearse en términos de capacidad instalada, presupuesto y adquisición tecnológica. Los casos examinados muestran que el punto crítico se sitúa antes: sin una norma que determine finalidades, sujetos, datos y controles, y sin vías de impugnación accesibles, el despliegue queda expuesto a una declaración de invalidez que puede inutilizar la inversión realizada. La regulación garantista no opera aquí como un freno a la innovación, sino como condición de su sostenibilidad jurídica.

7. El caso mexicano y la necesidad de una regulación garantista

7.1. Marco constitucional y normativo existente

México enfrenta una realidad compleja en la que convergen vulnerabilidades tecnológicas, dependencia creciente de servicios digitales, riesgos a infraestructura crítica y presencia de dinámicas criminales con capacidad de adaptación. En ese contexto, la idea de fortalecer capacidades estatales de detección y prevención mediante IA resulta comprensible. No obstante, la necesidad institucional no equivale a habilitación jurídica automática.

El ordenamiento mexicano dispone de bases constitucionales para afirmar la obligación estatal de protección, pero carece todavía de una regulación específica y suficientemente desarrollada sobre gobernanza algorítmica pública en tareas preventivas de alta sensibilidad. Persisten preguntas esenciales: qué autoridades podrían utilizar estos sistemas, bajo qué finalidades exactas, con qué parámetros de activación, qué tipo de datos podrían procesarse, qué controles externos deberían intervenir y qué derechos tendrían las personas eventualmente afectadas por decisiones o clasificaciones asistidas por IA.

La Constitución Política de los Estados Unidos Mexicanos establece en su artículo 6° el derecho de acceso a la información pública y la protección de datos personales como derechos fundamentales. El artículo 16 constitucional consagra el derecho a la privacidad y establece que las comunicaciones privadas son inviolables, salvo mediante resolución de autoridad judicial y con las formalidades previstas en la ley. Estas disposiciones constitucionales constituyen el piso mínimo de protección que cualquier sistema de detección algorítmica del ciberterrorismo debe respetar. Por su parte, el Código

Penal Federal no contiene una definición autónoma del ciberterrorismo como tipo penal, lo que obliga a recurrir a la figura general del terrorismo (artículo 139 CPF) y a los delitos informáticos (artículo 211 bis CPF), con las dificultades que ello conlleva en términos de determinación y previsibilidad normativa.

7.2. Instituciones competentes y estado actual de las capacidades

En el ámbito de la ciberseguridad, México cuenta con diversas instituciones con competencias relevantes, aunque su coordinación no siempre es clara. La Secretaría de Seguridad y Protección Ciudadana (SSPC) y la Policía Federal Ministerial tienen competencias en materia de investigación de delitos cibernéticos. La Guardia Nacional cuenta con una División Científica con capacidades en ciberseguridad e investigación digital. La Secretaría de la Defensa Nacional (SEDENA) y la Secretaría de Marina (SEMAR) tienen capacidades de ciberdefensa dentro de sus respectivos ámbitos. El Centro Nacional de Inteligencia (CNI) tiene funciones de inteligencia estratégica que incluyen el ciberespacio como dominio de atención.

Esta distribución institucional genera el riesgo de duplicación de esfuerzos, falta de coordinación y vacíos en la cadena de mando, especialmente en la respuesta a incidentes que tienen simultáneamente dimensiones de seguridad pública y seguridad nacional. La Estrategia Nacional de Ciberseguridad publicada en 2017 estableció un marco general de gobernanza en la materia, pero no fue acompañada de la legislación específica necesaria para su implementación efectiva, ni contempló de manera expresa el uso de sistemas de IA en las funciones de detección y prevención.

Es menester mencionar que esta última mencionada se encuentra en el total olvido y se requiere una actualización necesaria, al ser la primera y única política pública para el Estado mexicano en la materia (hasta la fecha). Lo anterior es únicamente mencionado para tener un entendimiento del contexto de México.

7.3. La brecha normativa y sus consecuencias

Esta ausencia de definición normativa genera un doble riesgo. Por un lado, puede provocar parálisis institucional o subutilización de herramientas potencialmente valiosas. Por otro, puede alentar implementaciones improvisadas, tecnocráticas u opacas, basadas más en disponibilidad tecnológica que en legitimidad constitucional. Entre ambos extremos, la única salida jurídicamente sostenible es una regulación garantista que integre desde el origen exigencias de legalidad, documentación, evaluación de impacto, auditoría, supervisión humana y vías de revisión.

En el contexto latinoamericano, México no es el único país que enfrenta esta brecha. Una revisión de los marcos normativos regionales muestra que, a diferencia de la Unión Europea o Estados Unidos, América Latina carece de regulaciones específicas sobre el uso de IA en seguridad pública

y prevención del terrorismo. En América Latina existen desarrollos normativos y de política pública heterogéneos en materia de protección de datos e inteligencia artificial; sin embargo, todavía no se observa una regulación regional consolidada sobre el uso estatal de IA en seguridad pública y prevención del terrorismo.

Esta situación regional contrasta con la persistencia de incidentes cibernéticos contra infraestructuras gubernamentales y servicios esenciales, lo que evidencia la necesidad de fortalecer capacidades institucionales y marcos normativos, así es como se abre una brecha entre la escalada de las amenazas y el rezago normativo es uno de los principales desafíos que enfrentan los sistemas jurídicos de la región.

8. Criterios mínimos para un uso legítimo de IA en esta materia

A partir del análisis desarrollado, es posible sostener que el uso de IA por autoridades públicas para la detección y prevención del ciberterrorismo sólo sería jurídicamente defendible si se cumplen de manera acumulativa ciertos criterios mínimos.

8.1. *Finalidad legítima, específica y delimitada*

En primer lugar, debe existir una finalidad legítima, específica y delimitada. La herramienta no puede habilitarse para fórmulas abiertas de seguridad o vigilancia general. Debe quedar claramente definido si su objetivo es proteger infraestructuras críticas, fortalecer la respuesta a incidentes o detectar amenazas concretas sobre sistemas estratégicos. El principio de finalidad, consagrado tanto en la LGPDPPSO como en los marcos internacionales revisados, exige que los datos no puedan ser tratados para finalidades distintas a las originalmente declaradas. En el contexto de los sistemas de IA, esto implica que el sistema debe ser diseñado para una función específica y no debe utilizarse para identificar, monitorear o clasificar a personas por razones distintas a la prevención del ciberterrorismo.

8.2. *Base normativa suficiente*

En segundo lugar, se requiere una base normativa suficiente. La regulación debe precisar autoridades competentes, categorías de datos, límites temporales, supuestos de activación, mecanismos de documentación y controles institucionales. Sin ello, el uso de IA se convierte en una práctica administrativa sin contornos jurídicos claros. Siguiendo el estándar de “calidad de la ley” desarrollado por el TEDH, la norma habilitante debe ser accesible al público, estar formulada con suficiente precisión para que los ciudadanos puedan prever, en la medida de lo razonablemente posible, las circunstancias en que las autoridades pueden recurrir a tales medidas, y contener garantías adecuadas contra los abusos.

8.3. *Idoneidad, necesidad y proporcionalidad*

En tercer término, es imprescindible superar un análisis de idoneidad, necesidad y proporcionalidad. La adopción del sistema debe justificarse como adecuada al fin perseguido, necesaria frente a la ausencia de medios menos intrusivos y proporcional en relación con la intensidad de afectación a derechos fundamentales. El test de proporcionalidad, ampliamente desarrollado por la doctrina constitucional y aplicado por los tribunales constitucionales en el ámbito iberoamericano, exige una fundamentación que demuestre:

1. que el sistema es apto para contribuir a la finalidad preventiva perseguida;
2. que no existen medios alternativos igualmente eficaces, pero menos restrictivos de derechos; y
3. que los beneficios en términos de seguridad son superiores a los costos en términos de restricción de derechos. Este análisis debe realizarse ex ante, antes del despliegue del sistema, y revisarse periódicamente para evaluar si las condiciones que lo justificaron siguen siendo válidas.

8.4. *Supervisión humana significativa*

En cuarto lugar, la supervisión humana significativa es indispensable. Ningún sistema debería generar por sí solo decisiones que afecten derechos, activen investigaciones o produzcan consecuencias jurídicas relevantes sin revisión humana cualificada y documentada. La UNESCO (2021) y la OCDE (2023) coinciden en subrayar que la supervisión humana no puede ser meramente formal. No basta con que exista un funcionario responsable en el organigrama; la supervisión debe ser efectiva, lo que implica que el funcionario debe tener la información, la formación y la autoridad necesarias para entender las recomendaciones del sistema, cuestionarlas cuando sea necesario y asumir la responsabilidad de la decisión final. El Reglamento (UE) 2024/1689 operacionaliza esta exigencia estableciendo que los sistemas de IA de alto riesgo deben ser diseñados de manera que los operadores humanos puedan ignorar, interrumpir o revocar las salidas del sistema en tiempo real.

8.5. *Calidad de datos, auditoría y validación independiente*

En quinto lugar, deben garantizarse calidad de datos, auditoría y validación independiente. Ello incluye evaluación de sesgos, pruebas de robustez, revisión continua y protocolos de suspensión o corrección ante errores estructurales. El NIST AI RMF (2023) establece que la gestión de la calidad de los datos es un componente esencial de la gobernanza de los sistemas de IA. Los datos de entrenamiento, validación y prueba deben ser representativos del dominio de aplicación, deben estar documentados y deben ser sometidos a evaluaciones periódicas de calidad. En el contexto de los sistemas de detección del ciberterrorismo, esto implica que los datos utilizados deben reflejar adecuadamente el panorama de amenazas actual y no estar sesgados hacia determinados tipos de actores, técnicas o vectores de ataque.

8.6. Trazabilidad y explicabilidad

En sexto lugar, debe asegurarse trazabilidad y explicabilidad suficiente. La autoridad tiene que poder reconstruir el funcionamiento del sistema en un caso concreto y justificar cómo su salida fue incorporada a la decisión institucional.

8.7. Régimen de impugnación y responsabilidad

En séptimo lugar, debe existir un régimen claro de impugnación y responsabilidad. La persona afectada por una actuación asistida por IA debe contar con medios efectivos de revisión y reparación. La administración no puede diluir su responsabilidad en el algoritmo ni en el proveedor tecnológico. Este principio de responsabilidad indelegable de las autoridades públicas es reconocido tanto por la OCDE (2023) como por el Reglamento (UE) 2024/1689, que establece expresamente que el uso de sistemas de IA de alto riesgo por entidades públicas no exime a dichas entidades de su responsabilidad jurídica conforme al derecho aplicable. En el ordenamiento mexicano, este principio encuentra apoyo en el régimen de responsabilidad patrimonial del Estado previsto en el artículo 113 de la Constitución Política de los Estados Unidos Mexicanos y en la Ley Federal de Responsabilidad Patrimonial del Estado.

9. Hacia una regulación garantista: propuestas para el contexto mexicano

El análisis desarrollado en las secciones precedentes permite formular algunas propuestas concretas para avanzar hacia una regulación garantista del uso de IA por autoridades públicas en la detección y prevención del ciberterrorismo en México. Estas propuestas no pretenden ser exhaustivas, sino orientar el debate legislativo y normativo hacia los elementos mínimos que una regulación de este tipo debería incorporar.

Una condición previa a cualquier regulación del uso de IA en la prevención del ciberterrorismo es contar con una definición jurídica clara y precisa de la conducta que se pretende prevenir. La ausencia de un tipo penal específico de ciberterrorismo en el Código Penal Federal genera una indeterminación normativa que es incompatible con el principio de legalidad y dificulta la delimitación del objeto preventivo de los sistemas algorítmicos. El legislador mexicano debería considerar la tipificación autónoma del ciberterrorismo, siguiendo los estándares de la Resolución 1373 del Consejo de Seguridad de las Naciones Unidas (Consejo de Seguridad de las Naciones Unidas, 2001).

El ordenamiento mexicano requiere una ley o un marco normativo específico que regule el uso de sistemas de IA por autoridades públicas en funciones de seguridad y prevención. Esta norma debería:

1. delimitar con precisión las autoridades competentes y sus respectivos ámbitos de actuación;
2. establecer un catálogo cerrado de finalidades para las cuales el uso de IA está autorizado;
3. definir los tipos de datos que pueden ser procesados por los sistemas, con prohibiciones expresas respecto a categorías especialmente sensibles;
4. establecer períodos máximos de conservación de datos y mecanismos de depuración;
5. crear un régimen de evaluación de impacto y auditoría independiente previo al despliegue de cualquier sistema; y
6. establecer mecanismos de revisión judicial efectiva de las actuaciones asistidas por IA.

La gobernanza del uso de IA en seguridad pública requiere un órgano de supervisión independiente, dotado de las competencias técnicas y jurídicas necesarias para evaluar el cumplimiento de los requisitos normativos, realizar auditorías, recibir quejas y emitir sanciones.

Dada la naturaleza transfronteriza del ciberterrorismo, México debería avanzar en la adhesión al Convenio de Budapest y en la negociación de acuerdos de cooperación bilateral y multilateral que permitan el intercambio de información, la asistencia técnica y la armonización de estándares para el uso de IA en la prevención del ciberterrorismo. La cooperación no debe limitarse al intercambio de inteligencia, sino extenderse al desarrollo conjunto de estándares técnicos, marcos de evaluación de riesgos y mejores prácticas en el diseño y despliegue de sistemas algorítmicos.

10. Conclusiones

El uso de inteligencia artificial por autoridades públicas para detectar y prevenir el ciberterrorismo no puede ser presentado como una solución jurídicamente neutra ni como un instrumento cuya sola eficacia técnica legitima su despliegue. Se trata, por el contrario, de una de las áreas más delicadas del derecho público tecnológico, precisamente porque coloca a la innovación en el núcleo mismo del poder preventivo del Estado.

La prevención del ciberterrorismo exige capacidades institucionales reales. El Estado necesita herramientas para identificar anomalías, proteger infraestructuras críticas y responder con oportunidad frente a amenazas complejas. Sin embargo, esa necesidad no autoriza la sustitución de la racionalidad jurídica por una lógica de automatización opaca. La prevención sigue siendo legítima sólo cuando permanece sometida a legalidad, proporcionalidad, supervisión y responsabilidad.

La revisión de los marcos internacionales y comparados muestra una convergencia clara: los usos públicos de IA en contextos sensibles sólo pueden admitirse bajo condiciones reforzadas de gobernanza y control. Esta convergencia es visible en la Recomendación de la UNESCO (2021), la Recomendación de la OCDE (2023), el NIST AI RMF (2023) y el Reglamento (UE) 2024/1689, que comparten un núcleo común de principios: legalidad, finalidad legítima, proporcionalidad, supervisión humana, trazabilidad, explicabilidad y responsabilidad.

Esa lección resulta plenamente aplicable al caso mexicano. Si el país opta por avanzar en el uso estatal de IA para la detección y prevención del ciberterrorismo, deberá hacerlo mediante una regulación específica, garantista y técnicamente seria, capaz de evitar que la promesa de anticipación tecnológica se convierta en una forma sofisticada de erosión de derechos fundamentales.

La experiencia jurisdiccional comparada refuerza esta conclusión con un dato práctico. En los tres casos analizados, los tribunales invalidaron el despliegue no por deficiencias en el rendimiento de los sistemas, sino por insuficiencia de la habilitación normativa, opacidad del modelo de riesgo o ausencia de vías de impugnación para las personas clasificadas. La lección para el legislador mexicano es que el diseño normativo previo no constituye un obstáculo para la adopción tecnológica, sino la condición que permite sostenerla en el tiempo.

El análisis del caso mexicano revela tres déficits normativos que deben abordarse de manera prioritaria: la ausencia de un tipo penal específico de ciberterrorismo, la falta de una regulación específica para el uso de IA en seguridad pública, y la inexistencia de un órgano de supervisión independiente con capacidades técnicas y jurídicas suficientes para el control de los sistemas algorítmicos. Superar estos déficits no es sólo una exigencia de modernización normativa, sino una condición para que el Estado pueda ejercer legítimamente sus funciones preventivas en el entorno digital.

En definitiva, la pregunta correcta no es si el Estado debe usar inteligencia artificial para enfrentar riesgos digitales complejos, sino bajo qué condiciones constitucionales puede hacerlo sin desfigurar el orden democrático que pretende proteger. La respuesta sostenible es clara: sólo dentro de una arquitectura de legalidad, auditoría, transparencia, supervisión humana y revisión efectiva.

11. Referencias

Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2025). Protecting human rights while using artificial intelligence to counter terrorism (PP/AI/CT). Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo.

Boix Palop, A. (2020). Los algoritmos son reglamentos: La necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones. *Revista de Derecho Público: Teoría y Método*, 1, 223-270.

Código Penal Federal. Cámara de Diputados.

Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión. (2013). *Libertad de expresión e internet*. OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13.

Constitución Política de los Estados Unidos Mexicanos. Cámara de Diputados.

Consejo de Seguridad de las Naciones Unidas. (2001). *Resolución 1373 (2001)*. S/RES/1373(2001).

- Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism*, 40(1), 77-98.
- Cotino Hueso, L. (2023). Reconocimiento facial automatizado y sistemas de identificación biométrica bajo la regulación superpuesta de inteligencia artificial y protección de datos. En F. Balaguer Callejón y L. Cotino Hueso (Coords.), *Derecho público de la inteligencia artificial* (pp. 347-402). Fundación Manuel Giménez Abad.
- Court of Appeal of England and Wales. (2020). *R (on the application of Bridges) v. The Chief Constable of South Wales Police*, [2020] EWCA Civ 1058, sentencia de 11 de agosto de 2020.
- Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*, ETS No. 185.
- Cybersecurity and Infrastructure Security Agency. (2023). *2023–2024 CISA Roadmap for Artificial Intelligence*. U.S. Department of Homeland Security.
- Danaher, J., Hogan, M. J., Noone, C., Kennedy, R., Behan, A., De Paor, A., Felzmann, H., Haklay, M., Khoo, S. M., Mingoia, J., & Shankar, R. (2017). Algorithmic governance: Developing a research agenda through the power of collective intelligence. *Big Data & Society*, 4(2), 1-21
- Denning, D. E. (2000). *Cyberterrorism*. Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives.
- European Court of Human Rights. (1978). *Klass and Others v. Germany*, Application no. 5029/71, Judgment of 6 September 1978.
- European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*.
- European Union Agency for Cybersecurity. (2023). *Artificial Intelligence and Cybersecurity Research*. ENISA.
- Ley Federal de Responsabilidad Patrimonial del Estado. (2004). Diario Oficial de la Federación.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. (2017). Diario Oficial de la Federación.
- Macdonald, S., Jarvis, L., & Lavis, S. (2022). Cyberterrorism today? Findings from a follow-on survey of researchers. *Studies in Conflict & Terrorism*, 45(8), 727-752.
- Mayer Lux, L. (2018). Una definición de ciberterrorismo. *Revista Chilena de Derecho y Tecnología*, 7(2), 5-25.
- Naciones Unidas. (2000). *Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional*. Oficina de las Naciones Unidas contra la Droga y el Delito.
- National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. U.S. Department of Commerce.
- Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an

algorithm used to manage the health of populations. *Science*, 366(6464), 447-453.

OCDE. (2023). *Recommendation of the Council on Artificial Intelligence*.

Oficina de las Naciones Unidas contra el Terrorismo y Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia. (2021). Algorithms and terrorism: The malicious use of artificial intelligence for terrorist purposes. UNOCT-UNCCT y UNICRI.

Organización de los Estados Americanos. (1969). *Convención Americana sobre Derechos Humanos*.

Rechtbank Den Haag. (2020). NJCM y otros c. Estado de los Países Bajos (SyRI), ECLI:NL:RBDHA:2020:1878, sentencia de 5 de febrero de 2020.

Secretaría de la Presidencia. (2017). *Estrategia Nacional de Ciberseguridad*. Gobierno de México.

Tribunal de Justicia de la Unión Europea. (2022). Ligue des droits humains ASBL c. Conseil des ministres, asunto C-817/19, ECLI:EU:C:2022:491, sentencia de la Gran Sala de 21 de junio de 2022.

UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence*.

UNODC. (s. f.). *Module 14: Hacktivism, terrorism, espionage, disinformation campaigns and cyber warfare*. Education for Justice Initiative.

Veale, M., y Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4), 97-112.

Venkatachary, S. K., Prasad, J., Alagappan, A., Andrews, L. J. B., Raj, R. A., & Duraisamy, S. (2024). Cybersecurity and cyber-terrorism challenges to energy-related infrastructures: Cybersecurity frameworks and economics: Comprehensive review. *International Journal of Critical Infrastructure Protection*, 45, 100677.

Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, 12(4), 505-523.

Nota de autor respecto al uso de Inteligencia Artificial: Se aclara que el uso de herramientas de Inteligencia Artificial Generativa tuvo un carácter estrictamente auxiliar, instrumental y no sustantivo dentro del proceso de preparación del manuscrito. Su empleo se limitó a tareas de revisión formal del texto, tales como corrección ortográfica, puntuación, acentuación, concordancia gramatical, depuración de repeticiones, mejora de fluidez sintáctica, uniformidad estilística y adecuación del registro académico. En este sentido, la herramienta funcionó como un apoyo editorial comparable a una revisión lingüística o de estilo, orientada a mejorar la claridad, legibilidad y corrección formal del manuscrito, sin sustituir el trabajo intelectual del autor. De manera específica, no se utilizó Inteligencia Artificial Generativa para producir contenido sustantivo del artículo, formular el problema de investigación, construir el enfoque teórico, definir la metodología, elaborar el análisis, interpretar hallazgos, generar argumentos, redactar apartados completos, incorporar ideas nuevas, producir conclusiones, seleccionar bibliografía ni crear referencias. Las decisiones académicas, conceptuales, metodológicas y argumentativas permanecieron bajo responsabilidad exclusiva del autor, quien revisó, validó y conservó el control sobre cada modificación formal realizada al texto. Asimismo, se precisa que el uso de la herramienta no tuvo por finalidad llenar vacíos de contenido, desarrollar secciones no elaboradas previamente ni reemplazar procesos propios de investigación, lectura, análisis crítico o escritura académica. El manuscrito fue concebido, estructurado y desarrollado por el autor; la asistencia tecnológica se empleó únicamente en una fase posterior de revisión lingüística y normalización formal, con el propósito de fortalecer la presentación académica del texto sin alterar su autoría, originalidad, contenido científico ni responsabilidad intelectual.

Luis Miguel Hernández Flores, Cristian Fernando Hernández Fores, Carlos Eduardo Ortega Tapia y Miguel Iván Pazmiño Sotomayor

Convergencia entre crimen organizado transnacional y terrorismo contemporáneo en América Latina: el caso ecuatoriano entre pragmatismo y utopía

Convergence between transnational organized crime and contemporary terrorism in Latin America: the Ecuadorian case between pragmatism and utopia

Resumen

El presente artículo examina la convergencia entre el crimen organizado transnacional y el uso instrumental del terror en América Latina, con especial énfasis en el caso ecuatoriano. Mediante un enfoque cualitativo-documental de alcance analítico-interpretativo, se integran literatura académica, informes de organismos internacionales, estadísticas oficiales y fuentes documentales verificables. El análisis sugiere que Ecuador constituye un caso especialmente ilustrativo de esta convergencia, observable en el aumento de la violencia letal, el uso de explosivos, la expansión de economías ilícitas y la actividad de actores armados no estatales con capacidad de autoridad fáctica en territorios estratégicos. Este estudio argumenta que las respuestas estatales predominantemente reactivas evidencian límites estructurales frente a amenazas híbridas de carácter adaptativo y transnacional. En consecuencia, se concluye que la efectividad de las respuestas estatales frente a esta amenaza híbrida depende de la articulación sostenida entre la comprensión del contexto internacional, control territorial, inteligencia financiera, investigación criminal especializada, cooperación internacional y prevención estructural de la violencia, más que de medidas coercitivas episódicas.

Palabras clave: crimen organizado, gobernanza criminal, terrorismo, seguridad regional

Abstract

This study examines the convergence between transnational organized crime and the instrumental use of terror in Latin America, with particular emphasis on the Ecuadorian case. Through a qualitative documentary approach with an analytical-interpretive scope, the study integrates academic literature, reports from international organizations, official statistics, and verifiable documentary sources. The analysis suggests that Ecuador constitutes a particularly illustrative case of this convergence, visible in the rise of lethal violence, the use of explosives, the expansion of illicit economies, and the activity of non-state armed actors with criminal governance capacity. This study argues that predominantly reactive state responses show structural limitations when confronted with hybrid threats of an adaptive and transnational nature. Consequently, it concludes that the effectiveness of state responses to this hybrid threat depends understanding the international context, the sustained articulation of territorial control, financial intelligence, specialized criminal investigation, international cooperation, and structural violence prevention, rather than on episodic coercive measures.

Keywords: organized crime, criminal governance, terrorism, regional security

Luis Miguel Hernández Flores, Capitán de Policía (Ecuador), Prospectivista, Especialista en Análisis de Inteligencia Estratégica, Ciberinteligencia y Contraterrorismo.

Cristian Fernando Hernández Fores, Teniente de Policía (Ecuador), Criminólogo, Especialista en Análisis de Crimen Organizado, Investigación Criminal y Terrorismo.

Carlos Eduardo Ortega Tapia, Coronel de Policía de Estado Mayor (Ecuador), Fue Director Nacional de Investigación Antidrogas, Jefe Nacional de la Unidad de Investigación Antidelincuencial y Agregado Policial de Ecuador en España.

Miguel Iván Pazmiño Sotomayor, Coronel de Policía de Estado Mayor (Ecuador), Fue Agregado Policial de Ecuador en Estados Unidos de América y Jefe Nacional de la Unidad de Lucha Contra el Crimen Organizado.

Para citar este artículo: Hernández Flores, L. et al. (2026), Convergencia entre crimen organizado transnacional y terrorismo contemporáneo en América Latina: el caso ecuatoriano entre pragmatismo y utopía, Revista Internacional de Estudios sobre Terrorismo, nº18, pp.30-48.

Recibido

23/04/2026

Aceptado

13/08/2026

1. Introducción

Ecuador enfrenta una transformación estructural de su escenario de seguridad, marcada por la convergencia entre criminalidad organizada transnacional, violencia extrema y dinámicas transfronterizas. Este proceso no constituye un fenómeno aislado ni exclusivamente coyuntural, sino que se inscribe en una tendencia regional latinoamericana en la que las organizaciones criminales han evolucionado hacia configuraciones con capacidad de incidir sobre la vida social y política. Esta transformación es facilitada por esquemas de neopatrimonialismo, donde el uso privado de la función pública incentiva una interdependencia funcional que permite a las estructuras criminales establecer órdenes locales ante la limitada presencia institucional del Estado (Alda-Mejías, 2021).

La literatura especializada en seguridad, criminología y gobernanza criminal ha conceptualizado esta mutación a partir de categorías como crimen organizado transnacional, gobernanza criminal y, en trabajos recientes, neocrimen organizado ¹(Hernández & Hernández, 2024). En este artículo, dicho término se emplea en sentido heurístico, sin pretender consolidarlo como categoría teórica establecida, con el propósito de aprehender la complejidad de las estructuras criminales contemporáneas más allá del narcotráfico clásico o de las bandas locales. El neocrimen se caracteriza por su lógica empresarial, su diversificación de portafolios ilícitos (narcotráfico, extorsión, minería ilegal, tráfico de armas, sicariato y lavado de activos), su articulación en redes transnacionales y su capacidad de operar simultáneamente en espacios urbanos, portuarios, carcelarios y fronterizos (Feldmann & Luna, 2022; Shelley, 2014). A diferencia de las organizaciones criminales del pasado, estas estructuras no dependen exclusivamente de liderazgos jerárquicos rígidos, sino que combinan jerarquía y redes flexibles, lo que incrementa su resiliencia frente a la acción estatal.

En este contexto, uno de los rasgos más relevantes del neocrimen organizado es el uso instrumental de repertorios de violencia asociados al terrorismo contemporáneo como mecanismo de control social, comunicación estratégica y disciplinamiento territorial. Lejos de responder a una motivación ideológica clásica, la violencia extrema, incluido el uso de explosivos, coches bomba, atentados selectivos y amenazas indiscriminadas, se integra al repertorio criminal como una táctica funcional, orientada a generar miedo colectivo, inhibir la cooperación ciudadana con el Estado y presionar decisiones institucionales en materia de seguridad y justicia (Farber, 2025; Makarenko, 2004; Phillips, 2018). Esta convergencia funcional entre crimen organizado y terrorismo ha sido reconocida incluso en el ámbito del derecho internacional y la seguridad global, al advertirse que ambos fenómenos comparten métodos, recursos y efectos desestabilizadores sobre la gobernabilidad democrática (Consejo de Seguridad de las Naciones Unidas [CSNU], 2019).

1 El neocrimen organizado emplea violencia extrema y tácticas de terror para obtener poder criminal, económico y territorial. No persigue fines ideológicos y genera graves consecuencias sociales, como el aumento de homicidios e inseguridad.

El caso ecuatoriano resulta particularmente ilustrativo de esta convergencia, ya que, durante los últimos años, el país ha registrado un deterioro acelerado de la seguridad interna, expresado en el aumento de la violencia letal, el colapso parcial del sistema penitenciario, la proliferación de armas y explosivos, y su posicionamiento estratégico como plataforma logística del narcotráfico transnacional, especialmente hacia mercados europeos y norteamericanos (Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC], 2024; Policía Nacional del Ecuador, 2024). Estas dinámicas se han visto agravadas por la fragmentación de las organizaciones criminales internas que se visibilizan descaradamente, y, por la creciente influencia de actores transnacionales que se mantienen en la invisibilidad, lo que ha generado disputas territoriales violentas y un escenario de inseguridad estructural.

Asimismo, en los espacios fronterizos amazónicos, la convergencia entre economías ilícitas, ausencia estatal y violencia armada ha propiciado la presencia y expansión de actores armados no estatales de orientación predominantemente criminal, como los Comandos de la Frontera. Estos grupos no solo controlan rutas estratégicas y economías ilegales, sino que también regulan la vida cotidiana de comunidades enteras mediante normas coercitivas, castigos ejemplarizantes y mecanismos de control social, configurando órdenes locales paralelos a la autoridad estatal (García-Pinzón & Mantilla, 2021; Williams et al., 2025).

Bajo este marco, el presente artículo propone analizar el impacto de la convergencia entre el crimen organizado transnacional y el terrorismo contemporáneo en América Latina, con especial énfasis en el caso ecuatoriano. El problema de investigación examina si la arquitectura estratégica del Estado frente a este fenómeno evidencia una adaptación pragmática y proporcional a la complejidad del neocrimen, o si permanece anclada en respuestas utópicas, reactivas y fragmentadas. Para ello, se adopta un enfoque cualitativo-documental de alcance analítico-interpretativo, que integra literatura académica especializada, informes de organismos internacionales, estadísticas oficiales y fuentes documentales verificables, con el propósito de aportar al debate sobre seguridad, gobernanza criminal y límites de la respuesta estatal frente a amenazas híbridas en contextos de alta criminalidad organizada.

2. Metodología

El presente estudio adopta un enfoque cualitativo-documental de alcance analítico-interpretativo, orientado a examinar la convergencia funcional entre crimen organizado transnacional y el uso instrumental del terror en América Latina, con énfasis en el caso ecuatoriano. La estrategia metodológica combinó revisión bibliográfica estructurada, análisis documental y examen interpretativo de casos recientes de alta relevancia pública e institucional, con el propósito de fortalecer el marco conceptual y la base empírica del manuscrito mediante fuentes académicas y documentales pertinentes.

El corpus bibliográfico se construyó mediante búsquedas estructuradas en Scopus, Web of Science y EBSCO. En total se identificaron 681 registros (Scopus, $n = 321$; Web of Science, $n = 185$; EBSCO, $n = 175$). Tras una depuración conservadora de duplicados exactos por DOI y título, el corpus quedó conformado por 488 registros únicos. Dado que el estudio no corresponde a una revisión sistemática de la literatura, no se aplicó un protocolo PRISMA, sino una selección intencional por pertinencia teórico-empírica. De ese universo se priorizó una muestra núcleo de 29 trabajos de utilidad directa para los cuatro ejes analíticos del manuscrito: (i) convergencia entre crimen organizado transnacional y terrorismo contemporáneo; (ii) indicadores empíricos del deterioro de la seguridad en Ecuador; (iii) gobernanza criminal y actuación de actores armados no estatales; y (iv) evaluación crítica de las respuestas estatales.

