



Recursos contextuales: En la intersección: análisis de los vínculos entre terrorismo, extremismo violento y crimen

Ciudad de México, octubre de 2026

A continuación se presenta una serie de artículos que exploran los vínculos entre terrorismo, extremismo violento y crimen. Fue preparada por la Global Network on Extremism and Technology (GNET, en español, Red mundial sobre extremismo y tecnología). GNET es el órgano de investigación académica del Global Internet Forum to Counter Terrorism (GIFCT, en español, el Foro mundial de Internet contra el terrorismo). La función del GNET es publicar estudios útiles para mejorar nuestros conocimientos cómo los terroristas y extremistas violentos explotan las plataformas digitales y evitar dicha explotación. El GNET trabaja bajo los auspicios del Centre for Statecraft and National Security, con sede en el Department of War Studies de la Universidad King's College London.

Insights de Latinoamérica

Contexto regional

[From Columbine to Teotihuacán: The Rise of Nihilistic Violence in Latin America \(De Columbine a Teotihuacán: el auge de la violencia nihilista en Latinoamérica\)](#)

Urszula Mrozowska, 23 de junio de 2026

A partir del tiroteo en Teotihuacán, este artículo examina algunos ataques recientes asociados a la violencia nihilista en Latinoamérica. Desde una perspectiva regional más amplia analiza el fenómeno y la circulación de contenido en redes sociales relacionado con la True Crime Community, o TCC (es decir, la comunidad del crimen real) que ensalza a atacantes locales.

[Shock and Awe: Geopolitical Disruption and Terrorist Narrative Opportunism Online \(Conmoción y asombro: los sucesos geopolíticos y el oportunismo del discurso terrorista en internet\)](#)

Sam David, 4 de febrero de 2026

Con la captura de Maduro como anclaje empírico, en este artículo se analiza la tendencia de utilizar los sucesos geopolíticos para reforzar simbolismos y promover ideologías dentro de los discursos en línea de terroristas y extremistas violentos, específicamente dentro de ecosistemas yihadistas. Dicha tendencia sugiere un efecto secundario que debería tenerse más en cuenta: los logros tácticos instrumentalizados de forma estratégica por agentes militantes no estatales para transmitir un mensaje de legitimidad en comunidades en línea con reclamos que se solapan.



Redes globales en Latinoamérica

[Reconceptualising Makarenko's Continuum in the Digital Age: The Case of Hezbollah \(Nuevas reflexiones sobre el concepto del proceso continuo de Makarenko en la era digital: el caso de Hezbollah\)](#)

Adriana Marin, 1 de octubre de 2026

En este artículo se alega que la innovación tecnológica está transformando el nexo contemporáneo entre crimen y terrorismo al mejorar la adaptabilidad, la resiliencia y el alcance transnacional de las redes financieras ilícitas de Hezbollah. Se aduce que la actual teoría del nexo entre crimen y terrorismo debería ampliarse para tener en cuenta el papel cada vez más importante de las tecnologías digitales. Dicha ampliación llevaría al análisis fuera de las formas tradicionales de interacción entre crimen y terrorismo para incluir el modo en que las tecnologías digitales facilitan nuevas formas de convergencia financiera, operativa y transnacional.

[Hezbollah's Latin American Networks: Stablecoins, Smuggling, and Sanctions Evasion \(Las redes latinoamericanas de Hezbollah: criptomonedas estables, contrabando y evasión de sanciones\)](#)

Adam Roussele, 21 de julio de 2025

En este artículo se explora cómo las redes de Hezbollah en Venezuela y en la Triple Frontera se están adaptando a nuevas realidades financieras, cómo se aprovechan de la inestabilidad regional y de la permisividad de los criptomercados, y lo que todo esto significa para las compañías de tecnología financiera, los profesionales del área de cumplimiento normativo y los responsables políticos que intentan anticiparse a esta amenaza en evolución.

[Sonic Hate: Examining Brazil's NSBM Scene and Its Global Networks \(Odio sónico: un examen de las bandas de black metal nacionalsocialista de Brasil y sus redes mundiales\)](#)

Ricardo Cabral Penteado, 10 de febrero de 2025

En este artículo se examina el panorama de las bandas brasileñas de black metal nacionalsocialista (NSBM, por sus siglas en inglés) y su papel en la propagación de ideologías extremistas, principalmente en relación con las conexiones transnacionales. Este estudio empleó un conjunto de datos de más de cien grupos musicales brasileños (activos entre 1993 y 2024) y más de mil canciones para realizar un análisis de red y de procesamiento de lenguaje natural (PLN) a fin de entender la forma en que estos grupos difunden sus discursos de odio y refuerzan las redes neonazis mundiales.