De manera complementaria, el estudio incorporó informes de organismos internacionales, estadísticas oficiales y documentos institucionales relevantes para el análisis del caso ecuatoriano, especialmente en materia de homicidios, incautaciones, violencia armada, actores armados no estatales y respuestas estatales. Asimismo, para el análisis de eventos recientes de alta visibilidad pública, se incorporaron fuentes periodísticas verificables y documentos institucionales concurrentes, utilizándolos con función contextual y de contraste, sin asignarles estatus probatorio autónomo cuando carecían de respaldo documental adicional. Este criterio buscó resguardar la trazabilidad de la información empírica y evitar inferencias no sustentadas a partir de fuentes secundarias aisladas.

Analíticamente, la revisión se organizó en torno a los cuatro ejes previamente descritos. El tratamiento del material fue de carácter interpretativo, orientado a identificar patrones recurrentes, convergencias conceptuales y tensiones entre literatura especializada, evidencia empírica disponible y discurso institucional.

Finalmente, se debe señalar que el estudio se apoya en fuentes secundarias de distinta densidad empírica, que el cribado bibliográfico priorizó pertinencia temática sobre exhaustividad, y que algunos eventos recientes del caso ecuatoriano dependen de información pública todavía sujeta a actualización. Estas limitaciones se discuten con mayor detalle en la sección correspondiente.

3. Convergencia entre crimen organizado transnacional y terrorismo contemporáneo: precisiones conceptuales

La convergencia entre crimen organizado transnacional y terrorismo contemporáneo² puede entenderse como un proceso de aproximación funcional y adaptación estratégica entre fenómenos que,

2 El terrorismo contemporáneo se manifiesta con el uso del terror como medio, instrumento y táctica, utiliza violencia, intimidación y nuevas tecnologías como drones para generar miedo, desestabilizar instituciones y alcanzar objetivos. Fuentes de inteligencia aseguran que en Ecuador y la región, se manifiesta principalmente mediante la convergencia con el crimen organizado con atentados con artefactos explosivos improvisados (AEI), amenazas y violencia extrema para controlar territorios y economías ilícitas.

aunque analíticamente distinguibles, pueden compartir repertorios de violencia, recursos logísticos, mecanismos financieros y formas de control territorial. En este sentido, la literatura clásica ha destacado que la relación entre ambos no debe reducirse a una fusión orgánica ni a una equivalencia conceptual automática, sino a un continuum de interacción que va desde vínculos instrumentales limitados hasta formas más complejas de cooperación, transformación o solapamiento operativo (Makarenko, 2004; Paoli & Fijnaut, 2022; Kleinschmidt & Palma, 2020). Esta distinción es importante, porque permite evitar clasificaciones excesivamente amplias y, al mismo tiempo, reconocer que determinados actores criminales adoptan tácticas, lenguajes y prácticas de intimidación que exceden la criminalidad convencional.

Desde esta perspectiva, la convergencia no implica que las organizaciones criminales persigan necesariamente fines ideológicos comparables a los del terrorismo clásico. Lo que la evidencia sugiere, más bien, es que ciertos grupos criminales incorporan repertorios de violencia de alta visibilidad y fuerte impacto psicológico cuando estos resultan funcionales para disciplinar territorios, inhibir la cooperación con el Estado, intimidar competidores o influir sobre decisiones políticas, judiciales y policiales. En América Latina, este patrón ha sido observado en casos donde la violencia pública, las amenazas abiertas, los ataques con explosivos y otras formas de comunicación coercitiva cumplen una función de ordenamiento criminal antes que de movilización ideológica (Bevilacqua et al., 2024; Johnson & Gillooly, 2023; Johnson, 2019; Phillips, 2018). La amenaza, en estos contextos, opera no solo como violencia física, sino también como mensaje de autoridad y regulación social.

La discusión más reciente ha desplazado el foco desde la sola violencia hacia la gobernanza criminal. Esta literatura muestra que numerosas estructuras criminales no se limitan a explotar rentas ilícitas, sino que establecen reglas, administran disputas, delimitan comportamientos aceptables y producen órdenes locales que pueden coexistir, competir o entrelazarse con la autoridad estatal. En el caso latinoamericano, este tipo de arreglos ha sido descrito como una de las transformaciones más relevantes de la relación entre crimen, política y violencia, ya que compromete la legitimidad estatal, los derechos fundamentales y la vigencia efectiva del Estado de derecho (Badillo-Sarmiento & Trejos-Rosero, 2025; Blattman et al., 2025; Feldmann & Luna, 2022). Desde este ángulo, la convergencia crimen-terror adquiere una dimensión más amplia: no se limita al uso de tácticas violentas, sino que se inserta en procesos de control social, territorial y simbólico con efectos directos sobre la gobernabilidad.

En América Latina, la literatura también advierte que estas dinámicas no son uniformes. Los patrones de convergencia varían según la densidad de las economías ilícitas, la fortaleza o fragmentación del aparato estatal, la relación entre actores armados y autoridades públicas, y el tipo de territorialidad en disputa. Estudios comparados sobre actores violentos no estatales en la región han cuestionado las versiones más expansivas de la hipótesis de convergencia, señalando que no toda combinación entre lucro, violencia y control territorial debe interpretarse como hibridación

plena entre crimen e insurgencia o entre crimen y terrorismo (Kleinschmidt & Palma, 2020). En la misma línea, investigaciones recientes sobre Tren de Aragua y otras estructuras regionales muestran que la transnacionalización criminal puede sostenerse a partir de franquicias, nodos territoriales, cooptación y coerción, sin que ello implique necesariamente una mutación hacia formas insurgentes clásicas (Sampó & Troncoso, 2024). Además, informes regionales recientes documentan que el lavado de activos, el tráfico de migrantes y otras economías ilícitas pueden operar como mecanismos de articulación entre crimen organizado transnacional y actores terroristas o híbridos en América Latina (Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia [UNICRI], 2024). En consecuencia, el uso del concepto debe ser analíticamente cuidadoso y empíricamente graduado.

La expansión de estos arreglos se ve favorecida por procesos más amplios de globalización ilícita, diversificación de mercados criminales y sofisticación de los mecanismos de financiamiento. La literatura reciente sobre el nexo crimen-terror ha subrayado que la convergencia no depende solo de repertorios de violencia, sino también de la circulación transnacional de capitales, tecnologías, armas, rutas y conocimientos tácticos. En particular, los mecanismos financieros ilícitos, los sistemas informales de transferencia de valor y el aprovechamiento de vacíos regulatorios fortalecen la capacidad de adaptación de organizaciones que combinan economías criminales con prácticas de intimidación de alto impacto (Farber, 2025; Jupp, 2025; Shelley, 2014). Del mismo modo, los corredores transfronterizos y las áreas periféricas con débil presencia estatal facilitan la consolidación de nodos criminales capaces de operar en varias jurisdicciones y de superar, en ocasiones, el nivel de coordinación interestatal disponible en la región (Penagos, 2024; Global Initiative Against Transnational Organized Crime, 2025).

En ese marco, la porosidad de las fronteras, la fragmentación institucional y la capacidad desigual de los Estados para producir seguridad contribuyen a que la violencia criminal adopte formas cada vez más expresivas, públicas y disciplinarias. La evidencia regional muestra que organizaciones criminales con vocación territorial pueden recurrir tanto a violencia letal como a violencia extra-letal, amenazas públicas y control reputacional para consolidar obediencia, resolver disputas y fijar jerarquías. Tales prácticas han sido documentadas, por ejemplo, en estudios sobre gobernanza criminal en ciudades colombianas y sobre violencia reputacional en México, donde la amenaza abierta constituye parte del ejercicio del poder criminal más que una mera externalidad del mercado ilícito (Badillo-Sarmiento & Trejos-Rosero, 2025; Johnson & Gillooly, 2023). Esta constatación resulta especialmente útil para el presente artículo, porque permite comprender la violencia extrema no solo como un problema de seguridad pública, sino como una tecnología de gobernanza criminal.

Desde una perspectiva estratégica, estos procesos plantean desafíos relevantes para las políticas de seguridad. Si la convergencia entre crimen organizado y terrorismo es variable, funcional y territorialmente situada, las respuestas basadas exclusivamente en categorías penales rígidas o

en esquemas tradicionales de lucha antiterrorista resultan insuficientes. La literatura coincide en la necesidad de enfoques más integrales, capaces de articular inteligencia financiera, control territorial, fortalecimiento institucional, cooperación internacional y comprensión de las formas locales de gobernanza criminal (Farber, 2025; Feldmann & Luna, 2022). En suma, más que asumir una identidad plena entre crimen organizado y terrorismo, el análisis contemporáneo tiende a reconocer una convergencia funcional, selectiva y empíricamente graduable, cuya expresión en América Latina exige marcos conceptuales flexibles, comparativos y atentos a la relación entre violencia, territorio y autoridad.

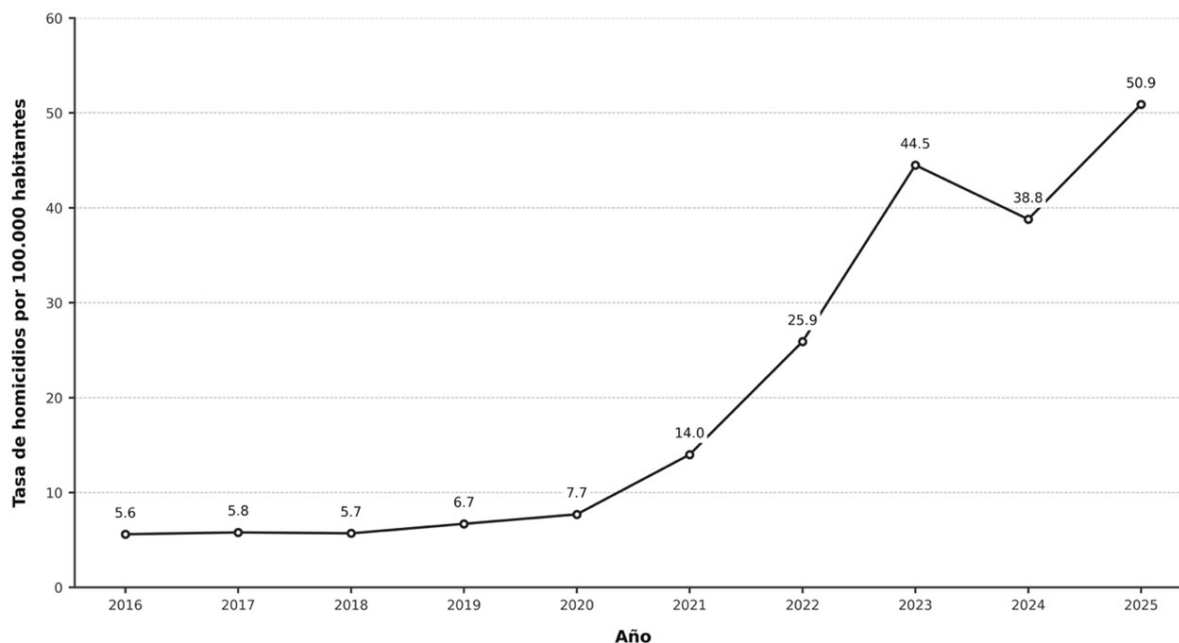
Figura 1. Portafolio de economías ilícitas y mecanismos funcionales del crimen organizado transnacional



Nota. Elaboración propia con base en Shelley (2014), Feldmann y Luna (2022) y Farber (2025).

4. El caso ecuatoriano: indicadores y manifestaciones de la convergencia

La evidencia disponible sitúa a Ecuador como un caso particularmente relevante para observar la convergencia funcional entre criminalidad organizada transnacional, violencia extrema y debilitamiento de la capacidad estatal. La serie reciente de homicidios intencionales muestra un deterioro abrupto de la seguridad interna: la tasa nacional pasó de 6,7 por cada 100.000 habitantes en 2019 a 46,5 en 2023, descendió a 38,8 en 2024 y registró un nuevo incremento en 2025, alcanzando 50,91 por cada 100.000 habitantes, según registros oficiales y series periodísticas elaboradas a partir de fuentes estatales (Ministerio del Interior del Ecuador, 2024; González, 2026; UNODC, 2024). Más que una progresión lineal, esta trayectoria sugiere un patrón de escalamiento, contención parcial y reactivación, consistente con disputas criminales adaptativas en contextos de intervención estatal intermitente.

Figura 2. Tasa de homicidios en Ecuador (2016-2025)

Nota. Elaboración propia con base en datos de Statista (2026).

Este deterioro no puede leerse de manera aislada del lugar que ha adquirido Ecuador en las rutas del narcotráfico regional. Las incautaciones superiores a 220 toneladas de sustancias sujetas a fiscalización registradas en 2024 confirman la centralidad logística del país dentro de circuitos ilícitos que articulan producción, acopio, tránsito y exportación hacia mercados extrarregionales. La coexistencia entre una interdicción creciente y la persistencia de niveles elevados de violencia indica que la presión operativa estatal no ha desarticulado las estructuras subyacentes, sino que coexiste con procesos de recomposición criminal y disputa territorial (Policía Nacional del Ecuador, 2024; UNODC, 2024). Este fenómeno genera un impacto económico cuantificable; de acuerdo con el Banco Interamericano de Desarrollo (Perez-Vincent et al., 2024), los costos directos de la criminalidad representaron el 3,44 % del Producto Interno Bruto (PIB) regional en 2022, lo que constituye una limitación macroeconómica para el crecimiento y la reducción de la pobreza. En este marco, la violencia no cumple solo una función de eliminación de competidores, sino también de regulación territorial y de señalización pública del poder criminal.

Un segundo rasgo empírico relevante es la adopción de formas de violencia de alto impacto simbólico. En Ecuador, los ataques con explosivos, los episodios de violencia penitenciaria extrema y la difusión pública de acciones armadas han ampliado el efecto intimidatorio de la coerción criminal más allá del enfrentamiento entre organizaciones rivales. La incursión armada al canal TC Televisión el 9 de enero de 2024 ilustra cómo un hecho criminal puede transformarse en un evento de terror mediatizado, capaz de producir miedo colectivo, percepción de vulnerabilidad estatal y amplia resonancia pública (Tusa et al., 2025). En términos analíticos, estos episodios no justifican una equiparación automática entre crimen organizado y terrorismo, pero sí son consistentes con el uso instrumental de repertorios de violencia destinados a comunicar poder, disciplinar audiencias y condicionar respuestas institucionales (Bevilacqua et al., 2024; Makarenko, 2004; Tusa et al., 2025).

A ello se suma la dimensión organizativa y financiera del fenómeno. Los reportes sobre el caso Euro 2024 y las capturas recientes de cabecillas ecuatorianos o vinculados al escenario criminal ecuatoriano en España, Colombia y otros países sugieren tres rasgos convergentes: sofisticación financiera, externalización del mando y capacidad de recomposición tras la neutralización de liderazgos. Considerados aquí con función ilustrativa y de contraste, y no como prueba autónoma concluyente, estos casos muestran que las economías ilícitas no dependen únicamente del control territorial inmediato, sino también de redes de lavado de activos, operadores transnacionales y esquemas de coordinación extraterritorial. Del mismo modo, las reacciones violentas posteriores a capturas de alto perfil refuerzan la hipótesis de que la coerción criminal opera como mecanismo de preservación del mercado ilícito y de presión sobre el sistema estatal (Shelley, 2014; Felbab-Brown, 2010; Primicias, 2024; Policía Nacional del Ecuador, 2025).

Tabla 1. Casos ilustrativos de convergencia entre criminalidad organizada, proyección transnacional y coerción estratégica

Caso / procedimiento	Estructura	Vector de convergencia	Hallazgo relevante	Documento-fuente
Caso Euro 2024	Red de lavado vinculada a Jezdimir Srdan	Sofisticación financiera transnacional	La causa documenta movimientos de capital, entramado societario y coordinación entre Ecuador y Europa, mostrando que la capacidad criminal no depende solo del control territorial.	Primicias (12 jun. 2025)
Recaptura de José Adolfo Macías Villamar (“Fito”)	Los Choneros	Centralidad del liderazgo y presión estatal sobre mandos de alto valor	La recaptura evidencia el peso simbólico y operativo de los liderazgos en la política de seguridad y en la comunicación pública del control estatal.	Primicias (25 jun. 2025)
Captura de William Joffre Alcívar Bautista (“Comandante Willy”)	Los Tiguerones	Mando extraterritorial	La detención en España, con uso de documentación falsa, apoya la hipótesis de externalización del mando y refugio operativo fuera de Ecuador.	Primicias (23 oct. 2024)
Captura de Wilmer Geovanny Chavarría Barré (“Pipo”)	Los Lobos	Resiliencia organizativa y fraude documental	La simulación de muerte y la captura en Málaga permiten observar estrategias de evasión internacional, sustitución identitaria y continuidad del mando criminal.	Primicias (17 nov. 2025)

Nota. Se incluyen únicamente casos con utilidad analítica directa para examinar sofisticación financiera, externalización del mando, resiliencia organizativa y coerción estratégica en el caso ecuatoriano. Los enlaces remiten al documento-fuente principal utilizado en cada fila.

En conjunto, estos indicadores permiten sostener que el caso ecuatoriano presenta rasgos consistentes con una convergencia funcional entre crimen organizado transnacional y uso instrumental del terror. La combinación de violencia letal elevada, intensificación de la interdicción antidrogas, visibilidad pública de ataques de alto impacto, crisis penitenciaria y proyección transnacional de actores criminales sugiere una transformación del problema de seguridad: de un esquema centrado en criminalidad organizada convencional hacia otro en el que la violencia cumple también funciones de gobernanza, intimidación social y disputa por autoridad territorial. En ese sentido, el caso ecuatoriano

no demuestra una identidad plena entre crimen y terrorismo, pero sí aporta evidencia relevante sobre la forma en que la violencia criminal contemporánea puede adquirir efectos políticos y sociales comparables a los analizados por la literatura sobre gobernanza criminal y amenazas híbridas (Badillo-Sarmiento & Trejos-Rosero, 2025; Feldmann & Luna, 2022).

5. Comandos de la Frontera como actor armado no estatal de orientación criminal

Los Comandos de la Frontera pueden entenderse, para efectos analíticos, como un actor armado no estatal de orientación predominantemente criminal, surgido en un entorno postinsurgente³ y vinculado a la reconfiguración del conflicto colombiano posterior a los acuerdos de paz. Su trayectoria no se ajusta plenamente al modelo de insurgencia clásica, en la medida en que su accionar aparece orientado prioritariamente al control de economías ilícitas, corredores estratégicos y mecanismos de regulación territorial antes que a la disputa abierta del poder estatal mediante un programa ideológico definido. Esta caracterización resulta consistente con la literatura reciente sobre actores armados híbridos en América Latina, que advierte la necesidad de distinguir entre continuidad organizativa, funcionalidad criminal y persistencia de repertorios armados sin asumir automáticamente una identidad insurgente plena ni trasladar de manera acrítica categorías de conflicto armado a configuraciones criminales territorialmente situadas (Badrán, 2024; Durán-Martínez, 2023; Kleinschmidt & Palma, 2020; Global Initiative Against Transnational Organized Crime, 2025).

Su relevancia para el caso ecuatoriano deriva de su inserción en espacios fronterizos amazónicos donde convergen baja densidad institucional, circulación transnacional de rentas ilícitas y alta dependencia de corredores fluviales y terrestres. En estos entornos, diversas fuentes han descrito formas de control que combinan coerción armada, regulación de actividades económicas y vínculos instrumentales con estructuras locales, rasgos que la literatura asocia con esquemas de gobernanza criminal más que con mera presencia armada ocasional. En este sentido, el interés analítico del grupo no radica solo en su capacidad de violencia, sino en su aptitud para operar como autoridad fáctica en territorios periféricos, administrando accesos, disciplinando conductas y protegiendo actividades ilícitas (Blattman et al., 2025; Feldmann & Luna, 2022; García-Pinzón & Mantilla, 2021; Penagos, 2024; Williams et al., 2025).

La evidencia disponible sugiere, además, que la expansión de los Comandos de la Frontera en Ecuador no debe interpretarse únicamente como una prolongación mecánica del conflicto colombiano, sino como parte de un proceso de adaptación transfronteriza a oportunidades logísticas, vacíos de control y alianzas locales. Los reportes sobre detenciones y operaciones en 2024 indican una presencia estructurada del grupo en territorio ecuatoriano, apoyada en operadores logísticos, mandos intermedios

³ La postinsurgencia principalmente en Colombia describe la transformación y persistencia de estructuras armadas tras los procesos de desmovilización y acuerdos de paz. Se manifiesta principalmente en disidencias guerrilleras y grupos residuales que mantienen control territorial, violencia armada y vínculos con economías ilícitas.

y redes de apoyo funcionales al transporte de droga, armas y recursos financieros. Considerados con la cautela propia de las fuentes documentales públicas, estos antecedentes son consistentes con un patrón de profundización territorial y con una lógica organizativa que combina visibilidad armada limitada y capacidad sostenida de coordinación criminal (García-Pinzón& Mantilla, 2020; Penagos, 2024; Primicias, 2024; Global Initiative Against Transnational Organized Crime, 2025).

Un elemento particularmente significativo es que la coerción atribuida al grupo no parece orientarse exclusivamente a la confrontación permanente con el Estado, sino a la preservación de corredores ilícitos, enclaves extractivos y zonas de influencia. Bajo esta lógica, la violencia funciona como mecanismo de protección de mercados y como tecnología de gobierno territorial. La emboscada en la que murieron once militares ecuatorianos en Alto Punino, atribuida por las autoridades nacionales a estructuras vinculadas a los Comandos de la Frontera --pese a que el grupo negó su autoría--, constituyó un punto de inflexión, al evidenciar la capacidad de un actor armado no estatal para infligir daño letal de alta intensidad a fuerzas estatales en un entorno de difícil control. Más que un hecho aislado, el episodio sugiere la existencia de capacidades tácticas, conocimiento del terreno y disposición a emplear violencia de alto impacto para defender posiciones estratégicas y disuadir la intervención estatal (Primicias, 2025; Global Initiative Against Transnational Organized Crime, 2025).

Tabla 2. Indicadores empíricos de inserción territorial y proyección transfronteriza de los Comandos de la Frontera en Ecuador

Indicador empírico	Manifestación documentada	Variable analítica	Relevancia para el caso ecuatoriano	Documento-fuente
Presencia estructurada en Ecuador	Llamamiento a juicio de 17 presuntos integrantes en 2025 por delincuencia organizada, tráfico de drogas, armas y lavado de activos.	Inserción operativa en territorio nacional	Sugiere una presencia no episódica, compatible con redes locales de apoyo, financiamiento y logística criminal.	Primicias (16 abr. 2025)
Red logística de alias “Chavalo”	La cobertura judicial y periodística vincula la red con el movimiento de droga desde Sucumbios hacia Centroamérica y Europa.	Articulación local–transfronteriza	Permite observar el papel de operadores intermedios y corredores amazónicos en la conexión entre frontera, puertos y mercados externos.	Primicias (13 sep. 2024)
Alto Punino	Emboscada contra una patrulla militar con 11 fallecidos; las autoridades la atribuyeron a Comandos de la Frontera, aunque el grupo negó responsabilidad.	Capacidad de violencia armada de alta intensidad	Indica capacidad de confrontación letal contra fuerzas estatales en un corredor vinculado a minería ilegal y economías ilícitas de frontera.	Primicias (9 may. 2025)
Captura y traslado de Roberto Carlos Álvarez Vera, alias Gerente	Detención en Abu Dabi y posterior traslado a Ecuador; autoridades lo identifican como cabecilla del grupo en el país.	Proyección extrarregional y separación entre nodos de coerción y nodos de resguardo/gestión	Refuerza la hipótesis de articulación entre anclaje amazónico, coordinación extraterritorial y protección del liderazgo.	Primicias (29 dic. 2025)

Nota. La tabla resume indicadores verificables de inserción territorial, articulación transfronteriza y proyección extrarregional de los Comandos de la Frontera en Ecuador. La atribución de Alto Punino se formula de manera prudente y conforme a la evidencia pública disponible.

A ello se agrega un rasgo organizativo relevante: la proyección extraterritorial de parte de su liderazgo y de sus circuitos de coordinación. Los reportes sobre capturas fuera de la región andina sugieren que, al igual que otras estructuras criminales contemporáneas, el grupo puede separar espacialmente los espacios de violencia directa de los espacios de gestión financiera y logística. Este patrón no convierte por sí solo a los Comandos de la Frontera en una organización globalmente integrada, pero sí refuerza la hipótesis de que opera bajo una racionalidad transnacional, con capacidad de articular nodos locales de coerción y nodos externos de resguardo, coordinación o lavado de activos (UNODC, 2019; Shelley, 2014). En conjunto, estos elementos permiten sostener que su importancia para el caso ecuatoriano reside menos en una supuesta “reaparición guerrillera” que en la consolidación de una forma de criminalidad armada transfronteriza, adaptable y territorialmente situada, cuyo análisis resulta central para comprender los límites de las respuestas convencionales de seguridad.

6. Estrategias estatales frente a la amenaza híbrida: entre pragmatismo y utopía

La disyuntiva entre pragmatismo y utopía no debe entenderse aquí como una oposición abstracta, sino como un criterio para evaluar la adecuación entre el diseño de las respuestas estatales y la naturaleza efectiva de la amenaza. En el caso ecuatoriano, esa adecuación depende menos de la intensidad discursiva de las medidas que de su capacidad para interrumpir circuitos financieros ilícitos, reducir la autonomía de los centros penitenciarios, sostener la cooperación transnacional y disminuir las condiciones sociales que facilitan el reclutamiento criminal. La literatura regional sugiere que las respuestas centradas exclusivamente en coerción, excepcionalidad y expansión punitiva pueden producir efectos inmediatos de visibilidad, pero tienden a ser insuficientes e incluso contraproducentes cuando no alteran las bases institucionales y territoriales de la gobernanza criminal (Badrán, 2024; Feldmann & Luna, 2022; Magaloni et al., 2020).

*Inteligencia financiera*⁴. Entre las herramientas disponibles, la inteligencia financiera constituye probablemente la estrategia más claramente pragmática, en la medida en que actúa sobre el soporte material de las organizaciones criminales: sus flujos de dinero, mecanismos de ocultamiento patrimonial y capacidad de reinversión. Su eficacia, sin embargo, no depende solo de la existencia formal de normas antilavado, sino de la articulación entre unidades de inteligencia financiera, fiscalías, sistemas de registro, supervisión bancaria y cooperación internacional. En un escenario como el ecuatoriano, donde las estructuras criminales muestran externalización de mando, uso de identidades encubiertas y circuitos económicos transnacionales, la brecha entre diseño normativo e implementación sostenida puede convertir una herramienta operativamente racional en una política de baja efectividad práctica. En ese punto, el problema no es la falta de pertinencia de la estrategia, sino su débil institucionalización (Grupo de Acción Financiera Internacional [GAFI], 2025; Shelley, 2014).

4 Inteligencia financiera. Estrategia orientada a identificar y afectar los flujos económicos y patrimoniales del crimen organizado, cuya eficacia depende de una sólida coordinación institucional y cooperación internacional (GAFI, 2025; Shelley, 2014).

*Investigación criminal especializada*⁵. Ortiz Luzuriaga, Flores Sánchez, Caicedo Leones y Ordóñez Guartazaca (2021) sostienen que la prevención del lavado de activos requiere un sistema integral de gestión del riesgo, en el que participen de manera coordinada las instituciones del Estado, el sistema financiero y los sujetos obligados. Los autores enfatizan que la identificación temprana de operaciones sospechosas, la supervisión efectiva y la cooperación interinstitucional son elementos esenciales para impedir que recursos de origen ilícito ingresen a la economía formal, fortaleciendo así la transparencia del sistema financiero y la seguridad del Estado.

Por lo tanto, la investigación criminal especializada en lavado de dinero trasciende la persecución de un delito económico y se convierte en una herramienta estratégica para proteger la seguridad integral del Ecuador permitiendo la aproximación para diferenciar lo pragmático de lo utópico, porque a diferencia de las investigaciones tradicionales, la investigación especializada en lavado de dinero requiere un enfoque multidisciplinario que combine varias técnicas y no se limita a identificar a los responsables del delito precedente, sino que busca desarticular la estructura económica que sostiene a las organizaciones criminales, privándolas de su capacidad financiera y reduciendo su influencia sobre las instituciones públicas y privadas, visibilizando el fin del negocio criminal.

*Control penitenciario*⁶. Un segundo ámbito decisivo es el sistema penitenciario. Como muestra la evidencia disponible para Ecuador y otros casos regionales, las cárceles han funcionado no solo como espacios de encierro, sino como nodos de mando, disciplinamiento interno y reproducción de economías ilícitas (Fondevila & Vilalta-Perdomo, 2024; Sozzo, 2022). La investigación reciente sobre prisiones latinoamericanas sugiere que la violencia carcelaria y la capacidad de control de las organizaciones no se explican únicamente por sobrepoblación o precariedad material, sino también por la existencia de esquemas de autogobierno o gobierno criminal al interior de los establecimientos (Sozzo, 2025). Este fenómeno se analiza con mayor precisión bajo la categoría de gobernanza nodal, donde el ejercicio del poder no se origina en un centro soberano exclusivo, sino en una red de actores interconectados que integra tanto a funcionarios estatales como a estructuras criminales que operan mediante la clandestinidad operativa (Ferreira, 2025).

*Cooperación internacional*⁷. La cooperación internacional constituye otro componente central, dado que las estructuras examinadas en este trabajo operan en redes que desbordan con facilidad la jurisdicción nacional. Intercambio de información, asistencia judicial, trazabilidad de activos, alertas migratorias y coordinación operativa son mecanismos indispensables frente a organizaciones con

5 Investigación criminal especializada. Enfoque multidisciplinario que busca identificar y desarticular las estructuras económicas del crimen organizado mediante la detección del lavado de activos, reduciendo su capacidad financiera e influencia institucional (Ortiz Luzuriaga et al., 2021).

6 Control penitenciario. Estrategia orientada a recuperar el control estatal de las cárceles y neutralizar su uso como centros de mando y reproducción criminal, limitando el autogobierno y la gobernanza ejercida por organizaciones delictivas (Sozzo, 2025; Ferreira, 2025).

7 Cooperación internacional. Estrategia para enfrentar redes criminales transnacionales mediante intercambio de información, asistencia judicial y coordinación operativa, cuya eficacia depende de la continuidad e interoperabilidad entre Estados (GAFI, 2025; Pont, 2025).

capacidad de mover personas, capitales y mercancías entre varios países. Sin embargo, la experiencia regional muestra que estas herramientas suelen verse limitadas por asimetrías institucionales, prioridades nacionales divergentes y, en ciertos casos, por una lectura insuficiente de las amenazas híbridas. La consecuencia es una cooperación que suele ser normativamente adecuada, pero operativamente fragmentaria. En ese sentido, la cooperación no constituye una estrategia utópica por definición; se vuelve utópica cuando no logra traducirse en continuidad, interoperabilidad y reconocimiento compartido del problema (GAFI, 2025; Pont, 2025).

*Prevención de vulnerabilidades y reclutamiento*⁸. La prevención estructural del reclutamiento y de la base social del crimen organizado suele ser presentada como una estrategia idealista frente a la urgencia de la violencia. Sin embargo, esa oposición es engañosa. La evidencia disponible sugiere que la vulnerabilidad juvenil, la exclusión educativa, la precariedad territorial y la ausencia de trayectorias legítimas de inserción social forman parte del entorno que facilita la expansión de organizaciones criminales en contextos de alta violencia. En el caso ecuatoriano, estudios recientes han vinculado explícitamente la discusión sobre violencia pública y terror mediatizado con la necesidad de fortalecer respuestas sociales duraderas, especialmente en educación e inclusión de jóvenes expuestos a reclutamiento por grupos criminales. La literatura regional sobre respuestas sociales a la violencia bajo gobernanza criminal sugiere, además, que este tipo de estrategias solo produce efectos consistentes cuando cuenta con anclaje comunitario, continuidad institucional y capacidad de sostenerse en territorios de alta conflictividad (Arias, 2019; Escotto Quesada, 2015; Tusa et al., 2025). Por ello, más que una política “utópica”, la prevención social constituye una dimensión de pragmatismo de mediano plazo que rara vez recibe el tiempo político, el financiamiento o la continuidad institucional que requiere para producir efectos acumulativos.

En conjunto, el caso ecuatoriano sugiere que la oposición entre pragmatismo y utopía no se resuelve escogiendo una única estrategia, sino evaluando la capacidad del Estado para articularlas de manera sostenida. La inteligencia financiera, la investigación criminal especializada, la reforma penitenciaria, la cooperación internacional y la prevención del reclutamiento solo resultan pragmáticas cuando se integran en una respuesta institucional continua, territorialmente diferenciada y capaz de adaptarse a una amenaza cambiante. Cuando estas dimensiones operan con asimetría sistémica, de forma episódica o subordinadas a crisis coyunturales, la eficacia instrumental de las estrategias se anula, reduciéndose a un formalismo inoperante (Badrán, 2024; Feldmann & Luna, 2022).

8 Prevención de vulnerabilidades y reclutamiento. Estrategia orientada a reducir factores sociales que favorecen el reclutamiento criminal, mediante educación, inclusión juvenil y fortalecimiento comunitario sostenido (Arias, 2019; Escotto Quesada, 2015; Tusa et al., 2025).

7. Discusión

Los hallazgos del presente estudio dialogan con la literatura reciente sobre convergencia entre crimen organizado y terrorismo en al menos cuatro planos. En primer lugar, el caso ecuatoriano refuerza, pero también matiza la tesis del continuum entre crimen y terrorismo: la evidencia examinada no permite sostener una fusión estructural ni ideológica entre ambos fenómenos, pero sí muestra una convergencia funcional y selectiva en la que repertorios de violencia de alto impacto son incorporados por organizaciones criminales cuando resultan útiles para proteger mercados ilícitos, disciplinar territorios, intimidar audiencias y condicionar respuestas estatales. En este sentido, el caso confirma que la clave analítica no reside en etiquetar a estos actores como “terroristas” en sentido estricto, sino en comprender bajo qué condiciones determinadas tácticas, efectos y racionalidades propias del terror son instrumentalizadas por estructuras criminales sin abandonar su orientación primordial hacia la acumulación ilícita (Farber, 2025; Kleinschmidt & Palma, 2020; Phillips, 2018; Makarenko, 2004).

En segundo lugar, el caso ecuatoriano amplía la literatura sobre gobernanza criminal al mostrar que la violencia no actúa solo como recurso destructivo, sino también como tecnología de regulación social y territorial. La combinación entre violencia letal elevada, control penitenciario disputado, corredores ilícitos transnacionales, enclaves extractivos y actores armados no estatales con capacidad de coerción localizada sugiere que parte de la criminalidad organizada contemporánea en Ecuador no se limita a explotar rentas ilegales, sino que produce órdenes situados, impone reglas, define jerarquías y modela comportamientos en espacios donde la autoridad estatal resulta fragmentaria, disputada o intermitente. Desde esta perspectiva, el principal desplazamiento analítico del manuscrito consiste en mostrar que el problema no es únicamente de seguridad pública, sino también de autoridad, gobernanza y producción de obediencia en contextos de pluralización fáctica del poder (Badillo-Sarmiento & Trejos-Rosero, 2025; Blattman et al., 2025; Feldmann & Luna, 2022).

En tercer lugar, los resultados permiten proponer una hipótesis interpretativa que, aun siendo exploratoria, ofrece un rendimiento explicativo relevante y se aparta de lecturas más convencionales. La neocriminalidad organizada más peligrosa no parece ser necesariamente aquella que intenta sustituir frontalmente al Estado en clave insurgente, sino aquella que aprende a operar en relación estratégica con una estatalidad fragmentada, reactiva o selectivamente coercitiva. En esta lectura, la amenaza no se expresa solo en la capacidad de desafiar al Estado, sino también en la capacidad de adaptarse a él, explotar sus discontinuidades, reordenar mercados ilícitos tras ciclos de intervención y convertir crisis institucionales en oportunidades de recomposición organizativa. Esta hipótesis es consistente con trabajos que muestran, por una parte, que la convergencia suele ser menos intensa y más graduada de lo que sugieren las versiones maximalistas del debate y, por otra, que la presencia estatal no siempre desplaza la gobernanza criminal, sino que bajo ciertas condiciones puede coexistir con ella o incluso reconfigurar sus incentivos (Blattman et al., 2025; Feldmann & Luna, 2022; Kleinschmidt & Palma, 2020; Magaloni et al., 2020).

En cuarto lugar, el análisis de las respuestas estatales permite discutir críticamente la aparente oposición entre pragmatismo y utopía. El caso ecuatoriano sugiere que esa dicotomía no se resuelve por la simple elección entre coerción y prevención, ni entre militarización y políticas sociales, sino por la capacidad del Estado para articular instrumentos heterogéneos en una secuencia institucional sostenida. La literatura regional respalda la idea de que las intervenciones fragmentadas, episódicas o exclusivamente punitivas pueden producir efectos inmediatos de visibilidad, pero no necesariamente alteran las estructuras de gobernanza criminal; en ocasiones, incluso intensifican la violencia o refuerzan la adaptabilidad de los grupos. Por ello, la contribución del artículo no consiste en oponer mecánicamente seguridad y derechos, ni prevención y control, sino en sostener que la eficacia estatal frente a amenazas híbridas depende de la coordinación entre inteligencia financiera, investigación criminal especializada, control penitenciario, cooperación transnacional, presencia territorial efectiva y estrategias sociales duraderas de reducción de vulnerabilidades (Arias, 2019; Badrán, 2024; GAFI, 2025; Pont, 2025; Tusa et al., 2025).

Desde esa base, el artículo aporta una implicancia más amplia para el debate latinoamericano: la necesidad de desplazar el foco desde la pregunta por la “naturaleza” de los actores hacia la pregunta por sus capacidades efectivas de producir orden, miedo, coordinación transnacional y condicionamiento político. En otras palabras, la categoría de neocriminalidad organizada adquiere valor no como etiqueta cerrada, sino como herramienta heurística para examinar configuraciones criminales que combinan racionalidad empresarial, flexibilidad organizativa, coerción comunicativa y vocación de regulación territorial.

Esta relectura evita tanto la inflación conceptual –que confunde toda violencia criminal con terrorismo– como el reduccionismo penal clásico, que subestima la dimensión política y social de formas contemporáneas de criminalidad organizada. En ese punto, el caso ecuatoriano no debe leerse como una anomalía aislada, sino como un laboratorio regional especialmente visible de transformaciones que probablemente seguirán expandiéndose en entornos marcados por fronteras porosas, circuitos ilícitos transnacionales y debilidad estatal diferenciada (Farber, 2025; Johnson & Gillooly, 2023; UNICRI, 2024; Global Initiative Against Transnational Organized Crime, 2025).

Como limitaciones, el estudio debe leerse en clave analítica e interpretativa. Se apoya en fuentes secundarias de distinta densidad empírica, incorpora eventos recientes todavía sujetos a actualización documental y emplea la noción de “neocrimen organizado” en sentido heurístico, no como categoría teórica cerrada. En consecuencia, las inferencias propuestas no pretenden establecer equivalencias causales definitivas entre criminalidad organizada y terrorismo, sino ofrecer una interpretación conceptualmente graduada de una convergencia funcional observable. De cara a investigaciones futuras, sería especialmente valioso contrastar esta hipótesis mediante diseños mixtos, datos primarios territoriales, análisis comparados subnacionales y estudios longitudinales sobre la relación entre intervención estatal, recomposición criminal y gobernanza coercitiva.

8. Conclusión

El caso ecuatoriano muestra que la violencia criminal contemporánea no se ajusta plenamente ni a las categorías clásicas de delincuencia organizada ni a las de terrorismo en sentido estricto, sino que expresa una convergencia funcional en la que actores criminales instrumentalizan repertorios de terror para asegurar control territorial, proteger economías ilícitas y condicionar la respuesta estatal. En este marco, el principal desafío analítico y político no radica en la clasificación nominal del fenómeno, sino en comprender su capacidad efectiva para erosionar autoridad estatal, producir gobernanza coercitiva y desestabilizar entornos democráticos. Desde esta perspectiva, Ecuador debe entenderse menos como una anomalía que como una manifestación particularmente visible de transformaciones regionales más amplias, lo que refuerza la necesidad de enfoques conceptualmente precisos e institucionalmente integrados frente a formas cada vez más híbridas, adaptativas y transnacionales de criminalidad organizada.

9. Referencias

- Alda-Mejías, S. (2021). La cultura del privilegio y la privatización de las funciones públicas, elementos esenciales para la gobernanza criminal. En S. Alda Mejías (Coord.), *Los actores implicados en la gobernanza criminal en América Latina* (pp. 11-44). Real Instituto Elcano.
- Arias, E. D. (2019). Social responses to criminal governance in Rio de Janeiro, Belo Horizonte, Kingston, and Medellín. *Latin American Research Review*, 54(1), 165–180.
- Badillo-Sarmiento, R., & Trejos-Rosero, L. F. (2025). Governing the underworld: How organized crime governs other criminals in Colombian cities. *Trends in Organized Crime*, 28(3), 359–385.
- Badrán, F. (2024). The signing of the peace agreement in Colombia. Old wine in new skins: Implications for national security and organized crime. *Trends in Organized Crime*, 27(2), 173–196.
- Bevilacqua, S., Cukla, A. R., & Tello Gamarra, D. F. (2024). Terrorism and police countermeasures in the fight against the “Novo Cangaço”. *Revista Criminalidad*, 66(3), 97–110.
- Blattman, C., Duncan, G., Lessing, B., & Tobón, S. (2025). Gang rule: Understanding and countering criminal governance. *The Review of Economic Studies*, 92(3), 1497–1531.
- Consejo de Seguridad de las Naciones Unidas. (2019, 28 de marzo). *Resolución 2462 (2019) sobre prevención y represión de la financiación del terrorismo (S/RES/2462)*.
- Durán-Martínez, A. (2023). Large-scale criminal violence in the 21st century. In A. Gruszczak & S. Kaempf (Eds.), *Routledge handbook of the future of warfare* (pp. 421–431). Routledge.
- Escotto Quesada, T. (2015). *Las juventudes centroamericanas en contextos de inseguridad y violencia: Realidades y retos para su inclusión social (LC/W.666)*. Comisión Económica para América Latina y el Caribe.
- Farber, S. (2025). The globalization of threat: A systematic review of crime-terror convergence. *Journal of Money Laundering Control*, 28(3), 533–549.
- Felbab-Brown, V. (2010). *Shooting up: Counterinsurgency and the war on drugs*. Brookings Institution Press.

- Feldmann, A. E., & Luna, J. P. (2022). Criminal governance and the crisis of contemporary Latin American states. *Annual Review of Sociology*, 48, 441–461.
- Ferreira, M.A. (2025): Organizaciones criminales y gobernanza criminal. Análisis Carolina, nº 11, Madrid, Fundación Carolina.
- Fondevila, G., & Vilalta-Perdomo, C. (2024). Prison violence in Latin America: Criminal governance and an absent state. *International Criminology*, 4, 149–165.
- García-Pinzón, V., Mantilla, J. (2021). Contested borders: organized crime, governance, and bordering practices in Colombia-Venezuela borderlands. *Trends in Organized Crime*, 24, 265–281.
- Global Initiative Against Transnational Organized Crime. (2025). *Índice global de crimen organizado 2025: La criminalidad en una encrucijada*.
- González, M. A. (2026, 11 de marzo). *Ecuador es el tercer país más violento de América Latina y el Caribe, según Insight Crime*. Primicias.
- Grupo de Acción Financiera Internacional. (GAFI). (2025). *International standards on combating money laundering and the financing of terrorism and proliferation: The FATF recommendations*.
- Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia. (2024, junio). *The nexus between transnational organized crime and terrorism in Latin America*.
- Johnson, P. L. (2019). The crime and state terrorism nexus: How organized crime appropriates counterinsurgency violence. *Perspectives on Terrorism*, 13(6), 16–26.
- Johnson, P. L., & Gillooly, S. N. (2023). Grammar of threat: Governance and order in public threats by criminal actors. *Comparative Political Studies*, 56(10), 1567–1596.
- Jupp, J. (2025). *The crime-terror nexus and the illicit trade in drugs*. *Studies in Conflict & Terrorism*. Advance online publication.
- Kleinschmidt, J., & Palma, O. (2020). The conceptual puzzle of violent non-state actors in Latin America: A critique of the convergence hypothesis. *Small Wars & Insurgencies*, 31(6), 1323–1348.
- Londoño-Bedoya, D. A., Padilla-Bueno, M., Areiza-Padilla, J. A., & Veas-González, I. (2025). The denying threat to national security and defense: Hezbollah's presence in Colombia. *Cogent Social Sciences*, 11(1), Artículo 2500653.
- Magaloni, B., Franco-Vivanco, E., & Melo, V. (2020). Killing in the slums: Social order, criminal governance, and police violence in Rio de Janeiro. *American Political Science Review*, 114(2), 552–572.
- Makarenko, T. (2004). The crime-terror continuum: Tracing the interplay between transnational organised crime and terrorism. *Global Crime*, 6(1), 129–145.
- Ministerio del Interior del Ecuador. (2024). *Informe estadístico de seguridad ciudadana y homicidios*.
- Oficina de las Naciones Unidas contra la Droga y el Delito. (2019). *World drug report 2019*.
- Oficina de las Naciones Unidas contra la Droga y el Delito. (2024). *World drug report 2024*.
- Ortiz Luzuriaga, M. T., Flores Sánchez, J., Caicedo Leones, W., & Ordoñez Guartazaca, M. (2021). Prevención del riesgo de lavado de activos. Caso Colombia y Ecuador. *Revista Universidad de Guayaquil*, 133(2).
- Paoli, L., & Fijnaut, C. (2022). Conceptualizing the nexus between organized crime and terrorism. En L. Paoli, J. Wouters, & C. Fijnaut (Eds.), *The nexus between organized crime and terrorism: Types and responses* (pp. 48–84). Edward Elgar Publishing.

- Penagos, L. (2024). *Reconfigurations institutionnelles sur la frontière colombo-vénézuélienne, frontière de tous les trafics* [Institutional reconfigurations on the Colombian-Venezuelan border, border of all organized crimes]. *Caravelle*, 122, 49–63.
- Perez-Vincent, S. M., Puebla, D., Alvarado, N., Mejía, L. F., Cadena, X., Higuera, S., & Niño, J. D. (2024). *Los costos del crimen y la violencia: ampliación y actualización de las estimaciones para América Latina y el Caribe*. Banco Interamericano de Desarrollo.
- Phillips, B. J. (2018). Terrorist tactics by criminal organizations: The Mexican case in context. *Perspectives on Terrorism*, 12(1), 46–63.
- Policía Nacional del Ecuador. (2024). *Reporte estadístico de incautaciones y operaciones contra el crimen organizado*.
- Policía Nacional del Ecuador. (2025). *Boletines operativos de capturas de objetivos de alto valor 2024–2025*.
- Pont, A. S. (2025). Strengthening transatlantic ties: Latin America-Europe cooperation against organized crime. In J. A. Sanahuja & R. Domínguez (Eds.), *The Palgrave handbook of EU-Latin American relations* (pp. 473–488). Palgrave Macmillan.
- Primicias. (2024, 29 de agosto). *Golpe a Comandos de la Frontera en Ecuador: 17 detenidos y USD 200 millones intervenidos*.
- Primicias. (2024, 20 de noviembre). *Caso Euro 2024: Cae red de lavado de activos vinculada al narcotráfico que operaba en Ecuador y Europa*.
- Primicias. (2025, 13 de mayo). *En la zona del alto Punino, donde asesinaron a 11 militares, está en auge el negocio millonario de la minería ilegal*.
- Sampó, C., & Troncoso, V. (2024). El Tren de Aragua: La transnacionalización del crimen organizado a través del tráfico de migrantes. *Análisis Político*, 37(108), 147–176.
- Shelley, L. I. (2014). *Dirty entanglements: Corruption, crime, and terrorism*. Cambridge University Press.
- Sozzo, M. (2022). Introduction: Inmate governance in Latin America. Context, trends and conditions. En M. Sozzo (Ed.), *Prisons, inmates and governance in Latin America* (pp. 1–32). Palgrave Macmillan.
- Sozzo, M. (2025). El auge de los esquemas de gobierno de los presos en las prisiones latinoamericanas. Condiciones, estrategias y luchas. *Latin American Law Review*, (14). 1–26.
- Tusa, F., Aguaded, I., Tejedor, S., & Rivera, C. (2025). Ecuador: A state of violence—Live broadcast of terror. *Journalism and Media*, 6(2), Artículo 56.
- Williams, M., Melendez, M., & Morales, R. (2025). Crimen Organizado y Violencia en América Latina y el Caribe. Informe Económico América Latina y el Caribe (Abril). Banco Mundial.

Nota de autor respecto al uso de Inteligencia Artificial: Se aclara que el uso de herramientas de Inteligencia Artificial Generativa tuvo un carácter estrictamente auxiliar, instrumental y no sustantivo dentro del proceso de preparación del manuscrito. Su empleo se limitó a tareas de revisión formal del texto, tales como corrección ortográfica, puntuación, acentuación, concordancia gramatical, depuración de repeticiones, mejora de fluidez sintáctica, uniformidad estilística y adecuación del registro académico. En este sentido, la herramienta funcionó como un apoyo editorial comparable a una revisión lingüística o de estilo, orientada a mejorar la claridad, legibilidad y corrección formal del manuscrito, sin sustituir el trabajo intelectual del autor. De manera específica, no se utilizó Inteligencia Artificial Generativa para producir contenido sustantivo del artículo, formular el problema de investigación, construir el enfoque teórico, definir la metodología, elaborar el análisis, interpretar hallazgos, generar argumentos, redactar apartados completos, incorporar ideas nuevas, producir conclusiones, seleccionar bibliografía ni crear referencias. Las decisiones académicas, conceptuales, metodológicas y argumentativas permanecieron bajo responsabilidad exclusiva del autor, quien revisó, validó y conservó el control sobre cada modificación formal realizada al texto. Asimismo, se precisa que el uso de la herramienta no tuvo por finalidad llenar vacíos de contenido, desarrollar secciones no elaboradas previamente ni reemplazar procesos propios de investigación, lectura, análisis crítico o escritura académica. El manuscrito fue concebido, estructurado y desarrollado por el autor; la asistencia tecnológica se empleó únicamente en una fase posterior de revisión lingüística y normalización formal, con el propósito de fortalecer la presentación académica del texto sin alterar su autoría, originalidad, contenido científico ni responsabilidad intelectual.

Mauricio Heise y Cristian Rodríguez

De la convergencia crimen-terrorismo a la violencia híbrida: ataques con drones en América Latina

From the convergence of crime and terrorism to hybrid violence: Drone attacks in Latin America

Resumen

El artículo analiza el uso de sistemas aéreos no tripulados (UAS) como instrumentos de “violencia híbrida”, debido a su empleo por actores no estatales en América Latina, particularmente en Colombia, México y Brasil, donde organizaciones criminales, con motivaciones económicas o político-económicas, entre los años 2020 y 2026, los han utilizado para el lanzamiento de explosivos, vigilancia y control territorial, desafiando la autoridad del Estado e impactando en la condición de seguridad pública en esos países.

Se aplica el modelo de *Crime-terror continuum* de Makarenko, donde se analizan casos empíricos, a partir de literatura académica, informes de inteligencia y registros de prensa, para identificar patrones de adaptación táctica, características y situación actual del fenómeno. En este sentido, se trataría de una amenaza que anula las ventajas tácticas estatales, incluso mediante el uso de drones guiados por fibra óptica, inmunes a inhibidores, y la dispersión de agentes químicos.

Palabras clave: drones, seguridad, América Latina, crime-terror continuum, amenaza híbrida, control territorial, innovación criminal.

Abstract

This article analyzes the use of Unmanned Aerial Systems (UAS) as instruments of “hybrid violence” due to their employment by non-state actors in Latin America, particularly in Colombia, Mexico, and Brazil. Between 2020 and 2026, criminal organizations with economic or politico-economic motivations have used these systems for the delivery of explosive devices, surveillance, and territorial control, challenging state authority and affecting public security conditions in these countries.

Drawing on Makarenko’s *Crime-Terror Continuum* model, the article examines empirical cases through academic literature, intelligence reports, and media sources to identify patterns of tactical adaptation, key characteristics, and the current state of the phenomenon. In this regard, the study suggests the emergence of a threat capable of reducing traditional state tactical advantages, including through the use of fiber-optic-guided drones that are resistant to electronic jamming, as well as the potential deployment of chemical agents.

Keywords: drones, security, Latin America, crime-terror continuum, hybrid threat, territorial control, criminal innovation

Mauricio Heise, Doctor en Ciencia Política (UB). Máster en Estudios sobre Terrorismo (UNIR). Analista de terrorismo y extremismos violentos.

Cristian Rodríguez, Graduado en Criminología y Ciencias de la Seguridad (VIU). Máster en Estudios Avanzados en Terrorismo (UNIR). Doctorando en Seguridad Internacional (UNED).

Recibido

15/08/2026

Aceptado

12/09/2026

Para citar este artículo: Heise, M. y Rodríguez, C. (2026), De la convergencia crimen-terrorismo a la violencia híbrida: ataques con drones en América Latina, *Revista Internacional de Estudios sobre Terrorismo*, nº18, pp.49-68.

1. Introducción

Durante décadas el uso de drones estuvo circunscrito casi exclusivamente al ámbito militar estatal, como medios de reconocimiento y ataque. No obstante, en los últimos años esta tecnología ha sido progresivamente incorporada por actores no estatales a sus repertorios de violencia. Este fenómeno constituye una innovación criminal, ya que combina el uso de tecnologías de fácil acceso, modificaciones artesanales y la proyección de la violencia desde el espacio aéreo, lo que representa un desafío en seguridad para América Latina.

Diversos actores armados no estatales como los cárteles del narcotráfico en México y las disidencias de las Fuerzas Armadas Revolucionarias de Colombia (FARC) han integrado los drones a sus tácticas operativas, principalmente para el lanzamiento de artefactos explosivos improvisados contra las fuerzas y cuerpos de seguridad, grupos rivales e incluso población civil. Estos incidentes, documentados con frecuencia desde 2020, evidencian un riesgo significativo para la seguridad pública, ya que implica la adaptación de estos actores armados, utilizando dispositivos que son accesibles y de bajo costo.

Lejos de sustituir completamente otras modalidades de violencia como el uso de “coches bomba”, emboscadas armadas o ataques con armas de fuego, el empleo de drones se suma a un repertorio táctico ampliado, ofreciendo ventajas operativas: posibilidad de ejecutar ataques a distancia, menor exposición directa de los operadores y un alto impacto psicológico sobre las fuerzas de seguridad y las comunidades afectadas. En este sentido, el dron no debe entenderse únicamente como un instrumento técnico, sino como coerción simbólica, destinada a exhibir poder, ejercer control territorial y demostrar la capacidad de desafiar al Estado.

Desde una perspectiva teórica, estas dinámicas encajan con precisión en el modelo del *crimerror continuum*¹ propuesto por Makarenko (2005), que describe la progresiva convergencia entre crimen organizado y terrorismo. El uso de drones por organizaciones criminales y disidencias armadas ilustra cómo estos actores adoptan tácticas que tradicionalmente son propias de la violencia política y el terrorismo, pero con motivaciones económicas, dando lugar a configuraciones híbridas de violencia. Casos como los ataques con drones del Cártel Jalisco Nueva Generación (CJNG) contra fuerzas policiales en México, o las de las disidencias de las FARC contra unidades militares y policiales en Colombia, reflejan esta convergencia operativa y simbólica, en la que el terror y la criminalidad se entrelazan para ejercer control territorial y erosionar la autoridad estatal.

El empleo de drones por actores armados en América Latina constituye la manifestación de una convergencia estructural profunda. En este fenómeno confluyen capacidades materiales, derivadas de la fácil adquisición de tecnología comercial, y una racionalidad estratégica que busca maximizar el daño táctico con el mínimo riesgo personal, lo que es posible por los ataques a distancia. No

1 El Modelo Continuo crimen-terrorismo describe una relación dinámica, donde el crimen organizado y el terrorismo no son fenómenos separados, sino que coexisten en un espectro continuo basado en sus métodos y motivaciones, por lo que pueden converger mediante alianzas tácticas, apropiación de técnicas mutuas o incluso transformarse el uno en el otro.

obstante, la dimensión tecnológica es insuficiente para explicar el fenómeno sin considerar el recurso de la violencia como el eje articulador e instrumento de coacción psicológica. Esta evolución resulta especialmente relevante en contextos de baja capacidad estatal, donde la innovación tecnológica se combina con vacíos de gobernanza y altos niveles de violencia estructural.

Para examinar esta dinámica, el presente trabajo se centra en el marco temporal transcurrido entre 2020 y 2026 —periodo en el que se registraría un aumento exponencial y documentado de ataques con explosivos mediante drones en la región—, analizando la situación de Colombia, México y Brasil, por constituir los escenarios más representativos de este fenómeno.

2. Desarrollo

2.1 *El crimeterror continuum de Makarenko: Violencia híbrida*

Uno de los aportes centrales del *crimeterror continuum* de Makarenko (2005) es la idea de que crimen organizado y terrorismo no deben entenderse como categorías normativas rígidas, sino como formas de violencia no estatal susceptibles de converger bajo determinadas condiciones estructurales. En este marco, los actores no estatales adoptan tácticas, estructuras y narrativas tradicionalmente asociadas al otro espectro cuando ello resulta funcional a sus objetivos estratégicos. Esta lógica permite explicar por qué organizaciones criminales contemporáneas, incluso en ausencia de un proyecto ideológico concreto, recurren a formas de violencia de alto impacto simbólico, como ataques reiterados contra fuerzas de seguridad, que históricamente han sido asociados al terrorismo, como una adaptación racional en contextos de disputa territorial, fragmentación estatal y competencia armada (Makarenko, 2005; InSight Crime, 2023).

Sin perjuicio de lo anterior, debe aclararse que no todo ataque de alto impacto debe ser considerado como terrorista, ya que el efecto psicológico o la intimidación no bastan por sí solos para tipificarlo como tal, por tanto, el empleo de drones se entiende como una herramienta de coerción que enriquece un repertorio táctico más amplio.

En México, el método de actuación del Cártel Jalisco Nueva Generación (CJNG) constituye uno de los ejemplos más evidentes de desplazamiento a lo largo del continuum descrito por Makarenko. Aunque su motivación central es económica, múltiples investigaciones periodísticas y de observatorios especializados han documentado cómo el CJNG ha incorporado de manera sistemática tácticas propias de la violencia política armada: ataques contra policías y militares, uso de explosivos improvisados y drones, bloqueos coordinados de infraestructuras y despliegues de violencia con fuerte carga comunicativa (InSight Crime, 2022; Villegas, 2025). Tras la muerte de uno de sus líderes regionales, lejos de observarse un repliegue organizativo, se produjeron acciones violentas coordinadas, para reafirmar control territorial y demostrar su capacidad de coerción, lo que refuerza una lógica de terror instrumental orientada a la disuasión estatal y al mensaje político, y no sólo a la represalia criminal (InSight Crime, 2021).

En tanto, Colombia representa un caso paradigmático del recorrido inverso previsto en el modelo de Makarenko, en el cual una organización de origen insurgente transita progresivamente hacia estructuras criminales sin abandonar completamente la violencia política. Como anticipó la propia Makarenko (2005) en su análisis original de las FARC, la creciente dependencia de economías ilícitas no implica necesariamente la renuncia a tácticas terroristas cuando estas siguen ofreciendo ventajas estratégicas.

Las disidencias de las FARC han consolidado su inserción en redes de narcotráfico, minería ilegal y extorsión, pero paralelamente han ejecutado ataques sistemáticos contra la fuerza pública, incluyendo el uso de drones con explosivos, una práctica documentada por medios nacionales e informes especializados desde 2021 (BBC Mundo, 2022; InSight Crime, 2024). Esta combinación de criminalidad y violencia simbólica refleja una configuración híbrida permanente, más que una fase transitoria.

Respecto a lo anterior, una diferencia de las disidencias con su antecesora es que “ambas organizaciones buscan control territorial, sin embargo, las antiguas FARC-EP pretendían cumplir su plan estratégico buscando doblarse en frentes y generar base social para lograr su objetivo, que era la toma del poder, mientras las disidencias pretenden conquistar territorios para la existencia de economías ilícitas o corredores estratégicos” (García y Hernández, 2024).

En este sentido, las fuerzas armadas y la policía de Colombia actualmente enfrentan un escenario estratégico complejo, caracterizado por la persistencia de la insurgencia residual, la intensificación de economías ilícitas y la consolidación de amenazas híbridas, con agrupaciones armadas como las FARC, ELN y el Clan del Golfo (Rios, 2025).

Estos grupos armados podrían entenderse bajo la categorización de “amenaza híbrida”, considerando que “lo híbrido ha experimentado un largo viaje conceptual desde sus orígenes hasta hoy en día. Heredera del concepto *guerra complejo-irregular*, esta idea se popularizó tras el choque entre Israel y Hezbolá de 2006 para describir la integración de tácticas, técnicas y procedimientos convencionales e irregulares, mezcladas con actos terroristas, propaganda y conexiones con el crimen organizado (Colom, 2019). Desde esta perspectiva, conceptos como “amenaza híbrida” o “tácticas terroristas son categorías descriptivas para examinar la adopción funcional de dinámicas intimidatorias por parte de organizaciones criminales.

En tanto, el caso brasileño refuerza adicionalmente la vigencia del *continuum* al mostrar cómo actores “estrictamente criminales” pueden adoptar prácticas cuasipolíticas, sin necesidad de articular una agenda política o ideológica formal. Organizaciones como el “Comando Vermelho” y el “Primeiro Comando da Capital” han consolidado enclaves de control territorial en favelas, donde regulan actividades económicas ilícitas, imponen normas sociales y ejercen coerción armada frente a la presencia estatal (InSight Crime, 2022; The Guardian, 2021). Desde la perspectiva del *crimeterror continuum*, estos grupos no se transforman en organizaciones terroristas en cuanto a sus motivaciones,

pero asimilan repertorios de intimidación colectiva y disciplinamiento social que cumplen funciones análogas a las del terrorismo, especialmente cuando los ataques se dirigen contra las fuerzas policiales como símbolos visibles del Estado y de su autoridad formal.

En conjunto, estos ejemplos latinoamericanos confirman la vigencia empírica del marco de análisis propuesto y sugieren la necesidad de emplearlo para interpretar las formas contemporáneas de violencia híbrida, caracterizadas por la superposición de racionalidades económicas, políticas y simbólicas. El uso de drones por parte de organizaciones criminales y disidencias armadas no debe entenderse únicamente como una innovación tecnológica, sino como un indicador de posición dentro del *continuum crimen-terror*, en que la adopción de tácticas terroristas responde tanto a incentivos operativos como a objetivos de control territorial, legitimación violenta y desafío abierto a la autoridad estatal (Makarenko, 2005; InSight Crime, 2023).

En este sentido, a los aspectos operativos y tecnológicos se suma una dimensión menos visible pero igualmente relevante: el contexto social, cultural y simbólico en el que estos ataques se producen. Como señala Crespo (2018), la violencia contra las fuerzas de seguridad no puede explicarse únicamente como una decisión táctica o reactiva, sino como el resultado de procesos previos de radicalización social y consolidación de subculturas de la violencia que legitiman la agresión contra el agente estatal. En los territorios donde la presencia policial o militar es percibida como una forma de ocupación, provocación u opresión, se configura un marco simbólico que facilita la deshumanización del “otro estatal” y su conversión en un objetivo legítimo de violencia. Este entorno sociocultural resulta clave para comprender por qué ataques sofisticados -como el uso de drones explosivos- pueden desplegarse de forma reiterada sin generar necesariamente un rechazo social proporcional al impacto que generan.