Nuevas amenazas y tecnologías

[Cloned Voices and Synthetic Recruiters: Generative AI at the Cartel–Far-Right Nexus \(Voces clonadas y reclutadores sintéticos: la IA generativa y el nexo entre cárteles y la ultraderecha\)](#)

Debaarjun Dasgupta

Este artículo expone el solapamiento operativo del uso de IA generativa entre nuevas organizaciones extremistas en Latinoamérica y movimientos extremistas violentos de la ultraderecha. Dicho solapamiento se aborda como una convergencia táctica dentro del nexo más amplio entre crimen y terrorismo, en vez de como una visión general del mal uso de la IA en la región.



[From Kyiv to Culiacán: How Mexican Cartels Are Adapting Drone Warfare Lessons from Ukraine \(De Kiev a Culiacán: cómo los cárteles mexicanos están adaptando lo aprendido en Ucrania con los ataques con drones\)](#)

Matilde Gamba, 28 de septiembre de 2026

En este artículo se analizan ejemplos específicos de operaciones con drones ejecutadas por cárteles junto a nueva evidencia de tácticas aprendidas en el conflicto ucraniano. El objetivo es investigar el modo en que los cárteles mexicanos de narcotráfico están adaptando tácticas con drones surgidas en la guerra rusoucraniana para aplicarlas en situaciones distintas a las tradicionales. También se estudia lo que dicha adaptación pone de relieve acerca del solapamiento cada vez mayor entre los métodos de criminales y de extremistas violentos para ejercer violencia facilitada por la tecnología. Con base en las conclusiones, el artículo presenta recomendaciones para mitigar el mal uso de tecnologías comerciales de drones y evitar que se propaguen nuevas tácticas de violencia.

Juventud, reclutamiento y explotación en línea

[Blurred Lines: The Child Safety Gap in the Crime-Terror Nexus \(Líneas difusas: la brecha de seguridad infantil en el nexo entre crimen y terrorismo\)](#)

Cecilia Polizzi, 29 de septiembre de 2026

Este artículo expone los mecanismos concretos (lingüísticos, audiovisuales y de infraestructura) con los que los contenidos de los cárteles evaden las reglas de moderación de las plataformas tecnológicas. Explora lo que supone esta deficiencia para los menores de edad y las consecuencias más generales para las plataformas. También pone de relieve los patrones comunes del nexo entre crimen y terrorismo, como las técnicas de evasión y las vías usadas para lograr la participación juvenil.

[Not Just Copycat: Digital Ecology of School-Targeted Violence in Lázaro Cárdenas \(Más que un simple imitador: ecología digital del violento ataque en la escuela de Lázaro Cárdenas\)](#)

Ricardo Cabral Penteado, 5 de mayo de 2026

En este artículo se examina el ataque en la escuela de Lázaro Cárdenas no como una tragedia aislada, sino como un caso que arroja luz sobre cómo los entornos digitales contemporáneos dan forma a la violencia perpetrada en centros educativos. En vez de presentar una nueva forma de violencia, el caso muestra cómo elementos conocidos –por ejemplo, la filtración antes del ataque a través de un video publicado por el atacante horas antes, las señales misóginas y la recirculación de contenido tras el ataque– pueden convergir en distintas plataformas de tal modo que los contenidos violentos y los repertorios de símbolos se hacen más visibles, reconocibles y reutilizables.

[From TechHaven to Telegram: How Latin American Youth Are Being Drawn into Jihadist Networks \(De TechHaven a Telegram: cómo las redes yihadistas están atrayendo a la juventud latinoamericana\)](#)

María Zuppello, 11 de noviembre de 2025

En este artículo se examina la transformación de la radicalización que ha tenido lugar, con especial atención en Brasil, y se expone cómo la web descentralizada está siendo caldo de cultivo de un ecosistema digital que, en Latinoamérica, espolea a nuevos agentes violentos que actúan en solitario.