2.2. *Uso de drones con explosivos por grupos armados en Latinoamérica*

En territorios donde las economías ilícitas (narcotráfico o minería ilegal) generan financiamiento para los grupos armados, los drones son una herramienta de “soberanía criminal”, que representa un desafío a la seguridad del Estado en los tres países analizados.

La táctica de ejecutar ataques mediante artefactos explosivos improvisados (AEI) empleando drones se ha intensificado en América Latina como parte de la adaptación de actores no estatales a un entorno tecnológico de alta disponibilidad y bajo costo. En Colombia y México -y crecientemente en otros países- el dron se consolida como plataforma ofensiva y de hostigamiento, con capacidad de proyectar violencia a distancia y alterar rutinas operativas de las fuerzas estatales y de los grupos rivales (De Lorenzo de Guindos, 2026; Ginn y Goodwin, 2025). En términos comparados, el patrón no es uniforme: en Colombia, los incentivos combinan componentes políticos y económicos (con predominio de estos últimos), mientras que en México la racionalidad se vincula de forma predominante al control de mercados criminales y territorios estratégicos (Heise, 2025; Institute for Economics & Peace, 2026).

Más allá de las motivaciones, existe un elemento convergente clave: el ataque con drones funciona como instrumento de intimidación, que genera efectos psicológicos desproporcionados respecto del daño físico inmediato, erosionando la moral del adversario mediante la amenaza persistente desde el aire. En México, el despliegue de “droneros” y el uso de *droppers* (drones que liberan cargas) ha contribuido a instalar una percepción de vulnerabilidad constante en territorios en disputa, afectando tanto a oponentes como a comunidades civiles (De Lorenzo de Guindos, 2026; Heise, 2025). En Colombia, la difusión del zumbido de drones en zonas de conflicto y la expansión de ataques documentados por prensa y reportes estratégicos refuerzan su función como herramienta de coerción simbólica y control territorial (Heise 2025; Institute for Economics & Peace, 2026).

En el plano operacional, los drones habilitan a estos actores a acceder y atacar objetivos situados en áreas donde la aproximación terrestre sería más lenta, arriesgada o fácilmente interceptable. Su utilidad radica en reducir la exposición directa de los operadores, ampliar el alcance táctico y facilitar ataques de oportunidad contra patrullas, convoyes e infraestructura, manteniendo la iniciativa con bajos costos relativos (Heise, 2025; Ginn y Goodwin, 2025). Aunque existen limitaciones -autonomía de vuelo, carga útil, vulnerabilidad a inhibidores o defensa por capas-, el balance costoimpacto favorece su adopción, especialmente cuando se combinan dispositivos comerciales con adaptaciones artesanales, aprendizaje acumulativo y redes logísticas para el abastecimiento de componentes (De Lorenzo de Guindos, 2026; Ginn y Goodwin, 2025).

En tanto, en Brasil se observan indicios de la incorporación del dron como recurso de violencia en entornos de conflicto urbano, asociado a la escalada armada de organizaciones criminales con control territorial en favelas. Por ejemplo, se reporta el uso de drones por parte del “Comando Vermelho” durante una ² operación en Río de Janeiro en octubre de 2025, que dejó 122 muertos (Folha de S.Paulo, 2025), lo que sugiere la difusión regional de esta innovación hacia escenarios de criminalidad organizada con alta capacidad de fuego y gobernanza criminal local (De Lorenzo de Guindos, 2026). Este caso resulta analíticamente relevante porque traslada el problema desde la disputa rural (corredores de narcotráfico y control periférico) hacia el espacio urbano denso, donde el impacto psicológico y el riesgo de daños colaterales pueden amplificarse.

Asimismo, fuera de los tres países mencionados el dron también comienza a aparecer como recurso en contextos de crisis estatal y violencia de bandas, como en Haití, donde se registran operaciones con drones en el marco de acciones gubernamentales contra pandillas, junto con amenazas explícitas de respuesta por parte de líderes de bandas mediante drones propios, en el marco de escenarios de gobernabilidad extremadamente frágil (De Lorenzo de Guindos, 2026; Ginn y Goodwin, 2025). En conjunto, estos casos muestran que la adopción de drones no es un fenómeno aislado, sino parte de una transformación regional de los repertorios de violencia no estatal, con impacto para la seguridad pública y la protección de fuerzas de seguridad e infraestructura crítica (Institute for Economics & Peace, 2026; Ginn y Goodwin, 2025).

2 La operación se denominó “Contenção”.

2.3 Adaptación táctica como amenaza híbrida

La principal motivación de los grupos que operan en México y Colombia sería ejercer el control territorial, en términos del despliegue de poder en determinadas zonas para desarrollar sus operaciones ilícitas, impidiendo que el Estado imponga su autoridad en esos territorios, por tanto, los ataques con drones son también una demostración de poder, para generar influencia a través de la intimidación. Desde esta perspectiva, la innovación táctica del uso de drones se enmarca en un fenómeno de actores no estatales, que poseen un alto nivel de organización jerárquica, con capacidades que pueden impactar en la condición de gobernabilidad y ejercer control territorial para realizar sus operaciones criminales, por lo que estos actores pasan a representar insurgencias criminales (Bustamante, 2020).

Sobre la base de lo expuesto, los ataques con drones generar efectos comparables a los de las tácticas terroristas, debido a que su uso ofensivo trasciende a los ataques puntuales y a las víctimas directas, ocasionando un clima de temor e impacto psicológico. En este sentido, “lo que distingue a los actos de terrorismo de otros tipos de acción violenta es su capacidad para provocar un intenso impacto psicológico y social (ansiedad o temor) desproporcionado con respecto a los daños físicos ocasionados a las personas u objetos elegidos como blanco de la agresión” (De la Corte, 2013).

Estas insurgencias criminales utilizan este método de ataque, de tipo terrorista, en el marco de una gama más amplia de acciones, configurando una amenaza híbrida, cuyo concepto, aunque tiene diferentes interpretaciones, implica el empleo de medios convencionales e irregulares, con la perpetración de ataques terroristas, despliegue de propaganda y que explota las debilidades del adversario para ejercer poder y coacción (Colom, 2019).

Las amenazas híbridas implican el uso de diferentes tácticas, incluso militares, situación que es aplicable a los casos analizados. En Colombia, pese al acuerdo de paz de 2016, persiste el conflicto armado con actores que emplean tácticas guerrilleras y terroristas; en tanto, los cárteles de México son grupos del crimen organizado que poseen capacidades específicas, incluso proto-insurgentes, mediante el uso de tácticas guerrilleras. Asimismo, en ambos casos hay uso del ciberespacio y desinformación, cuya aplicación en su conjunto genera desestabilización y la posibilidad de erosionar la cohesión social, debilitar instituciones, atemorizar poblaciones y ejercer control territorial (Ortiz, 2015). Aunque no se trata de una “invasión militar” convencional, inequívocamente se está en presencia de un fenómeno multidimensional, con impacto en los sistemas políticos.

Las agrupaciones criminales emplean los drones con fines que van desde lo propagandístico a lo táctico ofensivo, lo que en esta última dimensión corresponde a ataques contra personal e infraestructura de fuerzas de seguridad, grupos rivales y población civil. Además, pueden hacer reconocimientos aéreos para vigilancia y planificación de ataques, transporte de pequeñas cantidades de drogas a centros penitenciarios, pero sobre todo ejercer temor, por ejemplo, grabando videos de ataques para su posterior difusión en internet.

2.4 Ataques con drones en Colombia

Los ataques con drones presentan una simetría directa con la cartografía de las economías ilícitas, específicamente relacionadas con las rutas de producción, procesamiento y tráfico de drogas, así como con la minería ilegal. Los departamentos donde se ha concentrado el despliegue de esta técnica incluyen Cauca, Norte de Santander, Arauca, Guaviare, Tolima, Cesar, Valle del Cauca y Putumayo (Torrado, 2025; Cifuentes, 2025b). En el nororiente del país, el departamento de Norte de Santander -particularmente la subregión del Catatumbo- se ha erigido como un epicentro de confrontación. En esta zona, el “Frente 33” de las disidencias de las FARC y el ELN han librado una violenta disputa territorial por el control de las rutas transfronterizas hacia Venezuela (Bonilla, 2025a; Torrado, 2025).

En el suroccidente, departamentos como Cauca y Valle del Cauca han sufrido ataques del “Estado Mayor Central”. En el Cauca, estructuras como el “Bloque Occidental Jacobo Arenas” y el “Frente Carlos Patiño” han utilizado los drones para asegurar el control sobre el Cañón del Micay, un enclave fundamental para el procesamiento de cocaína (Torrado, 2025). Por su parte, Arauca, Guaviare y Putumayo funcionan como zonas de retaguardia estratégica y corredores de exportación, donde la negación del espacio aéreo dificulta las labores de erradicación y el control estatal.

El uso de estos aparatos en el conflicto colombiano transitó desde una fase experimental a un estado de “madurez técnico-militar”. Inicialmente, los grupos armados adaptaban drones comerciales y recreativos para arrojar artefactos explosivos rudimentarios, tales como cilindros de PVC cargados con nitrato de amonio y metralla (Bonilla 2025a). Sin embargo, el ELN y las disidencias de las FARC han incrementado drásticamente la inversión en tecnología para lograr una mayor precisión y letalidad (Cifuentes, 2025b). La búsqueda de mayor certeza ha llevado a las organizaciones criminales a reclutar especialistas en programación y pilotaje remoto, conformando “escuelas de droneros” en zonas como el Pacífico y el Cauca (Bonilla, 2025a).

Asimismo, como respuesta a la implementación de sistemas de inhibición de radiofrecuencia (*jammers*) por parte del Estado, los actores armados han iniciado una fase de adaptación tecnológica mediante la importación de drones guiados por fibra óptica. Esta innovación, que Cifuentes (2025b) vincula a flujos tecnológicos transnacionales procedentes de Irán vía Venezuela, asegura un enlace de mando, control y video en tiempo real absolutamente inmune a las contramedidas electromagnéticas, por lo que los grupos criminales “van un paso adelante”. Adicionalmente, otro aspecto crítico es la reconversión de drones agrícolas de alta capacidad para dispersar agentes químicos (Torrado, 2025). Esta táctica no solamente posee una dimensión de “guerra química a pequeña escala”, sino que eventualmente satura las capacidades de respuesta de emergencias, y además vulnera los principios fundamentales del Derecho Internacional Humanitario, maximizando el terror psicológico por la invisibilidad del ataque.

Para dimensionar la amenaza asimétrica actual, resulta imperativo analizar eventos que evidencian la sofisticación técnica y las capacidades del Ejército de Liberación Nacional (ELN) con el uso de drones. Un hito crítico ocurrió el 20 de julio de 2025 en el municipio de El Carmen, Norte de Santander, donde en una base militar fueron atacadas tropas de la Fuerza de Tarea Vulcano del Ejército Nacional mediante drones con artefactos explosivos. El saldo de este ataque, de tres soldados profesionales asesinados y ocho militares heridos de gravedad, no sólo representa una tragedia humana, sino que marca un punto de inflexión en la capacidad de los actores no estatales para vulnerar enclaves militares protegidos (Cifuentes, 2025b).

De este incidente es necesario poner atención en que se trató de una operación coordinada, con la “saturación del espacio aéreo”, lo que implica que existe un mando que coordina y que habría existido planificación, considerando además que, esta técnica permite que si uno o dos drones son interceptados otro pueda atacar el objetivo.

Respecto a lo anterior, este hecho, atribuido al ELN, evidenció la vulnerabilidad de las fuerzas de seguridad del Estado y la capacidad de los grupos armados para realizar “operaciones de saturación”. La precisión y el éxito operativo del ataque sugieren un proceso de entrenamiento y transferencia de conocimientos que sobrepasa el aprendizaje empírico, incluso, abre la posibilidad de que grupos insurgentes latinoamericanos estén adoptando manuales de combate de conflictos como del Medio Oriente.

Posteriormente, otro incidente ocurrió el 21 de agosto de 2025 en la zona rural del municipio de Amalfi, en el departamento de Antioquia, donde fue derribado un helicóptero de la Policía Nacional por un ataque con un dron, en el que fallecieron 13 policías. La aeronave se dirigía a apoyar a un grupo de efectivos que realizaban labores de erradicación manual de cultivos ilícitos en la zona (Ávila y Cueto, 2025b). El ataque expuso falencias de anticipación, pues informes de inteligencia habrían advertido sobre la intención de grupos criminales de atacar aeronaves en la zona. Aunque inicialmente la autoría generó confusión, el “Frente de Guerra Darío Ramírez Castro” del ELN se atribuyó la autoría del ataque mediante un video en redes sociales el 4 de septiembre de 2025 (Bernal, 2025a). Se destaca este evento en el conflicto colombiano, en el que confirma que los actores armados poseen ahora una capacidad real de “defensa antiaérea”, limitando drásticamente la superioridad tradicional del Estado en el espacio aéreo de baja altitud.

Como expone Cifuentes (2025a) para enfrentar esta amenaza, las autoridades han invertido en tecnología militar antidrones, proveniente de Canadá y España. La respuesta institucional se ha articulado principalmente en torno a dos grandes frentes: la adquisición de sistemas defensivos masivos y el desarrollo de plataformas ofensivas propias. En el ámbito defensivo, el Gobierno Nacional implementó el “Proyecto Escudo Nacional Antidrones”. Con una inversión que supera los 1.680 millones de dólares, esta estrategia busca desplegar radares de alerta temprana y sistemas de inhibición en guarniciones estratégicas, refinerías y la Casa de Nariño (Bonilla, 2025b). En el ámbito ofensivo,

la Corporación de la Industria Aeronáutica Colombiana (CIAC) desarrolló el dron DRAGOM (Dron de Reconocimiento y Ataque Guiado para Operaciones Militares). Este dispositivo cuenta con más de 90 minutos de autonomía, capacidad para transportar cargas útiles de hasta 10 kilogramos, cámaras de alta definición y un doble canal de comunicación encriptado y satelital, permitiendo inteligencia táctica y la ejecución de ataques precisos con explosivos (Cifuentes, 2025a).

No obstante, la eficacia de estas medidas ha sido severamente cuestionada. Como bien argumenta Bonilla (2025b), la respuesta del Estado colombiano ha sido tardía y fragmentada. Los análisis técnicos y estratégicos exponen una desconexión fundamental entre las capacidades adquiridas y la realidad operativa del conflicto, debido a que en primer lugar, los sistemas estáticos de inhibición del Escudo Nacional están diseñados principalmente para proteger infraestructuras críticas en entornos urbanos o semiurbanos, dejando desprotegidas las áreas selváticas donde realmente se libra el conflicto, ya que el Estado argumenta no tener capacidad de equipar con inhibidores a los más de 3.000 pelotones desplegados (Bonilla, 2025b; Torrado, 2025); en segundo lugar, la burocracia estatal presenta un desfase temporal frente a la innovación insurgente, ya que mientras el Estado requiere largos procesos de compra, los grupos armados logran superar estas defensas rápidamente cambiando frecuencias, volando de manera autónoma y adoptando drones controlados por fibra óptica.

El conflicto colombiano ha ingresado en la era de la guerra aérea no tripulada. La capacidad de estas organizaciones para derribar aeronaves del Estado y penetrar bases militares demuestra un nivel de sofisticación que anula las ventajas logísticas tradicionales de las fuerzas militares. Asimismo, la dispersión de agentes químicos, el uso de fibra óptica para evadir inhibidores y la precisión quirúrgica configuran un panorama de amenaza asimétrica altamente complejo.

2.5 Ataques con drones en México

En México, las pugnas entre cárteles de droga han llevado a éstos a buscar nuevas formas de desplegar violencia para ejercer control territorial y primar en el negocio ilícito, por lo que han incorporado “minas Claymore, granadas propulsadas por cohetes, morteros fabricados a partir de tubos de tanques de gasolina y camiones blindados equipados con ametralladoras pesadas. Están enterrando artefactos explosivos improvisados para matar a sus rivales y modificando drones comprados por internet para convertirlos en drones de ataque, cargados con sustancias químicas tóxicas y bombas” (Villegas, 2025).

En este contexto, la táctica de ataques con explosivos utilizando drones es usada por los cárteles de drogas contra otros cárteles, pero también contra la policía y el ejército. De hecho, estos ataques han dejado a militares fallecidos. Esta táctica es utilizada principalmente por los cárteles “Jalisco Nueva Generación” (CJNG), “Sinaloa” y “La Familia Michoacana”, en Michoacán, Chihuahua y Guanajuato (Jaramillo, 2025).

Los artefactos explosivos son de elaboración casera. De hecho, “las carcasas suelen estar hechas con botellas de plástico, tubos de desagüe cortados e incluso extintores. A los dispositivos se les colocan aletas de acero, vidrio y plástico para estabilizarlos durante el vuelo. En su interior contienen pólvora casera y nitrato de amonio con combustible, un explosivo utilizado a menudo en la minería y la construcción” (Villegas, 2025).

El CJNG sería el precursor en México de esta modalidad, incluso actualmente cuenta con una célula dedicada a esta tarea, bajo la denominación de “operadores droneros”, con un estilo militar y uso de atuendos tácticos. Sin embargo, “analistas de seguridad y funcionarios mexicanos señalan que los cárteles comenzaron a militarizarse a mediados de la década de 2000, cuando “Los Zetas”, un grupo formado por antiguos miembros del ejército, introdujeron la disciplina del campo de batalla, las comunicaciones encriptadas y el armamento pesado al crimen organizado” (Villegas, 2025). “El CJNG comenzó a emplear drones con explosivos en Michoacán alrededor de 2020, utilizándolos en ataques contra grupos rivales y comunidades locales. Con el tiempo, esta táctica fue replicada en Guerrero por La Familia Michoacana, que ha recurrido a estos dispositivos para fortalecer su dominio territorial y expandir su influencia” (Jaramillo, 2025).

Estos grupos habrían adquirido conocimientos de la experiencia militar: “adicionalmente, grupos criminales mexicanos han acudido a la experiencia de exmilitares colombianos para mejorar y profesionalizar la adaptación de explosivos en los drones” (Jaramillo, 2025).

Respecto al origen de los drones, éstos serían adquiridos en el comercio, pero adaptados para cargar y soltar los artefactos explosivos, sin embargo, también podría haber drones-explosivos adquiridos en el extranjero, con mayor sofisticación.

En abril de 2024, en Michoacán el CJNG usó drones para lanzar artefactos explosivos con sustancias químicas en su interior, cuyos gases habrían producido efectos sobre las vías respiratorias de los habitantes de la zona, similar a los incidentes que se han reportado en Colombia (Jaramillo, 2025),

2.6 Ataques con drones en Brasil

La proliferación de Vehículos Aéreos No Tripulados (VANT) en el ecosistema del crimen organizado brasileño ha transformado radicalmente las dinámicas de la violencia urbana y la seguridad pública (Pyatakov, 2025), debido a la apropiación y modificación de drones comerciales por parte de grupos como el “Comando Vermelho” (CV), el “Primeiro Comando da Capital” (PCC) y el “Terceiro Comando Puro” (TCP) (Portal CIP, 2025).

Aunque las primeras documentaciones de “narco-drones” armamentizados surgieron en la frontera entre México y Estados Unidos de la mano de cárteles como el “Cártel de Jalisco Nueva

Generación” (Diálogo Américas, 2023), la amenaza se ha expandido geográficamente, y Brasil se ha consolidado como un epicentro crítico de esta escalada (Pyatakov, 2025). En un contexto marcado por la histórica militarización del espacio urbano y la metáfora de la guerra en la gestión de las favelas (Leite, 2012), las organizaciones criminales brasileñas han incorporado el dominio aéreo para eludir los tradicionales perímetros terrestres de las fuerzas de seguridad y proyectar un control territorial tridimensional (Portal CIP, 2025).

La operatividad actual se puede clasificar en tres categorías: en primer lugar, destacan las labores de Inteligencia, Vigilancia y Reconocimiento (ISR), llevadas a cabo por actores como el PCC, el CV y el TCP, para mapear despliegues policiales, vigilar a autoridades del sistema de justicia e identificar vulnerabilidades mediante la incorporación de cámaras térmicas e infrarrojas y software de vuelo autónomo (Portal CIP, 2025; Pyatakov, 2025). En segundo lugar, se encuentra la logística e infiltración, operada principalmente por facciones carcelarias y redes portuarias para el contrabando de narcóticos, armas y dispositivos de comunicación, a través de drones de carga con mecanismos de liberación (Pyatakov, 2025; Portal CIP, 2025). En tercer lugar, el narcoterrorismo, liderado por el CV y el TCP, enfocado en el “bombardeo aéreo” con artefactos explosivos improvisados y granadas contra rivales, civiles y policías, valiéndose de garras electromecánicas adaptadas y sistemas de visión en primera persona (InfoMoney, 2024; Pyatakov, 2025).

La transición del uso de drones como plataformas de ataque letal ha alterado la balanza del conflicto urbano en Brasil, debido a que por ejemplo es posible liberar granadas sin el pasador de seguridad directamente sobre objetivos terrestres (InfoMoney, 2024). La fragmentación territorial entre el “Comando Vermelho”, el “Terceiro Comando Puro” y grupos paramilitares ha precipitado una “carrera armamentista aérea” (The Dialogue, 2024). Los registros policiales indican que la armamentización sistemática se inició durante disputas territoriales cuando el TCP, bajo el liderazgo de traficantes comenzó a utilizar drones para bombardear áreas dominadas por el CV (InfoMoney, 2024). En un incidente documentado que ilustra la naturaleza indiscriminada de estos ataques, una granada fue lanzada desde un dron sobre una plaza pública en la que jugaban niños, generando pánico masivo y un profundo terror psicológico en la comunidad (Band Jornalismo, 2024).

Los ataques también se han dirigido frontalmente contra el Estado. El 28 de octubre de 2025, en el marco de la “Operación Contenção”, ejecutada en los complejos da Penha y do Alemão, el CV utilizó drones para lanzar artefactos explosivos sobre agentes de la Coordenadoria de Recursos Especiais de la Policía Civil (G1 Rio, 2025), incidente que el gobernador calificó como “narcoterrorismo” (G1 Rio, 2025).

Las investigaciones revelan además un peligroso desbordamiento de conocimientos tácticos desde las instituciones militares hacia el crimen organizado. En septiembre de 2024, la “Operación Buzz Bomb” de la Policía Federal desarticuló una red en Gardênia Azul que operaba drones lanza-granadas (Polícia Federal do Brasil, 2024). Se descubrió que un cabo de la Marina de Brasil estaba

directamente involucrado en el pilotaje y la adaptación militar de estos equipos para las facciones criminales (G1 Rio, 2024).

A diferencia de la beligerancia abierta en Río, el PCC en São Paulo emplea los drones bajo una lógica corporativa y mafiosa orientada a la inteligencia táctica de alta precisión (Pyatakov 2025). A finales de 2025, investigaciones del Ministerio Público revelaron los planes de la “Sintonia Restrita”, una célula del PCC dedicada a perpetrar atentados contra autoridades del Estado (Record News, 2025). Los criminales utilizaron drones para monitorear minuciosamente las residencias y rutinas de Lincoln Gakiya, fiscal histórico en la lucha contra el PCC, y de Roberto Medina, coordinador del sistema penitenciario (G1 São Paulo, 2025), para lo cual miembros de la facción alquilaron propiedades adyacentes para operar los drones con línea de visión directa, evaluando la altura de los muros, la ubicación de cámaras y las vulnerabilidades de seguridad de las familias de los funcionarios, con el objetivo de planificar asesinatos selectivos (G1 São Paulo, 2025).

Esta tecnología de VANT armados ha superado las barreras de los grandes centros urbanos. En Itaberaí, Estado de Goiás, un grupo criminal operó un dron con explosivos para extorsionar y atentar contra la vida de un empresario local (Ôguen, 2026), sin embargo, el ataque fracasó debido a un error de pilotaje que provocó la colisión del aparato contra un árbol, pero demostró que la barrera técnica para ejecutar actos de terror aéreo es actualmente mínima y accesible a estos grupos (InfoMoney, 2024).

Para contrarrestar esta asimetría, las fuerzas de seguridad están adoptando sistemas contra vehículos aéreos no tripulados. Las contramedidas actuales operan principalmente en la detección y rastreo mediante el uso de sistemas pasivos de radiofrecuencia (RF) y radares de feixe digital 3D impulsados por inteligencia artificial para discriminar drones autónomos (Ôguen, 2026). Asimismo, operan en la neutralización, para la cual el gobierno del Estado de Río de Janeiro ha iniciado la adquisición de rifles anti-drones portátiles que interfieren la señal GPS a distancias de hasta 2 kilómetros (Portal Nacional de Contratações Públicas, 2024). No obstante, la criminalidad adaptativa genera contramedidas inmediatas, por lo que ante el uso de inhibidores de radiofrecuencia, se genera la incorporación criminal de drones guiados por fibra óptica (Jovem Pan News, 2024). Estos dispositivos, conectados por microcables de hasta 50 km de longitud, no emiten señales de radio y son completamente inmunes a la interferencia electrónica (Jovem Pan News, 2024).

En definitiva, la adopción de drones armados y de vigilancia por parte de las organizaciones criminales brasileñas no es una simple anomalía tecnológica, sino una evolución sistémica en la gobernanza criminal y el conflicto asimétrico. Grupos como el CV, el TCP y el PCC han demostrado capacidad para aplicar la “criminalidad adaptativa”, transformando aparatos comerciales en armas de terror psicológico y letalidad dirigida. Enfrentar esta amenaza exige una respuesta multidimensional que integre contramedidas avanzadas, reformas jurídicas contundentes y políticas orientadas a erradicar la transferencia de doctrina militar hacia las redes del narcotráfico.

2.7 Convergencias y particularidades observadas en los tres países

El empleo de drones por actores no estatales criminales, con motivaciones económicas y/o políticas presenta similitudes en los tres países, pero también matices y diferencias, debido a sus propios contextos y a los objetivos que persiguen las agrupaciones que recurren a esta táctica, incluso a las realidades espaciales en que operan.

En el caso de Colombia, a diferencia de los otros dos países, ocurre en el marco de un conflicto armado interno, en que estos dispositivos fueron incorporados como una extensión de las capacidades armadas de las agrupaciones implicadas, como una forma de compensar la asimetría respecto a las capacidades estatales, además de la necesidad de operar en zonas de difícil acceso. En lo táctico, se ha visto la incorporación de tecnología de fibra óptica, para evadir los sistemas de inhibición, como también la diseminación de agentes químicos desde drones, situación que genera un alto impacto psicológico. Debe precisarse, que en este país los actores persiguen objetivos que hibridan las motivaciones políticas con las económicas, con preeminencia de éstas últimas, mientras que en los otros dos países se trata de motivaciones exclusivamente económicas.

En México, el rasgo preponderante de este fenómeno es que su propósito es el control de los mercados criminales, con sus implicancias territoriales, respecto a zonas estratégicas para desarrollar los negocios ilícitos, por tanto, los ataques con drones son una forma de amedrentar a fuerzas de seguridad y a grupos rivales, por su impacto psicológico, para operar sin dificultades, es decir, este método se orienta al control de los mercados criminales. Un elemento distintivo son las “unidades de droneros” del CJNG, con atuendo táctico y una implícita “profesionalización”.

Por otra parte, en Brasil la principal particularidad es que, a diferencia de los casos anteriores, es que se ejerce en entornos urbanos densamente poblados, en las favelas, que son lugares con confinamiento de construcciones y cantidad de habitantes, destinando su uso para contrarrestar la acción policial, incrementándose de la posibilidad de producir daños colaterales a causa de la concentración poblacional. Asimismo, se ha evidenciado el uso de drones para vigilancia de autoridades, en el marco de planes de asesinato.

Tabla 1: Comparación uso de drones en los tres países.

Variable	Colombia	México	Brasil
Actores	Disidencias de las FARC y el ELN.	Cárteles “Jalisco Nueva Generación”, “Sinaloa”, “Familia Michoacana”	“Comando Vermelho” y “Primeiro Comando da Capital”
Entorno de operación	Selva y áreas rurales	Rural y semiurbano	Urbano, densamente poblado
Objetivo de uso	Enfrentamiento con fuerzas armadas, búsqueda de desgaste de éstas; control territorial para cultivo de drogas y otras actividades ilícitas	Control territorial, intimidación a cárteles rivales y a fuerzas de seguridad	Ofensiva contra operaciones policiales en favelas, ataques a grupos rivales
Característica diferenciadora	Fibra óptica para evadir inhibidores de señal, uso de drones agrícolas, dispersión de agentes químicos	Mecanismo de liberación de explosivos de alta precisión, ataques “enjambre”, confección de drones artesanales, profesionalización de “operadores droneros”	Ataques en áreas urbanas, vigilancia aérea y planes de asesinatos selectivos

Fuente: Elaboración propia.

Este fenómeno muestra que la convergencia estratégica, en que esta tecnología se consolida como una herramienta para la protección y fortalecimiento de economías ilícitas, mediante el control territorial. En los tres contextos, el uso de estos dispositivos busca compensar la asimetría táctica frente a los cuerpos de seguridad, funcionando como un multiplicador de fuerzas que permite a guerrillas, cárteles y grupos criminales desgastar a las fuerzas de seguridad y someter, o a lo menos intimidar, a grupos rivales. Esta adopción tecnológica de fácil acceso no sólo responde a una necesidad operativa, sino que también, como ya se ha explicado, persigue un impacto psicológico y coercitivo, utilizando la vigilancia y el ataque aéreo para amedrentar tanto a las autoridades como a la población civil y así “operar con tranquilidad”. La similitud más crítica radica en la capacidad de estos grupos para evadir las contramedidas, logrando saturar o evadir las respuestas estatales mediante la innovación técnica y el aprovechamiento de entornos geográficos complejos, como la selva o las favelas, lo que plantea un desafío de seguridad pública.

Sobre la base de lo expuesto, se muestran desafíos específicos para cada país, en lo referente a la neutralización de drones por parte de los cuerpos y fuerzas de seguridad, como por ejemplo, el teatro de operaciones de las favelas brasileñas, donde la alta densidad urbana dificulta el despliegue de contramedidas por la policía; mientras que en Colombia el uso de tecnología de fibra óptica representa una limitante para contramedidas como los inhibidores de señales, además del contexto donde ocurre, que por tratarse de un conflicto armado, incrementa la temporalidad e intensidad de su uso; en tanto; en México la complejidad para enfrentar esta amenaza es la escalada táctica, determinada por “ataques enjambres” y dispositivos de liberación de explosivos de alta precisión, que limitan o saturan la capacidad de respuesta policial.

3. Conclusiones

La realidad de la seguridad en América Latina muestra que la proliferación de sistemas aéreos no tripulados (UAS) ha dejado de ser una innovación táctica para convertirse en el eje de una amenaza híbrida que redefine el control territorial. Este método pasó de ser una amenaza emergente para convertirse en una amenaza presente.

Este fenómeno representa la materialización del *crime-terror continuum*, en que organizaciones criminales en México, Colombia y Brasil adoptan tácticas de “guerra asimétrica” para disputar el monopolio de la fuerza. Integrar capacidades tecnológicas emergentes, economías ilícitas y marcos simbólicos de legitimación de la violencia, consolidan que estos actores criminales refuerzan las formas híbridas de coerción y refuerzan la pertinencia del modelo de Makarenko para analizar la transformación contemporánea de la violencia no estatal en América Latina. En este sentido, el uso de drones para ejecutar ataques, vigilancia y transporte de narcóticos ha erosionado la superioridad aérea tradicional de los Estados, obligándolos a una reingeniería profunda de las doctrinas de defensa nacional.

En Colombia, el derribo del helicóptero en Amalfi el 21 de agosto de 2025, que resultó en la muerte de 13 policías y fue reivindicado por el ELN, marcando un hito en la capacidad de los grupos armados para negar el espacio aéreo al Estado. Esta sofisticación se manifiesta también en el uso de drones guiados por fibra óptica, los cuales son inmunes a los sistemas de interferencia electrónica convencionales.

A pesar de los esfuerzos institucionales por desarrollar soberanía tecnológica e instalar sistemas antidrones, la falta de una estrategia integral ha generado una contención ineficaz. La respuesta del Estado requiere de una reingeniería profunda que priorice la movilidad táctica, la inteligencia preventiva y la capacidad de adaptación tecnológica en tiempo real.

En México, cárteles como el CJNG y “La Familia Michoacana” han militarizado sus acciones mediante unidades de “operadores droneros” que emplean explosivos improvisados para asediar comunidades y atacar a las fuerzas federales. Asimismo, el uso de drones para la dispersión de agentes químicos en Michoacán y Guerrero implica una dimensión de terrorismo que ocasiona desplazamiento forzado e impacto psicológico en la población civil.

En Brasil, la “Operación Contenção” de 2025 mostró cómo el “Comando Vermelho” emplea drones con explosivos para hostigar a unidades de élite en entornos urbanos densos. En tanto, en São Paulo, el PCC utiliza esta tecnología para una vigilancia de precisión sobre altos funcionarios judiciales, demostrando que el dron es una herramienta versátil tanto para la ofensiva directa como para la inteligencia criminal avanzada.

En Colombia, las fuerzas armadas están incorporando sistemas antidrones y también se encuentra en trámite un proyecto de ley para regular su tenencia y uso; no obstante, sería complejo garantizar la seguridad de todos los efectivos que son desplegados en terreno. En conjunto con la adquisición de tecnología y modificaciones legales, es fundamental establecer planes de protección civil y potenciar la coordinación entre las instituciones estatales con incidencia en la materia.

Hacia 2030, el desarrollo de esta amenaza se encamina hacia el despliegue de enjambres autónomos coordinados por inteligencia artificial y el uso de tecnologías de fibra óptica para evadir la guerra electrónica. La transición hacia ataques autónomos y la posible dispersión de agentes biológicos en centros urbanos representan riesgos para la estabilidad regional.

Respecto a lo anterior, el éxito institucional no dependerá de adquisiciones tecnológicas aisladas, sino de una gobernanza aérea integral, que incluya la armonización legal hemisférica y la cooperación transnacional.

Debe precisarse que, si se tratara de un fenómeno exclusivamente de violencia política, en la respuesta estatal sería fundamental atacar la narrativa que sustenta la lucha de los actores armados para mermar su base social de apoyo, deslegitimar su mensaje y generar desmovilización. Sin embargo, dado que las motivaciones de estos grupos armados no son políticas o ideológicas, la estrategia no debe centrarse en la dimensión política del fenómeno, sino principalmente en abordar ilícitos como el narcotráfico y la minería ilegal, que constituyen las fuentes de financiamiento y motivación de estas agrupaciones, situación que requiere de una respuesta policial-militar, incluyendo la función de inteligencia, además de reformas jurídicas e intensificar la presencia estatal en determinados territorios.

4. Referencias bibliográficas

- Ávila-Claudio, R. y Cueto, J. (2025a). Ataque aéreo en Amalfi: El derribo de helicóptero de la Policía y sus repercusiones. *Análisis de Conflicto y Seguridad*.
- Ávila-Claudio, R. y Cueto, J. (2025b, 24 de agosto). Qué se sabe del ataque contra una base militar y el derribo de un helicóptero de la policía que dejaron al menos 19 muertos y decenas de heridos en Colombia. *BBC News Mundo*.
- Band Jornalismo. (2024). *Traficantes usam drone para lançar granada em praça no Rio de Janeiro* [Vídeo]. YouTube.
- BBC Mundo. (2022). *Cómo los grupos armados en Colombia usan drones con explosivos*.
- Bernal, J. (2025a, 4 de septiembre). Atentado terrorista contra un helicóptero que dejó 13 policías muertos en Amalfi, Antioquia fue realizado por el ELN: El mismo grupo terrorista confirmó el ataque. *Infobae*.

- Bernal, J. (2025b). El Frente de Guerra Darío Ramírez Castro se atribuye ataque en Antioquia. *Reportes de Seguridad en Redes Sociales*.
- Bonilla, L. (2025a, 24 de abril). Drones de guerra: Así operan los grupos colombianos la nueva arma que siembra terror. *El Espectador*.
- Bonilla, L. (2025b). El ambicioso escudo antidrones con el que Colombia quiere combatir las ofensivas aéreas de los grupos armados. *BBC News Mundo*.
- Bustamante, A. (2020). Insurgencias criminales y guerra urbana en Latinoamérica: Una aproximación al proceso de urbanización regional y su impacto en la evolución táctica y operativa de las organizaciones criminales transnacionales. *Entretextos*, 12(35), 1-17.
- Cifuentes, I. (2025a). Desarrollo de tecnología militar y sistemas antidrones en el conflicto colombiano. *Ciencia y Poder Aéreo*, 18(2).
- Cifuentes, S. (2025b, 26 de julio). ELN y las disidencias de las Farc podrían estar usando drones con fibra óptica y visión nocturna para ataques y vigilancia precisa. *Infobae*.
- Colom, G. (2019). *La amenaza híbrida: Mitos, leyendas y realidades* (Documento de Opinión IEEE No. 24/2019). Instituto Español de Estudios Estratégicos.
- Crespo Alcázar, A. (2018). Radicalización social y subcultura de la violencia como legado de ETA: La agresión a la Guardia Civil en Alsasua como caso de estudio. *SCIO. Revista de Filosofía*, (14), 53-82.
- De la Corte, L. (2013). ¿Hasta qué punto convergen el terrorismo global y la criminalidad organizada? Parámetros generales y escenarios críticos. *Revista del Instituto Español de Estudios Estratégicos*, (1), 149-176.
- De Lorenzo de Guindos, D. (2026). La muerte desde arriba: Empleo de drones de ataque por organizaciones terroristas. *Logos Guardia Civil: Revista Científica del Centro Universitario de la Guardia Civil*, 4(1), 53-82.
- Diálogo Américas. (2023). *Organized crime and its use of drones to sow terror*.
- Folha de S.Paulo. (2025, 29 de octubre). *El gobernador de Río de Janeiro califica de éxito la operación con al menos 121 muertos; familiares hablan de masacre*.
- G1 Rio. (2024). Cabo da Marinha é preso em operação da PF contra drones lança-granadas do tráfico. *Globo*.
- G1 Rio. (2025). Em retaliação à ação policial, criminosos lançam bombas com drones no Complexo da Penha. *Globo*.
- G1 São Paulo. (2025). PCC alugou casa vizinha e usou drones para monitorar promotor jurado de morte. *Globo*.
- García, J., & Hernández, A. (2024). Las disidencias de las FARC-EP: ¿Continuación de esta guerrilla o nuevos grupos criminales? *Política y Sociedad*, 61(2), 1-16.
- Ginn, P. & Goodwin, A. (2025, 30 de octubre). *Crime by drone: A new paradigm for organized crime*. Global Initiative Against Transnational Organized Crime.
- Heise, M. (2025). Ataques con drones en Colombia y México como amenaza híbrida. *Al-Ghurabá*, (98), 12-19.

- InfoMoney. (2024). *Como funcionam os drones usados pelo tráfico para jogar explosivos em policiais*.
- InSight Crime. (2021). *How the CJNG responds to the death of its leaders*.
- InSight Crime. (2022). *Brazil's criminal groups and the challenge to state authority*.
- InSight Crime. (2023). *Drone warfare and criminal innovation in Latin America*.
- InSight Crime. (2024). *Colombia's FARC dissidents and the return of armed attacks*.
- Institute for Economics & Peace. (2026). *Global terrorism index 2026*. Institute for Economics & Peace.
- Jaramillo, J. (2025, 6 de marzo). *Los drones refuerzan el arsenal criminal en América Latina y el Caribe*. InSight Crime.
- Jovem Pan News. (2024). *Especialistas alertam para uso de drones guiados por fibra óptica pelo crime organizado* [Vídeo]. YouTube.
- Leite, M. (2012). The metaphor of war extends across various urban domains. *SciELO Brasil*.
- Makarenko, T. (2005). *The crime-terror continuum: Modelling 21st century security dynamics*. University of Wales.
- Ôguen. (2026). *Drones armados no Brasil: O caso de Itaberai e o novo risco à segurança*. Ôguen Segurança Perimetral.
- Ortiz, R. (2015). El concepto de guerra híbrida y su relevancia para América Latina. *Revista Ensayos Militares*, 1(2), 131-148.
- Polícia Federal do Brasil. (2024). *PF reprime uso de drones lança-granadas utilizados por organização criminosa*. Ministério da Justiça e Segurança Pública.
- Portal CIP. (2025). *Unmanned aerial vehicles and organized crime in ports*.
- Portal Nacional de Contratações Públicas. (2024). *Facções criminosas do RJ usam drones carregados para "bombardear" inimigos*. PNCP.
- Pyatakov, A. N. (2025). The criminal use of drones in Latin America. *Aurora Journals*.
- Record News. (2025). *Veja detalhes do plano do PCC para matar autoridades em São Paulo* [Vídeo en programa Fala Brasil]. YouTube.
- Rios, H. (2025). Desarrollo estratégico del Ejército Nacional de Colombia, 75 años: Historia, modernización y desafíos del siglo XXI. *Escenarios Actuales*, (2), 203–225. Centro de Estudios e Investigaciones Militares.
- The Dialogue. (2024). *Is Brazil's security strategy making the country safer?* [Análisis].
- The Guardian. (2021). *Brazil's favelas and the rise of armed criminal governance*.
- Torrado, S. (2025, 30 de agosto). Las disidencias multiplican los ataques con drones y encienden las alarmas en Colombia. *El País*.
- Villegas, P. (2025, 1 de septiembre). Drones y explosivos improvisados: Los cárteles de México adoptan armas de guerra moderna. *The New York Times*.

Nota de autor respecto al uso de Inteligencia Artificial: Durante la preparación de este artículo, se emplearon las herramientas de Inteligencia Artificial generativa Gemini y ChatGPT con el propósito de asistir en la búsqueda preliminar de fuentes bibliográficas y para la revisión y corrección de estilo del texto. Tras la utilización de dichas herramientas, los autores revisaron y verificaron exhaustivamente la literatura citada, además de editar el contenido final, asumiendo la responsabilidad exclusiva y total sobre la originalidad, el rigor analítico y la precisión del manuscrito.

Jocelyn Vega Vargas y Dulce Sarai González González

Radicalización a través de las imágenes: la propaganda extremista en la revista Dabiq

Radicalization Through Images: Extremist Propaganda in Dabiq

Resumen

Este artículo analiza las imágenes utilizadas en los quince números de la versión inglesa de Dabiq como dispositivo propagandístico del Estado Islámico (EI) entre 2014 y 2016. Para ello, se desarrolló una metodología de diseño propio destinada a analizar cómo las imágenes construyen narrativas de identidad colectiva, victimización, poder de la organización y legitimidad estatal, elementos que pueden contribuir a la radicalización ideológica y a la legitimación simbólica de la violencia. Mediante el software ATLAS.ti, se realizó un estudio exploratorio cualitativo basado en la codificación manual original de las fotografías incluidas en la revista y en la categorización sistemática de los marcos visuales predominantes conforme al enfoque de marco (o framing) de Entman (1993). A diferencia de estudios anteriores que enfatizan principalmente las representaciones utópicas del califato, los hallazgos sugieren un predominio más marcado de imágenes asociadas con la capacidad militar de EI.

Esto indica que la propaganda fotográfica utilizada en Dabiq se centra, en gran medida, en enaltecer el poder bélico de la organización y en representar a sus enemigos mediante la ridiculización y la deshumanización, contribuyendo así a normalizar y legitimar la violencia y, potencialmente, a reforzar narrativas favorables a procesos de radicalización.

Palabras clave: Estado Islámico, Dabiq, propaganda, ideological radicalization, visual frames.

Abstract

This article analyzes the images used in the fifteen issues of the English-language edition of Dabiq as a propaganda tool of the Islamic State (IS) between 2014 and 2016. To this end, a proprietary methodology was developed to facilitate the analysis of the images as constructions of narratives of collective identity, victimization, the organization's power, and its legitimacy as a state—all of which contribute to ideological radicalization and the symbolic legitimization of violence. Using ATLAS.ti software, a qualitative exploratory study was conducted with original manual coding of each photograph featured in the magazine, systematically categorizing the visual frames according to Entman's (1993) framing approach that predominated throughout its publications. Unlike previous studies that primarily emphasized utopian representations of the caliphate, the findings suggest a more pronounced predominance of images associated with its military capabilities.

This indicates that the photographic propaganda used in Dabiq largely focuses on glorifying the organization's military power and portraying its enemies through ridicule and dehumanization, thereby contributing to the normalization and legitimization of violence and potentially reinforcing narratives conducive to radicalization.

Keywords: Islamic State, Dabiq, propaganda, ideological radicalization, visual frames

Jocelyn Vega Vargas, Doble grado en Derecho y Relaciones Internacionales por el Instituto Tecnológico y de Estudios Superiores de Monterrey.

Dulce Sarai González González, Doble grado en Derecho y Relaciones Internacionales por el Instituto Tecnológico y de Estudios Superiores de Monterrey.

Para citar este artículo: Vega, J. y González, D. (2026), Radicalización a través de las imágenes: la propaganda extremista en la revista Dabiq, Revista Internacional de Estudios sobre Terrorismo, nº18, pp.69-87.

Recibido

23/06/2026

Aceptado

30/07/2026

1. Introducción

Como explica Cottee (2023, pp. 12-14), al igual que el terrorismo, el término “radicalización” posee múltiples significados; sin embargo, mediante el análisis de 50 estudios sobre el tema, señala que, si bien cualquiera puede ser radicalizado, lo entiende como un proceso complejo y multifacético, y lo describe como la acumulación de elecciones a lo largo del tiempo, que involucra tanto a los Estados como a la “vulnerabilidad” del individuo.

Como señala Entman (1993, p. 2), la propaganda contemporánea consiste en seleccionar determinados aspectos de la realidad percibida y hacerlos más prominentes en un texto, de modo que se facilite una interpretación causal, moral y/o orientada al tratamiento. De manera similar, Bunzel (2015) observa que el Estado Islámico (EI) fue “fundado por Al-Qaeda en Irak en un momento en que la insurgencia suní iraquí estaba perdiendo rápidamente impulso”. No obstante, el EI se benefició de la inestabilidad política surgida tras la Primavera Árabe, utilizándola para expandirse regionalmente y establecer un Estado yihadista en Irak, donde se intensificó su retórica radical, y que después se expandiría, especialmente después de la guerra en Siria en 2011 (Hoffman y Zeidel, 2021).

Sin embargo, para lograr su expansión en la región, fue importante desarrollar una estrategia mediática. Como parte de esta, el EI amplió su público objetivo y comenzó a publicar ediciones en lengua inglesa dirigidas a audiencias occidentales, a través de revistas como Dabiq (posteriormente Rumiya) (Milton, 2020, citado en Qi, 2024).

Adaptándose a la cultura occidental, el EI seleccionó imágenes para Dabiq que proyectaban narrativas de victimización, heroísmo y gobernanza, empleando herramientas de marketing contemporáneas como estrategia de poder blando para construir una imagen positiva e idealizada del “califato” y reforzar su legitimidad (Fahmy, 2020; Venkatesh et al., 2020; Kruglova, 2020; Archambault y Veilleux-Lepage, 2020, citados en Qi, 2024).

Según Entman (2004, citado en Winkler et al., 2021), la fotografía no es neutral; es posible moldear la percepción pública a través de la política, las emociones y la ideología (Goffman, 1974; Iyengar y Kinder, 1987; Scheufele, 1999, citados en Winkler et al., 2021). En el caso del EI, la revista Dabiq funcionó como herramienta de propaganda orientada a proyectar una imagen de comunidad, poder, victimización y legitimidad.

Por tanto, este artículo analiza cómo la propaganda visual contribuye a los procesos de radicalización ideológica hacia el extremismo violento a través de las imágenes publicadas en los quince números de la revista Dabiq del Estado Islámico, editados entre 2014 y 2016 (Fahmy, 2020, pp. 264-265).

En lugar de centrarse en las narrativas textuales, el estudio examina cómo los elementos visuales construyen significados, refuerzan mensajes ideológicos y legitiman la violencia. El principal marco teórico es la teoría del marco (o *framing*) de Robert Entman, que permite analizar cómo las imágenes seleccionan, enfatizan y organizan la realidad para moldear la interpretación de la audiencia.

Desde esta perspectiva, las imágenes publicadas en Dabiq pueden contribuir a la radicalización ideológica al enmarcar visualmente la identidad colectiva, la victimización, el heroísmo y la amenaza existencial, creando así narrativas simbólicas que normalizan la violencia y refuerzan la legitimidad extremista.

2. Marco teórico

Esta investigación emplea la teoría del marco de Robert M. Entman para analizar la propaganda. Entman señala que “el marco implica esencialmente selección y prominencia” (1993, p. 53). El marco consiste en seleccionar ciertos aspectos de una realidad percibida y hacerlos más relevantes en la comunicación. Los marcos pueden desempeñar cuatro funciones principales: definir problemas, diagnosticar causas, emitir juicios morales y sugerir remedios o tratamientos (Entman, 1993, p. 52).

La teoría del marco opera subrayando determinados hechos y otorgándoles mayor relevancia. Esto se logra mediante técnicas como la repetición, la colocación estratégica o la asociación con símbolos familiares, lo que hace que algunos elementos resulten más memorables mientras que otros quedan fuera del campo de atención del receptor. De este modo, el marco influye directamente en la interpretación y el procesamiento de la información (Entman, 1993, pp. 53-54). Posee un gran poder persuasivo, ya que es menos intrusivo que el texto; por esta razón, funciona como una herramienta de propaganda que permite la construcción de narrativas dominantes (Fahmy, 2020, p. 268).

Las imágenes son más eficaces que el texto a la hora de transmitir mensajes, puesto que captan la atención de forma más efectiva, amplifican las emociones y refuerzan las narrativas de manera más visceral y memorable, influyendo así en las actitudes políticas (Baele et al., 2019, pp. 1-3). Además, ayudan a procesar realidades complejas e influyen en lo que se percibe como real (El Damanhoury y Winkler, 2018, p. 4). Este poder persuasivo se fundamenta en la “traición de la fotografía”, mediante la cual las imágenes construyen una representación aparentemente auténtica de la realidad y legitiman la guerra y el conflicto (Anfinson, 2021, p. 722).

La propaganda del EI se apoya en gran medida en el marco visual para atraer y mantener la atención de la audiencia, reforzar sus narrativas y preservar su credibilidad incluso ante las pérdidas de liderazgo (Winkler et al., 2021, pp. 3, 9). Según Ellul, la propaganda resulta más eficaz cuando normaliza su ideología hasta el punto en que los individuos obedecen impulsos externos a sí mismos (1962, citado en Winter, 2020, p. 669). Así, la propaganda del EI se convierte en una estrategia integral de radicalización.

Por otra parte, un estudio sobre los vídeos del EI señala que su propaganda visual se construyó mediante técnicas de “abyección, shock y horror”, mostrando escenas violentas y explícitas para generar adrenalina, erosionar la empatía y normalizar el sufrimiento, impulsando de este modo procesos de radicalización (Venkatesh et al., 2020, pp. 1754, 1768). Otra investigación afirma que estos vídeos buscaban intimidar a los adversarios, reclutar simpatizantes y reforzar la narrativa del grupo, revelando una nueva dimensión del terrorismo digital basada en estrategias psicológicas, retóricas y teológicas (2024:3; Fahmy, 2020:260).

3. Metodología

Para el análisis cualitativo de las imágenes de los 15 números de Dabiq se utilizó el software ATLAS.ti. El análisis se dividió en tres grupos: Dabiq 1-5, Dabiq 6-10 y Dabiq 11-15. Además, se desarrolló una metodología propia para analizar el marco visual, que implicó la creación de códigos específicos.

Los códigos se basaron en cinco temas: utopía, imágenes que retratan el Califato como una sociedad ideal y próspera; gobernanza y Estado, imágenes que proyectan al EI como un Estado legítimo con capacidades militares, control territorial y capacidad de imponer el orden y la coerción; martirio y heroísmo, imágenes en las que niños y combatientes son martirizados, y líderes o combatientes son glorificados como héroes; enemigo, imágenes que exponen o muestran al enemigo como derrotado; y victimización, donde se presentan las consecuencias de las acciones del enemigo.

Aunque el análisis se centró en las imágenes y el marco visual, también se analizaron los textos y los pies de foto para comprenderlos y codificarlos mejor.

El tema de la “Utopía” incluye las siguientes etiquetas: UTOPIAN_CHILDHOOD, que retrata a niños felices en el centro del Califato; COLLECTIVE_IDENTITY, que proyecta una imagen de comunidad y camaradería; y CALIPHATE_UTOPIA, que representa un Califato idealizado con mercados abundantes, una sociedad feliz e incluso médicos.

Bajo “Gobernanza y Estado” se encuentran: CALIPHATE_GOVERNANCE, relacionada con el ejercicio del control, el monopolio de la violencia y la capacidad militar; RELIGIOUS_AUTHORITY y RELIGIOUS_SYMBOLS, vinculadas a la imposición ideológica y el imaginario religioso acompañados de narrativas arraigadas en la religión; STATE_SYMBOLS, como los emblemas del EI, banderas, uniformes e imágenes de las monedas creadas por el EI; y EXPLOITED_CHILDREN, que refleja el uso de menores dentro de las narrativas propagandísticas, por ejemplo, para exponer al enemigo, construir una imagen utópica del Califato y retratar a los niños como el futuro del EI mostrándolos portando armas, vistiendo uniformes y/o siendo entrenados como combatientes.

La categoría de “Martirio y heroísmo” incluye: MARTYRDOM_CHILDREN y MARTYRDOM_ADULTS, que se refieren a imágenes del martirio de civiles; MARTYRDOM_HERO y HEROIC_FIGURE, imágenes destinadas a mostrar a combatientes martirizados con el fin de glorificarlos, retratar una imagen heroica de una figura significativa en la historia del EI, o presentar escenas dramatizadas como hombres a caballo con espadas curvas; y FIGHTER_GLORIFICATION, centrada en la idealización de los combatientes.

El tema del “Enemigo” incluye: DEFEAT_THE_ENEMY, que presenta imágenes del adversario siendo destruido o debilitado; DEHUMANIZATION_OF_THE_ENEMY, en las que el enemigo es representado de manera violenta y despojado de individualidad, ya sea muerto o a punto de ser ejecutado; y EXPOSURE_OF_THE_ENEMY, imágenes que dan un rostro al enemigo para identificarlo o revelar su ubicación.

Por último, bajo “Victimización” se encuentra el código VICTIMIZATION, utilizado para identificar representaciones en las que el EI muestra víctimas o destrucción resultantes de ataques enemigos.

La decisión de crear los códigos en mayúsculas se tomó con el fin de facilitar el proceso de codificación en el software y de hacer más fácil la identificación de los códigos.

4. Dabiq como dispositivo de propaganda visual

A través de Dabiq, el EI amplió el alcance internacional de su propaganda mediante la publicación de contenidos en múltiples idiomas, promoviendo una narrativa orientada a influir en potenciales simpatizantes occidentales y a guiarlos hacia la radicalización, al tiempo que deshumanizaba e identificaba a sus enemigos (Fahmy, 2020, pp. 264-265). Asimismo, Dabiq funciona como un sistema competitivo de significados que moldea percepciones, fomenta la polarización y busca movilizar a sus partidarios (Ingram, 2017, p. 358).

Por otra parte, el contenido gore, caracterizado por la representación de violencia extrema y sufrimiento explícito, fue utilizado por el EI para amplificar su propaganda y explotar la fascinación por lo macabro, el horror y el mal. La exposición prolongada a imágenes grotescas puede producir desensibilización y fomentar comportamientos agresivos. En este sentido, un estudio sobre el contenido visual de Dabiq señaló que su uso del gore difería de la mayoría de las producciones audiovisuales del EI, ya que se dirigía principalmente a “musulmanes anglófonos, especialmente aquellos con inclinaciones wahabíes y salafíes”, con el propósito de persuadirlos para unirse al EI. Por lo tanto, las imágenes brutales se emplearon de manera calculada y estratégica para generar impacto en la audiencia objetivo (Lakomy, 2019, pp. 146, 149, 157, 158).

5. Marco visual de la identidad colectiva y la alteridad

La propaganda contribuye a la construcción binaria de la alteridad, enmarcada como “nosotros frente a ellos”, en la que el EI se presenta a sí mismo como el legítimo defensor del islam, mientras que cualquiera que se oponga a la organización es retratado como malvado, incrédulo y destinado al fracaso (Qi, 2024:54).

Esta narrativa se legitima aún más a través de las experiencias históricas y contemporáneas de las comunidades musulmanas, fomentando una identidad colectiva entre los seguidores del EI y justificando las acciones hostiles de la organización (Qi, 2024, sección Discussion:1).

De hecho, Milton (2020, citado en Qi, 2024:12) analizó la propaganda del EI a través de 1.700 imágenes, observando que la organización seleccionaba deliberadamente visuales que se representaban tanto a sí misma como a sus enemigos, retratando a estos últimos mediante imágenes violentas diseñadas para captar la atención del lector.

La estrategia propagandística del EI también se inserta en el debate más amplio sobre la relación entre el islam y el terrorismo. En este sentido, Qi (2024:4) se refiere al ensayo de Graeme Wood (2015), quien sostiene que la posición del EI sobre lo que presenta como el “verdadero islam” generó un amplio debate entre quienes coinciden con esta interpretación y quienes la rechazan por completo. Esta discusión resulta particularmente relevante porque el EI empleó narrativas religiosas como mecanismo de legitimación ideológica y de construcción de identidad entre sus seguidores.

Según Qi (Makdisi y John, 1985; Mutahhari, 2014, citados en Qi, 2024, sección Discussion:6), el frecuente énfasis en temas como la ley islámica y el yihad violento contribuyó a la justificación teológica del EI, que se convirtió en uno de los fundamentos ideológicos de la organización.

Aunque el mensaje central permaneció consistente, la intensidad con la que se enfatizaban ciertos temas varió, particularmente en lo referente a las narrativas religiosas y a la identificación del enemigo, especialmente en Dabiq, la revista oficial del grupo en lengua inglesa (Colas, 2016a, citado en Qi, 2024, sección Discussion:9).

Sin embargo, con el tiempo la propaganda del EI evolucionó de mensajes amplios y generalizados a contenidos propagandísticos dirigidos a audiencias específicas. En otras palabras, la organización desarrolló una comprensión de su audiencia occidental, lo que permitió que los vídeos en lengua inglesa se convirtieran en una herramienta eficaz de reclutamiento mediante la explotación de frustraciones e inclinaciones ideológicas (Cotte y Cunliffe, 2020, citados en Qi, 2024, sección Literature Review:13).

En efecto, al utilizar vídeos en lengua inglesa que apelaban a la identidad, la religión y la injusticia, el grupo logró alcanzar a una audiencia más amplia y generar un impacto mucho mayor (Qi, 2024, sección Literature Review:11). Esto permitió al EI conectar con individuos que experimentaban

sentimientos de exclusión, crisis de identidad o alienación, reforzando así una identidad colectiva fundamentada en la pertenencia religiosa y política (Coolsaet, 2016; Roy, 2016, citados en Qi, 2024, sección Discussion:22).

En otras palabras, el fundamento religioso del EI facilitó la construcción de una narrativa que proyectaba y legitimaba lo que la organización presentaba como la interpretación “verdadera y correcta” del islam. Al mismo tiempo, esta narrativa se reforzó mediante referencias históricas a conflictos que involucraban a musulmanes. Además, al emplear estrategias discursivas y técnicas propagandísticas diseñadas para evocar sentimientos de resentimiento, injusticia, alteridad e identidad, el EI pudo expandirse regionalmente a través de su discurso radical. Sin embargo, otra técnica que contribuyó al rápido crecimiento de la organización fue el uso de imágenes alusivas a la victimización y a la amenaza existencial.

6. Marco visual de la victimización y la amenaza existencial

Asimismo, el EI utilizó la revista Dabiq como herramienta de propaganda para difundir su estrategia política e ideológica, desafiar a otros grupos yihadistas y amenazar a sus enemigos occidentales (Gambhir, 2014, p. 2). En sus primeras ediciones, la revista reforzó una visión binaria del mundo dividida entre creyentes e incrédulos, proyectando un sentido de amenaza hacia sus adversarios mientras transmitía legitimidad y pertenencia a sus simpatizantes (Gambhir, 2014, p. 4).

Esta dualidad entre imágenes de horror dirigidas a los enemigos y promesas utópicas ofrecidas a los partidarios funcionó como un mecanismo de legitimación de la violencia, que la organización presentaba como un medio necesario para alcanzar un propósito sagrado (Venkatesh et al, 2020)).

Temas como “victimización, crueldad, utopismo, martirio y apocalipsis” también aparecieron de manera prominente (Johnston, 2022; Lakomy, 2020; Price y Mooney, 2022; Winter, 2015, citados en Qi, 2024). Estos elementos buscaban construir una percepción constante de amenaza y conflicto, reforzando narrativas emocionales capaces de justificar la violencia extremista.

Esto puede observarse en ejemplos discursivos en los que, en lugar de referirse a “cristianos”, la revista emplea un lenguaje como “adoradores de la cruz” o “bárbaros” (Rasoulislamaki et al., 2025, sección “Sameness and Negative Diversity”).

Según Rasoulislamaki et al. (2025, p. 379), la revista emplea un marco discursivo en el que los musulmanes son retratados como “víctimas” de la opresión, mientras que el ISIS se presenta a sí mismo como el protector de la comunidad islámica. De este modo, las acciones violentas llevadas a cabo por la organización se interpretan como una respuesta justificada a la victimización sistemática impuesta por los “otros”.

Más allá de la victimización representada en sus imágenes, la organización también buscó generar identificación emocional entre individuos que experimentaban sentimientos de exclusión, alienación o desplazamiento, lo que potencialmente facilitaba los procesos de reclutamiento.

Asimismo, según Cottee (2023, p. 13), la radicalización no necesariamente deriva de diferencias patológicas, sino también de factores como la ira, la alienación, el aislamiento y la búsqueda de comunidad. En este sentido, la propaganda del EI explotó los sentimientos de exclusión y desplazamiento con el fin de atraer a individuos vulnerables al extremismo violento.

De manera similar, Cottee (2023, p. 15) analiza la vulnerabilidad y la impresionabilidad de algunos reclutas occidentales del EI, subrayando el potencial papel de la propaganda dentro de procesos más amplios de radicalización.

En otras palabras, el EI no solo empleó un lenguaje que permitía a los lectores identificar fácilmente quiénes eran los grupos “alienados” y quiénes los “protectores” del islam, sino también narrativas de victimización y amenaza existencial. De este modo, la organización legitimó la violencia al tiempo que generaba un sentido de pertenencia entre individuos susceptibles a los procesos de radicalización.

7. Marco visual del heroísmo y el martirio

Un estudio sobre Dabiq indicó que la identidad del EI se centraba en proyectar confianza y un camino divino, en el que la hijrah (migración) y la yihad (guerra santa o autosacrificio militar) se presentaban como obligaciones del verdadero musulmán y el único camino hacia la salvación y la felicidad eterna. Temas como “Virtudes del martirio”, “Yihad obligatorio” y “Temor de Dios” reforzaban la idea del sacrificio como algo urgente y necesario (Hooker, 2015, pp. 58, 75, 86).

Herbers describe la propaganda del EI como un culto a la muerte que glorifica tanto las muertes de sus enemigos como el martirio de sus propios miembros. A través de imágenes de muerte, el EI transformó a los mártires en herramientas de propaganda y reforzó una narrativa en la que morir bajo la voluntad de Dios adquiriría valor simbólico. La abundancia de imágenes de mártires en Dabiq demuestra la necesidad de la organización de hacerlos visibles y públicamente reconocidos (pp. 34, 38, 41).

En Dabiq, los mártires eran retratados mediante imágenes distanciadas del gore y de las escenas explícitamente violentas. Los cuerpos se mostraban intactos, con las heridas cubiertas y expresiones faciales pacíficas. Algunas imágenes alteradas incluso incluían un resplandor semejante a la aureola de un santo cristiano, simbolizando a los muyahidín considerados shahids por Alá. Así, en lugar de conmocionar al lector, estas imágenes buscaban familiarizar a las audiencias con el martirio, transformarlo en una fuente de inspiración y reforzar la idealización de la figura del mártir (Lakomy, 2019, p. 159).

En cuanto al heroísmo, el EI empleó estrategias de nominación e individualización en Dabiq, destacando a los combatientes a través de sus nombres e historias personales con el fin de generar reconocimiento, cercanía y empatía, como ilustra el caso de un soldado que murió mientras ayudaba a otro combatiente (Rasoulikolamaki et al., 2025, pp. 883-884). Esto contrasta con la representación de sus adversarios como actores colectivos, pasivos e inferiores (Rasoulikolamaki et al., 2025, p. 382; Rasoulikolamaki y Kaur, 2021, p. 656).

Asimismo, Dabiq está repleta de imágenes de guerreros vestidos de negro, portando banderas del EI, montando a caballo y blandiendo espadas, acompañadas de textos que los retratan como valerosos caballeros. Esta estética islámica medieval asocia a los yihadistas con una forma antigua y pura de guerra, evocando coraje y compromiso. El marco visual comunica el heroísmo del martirio y proyecta una imagen poderosa de combatientes valerosos con el fin de atraer a más seguidores (Toguslu, 2019, p. 116).

El EI también tiende a enmarcar la responsabilidad de resolver las crisis como perteneciente a los hombres, promoviendo la idea de que deben movilizarse para proteger a sus hermanas, construyendo así la figura del héroe como un defensor necesario y asociando la movilización con la masculinidad (Ingram, 2023, pp. 345-346). Además, la organización instrumentaliza la imagen de los niños al retratarlos como futuros guerreros mediante representaciones de entrenamiento militar y de soldados que actúan como figuras paternas (Kaczkowski, 2019, pp. 31-32).

De este modo, el EI emplea dispositivos de marco visual y textual para reforzar su imagen de heroísmo. La organización se presenta a sí misma como el grupo interno (in-group) capaz de proporcionar soluciones y como el único defensor de los musulmanes suníes, mientras que el grupo externo (out-group) enemigo se representa como responsable tanto de la crisis como de su continuidad (Ingram, 2023, p. 340; Kaczkowski, 2019, p. 26).

8. Marco visual de la gobernanza y la utopía del Califato

A través del marco visual, el EI retrató el Califato en Dabiq como una sociedad-Estado utópica e ideal en la que el islam se practicaba de manera perfecta. Mediante imágenes de mercados bien abastecidos, comunidades unidas, calles limpias, ayuda a los necesitados y servicios médicos, el grupo construyó la imagen del Califato como un Estado estable, próspero y plenamente religioso. Asimismo, la representación de agricultores y recolectores de zakat reforzaba la idea de una comunidad musulmana devota y solidaria (Baele et al., 2019, p. 11; Toguslu, 2019, p. 109).

El atractivo de la propaganda utópica del Estado Islámico también derivaba del hecho de que ofrecía una alternativa ideológica al statu quo, fundamentada en bases milenarias y asociada a la redención y el empoderamiento (Anfinson, 2021, p. 722). Este marco de la gobernanza fue central para el atractivo global del EI, ya que Dabiq representaba al Estado Islámico como un Estado funcional,

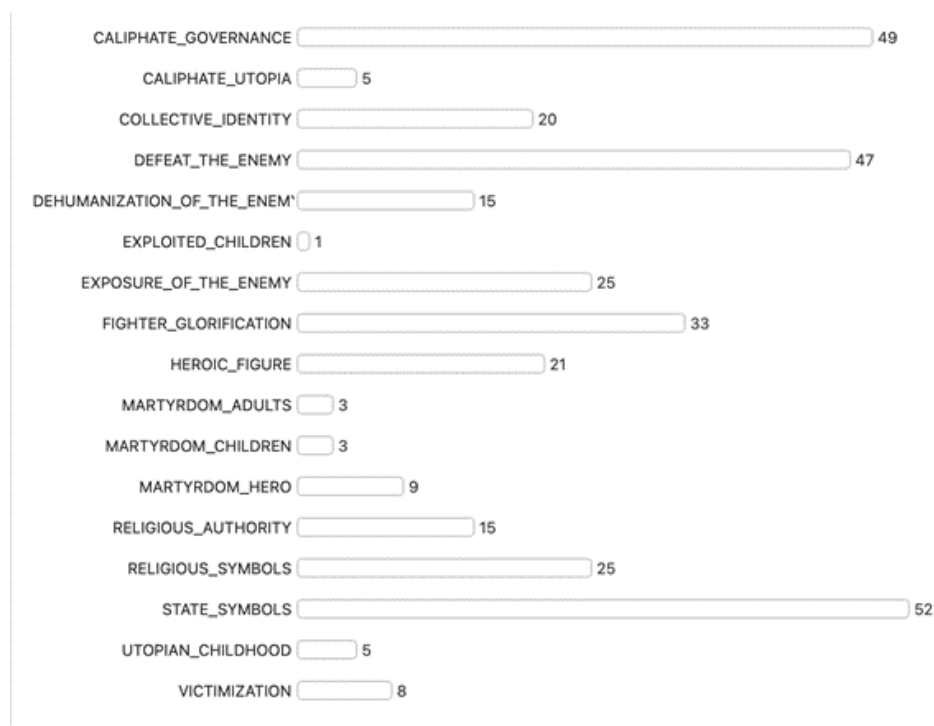
estable y legítimo con instituciones, orden y control sobre la población, aunque en la práctica su gobernanza distaba mucho de ser efectiva (Anfinson, 2021, p. 732).

Las imágenes publicadas en Dabiq se utilizaron para retratar al EI como un Estado legítimo que poseía territorio, población, gobernanza y apoyo internacional. Este marco visual buscaba atraer a reclutas extranjeros y reforzar la idea del Califato como un proyecto soberano y una comunidad musulmana global (Anfinson, 2021, pp. 720, 725-727).

Asimismo, Dabiq funcionó como una estrategia para construir la idea de una sociedad musulmana total, recurriendo a conceptos religiosos y políticos del islam para legitimar al EI y al Califato como una sociedad ideal. Basándose en la idea de que “No hay islam excepto con jama’ah (comunidad), y no hay jama’ah excepto con imarah (liderazgo), y no hay imarah excepto con ta’ah (obediencia)”, el EI argumentaba que el islam solo podía existir plenamente dentro de una comunidad unificada. En consecuencia, se retrataba a los musulmanes como poseedores de la obligación religiosa de unirse al Califato y aceptar su liderazgo (Anfinson, 2021, p. 120; Toguslu, 2019, p. 109).

9. Resultados

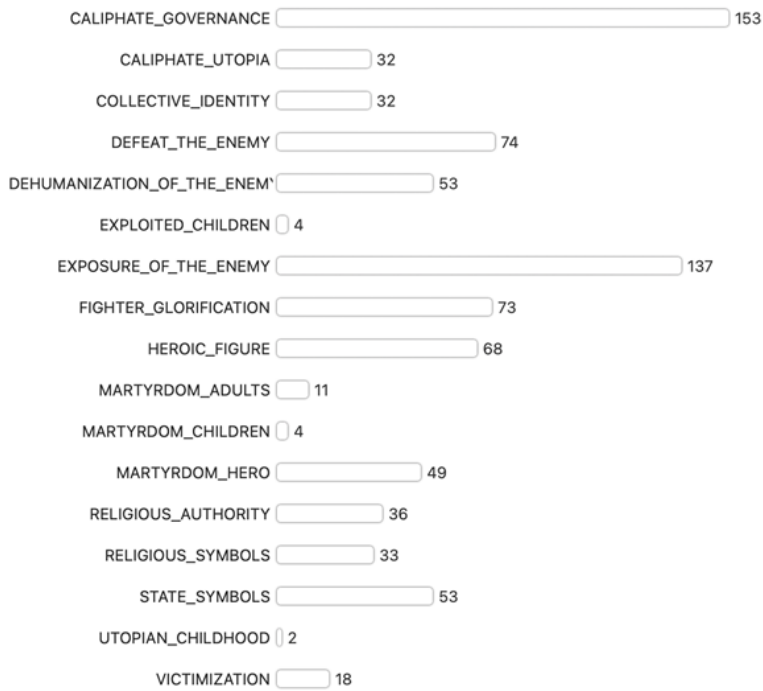
Figura 1. Análisis con Atlas.ti de Dabiq 1-5



Fuente: Elaboración propia

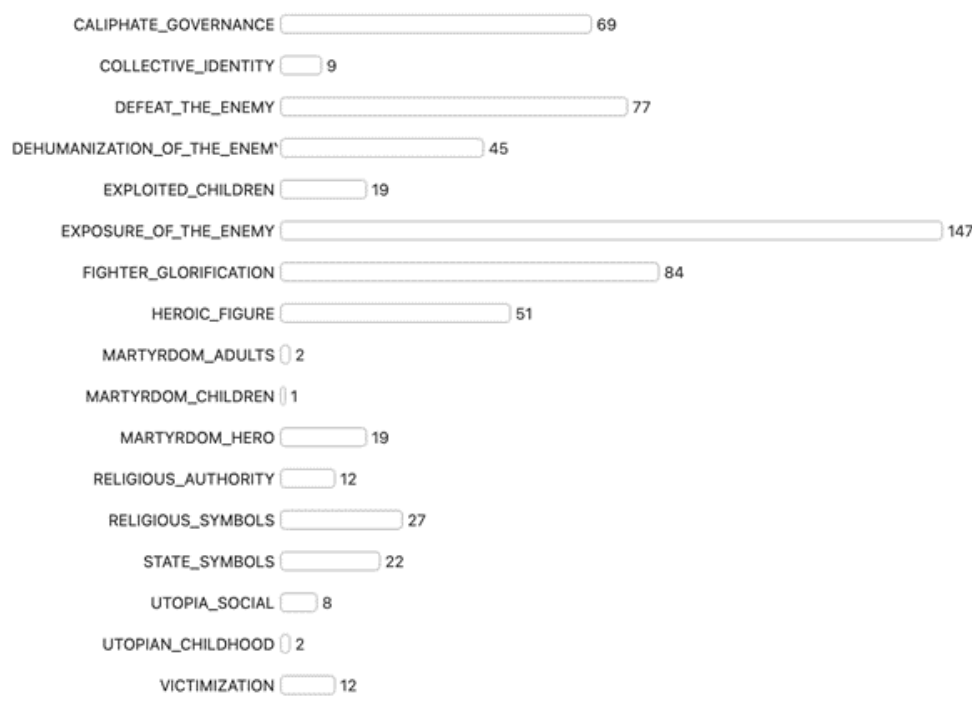
En este grupo, los códigos más predominantes fueron STATE_SYMBOLS, seguidos de CALIPHATE_GOVERNANCE y DEFEAT_THE_ENEMY. En contraste, los códigos menos recurrentes fueron EXPLOITED_CHILDREN, MARTYRDOM_CHILDREN y MARTYRDOM_ADULTS.

Figura 2. Análisis con Atlas.ti de Dabiq 6-10



Fuente: Elaboración propia

A lo largo de los volúmenes 6-10, los códigos más prominentes fueron CALIPHATE_GOVERNANCE, EXPOSURE_OF_THE_ENEMY y DEFEAT_THE_ENEMY. Los códigos menos frecuentes fueron UTOPIAN_CHILDHOOD, MARTYRDOM_CHILDREN y EXPLOITED_CHILDREN.

Figura 3. Análisis con Atlas.ti de Dabiq 11-15

Fuente: Elaboración propia

El código más predominante a lo largo de los volúmenes 11-15 fue EXPOSURE_OF_THE_ENEMY, seguido de FIGHTER_GLORIFICATION y DEFEAT_THE_ENEMY. Los códigos menos predominantes fueron MARTYRDOM_ADULTS, UTOPIAN_CHILDHOOD y MARTYRDOM_CHILDREN.

10. Discusión

En el grupo de Dabiq 1-5, a diferencia de los otros dos grupos, se codificó un gran número de imágenes como STATE_SYMBOLS, con una alta prominencia de banderas que portaban el emblema del EI. Además, se identificaron más imágenes relacionadas con CALIPHATE_GOVERNANCE, que representaban tanques, armas y aviones con el fin de enfatizar la capacidad militar del grupo. Esto sugiere que, durante sus etapas iniciales, el EI buscó proyectar una imagen de legitimidad estatal.

Otra observación a lo largo de los 15 volúmenes de Dabiq es que las armas que se mostraban con mayor frecuencia eran los fusiles AK-47, convirtiendo esta arma en parte de la propaganda del EI y de la identidad estética del muyahidín.

En cuanto a la utopía del Califato, a diferencia de lo argumentado por Toguslu (2019, p. 109), solo se identificó un número muy limitado de imágenes relacionadas con servicios o bienestar, tales como médicos, mercados abundantes, la restauración de la electricidad o la ayuda a los necesitados.

En su lugar, predominaron los paisajes simbólicos y naturales, incluyendo montañas, árboles, águilas y templos, a menudo acompañados de narrativas o versículos del Corán con el fin de construir una visión idealizada del Califato. Asimismo, dentro de la imagen utópica de comunidad, las representaciones de camaradería entre muyahidines fueron más recurrentes que las representaciones de multitudes o de poblaciones comunales más amplias.

Respecto a las imágenes que denotaban autoridad religiosa, se observó una alta prominencia de líderes considerados importantes por el EI, acompañados de textos que los glorificaban. Particularmente en Dabiq 11-15, se produjo un aumento de imágenes que retrataban a miembros del EI destruyendo templos o símbolos religiosos enemigos. Además, estos volúmenes posteriores incluyeron representaciones de líderes de la religión católica; de hecho, la portada del volumen final representa a un hombre destruyendo una cruz.

Un símbolo religioso altamente recurrente fue el Corán, con numerosas imágenes que mostraban a personas leyéndolo, especialmente a muyahidines. Asimismo, en la mayoría de los volúmenes, individuos, líderes, muyahidines e incluso niños se representan levantando el dedo índice, un símbolo que significa “No hay más dios que Alá”, el cual fue apropiado por el EI como parte de su propaganda (Skoler, 2014).

En cuanto a las imágenes de niños instrumentalizados, estas fueron más frecuentes en Dabiq 6-10 y 11-15, donde los niños aparecían portando armas, vistiendo uniformes del EI, sometidos a entrenamiento militar o acompañados de un muyahidín que actuaba como figura parental. Estas imágenes iban acompañadas de textos que presentaban el entrenamiento de los niños y el camino del muyahidín como un deber divino, al tiempo que retrataban a los niños como el futuro del EI y del Califato.

En contraste, en Dabiq 1-5 la instrumentalización de los niños se produjo principalmente a través de imágenes de martirio, que representaban a menores fallecidos con el fin de apelar a las emociones del espectador; este tipo de imagen desapareció en los volúmenes posteriores. Los textos que las acompañaban se referían a ellos como shahid (mártires) y enmarcaban sus muertes como resultado de ataques enemigos. En cuanto al martirio de civiles adultos, las imágenes fueron escasas y representaban cuerpos con expresiones pacíficas y heridas limpias, reduciendo el impacto grotesco.

La mayoría de las imágenes relacionadas con el martirio retrataban a muyahidines muertos en combate o en operaciones suicidas. Aunque algunas incluían sangre, la mayoría consistía en fotografías que los mostraban vivos y sonrientes, acompañadas de textos que glorificaban su sacrificio e idealizaban su destino ante Dios. Estas imágenes funcionaron como una estrategia de individualización al otorgar al mártir un rostro, un nombre y una historia personal con el fin de generar empatía y fomentar el reclutamiento.

Respecto a las figuras heroicas, se identificaron escenas dramatizadas de guerreros medievales a caballo portando espadas curvas, como señaló Toguslu (2019, p. 116). Esta construcción heroica también incluía a líderes prominentes del EI y a mártires idealizados.

En cuanto a la glorificación de los combatientes, las representaciones de muyahidines armados posando o disparando armas fueron extremadamente frecuentes. A lo largo de todos los números, las imágenes de martirio heroico, yihad heroica y glorificación de combatientes estuvieron consistentemente presentes. Tanto las imágenes como los textos que las acompañaban incluían llamados reiterados a la hijrah (migración) y a la yihad (guerra santa o autosacrificio militar), instando a los extranjeros a unirse al EI y a participar en la yihad como muyahidín (Hooker, 2015, pp. 58, 75, 86).

En lo que respecta a las imágenes que retrataban la derrota del enemigo, las escenas más comunes representaban templos o espacios destruidos tras ataques del EI, cadáveres de combatientes o civiles enemigos, e imágenes exhibidas ante poblaciones “subyugadas” en territorios bajo control del EI.

Respecto a la deshumanización del enemigo, muchas imágenes retrataban los cuerpos de combatientes muertos sin rostros visibles, colocados dentro de bolsas o rodeados de grandes cantidades de sangre, acompañados de textos que expresaban ridículo y odio. Por lo general, no se mencionaban sus nombres, despojándolos así de individualidad.

En cuanto a la deshumanización, esta se evidenció de manera particular en la representación de rehenes, principalmente periodistas y figuras públicas, que se mostraban vestidos con ropa de estilo prisionero de color naranja, con la cabeza afeitada, golpeados y retenidos por individuos encapuchados que les sostenían cuchillos en el cuello. Posteriormente, algunas imágenes los retrataban con carteles que rezaban “prisionero en venta” con el fin de exigir pagos de rescate, y más tarde aparecían a punto de ser ejecutados o en proceso de ejecución mediante fusilamientos o decapitaciones.

Se observó que en cada grupo analizado de Dabiq (1-5, 6-10 y 11-15) había al menos una imagen que representaba una decapitación. No obstante, el nivel de violencia visual aumentó progresivamente en cada número, siendo las imágenes posteriores las más gráficas y grotescas.

Respecto a la exposición del enemigo, se identificaron dos categorías principales: occidentales, tales como líderes gubernamentales, periodistas y fuerzas militares, y traidores, representados por líderes de países como Arabia Saudí o miembros de grupos como Al-Qaeda. Aunque pertenecían al islam, eran retratados como apóstatas o traidores. Estas imágenes aumentaron considerablemente con el tiempo, con una fuerte presencia en Dabiq 6-10 y una presencia aún mayor en Dabiq 11-15.

Finalmente, la victimización predominó en Dabiq 1-5, donde se representaban con frecuencia niños, civiles y destrucción atribuida a los enemigos. En los volúmenes posteriores, el EI se centró más en proyectar poder y enfatizar la debilidad de sus enemigos; por lo tanto, Dabiq 11-15 presentó una marcada ausencia de estos elementos.

11. Conclusión

Este estudio examinó la propaganda visual publicada a lo largo de los quince números de Dabiq a través de la teoría del marco (o *framing*) de Robert M. Entman y de un análisis visual cualitativo realizado con ATLAS.ti. Mediante el examen sistemático de los marcos visuales asociados a la utopía, la gobernanza y la estatalidad, el martirio y el heroísmo, la representación del enemigo y la victimización, la investigación ofrece una descripción integral de cómo el EI utilizó el imaginario fotográfico para construir y reforzar sus narrativas ideológicas. Los hallazgos indican que la propaganda visual en Dabiq no debe entenderse meramente como un complemento estético del discurso textual, sino como un componente integral de la estrategia comunicativa más amplia de la organización, a través de la cual se construyeron visualmente la legitimidad política, la identidad colectiva, la fuerza militar, la victimización y la justificación moral de la violencia.

Una de las principales contribuciones de este estudio reside en la identificación de la evolución de estos marcos visuales a lo largo de la publicación de Dabiq. El análisis revela que la revista no mantuvo una estrategia visual estática entre 2014 y 2016. En los números anteriores, las imágenes asociadas a los símbolos estatales, la gobernanza, la victimización y la construcción del Califato como entidad política y territorial fueron particularmente prominentes. Estas representaciones contribuyeron a retratar al EI no solo como una organización armada, sino también como un actor gobernante capaz de ejercer el control territorial, imponer la autoridad y proporcionar los atributos simbólicos asociados a la estatalidad. Sin embargo, a medida que la publicación evolucionó, el énfasis visual se desplazó cada vez más hacia la capacidad militar, la exposición y derrota de los enemigos, y la glorificación de los combatientes. Esta transformación sugiere que la comunicación visual de Dabiq se adaptó a las circunstancias políticas y militares cambiantes a las que se enfrentaba el EI.

Un hallazgo particularmente relevante concierne a la representación del Califato como proyecto utópico. Si bien investigaciones previas han subrayado las imágenes de prosperidad, bienestar social, comunidad, servicios públicos y vida cotidiana como componentes importantes de la propaganda del EI, el presente análisis halló que estas representaciones eran comparativamente limitadas. En su lugar, la construcción visual del Califato se apoyó de manera más acusada en símbolos de autoridad, poder militar, control territorial, legitimidad religiosa e identidad colectiva. En consecuencia, los hallazgos matizan la idea de que Dabiq proyectaba predominantemente una imagen idealizada de la vida cotidiana bajo el Califato. La legitimidad visual del EI parece haberse construido no solo a través de promesas de una sociedad islámica próspera, sino también, y de manera más prominente, a través de demostraciones de capacidad coercitiva, autoridad religiosa, fuerza militar y la capacidad de derrotar a sus adversarios. Esto constituye una de las principales contribuciones empíricas del estudio.

El análisis también revela una importante asimetría en la construcción visual del grupo interno (in-group) y del grupo externo (out-group). Los combatientes, líderes y mártires del EI fueron frecuentemente individualizados mediante fotografías, nombres, historias personales y narrativas de

sacrificio, coraje y compromiso religioso. Tales representaciones proporcionaban a los miembros de la organización identidades reconocibles y los presentaban como figuras heroicas cuyas acciones encarnaban los valores promovidos por el EI. Por el contrario, los enemigos fueron frecuentemente representados a través de procesos de deshumanización, humillación, anonimato y derrota física. Cadáveres, prisioneros, rehenes y adversarios derrotados eran a menudo despojados de individualidad o presentados principalmente como símbolos de la debilidad e inferioridad moral del grupo externo. La individualización y glorificación simultáneas del grupo interno (in-group) y la deshumanización del grupo externo (out-group) emergen, por tanto, como mecanismos visuales complementarios a través de los cuales Dabiq reforzaba una visión binaria del mundo basada en la pertenencia, la exclusión, la superioridad moral y el antagonismo.

Los hallazgos demuestran, además, que la violencia misma se enmarcaba de manera diferente según la identidad de quienes eran representados. Las muertes de los miembros del EI se asociaban generalmente con el martirio, el heroísmo, el sacrificio y la trascendencia religiosa, mientras que la violencia contra los adversarios se vinculaba con mayor frecuencia a la humillación, el castigo, la derrota y la deshumanización. De manera similar, las imágenes de victimización civil fueron particularmente visibles en los números anteriores y se utilizaron para atribuir la responsabilidad del sufrimiento musulmán a los enemigos del EI. En conjunto, estas diferentes representaciones contribuyeron a construir un marco moral en el que la violencia cometida por la organización podía presentarse como legítima, necesaria, defensiva o divinamente sancionada, mientras que la violencia atribuida a sus adversarios reforzaba narrativas de injusticia y amenaza existencial.

Estos hallazgos resultan relevantes para el estudio de la radicalización, aunque la relación debe interpretarse con cautela metodológica. La investigación no demuestra que la exposición a imágenes particulares cause directamente la radicalización individual, ni mide la recepción por parte de la audiencia ni el cambio de comportamiento. Más bien, identifica mecanismos visuales capaces de apoyar narrativas asociadas a los procesos de radicalización. Al reforzar la identidad colectiva, establecer distinciones claras entre el grupo interno y el grupo externo, legitimar la violencia, glorificar a combatientes y mártires, construir narrativas de victimización y deshumanizar a los adversarios, las imágenes analizadas crean un entorno simbólico potencialmente conducente a la aceptación de interpretaciones extremistas y de la acción violenta. En este sentido, la contribución del estudio no consiste en establecer una relación causal entre las imágenes y la radicalización, sino en identificar y analizar sistemáticamente los marcos visuales a través de los cuales la propaganda extremista puede contribuir a procesos más amplios de socialización ideológica, legitimación de la violencia y movilización.

De manera más amplia, el estudio contribuye a la literatura sobre propaganda extremista al demostrar el valor analítico de examinar el contenido visual de forma longitudinal, en lugar de tratar la propaganda de una organización como un cuerpo homogéneo de material. La comparación de los tres períodos de publicación, Dabiq 1-5, 6-10 y 11-15, muestra que el marco visual cambió junto

con las circunstancias estratégicas del EI. Esto sugiere que la propaganda visual extremista puede funcionar como un sistema de comunicación adaptativo en el que las imágenes se seleccionan y enfatizan de acuerdo con las prioridades organizacionales, las condiciones militares y las narrativas políticas cambiantes. La propaganda visual debe, por tanto, analizarse no solo en términos de lo que representa, sino también en términos de cómo esas representaciones evolucionan a lo largo del tiempo.

El estudio tiene, no obstante, limitaciones. Como análisis cualitativo del contenido producido por el EI, examina los mensajes contruidos por la organización más que su recepción por parte de las audiencias. En consecuencia, no puede realizarse ninguna inferencia causal directa respecto al efecto de imágenes individuales sobre la radicalización, el reclutamiento o la movilización. Investigaciones futuras podrían abordar esta limitación combinando el análisis de contenido visual con estudios de audiencia, entrevistas, enfoques experimentales o análisis de individuos que consumieron propaganda extremista. La investigación comparativa que involucre otras publicaciones del EI, como Rumiya, o propaganda producida por otras organizaciones yihadistas también podría determinar si los patrones visuales identificados en Dabiq representan características distintivas de la comunicación del EI o rasgos más amplios de la propaganda yihadista contemporánea.

En última instancia, el análisis demuestra que la dimensión visual de Dabiq no era secundaria a su mensaje ideológico. Las imágenes constituyeron un mecanismo central a través del cual el EI se representó a sí mismo, su proyecto político, sus combatientes, sus víctimas y sus enemigos. La principal contribución de este artículo es, por tanto, mostrar que la propaganda visual del EI combinó marcos diferentes y en evolución de legitimidad estatal, poder militar, heroísmo, victimización, identidad colectiva y deshumanización del enemigo, adaptando al mismo tiempo su prominencia relativa a las circunstancias estratégicas cambiantes de la organización. Al identificar estos patrones a lo largo del cuerpo completo de Dabiq, el estudio proporciona una comprensión más matizada de cómo las organizaciones extremistas utilizan la comunicación visual para construir legitimidad, normalizar la violencia y crear narrativas simbólicas potencialmente conducentes a la radicalización ideológica.

12. Referencias

- Anfinson, A. (2021). The treachery of images: Visualizing “statehood” as a tactic for the legitimization of non-state actors. *Terrorism and Political Violence*, 33(4), 720–742.
- Baele, S. J., Boyd, K. A., y Coan, T. G. (2019). Lethal images: Analyzing extremist visual propaganda from ISIS and beyond. *Journal of Global Security Studies*, 4(4), 514–537.
- Bunzel, C. (2015). *From paper state to caliphate: The ideology of the Islamic State* (Analysis Paper No. 19). The Brookings Project on U.S. Relations with the Islamic World.

- Cottee, S. (2023). *Radicalisation discourse: Consensus points, evidence base and blind spots*. Commission for Countering Extremism.
- El Damanhoury, K., y Winkler, C. (2018). Picturing law and order: A visual framing analysis of ISIS's Dabiq magazine. *Arab Media & Society*, (25), 1–30.
- Entman, R. M. (1993). Framing: Toward clarification of a fractured paradigm. *Journal of Communication*, 43(4), 51–58.
- Fahmy, S. S. (2020). *The age of terrorism media: The visual narratives of the Islamic State Group's Dabiq magazine*. ResearchGate.
- Gambhir, H. K. (2014). *Dabiq: The strategic messaging of the Islamic State*. Institute for the Study of War.
- Herbers, L. J. (2016). *Media wars: The caliphate strikes back. Islamic State's propaganda magazine Dabiq as a possible paradigm shift in visual war reporting and propaganda* (Master's thesis, Lund University). LUP Student Papers.
- Hoffman, A., y Zeidel, R. (2021). ISIS in its own words: The history, strategy and ideology of the Islamic State [Book review]. *Strategic Assessment*, 24(1).
- Hooker, D. (2015). *Leadership in the reborn caliphate: Thematic network analysis of ISIL's e-zine Dābiq* (Master's thesis, Macquarie University). Macquarie University ResearchOnline.
- Ingram, H. J. (2017). An analysis of Inspire and Dabiq: Lessons from AQAP and Islamic State's propaganda war. *Studies in Conflict & Terrorism*, 40(5), 357–375.
- Ingram, K. M. (2023). An analysis of Islamic State's gendered propaganda targeted towards women: From territorial control to insurgency. *Terrorism and Political Violence*, 35(2), 338–354.
- Kaczkowski, W. (2019). Qualitative content analysis of images of children in Islamic State's Dabiq and Rumiya magazines. *Contemporary Voices: St Andrews Journal of International Relations*.
- Lakomy, M. (2019). Danse macabre: Gore images in the Islamic State's "Dabiq" magazine as a propaganda device. *The International Journal of Intelligence, Security, and Public Affairs*, 21(2), 143–161.
- Qi, Y. (2024). Propaganda in focus: decoding the media strategy of ISIS. *Humanities and Social Sciences Communications*, 11.
- Rasoulkolamaki, S., y Kaur, S. (2021). How ISIS represented enemies as ineffectual in Dabiq: A multimodal critical discourse analysis. *Discourse & Communication*, 15(6), 650–671.

Rasoulkolamaki, S., Kaur, S., Zhdanava, A., y Mat Isa, N. A. N. (2025). In-group and out-group identity construction in extremist discourse: A critical multimodal approach. *Behavioral Sciences of Terrorism and Political Aggression*, 17(4), 377–395.

Skoler, M. (2014, 4 septiembre). ISIS has a new hand sign — and it means far more than ‘We’re #1’. *The World from PRX*.

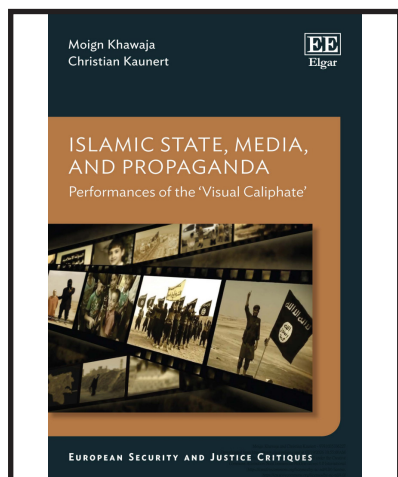
Toguslu, E. (2019). Caliphate, hijrah and martyrdom as performative narrative in ISIS Dabiq magazine. *Politics, Religion & Ideology*, 20(1), 94–120.

Venkatesh, V., Podoshen, J. S., Wallin, J., Rabah, J., y Glass, D. (2020). Promoting extreme violence: Visual and narrative analysis of select ultraviolent terror propaganda videos produced by the Islamic State of Iraq and Syria (ISIS) in 2015 and 2016. *Terrorism and Political Violence*, 32(8), 1753–1775.

Winkler, C., El-Damanny, K., Saleh, Z., Hendry, J., y El-Karhili, N. (2021). Intersections of ISIS media leader loss and media campaign strategy: A visual framing analysis. *Media, War & Conflict*, 14(4), 401–418.

Winter, C. (2020). Framing war: Visual propaganda, the Islamic State, and the battle for east Mosul. *Cambridge Review of International Affairs*, 33(5), 667–689.

Nota sobre inteligencia artificial (IA): Este documento se elaboró con la asistencia de herramientas de inteligencia artificial (IA), particularmente en aspectos relacionados con la estructura del documento y la revisión de algunas citas y referencias. Todas las sugerencias y textos generados con asistencia de IA fueron revisados y editados por los autores para garantizar la exactitud, la claridad, el tono académico apropiado y la coherencia con el análisis propio de los autores. El contenido final refleja las ideas y argumentos de los autores.



Islamic State, Media, and Propaganda: Performances of the 'Visual Caliphate'

Aarón Ferrando-Mkarbel

AUTORES: Moign Khawaja y Christian Kaunert

AÑO: 2025

EDITORIAL: Edward Elgar Publishing

Islamic State, Media, and Propaganda: Performances of the 'Visual Caliphate', de Moign Khawaja y Christian Kaunert, es un libro valioso para los estudios sobre terrorismo porque desplaza la mirada desde la violencia espectacular del Estado Islámico hacia un problema más preciso: cómo una organización terrorista intentó ser percibida como un Estado mediante una política sistemática de imágenes. Esta es su principal virtud. En lugar de volver sobre la discusión acerca de cuánto había de 'islámico' en la organización, la obra interroga su pretensión de 'Estado' a partir de una muestra amplia, cuidadosamente definida y analizada con solvencia metodológica.

Los autores parten de una intuición simple, pero muy productiva: si el autodenominado Estado Islámico quiso que sus sujetos y simpatizantes reconocieran su pretensión de Estado y respaldaran un proyecto político con vocación de permanencia, tuvo que emitir evidencias visibles de esa estatalidad. De ahí la noción de «*Visual Caliphate*» [califato visual], entendida como un régimen propagandístico que no solo proclama autoridad, sino que la exhibe, la escenifica y la dota de apariencia documental. El libro se pregunta, en consecuencia, cómo la organización proyectó una «*modern stateness*» [estatalidad moderna] en sus vídeos oficiales y con qué fines lo hizo. La respuesta se articula mediante un análisis visual longitudinal de 374 vídeos oficiales publicados entre julio de 2014 y julio de 2017, extraídos tras un cribado riguroso de unas 700 piezas localizadas en redes sociales y repositorios digitales (pp. 12-13).

Aarón Ferrando-Mkarbel. Investigador predoctoral en el Departamento de Ciencias de la Comunicación de la Universitat Jaume I (Castellón).

El diseño metodológico es uno de los grandes aciertos del texto. La investigación no se limita a las producciones más célebres ni a los vídeos de extrema violencia que más circularon en prensa y redes sociales, sino que analiza materiales que abordan temas como la población, el territorio, la gobernanza y las relaciones exteriores. La decisión es importante porque reconstruye la propaganda del Estado Islámico no solo como una mera exhibición de terror, sino como una tecnología de legitimación. En otras palabras, Khawaja y Kaunert muestran que la organización no buscaba únicamente intimidar; también trató de persuadir a sus públicos proyectando la apariencia de un orden político en funcionamiento.

La estructura del libro responde con claridad a este objetivo. Tras un prólogo de fuerte carga interpretativa, el segundo capítulo sitúa la transición histórica del «*paper state*» [Estado de papel] al califato territorial; el tercero desarrolla la categoría de «*modern stateness*» a partir de la Convención de Montevideo; y los cuatro capítulos siguientes analizan, respectivamente, estas «*performances*» [actuaciones] ligadas a la población, el territorio, la gobernanza y las relaciones exteriores (pp. 37-38). El capítulo final sintetiza los hallazgos y ofrece una lectura global del proyecto audiovisual del Estado Islámico como una combinación de teatralidad, cálculo propagandístico y administración de la visibilidad.

La escena de Abu Bakr al-Baghdadi en la mezquita Al Nuri de Mosul, en julio de 2014, se interpreta no como un simple documento histórico, sino como una puesta en escena cuidadosamente construida. Los autores describen la pieza como un vídeo «*full of anomalies and theatrics*» [lleno de anomalías y teatralidad] y convierten esa dimensión escénica en el punto de partida del análisis. No se trata de determinar si el Estado Islámico fue o no un Estado en sentido pleno, sino de examinar cómo quiso parecerlo, qué atributos proyectó y qué tipo de reconocimiento buscó obtener de sus sujetos, de sus simpatizantes y de sus enemigos.

Los capítulos empíricos son, en conjunto, lo más sólido del libro. El dedicado a la población muestra cómo la propaganda escenifica una vida cotidiana aparentemente normalizada y ordenada bajo las normas del califato. El ejemplo de *A Visit to Mosul* resulta especialmente ilustrativo. El vídeo combina el testimonio favorable de un vecino con el recorrido de un combatiente extranjero por distintos enclaves de Mosul. Las referencias a la conquista se alternan con imágenes de actividad comercial, circulación urbana, niños jugando en un parque y tribunales de la sharía, hasta culminar en la promesa de una justicia basada en la palabra de Dios (p. 70). Aquí, la operación propagandística no consiste solo en informar, sino en producir una experiencia de recorrido. La ciudad se presenta como un espacio gobernado, inteligible y administrado. Esta lectura ayuda a entender por qué el contenido producido por el Estado Islámico no puede reducirse a una mera estética de la crueldad, pues una parte sustancial de su eficacia dependía de mostrar una aparente normalidad.

El capítulo dedicado a la territorialidad es igualmente convincente. La obra identifica una estrategia de autenticación en tres fases: localizar objetivos mediante mapas, drones y otros recursos técnicos; atacarlos y ocuparlos; y, por último, exhibir el control sobre la población y las infraestructuras (pp. 114-116). El análisis resulta persuasivo porque muestra que la tecnología desempeña una doble función. Sirve para operar militarmente, pero también para persuadir. En este contexto, el dron y el mapa operan como marcas de racionalidad técnica, como signos destinados a presentar el proyecto estatal no como una mera consigna, sino como una maquinaria supuestamente capaz de planificar, conquistar y gobernar.

Por su parte, el capítulo sobre la gobernanza añade un matiz decisivo. Aquí el Estado Islámico aparece atrapado entre dos necesidades: presentarse como un proveedor del orden y seguir explotando el terror como una de sus señas de identidad. Khawaja y Kaunert muestran cómo ciertas piezas adoptan convenciones propias de los formatos televisivos de investigación criminal y del documental procedimental para envolver la violencia en una gramática visual de prueba, confesión y castigo (p. 151). El apartado sobre las relaciones exteriores completa esa lógica. Las ejecuciones de rehenes occidentales son vistas como una forma de ‘política exterior’ informal y como unos mensajes dirigidos tanto al adversario como a la opinión pública internacional. La propaganda, por tanto, no funciona como un simple escaparate, sino como un instrumento para administrar estratégicamente qué facetas de la organización se hacen visibles y cuáles permanecen ocultas (pp. 171-173; 220).

A partir de ahí, la contribución distintiva del libro reside en sistematizar esa intuición mediante una muestra longitudinal y en vincular las imágenes de gobierno con una estrategia más amplia de proyección de esa supuesta capacidad de Estado. Esta constatación es novedosa a la par que reveladora para los estudios sobre terrorismo, pues obliga a pensar la propaganda no solo como instrumento de radicalización o reclutamiento, sino también como una forma de administración simbólica del poder. El libro es preciso, además, al insistir en que estas puestas en escena no deben tomarse al pie de la letra, pues están cuidadosamente guionizadas, editadas y presentadas para proyectar una imagen favorable del califato en un contexto de baja capacidad de Estado real y fuerte escrutinio público.

Sin embargo, el volumen presenta dos límites que conviene señalar. El primero deriva de su propio enfoque. La recepción se infiere a partir de la puesta en escena, pero no se triangula con datos de consumo o de interpretación efectiva por parte de las audiencias. Esta observación no invalida los hallazgos, pero sí delimita su alcance, pues el libro explica cómo se diseña al espectador, no cómo ha respondido realmente cada público a esas piezas. El segundo límite es temporal. La delimitación 2014-2017 es plenamente coherente con el objeto ‘califato’, pero deja fuera las transformaciones más recientes en la circulación y difusión de propaganda, especialmente las relativas a la automatización y la algoritmización.

La comparación con tres obras recientes ayuda a precisar mejor su contribución. *Frente a ISIS' Propaganda Machine*, de Ahmed Al-Rawi, que cartografía un ecosistema mucho más amplio de canales y formatos, Khawaja y Kaunert renuncian a la amplitud para ganar profundidad explicativa. Frente a *The Film of the Islamic State*, una obra referencia de Yorck Beese, comparten la atención al lenguaje audiovisual, pero no el mismo diagnóstico. Donde Beese subraya la cineficación del yihadismo mediático, Khawaja y Kaunert inscriben la estética en una estrategia política de legitimación política. Y, contrastándola con *Radicalization at High Speed*, de Katarzyna Maniszewska, el libro puede leerse como un antecedente de los repertorios de autenticación y administración afectiva que hoy circulan en un entorno de mayor automatización tecnológica.

En pocas palabras, *Islamic State, Media, and Propaganda* es un libro serio, bien construido y útil. Su principal mérito reside en tratar al Estado Islámico con la distancia analítica suficiente para comprenderlo como un actor que persigue el reconocimiento mediante distintas pruebas audiovisuales. Gracias a ello, la obra obliga a pensar el terrorismo no solo como una forma de violencia, sino también como una disputa por el régimen de verosimilitud: qué se acepta como una evidencia, qué se percibe como orden y qué se interpreta como una muestra autoridad. Se trata de una contribución relevante, y no porque ponga fin al debate sobre la legitimidad del terrorismo, sino porque ofrece una matriz de análisis robusta y replicable para seguir estudiando cómo las organizaciones violentas construyen y diseminan su legitimidad a través de las pantallas.

PIRA

PROVISIONAL IRISH REPUBLICAN ARMY (OGLAIGH NA HÉIREANN)

**TIPO DE ORGANIZACIÓN:****No estatal, terrorista****IDEOLOGÍA:****Nacionalista irlandés, republicana****FUNDADORES:****Seán Mac Stíofáin, Ruairi Ó Brádaigh,
Joe Cahill****PRINCIPALES LÍDERES:****Seán Mac Stíofáin, Seamus Twoney,
Martin McGuinness, Kevin McKenna,
Thomas "Slab" Murphy****LUGARES DE ACTUACIÓN:****Irlanda del Norte, República de Irlanda,
Gran Bretaña****AÑOS DE ACTIVIDAD:****1969-2005****ALIANZAS Y SIMPATIZANTES:****ETA, OLP, régimen de Gadafi, NORAI****Nº ESTIMADO DE MIEMBROS:****8.000-10.000 a lo largo de su historia**

El IRA Provisional (Provisional Irish Republican Army), que se autodenominaba Óglaigh na hÉireann, nació en diciembre de 1969 como escisión del IRA histórico. El cisma se produjo en una convención del Ejército Republicano Irlandés celebrada en el condado de Roscommon: un sector acusó a la dirección oficial de haber abandonado la lucha armada a favor de una estrategia política. Seán Mac Stíofáin fue el primer jefe de Estado Mayor de la nueva organización. Su objetivo declarado era forzar la retirada británica de Irlanda del Norte y la reunificación de la isla.

Durante los años setenta el grupo pasó de una estructura de batallones relativamente abierta a un modelo celular de Unidades de Servicio Activo, más difícil de penetrar por los servicios de seguridad. En paralelo, Sinn Féin funcionó como su expresión política; figuras como Gerry Adams y Martin McGuinness encarnaron el tránsito de la campaña armada a la negociación.

El IRA Provisional fue la organización más letal del conflicto norirlandés: se le atribuyen 1.768 de las algo más de 3.500 muertes de The Troubles, entre ellas más de 450 soldados británicos y cientos de civiles. Entre sus acciones más conocidas figuran el Bloody Friday de Belfast (1972), el asesinato de Lord Mountbatten (1979), el atentado contra el hotel Grand Brighton durante el congreso del Partido Conservador (1984) y la bomba de Enniskillen (1987). El grupo decretó alto el fuego en 1994 y de nuevo en 1997, encajó el Acuerdo de Viernes Santo de 1998 y anunció el final de la campaña armada el 28 de julio de 2005. El 26 de septiembre de ese año la Comisión Independiente de Desarme certificó la puesta fuera de uso de su arsenal.

El atentado de Marrakech, 24 de agosto de 1994

Antecedentes históricos y contextuales

Para una comprensión adecuada de los atentados de Marruecos de 1994, es necesario contextualizarlos dentro de la evolución del extremismo islamista en el Magreb, una región marcada por la descolonización incompleta, las rivalidades de liderazgo entre Rabat y Argel, y la irrupción de una yihad armada que, desde Argelia, comenzó a desbordar fronteras. Marruecos, monarquía alauí de tradición autoritaria bajo Hassan II, se presentaba entonces como un polo de estabilidad relativa frente a la conflagración argelina: un Estado que controlaba el islam oficial a través del Ministerio de Habous y de una red de ulemas leales, que había atravesado los llamados “años de plomo” y que basaba una parte sustancial de su imagen internacional y de sus divisas en el turismo europeo. Esa imagen de enclave seguro fue precisamente el objetivo simbólico que el comando de 1994 buscó perforar.

El precursor inmediato no fue un movimiento endógeno marroquí de gran envergadura, sino la guerra civil argelina. Tras la independencia de 1962, Argelia se consolidó como Estado socialista de partido único bajo el Frente de Liberación Nacional. A finales de la década de 1980, el deterioro económico, el desempleo juvenil y la corrupción abrieron paso al islamismo político. En diciembre de 1991, el Frente Islámico de Salvación (FIS) estaba a punto de ganar las elecciones legislativas. El ejército anuló el proceso, disolvió el partido e inició una represión brutal. Lo que siguió fue la “Década Negra”: una guerra civil entre las fuerzas de seguridad y grupos armados islamistas, especialmente el Grupo Islámico Armado (GIA), que se cobró entre 150.000 y 200.000 vidas. Masacres de civiles, asesinatos de intelectuales, periodistas y extranjeros, y una espiral de violencia extrema marcaron aquellos años y generaron una diáspora militante que encontró en Europa (sobre todo en Francia) retaguardia, reclutamiento y financiación.

De esta matriz surgieron redes de apoyo en las banlieues francesas. Las cités de Seine-Saint-Denis (en particular la cité des 4000 de La Courneuve) y la periferia de Lyon se convirtieron en espacios de radicalización. Jóvenes de origen argelino y marroquí, muchos de ellos con antecedentes

de delincuencia menor, se acercaron a mezquitas salafistas y a predicadores que presentaban la yihad argelina como un deber religioso. Algunos viajaron a campos de entrenamiento en Afganistán o participaron en la guerra de Bosnia. Desde esas redes se organizó el comando que actuó en Marruecos. Detrás de los ejecutores de calle operaban figuras como Abdelilah Ziyad (conocido como Rachid) y Mohamed Zinedine (Saïd), vinculados al Movimiento de la Juventud Islámica Marroquí y a contactos con el GIA.

El contexto geopolítico inmediato fue igualmente decisivo. Rabat y Argel mantenían una rivalidad profunda centrada en el Sáhara Occidental, ocupado por Marruecos tras la Marcha Verde de 1975, y en el liderazgo del Magreb. En 1993, Hassan II había entregado a las autoridades argelinas a Abdelhaq Layada, uno de los fundadores del GIA, un gesto que, según versiones posteriores, no fue bien recibido por ciertos sectores de los servicios de inteligencia argelinos (DRS). Algunos analistas y testimonios posteriores han sostenido que elementos de esos servicios pudieron haber facilitado o tolerado acciones destinadas a desestabilizar a Marruecos, aunque esta tesis nunca fue probada de forma concluyente en un tribunal. Marrakech fue seleccionado como objetivo por su simbolismo: un paraíso turístico que representaba, a ojos de los militantes, la apertura del régimen “apóstata” hacia Occidente y la presencia de extranjeros “infieles” en suelo musulmán, maximizando el impacto psicológico, económico y diplomático.

El asalto al Atlas Asni no fue un hecho aislado, sino la culminación visible de una escalada que había comenzado en 1993. El 2 de septiembre de aquel año se produjo el asalto al primer restaurante McDonald's abierto en África, situado en Casablanca, que se saldó con tres muertos y once heridos. Poco después, un ataque a una entidad bancaria en Oujda, cerca de la frontera argelina, dejó varios agentes de seguridad muertos y un cuantioso botín. Estos hechos se atribuyeron inicialmente a la delincuencia común, pero las confesiones posteriores de los detenidos de 1994 obligaron a reinterpretarlos como los primeros pasos de una campaña yihadista destinada a golpear la estabilidad del reino y su industria turística.

Planificación y preparación de los atentados

La planificación de los atentados se inició varios meses antes, revelando una operación coordinada desde Francia, orquestada por una red franco-magrebí inspirada por la yihad argelina y conectada con el GIA. Los preparativos involucraron a un grupo de jóvenes reclutados en las banlieues. Entre ellos se encontraban Stéphane Aït Idir, franco-argelino de 22 años originario de La Courneuve; Redouane Hammadi, franco-marroquí de 24 años, también de la misma cité; Tarek Felah; Kamal Benachka; Abdesslam Guerrouaz; Hamel Marzoug y otros. Según las propias confesiones de Aït Idir ante el juez instructor de Fez, había viajado a Marruecos “para participar en la guerra santa” y se le había prometido “una de las mejores plazas en el paraíso”.

El entrenamiento incluyó el manejo de armas automáticas Uzi, Kalashnikov y escopetas de combate, tácticas de asalto rápido y un adoctrinamiento ideológico que presentaba al régimen de Hassan II como ilegítimo y a los turistas europeos como parte de una presencia occidental a expulsar. La logística contemplaba el paso de armas a través de la frontera oriental y el uso de vehículos robados o alquilados. El objetivo principal era el turismo, principal fuente de divisas del reino, y en particular Marrakech, ciudad símbolo de la prosperidad y de la apertura al mundo occidental. El hotel Atlas Asni, situado en el barrio de Guéliz, fue elegido con cuidado: era un establecimiento de categoría que alojaba habitualmente a turistas europeos, especialmente españoles y franceses. Los atacantes conocían el edificio: entraron por un pasillo de servicio poco visible y eligieron la hora en que se contabilizaba la caja del día anterior. La intención no era solo el robo, ya que se llevaron una cantidad modesta, en torno a 10.000 dirhams, sino generar terror, maximizar el impacto mediático y enviar un mensaje político claro al palacio.

Esta fase preparatoria ilustra la naturaleza híbrida del comando: no se trataba de una organización jerárquica de alcance regional, sino de una célula pequeña, transnacional y relativamente amateur, alimentada por predicadores, redes de barrio y la contigüidad geográfica con la guerra argelina. La operación involucró a al menos una quincena de individuos, con roles divididos entre reclutamiento e ideología (Ziyad y Zinedine), logística (paso de armas y alojamiento), ejecución (el trío que irrumpió en el Atlas Asni) y acciones de acompañamiento en otras ciudades. Sin embargo, errores como el uso de vehículos robados abandonados a poca distancia, la concentración de un arsenal en domicilios de familiares y la facilidad con que varios integrantes fueron localizados en Fez, Taourirt y Aknoul revelaron un nivel organizativo limitado, aunque no impidieron la letalidad puntual del asalto principal.

Desarrollo de los ataques

El 24 de agosto de 1994, un miércoles de verano en plena temporada turística, Marrakech bullía de actividad con miles de visitantes europeos recorriendo la medina, la plaza de Jemaa el-Fna y los hoteles del ensanche de Guéliz. La secuencia de eventos se concentró hacia las 10:30 de la mañana, en un momento calculado para coincidir con las operaciones de caja del hotel y con la presencia de un grupo reducido de turistas en el vestíbulo.

Tres hombres encapuchados, Stéphane Aït Idir, Redouane Hammadi y Tarek Felah, irrumpieron en el vestíbulo del hotel Atlas Asni por un pasillo de servicio. Abrieron fuego indiscriminado, se dirigieron a la caja y se llevaron alrededor de 10.000 dirhams. Dispararon contra el pequeño grupo de turistas presentes. Murieron Antonia Cuevas, de 35 años, y Salvador Torras Turrel, de 43 años, ambos españoles. Una ciudadana francesa resultó gravemente herida. El director del hotel afirmaría más tarde que los atacantes conocían perfectamente el edificio y el horario de las operaciones de caja. Los asaltantes huyeron en un vehículo robado que abandonaron poco después.



Figura 1: El hotel Atlas Asni de Marrakech, escenario del principal atentado del verano de 1994.

No fue un hecho aislado. En los días siguientes se produjeron otras acciones del mismo entorno. El 25 de agosto, un grupo abrió fuego contra policías en Fez sin causar heridos. Se registraron tiroteos y amenazas en Casablanca, incluido un ataque al muro del cementerio judío. Las autoridades marroquíes vincularon estos hechos con los asaltos de 1993 al McDonald's y a la entidad bancaria de Oujda. El patrón era claro: grupos pequeños, altamente motivados, que combinaban el atraco con la voluntad de causar bajas civiles y de desestabilizar el clima de seguridad del país. Tarek Felah logró escapar hacia Europa. Los demás fueron detenidos en los días siguientes en Fez, Taourirt y Aknoul. En el domicilio de familiares de uno de los detenidos se descubrió un arsenal compuesto por fusiles, granadas, munición y radios portátiles. Las confesiones de los capturados revelaron la existencia de una red más amplia y la intención de continuar con ataques similares en otras ciudades turísticas.

El caos inmediato en el Atlas Asni fue breve pero intenso, como describieron testigos oculares: disparos en un vestíbulo cerrado, turistas tirados en el suelo, una recepcionista amenazada con el arma en la sien, y la huida precipitada de los asaltantes hacia un vehículo que no tardaron en abandonar. El daño material al edificio fue limitado, pero el daño humano y simbólico, en cambio, fue inmediato. La elección del objetivo y de la hora fue estratégica: un hotel de categoría en la ciudad más emblemática del turismo marroquí, con víctimas europeas garantizadas, maximizando la repercusión en la prensa española y francesa y obligando al régimen a reconocer que la yihad argelina había cruzado la frontera.

Víctimas, consecuencias inmediatas y respuesta humanitaria

El balance final de la campaña de 1994 confirmó dos personas asesinadas de nacionalidad española en el Atlas Asni y varios heridos, entre ellos una ciudadana francesa, ciudadanos marroquíes y agentes de seguridad.

La respuesta de las fuerzas de seguridad, dirigidas por el poderoso ministro del Interior Driss Basri, fue rápida y contundente. En las horas y días posteriores al asalto se detuvo a la mayor parte del comando. Se produjeron amenazas de bomba en la estación central de Rabat y en el Palacio de Congresos de Marrakech, que resultaron falsas, pero generaron pánico y demostraron la capacidad de los grupos para crear alarma. El gobierno de Hassan II acusó oficialmente a los servicios de inteligencia argelinos de estar detrás de la operación, una acusación que Argel rechazó con virulencia. El 27 de agosto de 1994 Marruecos cerró unilateralmente la frontera terrestre con Argelia, una medida que se mantiene hasta el día de hoy y que simbolizó la ruptura total entre los dos países.

Económicamente, el turismo de Marrakech sufrió un golpe inmediato: cancelaciones masivas de reservas y una percepción de inseguridad que el régimen se apresuró a combatir mediante una intensa campaña de comunicación y un refuerzo visible de la presencia policial. El coste material fue limitado en comparación con atentados posteriores como los de Casablanca 2003 o Marrakech 2011, pero el daño simbólico fue enorme. Marruecos, que se presentaba como un destino estable y seguro frente a la violencia argelina, se vio forzado a reconocer la permeabilidad de sus fronteras y la existencia de células yihadistas con conexiones externas. El cierre de la frontera con Argelia tuvo consecuencias económicas y humanas duraderas para las poblaciones de ambos lados.

Investigación, arrestos y colaboración internacional

La investigación, liderada por el Ministerio del Interior marroquí bajo Driss Basri, involucró una colaboración forzada pero decisiva con Francia (país de residencia de la mayoría de los detenidos) y un seguimiento atento por parte de España, dada la nacionalidad de las dos víctimas mortales. Las pistas operativas incluyeron el vehículo robado abandonado tras el asalto, los testimonios del personal del hotel y, sobre todo, la localización de un arsenal en Aknoul. Esas pistas llevaron a una serie rápida de detenciones en Fez, Taourirt y Aknoul. Tarek Felah.

Los arrestos permitieron reconstruir la red. El interrogatorio de los detenidos proporcionó detalles sobre el reclutamiento en las banlieues, el adoctrinamiento, la logística de armas y la intención de reiterar ataques en otras ciudades turísticas. Francia se vio obligada a colaborar: se realizaron detenciones y registros en varias ciudades francesas. El juez Jean-Louis Bruguière abrió una investigación que reveló los vínculos con las redes islamistas argelinas y el reclutamiento en las cités. Las autoridades francesas se encontraron atrapadas entre la presión de Rabat, que exigía una acción firme, y la realidad de una comunidad magrebí que vivía con recelo cualquier endurecimiento de las políticas antiterroristas.

Esta fase investigadora expuso el carácter transnacional del fenómeno: no se trataba de una banda local de atracadores, como se había querido creer en 1993, sino de una célula yihadista con retaguardia en Francia, inspiración en la guerra argelina y objetivo declarado en el turismo marroquí. Al mismo tiempo, la tesis del control directo por parte de los servicios argelinos, sostenida con fuerza por Rabat, nunca fue demostrada de forma concluyente, y Argel la rechazó como una maniobra diplomática. La “colaboración internacional” de 1994 fue, por tanto, desigual y cargada de sospecha: eficaz para detener a la mayor parte del comando, insuficiente para resolver el enigma geopolítico que el atentado dejó abierto entre las dos orillas del Magreb.



Figura 2: Stéphane Aït Idir el 27 de enero de 1995, a la salida del juicio celebrado en Fez en el que se le sentenció a muerte.

Juicios, sentencias y justicia retrospectiva

Los juicios se iniciaron en Fez el 10 de enero de 1995 y concluyeron el 28 de enero ante la Corte de Apelación. Diecisiete acusados, de los cuales siete eran franco-magrebíes y el resto locales, comparecieron en un proceso que el régimen presentó como demostración de contundencia estatal. Stéphane Aït Idir, Redouane Hammadi y Hamel Marzoug fueron condenados a muerte. Otros recibieron cadena perpetua o penas de entre seis y veinte años. Amnistía Internacional denunció irregularidades procesales, alegaciones de tortura durante la detención y un juicio que consideró precipitado. Finalmente, las condenas a muerte no se ejecutaron.

En 1996 se celebró en París otro juicio contra la red. Abdelilah Ziyad admitió haber organizado el ataque al Atlas Asni y asumió la responsabilidad de haber ordenado a los asaltantes atacar a turistas. Los vínculos con el GIA y con comandantes argelinos quedaron parcialmente esclarecidos, aunque la

tesis del control directo por parte de los servicios argelinos nunca fue probada de forma concluyente. Estos procesos destacaron tensiones éticas y diplomáticas: críticas al rigor del procedimiento marroquí, el dilema francés entre cooperación antiterrorista y tutela consular, y el debate sobre si el episodio era un crimen común radicalizado o el primer acto de una yihad exportada. El episodio formó parte del contexto que, meses después, en el verano de 1995, desembocaría en la ola de atentados del GIA en Francia, protagonizada por otra célula (la de Khaled Kelkal), pero con raíces ideológicas y de reclutamiento similares.

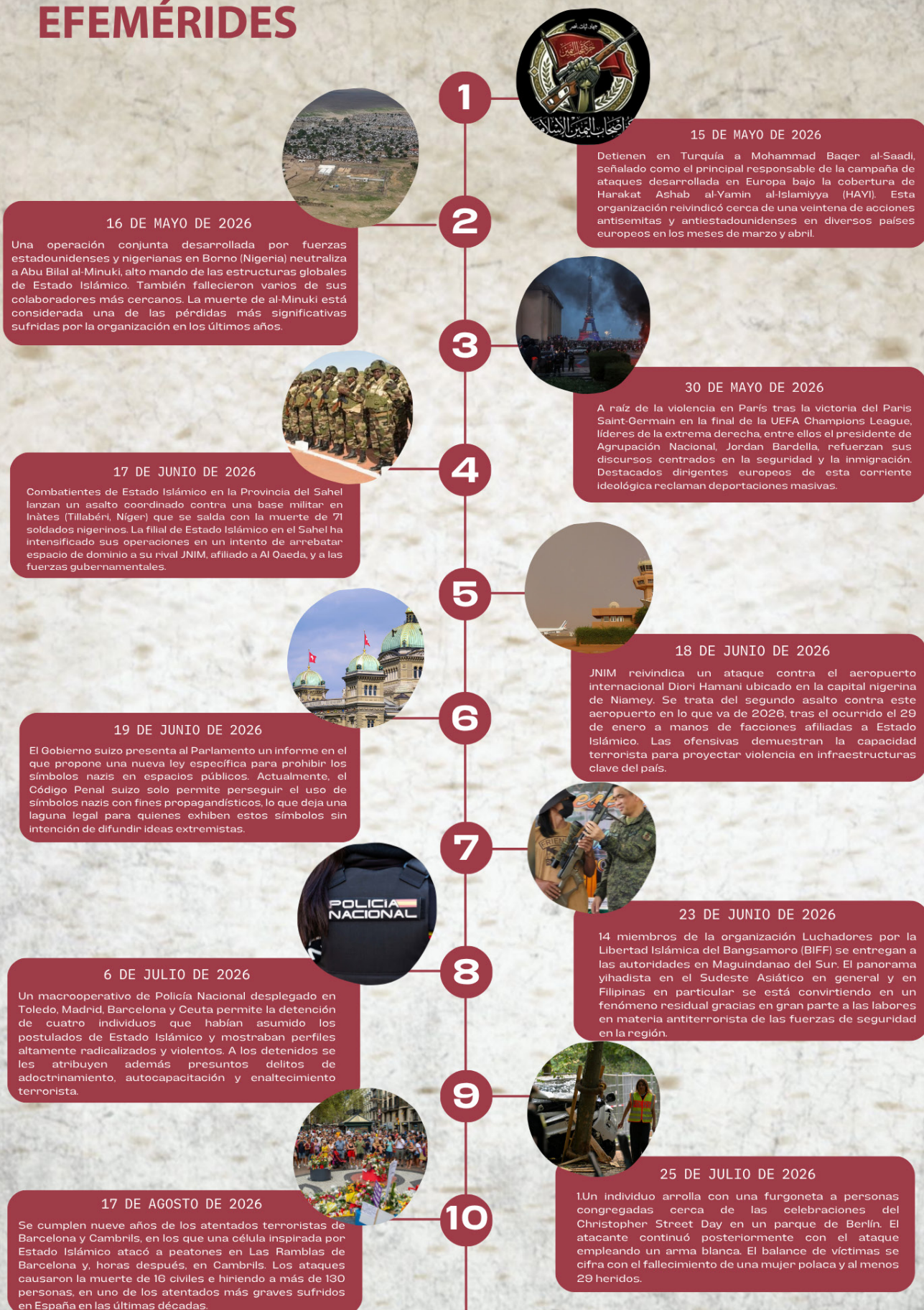
Impacto a largo plazo y lecciones aprendidas

Los atentados de 1994 y el juicio de 1995 obligaron a Marruecos a reforzar su aparato de seguridad interior y a estrechar la cooperación con Francia y España. Se intensificó la vigilancia de las redes islamistas y de los flujos de armas hacia Argelia. A nivel regional, el cierre de la frontera se convirtió en un símbolo de la ruptura entre los dos países y de la incapacidad de la Unión del Magreb Árabe para avanzar. Para las autoridades marroquíes, el episodio demostró que el reino no era inmune a la exportación de la yihad argelina. Para Francia, puso de relieve el problema de la radicalización en las banlieues años antes de que estallara con mayor fuerza en 1995 y, más tarde, en la década de 2010.

El turismo en Marrakech se recuperó con el tiempo y la ciudad demostró resiliencia, pero la memoria de aquellos días permaneció como un recordatorio de la fragilidad de la seguridad en un contexto de radicalización transnacional. El recuerdo del Atlas Asni quedó en segundo plano frente a los grandes atentados posteriores (los ya mencionados Casablanca 2003 y Marrakech 2011), que superaron con creces la letalidad de 1994 y obligaron a un rediseño más profundo de la arquitectura contraterrorista del reino. No obstante, aquellos hechos de agosto de 1994 constituyeron el primer aviso serio de que el terrorismo islamista había llegado a Marruecos, y de que las fronteras del Magreb ya no aislaban del todo a ninguna de las dos orillas del Mediterráneo.

Aunque las condenas a muerte no se cumplieron y algunos de los condenados fueron posteriormente objeto de procedimientos en Europa, el mensaje de contundencia del Estado marroquí quedó claro. Algunas lecciones clave incluyen la necesidad de no subestimar amenazas que parecen “importadas” o de baja intensidad, la importancia de la inteligencia compartida con los países de residencia de los atacantes (en este caso Francia), el riesgo de que hoteles y enclaves turísticos concentren el cálculo simbólico de células pequeñas, y el coste geopolítico duradero de una crisis de seguridad que se lee, al mismo tiempo, como crimen yihadista y como episodio de la rivalidad magrebí. El Atlas Asni fue, ante todo, el momento en que un reino que se creía a resguardo descubrió que la yihad contemporánea ya operaba en su territorio.

EFEMÉRIDES



¿SABÍAS QUÉ?

El 22 de diciembre de 2001, apenas tres meses después del 11-S, el británico Richard Reid, conocido desde entonces como el shoe bomber, embarcó en el vuelo 63 de American Airlines, que cubría la ruta París-Miami, con explosivo oculto en las suelas de sus zapatos.

A bordo intentó activar el dispositivo y fue reducido por la tripulación y varios pasajeros. El avión desviado aterrizó en Boston. Reid, convertido y adiestrado en el entorno de Al Qaeda, fue condenado a cadena perpetua. El episodio explica por qué, desde entonces, en innumerables aeropuertos del mundo se pide a los viajeros que se quiten el calzado en el control de seguridad.



El 9 de abril de 1985, Sana Yusuf Muhaydli, libanesa de 16 años militante del Partido Social Nacionalista Sirio (PSNS), condujo un vehículo cargado de explosivos contra un puesto y un convoy israelíes en las inmediaciones de Jezzine, en el sur del Líbano. En el atentado murieron soldados israelíes y, según algunas crónicas, también un militar libanés.

Muhaydli no era yihadista: el PSNS es una organización nacionalista laica, de tradición siria, entonces integrada en el Frente de Resistencia Nacional Libanés contra la ocupación israelí del sur del país.

Horas antes había grabado un vídeo de despedida, sentada ante una mesa, con el tono de quien lee un comunicado. Ese mismo 9 de abril la pieza se emitió en los informativos de Télé Liban y después circuló en cintas VHS. La prensa de Beirut la bautizó como “la novia del Sur”. Investigadores del fenómeno coinciden en considerarla la primera mujer que cometió un atentado suicida en la era contemporánea, y su grabación, uno de los primeros videotestamentos difundidos por televisión.



Tras el ataque a la villa olímpica de Munich el 5 de septiembre de 1972, Alemania Federal decidió crear una fueraz antiterrorista. El 26 de septiembre de 1972, el ministro del Interior Hans-Dietrich Genscher ordenó crear, dentro de la Guardia Federal de Fronteras, el Grenzschutzgruppe 9 (GSG9).

Cinco años después, el 13 de octubre de 1977, en pleno “otoño alemán” (una campaña de atentados masivos llevados a cabo por la RAF), un comando vinculado al FPLP secuestró el vuelo 181 de Lufthansa, que cubría la ruta Palma de Mallorca-Frankfurt, y exigió la liberación de presos de la Fracción del Ejército Rojo (RAF).

Tras escalas en Oriente Medio, el asesinato del capitán Jürgen Schumann y el aterrizaje en Mogadiscio, un equipo del GSG 9 dirigido por el propio Wegener asaltó, en la denominada Operación Feuerzauber, el aparato en la madrugada del 18 de octubre. En pocos minutos fueron abatidos o heridos los cuatro secuestradores y liberados todos los rehenes que quedaban a bordo.



En colaboración con:



Los «traidores» de ETA

Inés Gaviria

Las organizaciones terroristas no solo necesitan armas, militantes y una causa con la que justificar sus crímenes. Necesitan también imponer obediencia. Quien entra en ellas no puede marcharse libremente, cuestionar sus decisiones ni reconocer que utilizar la violencia para conseguir objetivos políticos siempre es ilegítimo. Un grupo terrorista difícilmente puede tolerar la discrepancia porque la existencia de alguien que ha conocido la organización desde dentro y ha decidido abandonarla demuestra que siempre hubo otra opción. Por eso ETA convirtió a algunos de sus antiguos miembros en enemigos y los señaló con una palabra que, dentro de su lógica totalitaria, equivalía a una condena a muerte: «traidor».

Pero abandonar una organización terrorista no es una traición. Traicionar habría sido perseverar en el asesinato después de comprender su injusticia radical. Rectificar, negarse a matar o defender que las armas debían desaparecer supone romper con una disciplina basada en el miedo y recuperar la capacidad de decidir libremente. Quienes dieron ese paso no borraron con él la responsabilidad derivada de sus crímenes ni de su militancia anterior. Haber terminado como víctimas de ETA tampoco convierte automáticamente en legítimo todo lo que hicieron antes. Sin embargo, nada de ello disminuye su condición de víctimas ni justifica el crimen cometido contra ellos.

María Dolores González Katarain, ‘Yoyes’, es quizá el caso más conocido. Había llegado a formar parte de la dirección de ETA militar, pero acabó profundamente desencantada con la organización. Se marchó a México, formó una familia y, tras varios años fuera, decidió regresar al País Vasco para reconstruir su vida. No tenía causas pendientes con la Justicia ni había proporcionado información a las Fuerzas de Seguridad. Su delito, a ojos de ETA, fue demostrar públicamente que era posible haber pertenecido a la organización y vivir después al margen de ella. ETA la asesinó el 10 de septiembre de 1986 en Ordizia, durante las fiestas de la localidad y en presencia de su hijo de tres años.

Su asesinato tenía un propósito ejemplarizante. ETA no solo pretendía acabar con ‘Yoyes’, sino utilizar su muerte para cerrar el camino a otros terroristas que pudieran estar planteándose abandonar la organización. Había que demostrar que nadie podía decidir por sí mismo abandonar ETA. ‘Yoyes’ representaba una amenaza precisamente porque su vida fuera de ETA podía convertirse en un precedente. Este 10 de septiembre de 2026 se han cumplido 40 años de su asesinato.

Dos años antes, ETA había asesinado a Miguel Francisco Solaun Angulo, ‘Mikel’, otro antiguo miembro de la organización terrorista. Solaun había participado en la histórica fuga de la cárcel de Basauri de 1970 y posteriormente se había beneficiado de la amnistía de 1977. A comienzos de los años ochenta, ETA lo obligó mediante amenazas contra su familia a colaborar en un atentado contra un edificio de Algorta destinado a albergar una casa cuartel de la Guardia Civil. Los terroristas colocaron cincuenta kilogramos de explosivos y pretendían hacerlos estallar durante la inauguración, cuando el inmueble estuviera lleno de personas.

Solaun se negó a conectar el artefacto. Según dejó escrito, no lo hizo porque no era un asesino. También trató de alertar de la existencia de los explosivos y terminó indicando personalmente dónde estaban ocultos. Fue detenido y condenado por su colaboración inicial, recibió una brutal paliza de otros presos de ETA en la cárcel y vivió sus últimos meses convencido de que la organización acabaría matándolo. El 4 de febrero de 1984, un terrorista le disparó en una cafetería de Algorta en presencia de su familia. ETA lo acusó de ser «traidor y colaborador de la policía» y presentó su asesinato como una advertencia para quienes buscasen una salida individual de la organización. Sus asesinos explicarían después con aterradora claridad la mentalidad que había detrás del crimen: en una guerra, dijeron, todo traidor debía ser ejecutado.

El caso de Eduardo Moreno Bergaretxe, ‘Pertur’, presenta diferencias importantes. Pertur no era un antiguo integrante de ETA que hubiera regresado a la vida civil, sino uno de los principales dirigentes de ETA político-militar cuando desapareció en el País Vasco francés el 23 de julio de 1976. Defendía la necesidad de subordinar el terrorismo a la acción política y había plasmado sus planteamientos en la ponencia Otsagabia. Sus tesis chocaban con las del sector más militarista de la organización, especialmente con los llamados ‘comandos *bereziak*’.

La autoría de su desaparición nunca ha sido esclarecida y su cuerpo continúa sin aparecer. A lo largo de los años se han planteado distintas hipótesis, incluida la participación de grupos de extrema derecha. Sin embargo, numerosos testimonios e indicios apuntan a que Pertur fue eliminado por miembros de su propia organización debido a sus discrepancias internas y a su apuesta por dar prioridad a la vía política. La última vez que fue visto con vida se encontraba con dos integrantes de los ‘*bereziak*’. Mientras quienes conocen lo sucedido continúen guardando silencio, su familia seguirá privada de la verdad y de la posibilidad de recuperar sus restos. El 23 de julio del presente año, 2026, se cumplieron 50 años desde su desaparición.

La trayectoria de Juan María Jáuregui fue distinta y permite observar la permanencia de esa lógica mucho tiempo después. Durante su juventud antifranquista militó brevemente en ETA, dentro de su frente cultural. Cuando en la VI Asamblea se planteó la continuidad de la vía armada, Jáuregui se apartó de ella. Militó posteriormente en el Partido Comunista, ingresó en el Partido Socialista de Euskadi y llegó a ser gobernador civil de Gipuzkoa. Su vida política estuvo marcada por la defensa de los derechos humanos y del Estado de derecho, también frente a los abusos cometidos en la lucha antiterrorista.

ETA lo asesinó el 29 de julio de 2000 en la cafetería del frontón Beotibar de Tolosa. Le dispararon por la espalda mientras conversaba con un amigo. Habían transcurrido décadas desde su breve militancia juvenil y su asesinato no fue presentado como una purga interna, sino que formó parte de la ofensiva de ETA contra representantes políticos y ciudadanos constitucionalistas. Pero su historia encierra una paradoja reveladora: un hombre que había conocido la organización desde dentro, que había rechazado la violencia y que había dedicado su vida adulta a defender las instituciones democráticas terminó siendo asesinado por aquella misma organización.

Los casos de ‘Yoyes’, ‘Pertur’, Solaun y Jáuregui no son intercambiables. Sus responsabilidades anteriores, sus procesos de ruptura y las circunstancias en las que fueron asesinados fueron diferentes. Tampoco todos ellos habían recorrido el mismo camino de autocrítica respecto a su militancia. Recordarlos como víctimas no significa idealizarlos ni convertir sus biografías en relatos simples de redención. Significa reconocer un principio elemental: nada permite a una organización terrorista arrogarse el derecho a ejecutar a quien discrepa, abandona sus filas o decide defender otra forma de hacer política.

Existe una razón por la que estos casos incomodan especialmente a la narrativa con la que ETA justificó su existencia. ‘Yoyes’, ‘Pertur’, Solaun y Jáuregui conocían la organización. No podían ser presentados como personas ajenas al supuesto «conflicto vasco» ni como enemigos incapaces de comprender sus motivaciones. Habían compartido, en distintos momentos y grados, su universo ideológico. Precisamente por eso, su discrepancia era mucho más peligrosa: demostraba que conocer las razones invocadas por ETA no obligaba a aceptar sus crímenes y que defender una determinada identidad o proyecto político no exigía matar.

El terrorismo no termina por completo cuando deja de matar. También es necesario desmontar las categorías morales que construyó para justificar sus asesinatos. Entre ellas se encuentra la idea de que abandonar ETA, colaborar con la Justicia o rechazar la violencia terrorista constituía una deslealtad merecedora de castigo.

Por eso debemos recordar estas historias con todos sus matices. Fueron miembros de ETA y algunos de ellos tuvieron responsabilidades criminales dentro de la organización. Pero también fueron víctimas de ella. ETA los asesinó, o presuntamente los hizo desaparecer en el caso de ‘Pertur’, porque representaban distintas formas de desobediencia: cuestionar la primacía de las armas, impedir

una matanza, abandonar la organización o defender abiertamente la democracia. En la lógica de ETA fueron «traidores». En realidad, lo que hicieron fue demostrar que incluso desde el interior del fanatismo siempre existe la posibilidad de elegir otro camino.

EDUARDO MORENO BERGARETXE

Nacido en: San Sebastián

Edad: 25

Hijos: 0

Estado civil: Soltero

Ocupación: Dirigente de ETA político-militar

Fecha del atentado: 23/07/1976

Lugar del atentado: San Juan de Luz

Asesinado por: ETA



Descripción del atentado:

Eduardo Moreno Bergaretxe, 'Pertur', desapareció el 23 de julio de 1976 en el País Vasco francés. La última vez que fue visto con vida se encontraba en compañía de Francisco Javier Garayalde, Erreka, y Miguel Ángel Apalategui, Apala, integrantes de los comandos bereziak de ETA político-militar. Su cuerpo nunca ha sido encontrado y nadie ha sido condenado por su desaparición.

Pertur era uno de los principales ideólogos de ETA político-militar. Defendía que la organización debía supeditar la actividad armada a la dirección política y había participado en la elaboración de la ponencia Otsagabia. Sus planteamientos provocaron un enfrentamiento creciente con el sector militarista. Aunque se han manejado distintas hipótesis sobre su desaparición, numerosos indicios y testimonios apuntan a que fue secuestrado y asesinado por miembros de la propia organización debido a sus discrepancias internas.

MIGUEL FRANCISCO SOLAUN ANGULO

Nacido en: Euskadi

Edad: 39

Hijos: 2

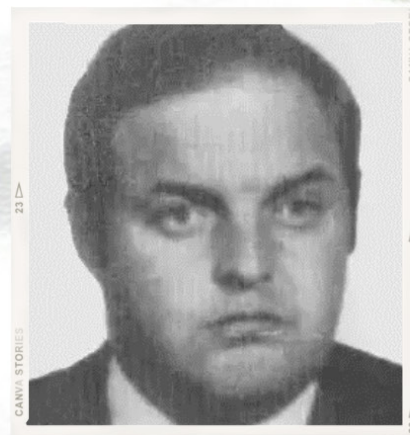
Estado civil: Casado

Ocupación: Ingeniero industrial y constructor

Fecha del atentado: 04/02/1984

Lugar del atentado: Algorta, Getxo (Bizkaia)

Asesinado por: ETA



Descripción del atentado:

El 4 de febrero de 1984, Miguel Francisco Solaun Angulo se encontraba con su familia en una cafetería de Algorta cuando un miembro de ETA le disparó por la espalda. La organización reivindicó el asesinato, lo calificó de «traidor y colaborador de la policía» y presentó el crimen como una advertencia contra quienes buscasen una salida individual de la banda.

Solaun había pertenecido a ETA durante el franquismo y organizado la fuga de quince presos de la cárcel de Basauri en 1970. Años después, ETA lo obligó mediante amenazas contra su familia a facilitar la colocación de cincuenta kilogramos de explosivos en un edificio destinado a convertirse en casa cuartel de la Guardia Civil. Solaun se negó a conectar la bomba y ayudó a las autoridades a localizarla. Fue detenido, condenado por colaboración e indultado posteriormente. Durante su estancia en prisión había sido brutalmente agredido por presos de ETA. Tras recuperar la libertad vivió amenazado hasta que la organización cumplió su advertencia.

MARÍA DOLORES GONZÁLEZ CATARAIN

Nacido en: Ordizia (Gipuzkoa)

Edad: 32

Hijos: 1

Estado civil: Casada

Ocupación: Economista

Fecha del atentado: 10/09/1986

Lugar del atentado: Ordizia (Gipuzkoa)

Asesinado por: ETA



Descripción del atentado:

El 10 de septiembre de 1986, María Dolores González Katarain, Yoyes, paseaba por Ordizia con su hijo de tres años durante las fiestas de la localidad. El miembro de ETA Antonio López Ruiz, Kubati, se acercó a ella y le disparó a corta distancia. Yoyes murió en el acto. Su asesinato había sido ordenado por la dirección de ETA para castigar públicamente su abandono de la organización y evitar que su regreso al País Vasco animara a otros militantes a seguir el mismo camino.

Yoyes había sido una de las primeras mujeres en alcanzar puestos de responsabilidad dentro de ETA militar. Tras el asesinato de José Miguel Beñarán, Argala, y sus crecientes discrepancias con la estrategia de la organización, abandonó la banda y se trasladó a México. Allí estudió, trabajó para Naciones Unidas y formó una familia. Regresó a España en 1985, sin causas pendientes con la Justicia y con el propósito de reconstruir su vida. ETA convirtió esa decisión personal en una afrenta y la castigó con la muerte.

JUAN MARÍA JÁUREGUI APALATEGUI

Nacido en: Legorreta (Gipuzkoa)

Edad: 48

Hijos: 1

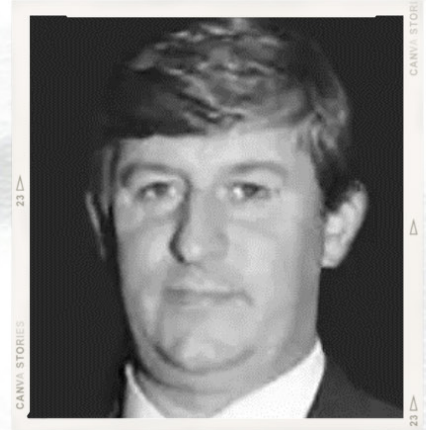
Estado civil: Casado

Ocupación: Directivo empresarial y
exgobernador civil de Gipuzkoa

Fecha del atentado: 29/07/2000

Lugar del atentado: Tolosa (Gipuzkoa)

Asesinado por: ETA



Descripción del atentado:

El 29 de julio de 2000, Juan María Jáuregui se encontraba conversando con un amigo en la cafetería del frontón Beotibar de Tolosa cuando dos miembros de ETA se acercaron a él y le dispararon por la espalda. Jáuregui residía entonces en Chile por motivos profesionales y había regresado al País Vasco para pasar unos días de vacaciones.

Durante su juventud había militado brevemente en ETA dentro del frente cultural, pero se apartó de la organización al rechazar la continuidad de la violencia. Posteriormente militó en el Partido Comunista y en el Partido Socialista de Euskadi. Entre 1994 y 1996 fue gobernador civil de Gipuzkoa, etapa durante la cual defendió la actuación de las instituciones democráticas contra ETA y promovió también la investigación de posibles abusos policiales. La organización terrorista lo asesinó décadas después de que hubiera roto con ella y tras haber dedicado buena parte de su vida a la defensa del Estado de derecho.

Sobre RIET

La Revista Internacional de Estudios sobre Terrorismo (RIET) es una publicación en forma de revista electrónica que nace con la idea de ofrecer a los investigadores una plataforma para la publicación de artículos académicos relacionados con el estudio del terrorismo desde cualquiera de sus diferentes enfoques y perspectivas (estrategias antiterroristas, víctimas, seguridad, prevención del radicalismo violento, inteligencia, etc.). La revista aportará flexibilidad en términos de contenido, estilo y extensión de los artículos, pero sin dejar de lado los estándares académicos profesionales.

Los artículos de investigación y otros contenidos de la revista serán revisados por miembros del Comité científico, expertos académicos y profesionales externos previamente a su publicación, aportando al autor la retroalimentación, correcciones, y apuntes pertinentes, en el caso de que fuesen necesarios.

Con una periodicidad de publicación cuatrimestral, RIET tiene la intención de convertirse en la referencia para aquellos autores que desean publicar en español o en inglés, así como en la opción prioritaria de consulta para el público hispanohablante que busca un contenido de calidad contrastado en el área objeto de estudio que aborda la revista.

RIET es una iniciativa del Observatorio Internacional de Estudios sobre Terrorismo (OIET). Todo el contenido de RIET es accesible a través de la siguiente página web: <https://rietjournal.org/>

La Revista de Estudios en Seguridad Internacional se encuentra indexada en Dialnet, RE-BIUN, Academic Index y Google Scholar.

About RIET

The Revista Internacional de Estudios sobre Terrorismo (RIET), is an electronic e-journal publication born from the idea of offering investigators a platform through which to publish academic articles related to the study of terrorism from any of its different approaches and perspectives (anti-terrorist strategies, security, prevention of violent radicalism, intelligence, etc.). The journal will provide flexibility in terms of content, style and length of the articles, without neglecting professional academic standards.

The research articles and other contents of the journal will be reviewed by members of the Scientific Committee, academic experts and external professionals prior to publication. They will provide the author with feedback, corrections, and pertinent notes if they were necessary.

Publishing every four months, RIET intends to become a reference for those authors who wish to publish in Spanish or English. RIET also intends to be the priority option of consultation for the Spanish-speaking public looking for contrasted quality content in the area of terrorism.

RIET is an Observatorio Internacional de Estudios sobre Terrorismo (OIET) initiative. All RIET content is accessible through the following web page:

<https://observatorioterrorismo.com/revistariet/>

Criterios de Publicación

El sistema de evaluación del contenido de los trabajos se realizará a través de una revisión por pares, garantizando el anonimato del autor. Dicha revisión será realizada por dos miembros del Comité científico o especialistas externos a la revista y serán susceptibles de evaluación la idoneidad de la temática, la originalidad del contenido, la aportación en términos académicos y el rigor científico. Los evaluadores expondrán su opinión sobre el trabajo, decidiendo si este cumple las condiciones para ser publicado o si es preciso realizar modificaciones. También podrán decidir, en el caso de que el texto analizado no cumpla los requisitos mínimos, su no validez para la revista. El proceso de evaluación será menor a las ocho semanas desde el momento en el que se acuse el recibo del artículo recibido, siendo informado el autor de la recepción del mismo en un plazo máximo de una semana. En el caso de aquellos trabajos que deban sufrir modificaciones a petición de los evaluadores, el tiempo máximo para enviar la versión definitiva del trabajo será de diez días desde el momento en el que se informa de ello al autor, período tras el cual será reevaluado el trabajo y se decidirá su publicación o no. En estos casos, las correcciones deberán limitarse a errores, quedando restringida la posibilidad de añadir contenido.

La periodicidad de la revista será de carácter cuatrimestral, por lo que habrá tres números anuales publicados en la primera semana de los meses de abril, agosto y diciembre. La fecha límite para los envíos será de tres meses antes de la publicación de cada número; en el caso de ser recibido el trabajo más tarde de la fecha estipulada, pasará a incorporarse a la revisión para el siguiente número.

El envío de los manuscritos originales debe hacerse llegar al Equipo editorial a través del correo jy@observatorioterrorismo.com, poniendo en copia de su contenido a la dirección: c@observatorioterrorismo.com. Se deberán enviar dos archivos en formato Word, uno con nombre del autor y su adscripción profesional, junto a una breve descripción de su CV a pie de página, y otro con una versión anónima.

Publication criteria

Articles and reviews sent to the journal must have scientific rigor. They must be original documents that have not been previously published or submitted for review in any other publication. Articles related to the study of terrorism from any of its multiple approaches will be accepted.

The evaluation system of the content submitted will be carried out through a peer review, guaranteeing the author's anonymity. Said review will be done by two members of the Scientific Committee or specialists external to the journal. The suitability of the subject, originality of the content, contribution in academic terms and its scientific rigor will be subject to evaluation.

The evaluators will present their opinion on the content, deciding whether it meets the conditions required to be published or if modifications are necessary. In the event that the analyzed text does not meet the minimum requirements they may also decide it is not valid for publication.

The author will be informed of the reception of the article within a week. The evaluation process will take less than eight weeks from the moment the article is received. For those articles that must undergo modifications, the maximum time to send the definitive version of the article will be ten days from the moment the author is informed. The definitive version will then be reevaluated. In these cases, corrections should be limited to errors, restricting the possibility of adding content.

About the periodicity, the journal will be published every four months. There will be three an

nual issues published in the first week of the months of April, August and December. The deadline for submissions will be three months before the publication of each issue. If the content is received later than the stipulated date, it will be incorporated into the review for the next issue.

***The submission** of the original manuscripts must be sent to the Editorial Team through the e-mail jy@observatorioterrorismo.com. The e-mail must be carbon copied (CC) to the direction: c@observatorioterrorismo.com.*

Two files must be sent in Word format. One including the author's name, professional affiliation and a brief description of the author's CV at the footer, and the other with an anonymous version of the paper.

Normas e instrucciones para los autores

- Los trabajos podrán estar escritos tanto en español como en inglés.
- Se deberán ajustar a las normas ortográficas de la Real Academia Española, siguiendo la actualización 2019 de la edición de 2010.
- La extensión mínima de los artículos científicos será de 4.000 palabras, y la máxima de 5.000, sin incluir el apartado de referencias ni las notas a pie de página, cuya extensión no deberá superar las 2.000 palabras. Todo artículo tendrá que incluir un resumen/*abstract* en español e inglés, sin superar las 200 palabras para cada uno y con un máximo de 5 palabras clave, también en ambos idiomas. Las reseñas bibliográficas tendrán una extensión máxima de 1.500 palabras.
- La estructura de los artículos científicos deberá ser:
 - Título, centrado.
 - Nombre del autor o de los autores junto a su afiliación institucional bajo el título y con los apellidos en mayúscula. Se añadirá una breve nota a pie de página junto a cada uno de los autores a modo de descripción de la trayectoria profesional.
 - Introducción
 - Apartados principales deberán estar numerados y resaltados en negrita (1.), siendo el primero de ellos la introducción.
 - Apartados de segundo nivel deberán estar numerados y en cursiva (1.1.).
 - Apartados de tercer nivel deberán estar numerados y subrayados (1.1.1.).
 - Conclusiones
 - Referencias bibliográficas ordenadas alfabéticamente.
- El texto deberá seguir el estilo Arial 12 con interlineado de 1.5. No se dejará doble espacio, excepto en el encabezado de cada apartado principal, y se evitarán las tabulaciones, salvo excepciones. El trabajo deberá presentar una alineación justificada.
- Las citas que tengan una extensión superior a las cuatro líneas deberán ir tabuladas y espaciadas respecto al párrafo superior e inferior.
- El modelo de citas será en base al estilo APA, añadiendo en el propio cuerpo del texto entre paréntesis el apellido o los apellidos de los autores junto al año de la publicación de la obra y la página, en caso de que fuese necesario (González, 2015:35), y se citará de forma completa en el apartado final de referencias bibliográficas. Las notas a pie de página quedarán reservadas para aclaraciones, comentarios o incisos puntuales, haciendo un uso moderado de ellas.
- Podrán incluirse tablas o gráficas ordenadas numéricamente. Todas ellas deberán tener una pequeña descripción y comenzarán con FIGURA X. (FIGURA 4. TABLA EVOLUCIÓN ATENTADOS). Será preciso indicar el correspondiente origen de la fuente, ya sea de otro trabajo o elaboración propia, al final de la descripción (FUENTE: elaboración propia).

Instructions for authors

- *The papers can be written both in Spanish and English.*
- *The papers must comply with the spelling standards of the Royal Spanish Academy, following the 2019 update of the 2010 edition.*
- *The minimum length of scientific articles will be 4,000 words, and the maximum of 5,000, excluding references and footnotes. The latter should not exceed 2,000 words. Every article must include a maximum 200-word abstract, and maximum 5 keywords. Both the abstract and the keywords must be included in Spanish and English. Bibliographic reviews will have a maximum length of 1,500 words.*
- *The structure of scientific articles must be:*
 - *Title, centered.*
 - *Name of the author or authors along with their institutional affiliation. Under the title and with the surnames in capital letters.*
 - *Introduction*
 - *Main sections must be numbered and highlighted in bold (1.), the first one being the introduction.*
 - *Second level sections must be numbered and in italics (1.1).*
 - *Third level sections must be numbered and underlined (1.1.).*
 - *Conclusions*
 - *Bibliographic references arranged alphabetically.*
- *The text must follow Arial 12 style with 1.5 line spacing. Double space will not be used except in the heading of each main section. Tabs will be avoided, with exceptions. The paper must present a justified alignment.*
- *Citations longer than four lines must be tabulated and spaced from the upper and lower paragraphs.*
- *The citation model will be based on APA format, adding in the text in parentheses the surname(s) of the authors along with the year of publication of the work and the page, if necessary (González, 2015:35). It will be fully cited in the final section of bibliographic references. Footnotes will be reserved for clarifications, comments or punctuations, and used with moderation.*
- *Numerically ordered tables or graphs may be included. All of them must have a short description beginning with FIGURE X. (FIGURE 4. EVOLUTION TABLE OF ATTACKS). It will be necessary to indicate the origin of the source at the end of the description, whether it is from another author or self-elaborated (SOURCE: own elaboration).*

Código de ética y detección del plagio

Todas las partes involucradas en la publicación de todo el contenido de RIET, incluyendo autores, editores de la revista y revisores, deben contemplar las normas de comportamiento ético esperadas y recogidas en Directrices de Buenas Prácticas para Editores de Revistas del Comité de Ética de la Publicación (COPE), Committee on Publication Ethics (Code of Conduct and Best Practices Guidelines for Journals Editors, COPE). La política de RIET es publicar trabajos originales, por lo que se implementa un procedimiento específico para evitar malas prácticas, especialmente el plagio. Previamente a iniciar el proceso de evaluación, se utilizan herramientas de búsqueda en Internet y softwares online a fin de corroborar la originalidad y evitar prácticas de plagio. Asimismo, se solicita a los revisores que durante su evaluación presten atención a posibles malas prácticas relacionadas con el plagio.

Code of ethics and plagiarism detection

All parties involved in the publication of all RIET content, including authors, journal editors and reviewers, must adhere to the standards of ethical behavior expected in the Committee on Publication Ethics (Code of Conduct and Best Practices Guidelines for Journals Editors, COPE). RIET's policy is to publish original work, so a specific procedure is implemented to avoid malpractice, especially plagiarism. Before starting the evaluation process, Internet search tools and online software are used in order to corroborate originality and avoid plagiarism practices. Reviewers are also asked to pay attention to possible malpractices related to plagiarism during their evaluation.

Derechos de autor

Todo el contenido publicado se encuentra bajo una licencia de Creative Commons Reconocimiento 4.0 Internacional.

- Los autores conservarán sus derechos de autor y garantizarán a la revista el derecho de primera publicación de su obra.
- Los autores podrán publicar sus trabajos en otros medios o revistas, siempre y cuando se indique a RIET como fuente original de su obra.
- Los autores podrán dar difusión pública de sus trabajos a través de sus instituciones, canales de Internet u otros medios asignados para la difusión del conocimiento, siempre que se cite correctamente la fuente original.
- Los autores son responsables de obtener las licencias y permisos necesarios en todo el material incluido en su obra que así lo requiera.
- Los autores no deben hacer ningún pago por la evaluación/publicación de sus artículos en RIET.

Política de acceso abierto y libre

Con el ánimo de contribuir a difundir el conocimiento entre los especialistas y el público en general, RIET es una plataforma académica de acceso abierto y libre.

Todo el contenido publicado se encuentra bajo una licencia de una licencia de Creative Commons Reconocimiento 4.0 Internacional

Se permite la copia, distribución y comunicación pública siempre y cuando se cite el autor del texto y la fuente, recomendándose la citación que acompaña a cada artículo. No se pueden hacer usos comerciales ni obras derivadas. Los derechos de los artículos publicados pertenecen a sus autores.



Esta obra está bajo una [licencia de Creative Commons Reconocimiento 4.0 Internacional](#).

Copyright

All published content is licensed under a Creative Commons Attribution 4.0 International license.

- The authors will keep their copyright and guarantee the magazine the right of first publication of his work.*
- Authors may publish their work in other media or magazines, provided RIET is indicated as the original source of their work.*
- The authors may give public diffusion of their work through their institutions, Internet channels or other means assigned for the diffusion of knowledge, as long as the original source is correctly cited.*
- The authors are responsible for obtaining the necessary licenses and permissions for all material included in their work that requires them to do so.*
- Authors should not make any payment for the evaluation/publication of their articles in RIET.*

Open and free access policy

With the aim of contributing to the dissemination of knowledge among specialists and the general public, RIET is an open and free access academic platform.

All published content is licensed under a Creative Commons Attribution 4.0 International license

Copying, distribution and public communication is permitted as long as the author of the text and the source are cited, and the citation that accompanies each article is recommended. No commercial use or derivative works may be made. The rights of the published articles belong to their authors.



Esta obra está bajo una [licencia de Creative Commons Reconocimiento 4.0 Internacional](#).

REVISTA INTERNACIONAL DE ESTUDIOS SOBRE TERRORISMO

Revista académica digital de publicación cuatrimestral.
Observatorio Internacional de Estudios sobre Terrorismo (OIET).
Colectivo de Víctimas del Terrorismo, San Sebastián, España.

ISSN 2660-9673



<https://rietjournal.org/>



@RIET_revista



Este obra está bajo una [licencia de Creative Commons Reconocimiento 4.0 Internacional](#).