[Guerrillas Online: Recruitment, Propaganda, and Control by Colombia's FARC-EP Dissidents and ELN \(Guerrillas en línea: reclutamiento, propaganda y control por parte de disidentes de las FARC-EP y el ELN\)](#)

Urszula Mrozowska, 28 de julio de 2025

En este artículo se analiza cómo estos dos grupos guerrilleros de extrema izquierda utilizan las redes sociales para mejorar sus tácticas de comunicación digital y reclutamiento de jóvenes. Se examina su presencia en línea y el uso de las plataformas para mantener su influencia territorial.

Intervenciones positivas, herramientas y prácticas

[Introducing BR-ECHO: A Tool to Fight Online Extremism in Brazilian Portuguese \(Presentación de BR-ECHO: una herramienta para combatir el extremismo en línea en portugués de Brasil\)](#)

Ricardo Cabral Penteado, 11 de agosto de 2025

Este artículo presenta la herramienta BR-ECHO (siglas en inglés de Brazilian Extremist Content Hashing Observatory), un sistema modular creado para cerrar la brecha en los sistemas de moderación que funcionan eficazmente en el contexto cultural y lingüístico brasileño. Al integrar explicabilidad, adaptabilidad y trazabilidad, la plataforma persigue contribuir a prevenir y combatir el extremismo violento a través de herramientas contextualizadas desde el punto de vista lingüístico y operativo y diseñadas para entornos con pocos recursos.

Artículos Insight sobre el nexo global entre crimen y terrorismo

El solapamiento del crimen, el terrorismo y el extremismo violento

[HAYI and State-Cover Networks: The Changing Landscape of Terrorist Financing in Europe \(El grupo HAYI y las redes con vínculos estatales: el panorama cambiante del financiamiento del terrorismo en Europa\)](#)

Fabrizio Minniti, 10 de junio de 2026

En este artículo se examina cómo están cambiando las prácticas de financiamiento del terrorismo en Europa ante el creciente solapamiento del crimen organizado y el extremismo violento respaldado por el Estado. También se explora la lógica financiera de lo que en este informe se denominan «state-cover networks», es decir, estructuras modulares con vínculos estatales cuya existencia se puede negar y que emplean intermediarios criminales para financiar y llevar a cabo ataques en jurisdicciones europeas.

[The Virtual Connection: Illicit Natural Resource Trade, Cryptocurrency, and Extremist Financing \(La conexión virtual: el comercio ilícito de recursos naturales, la criptomoneda y el financiamiento del extremismo\)](#)

Dan Bruton, 23 de abril de 2025

Este artículo examina evidencia de redes criminales que emplean divisas virtuales para administrar las ganancias derivadas de la explotación ilícita de recursos naturales. También expone las posibilidades que dichas divisas ofrecen a grupos extremistas al utilizarlas como poderosa herramienta con el mismo objetivo. Pone de relieve las coincidencias que existen en los métodos de financiamiento usados por redes criminales y por grupos extremistas.

Nuevas amenazas y tecnologías

[Innovation in AI-Enabled Harms: The Transference of AI Knowledge from Cybercriminals to Extremists \(Innovación en daños facilitados por la IA: la transferencia de conocimientos de IA de ciberdelincuentes a extremistas\)](#)

Yuri Neves y Emily Klein, 8 de junio de 2026

En este artículo se aduce que una aceleración de la convergencia entre ciberdelincuentes y extremistas violentos está facilitando la transferencia de capacidades de IA a espacios extremistas. Esto se debe a que hay quienes pertenecen a ambas comunidades a la vez y al desarrollo de herramientas de IA para prácticas de doxing, acoso y extorsión promocionadas específicamente para comunidades extremistas.

[“Agentic Smurfing”: How AI-Autonomous Micro-Laundering is Outpacing Traditional Terrorist Financing Detection \(Ataques smurf: las operaciones de microblanqueo a cargo de agentes IA están sacando ventaja a los sistemas tradicionales de detección de financiamiento del terrorismo\)](#)

Daria Alexe, 28 de enero de 2026

Este informe analiza los mecanismos técnicos que sustentan el blanqueo de capital realizado por agentes IA, examina su uso por parte de redes que respaldan a Hamás y al ISKP, y propone medidas preventivas prácticas para plataformas tecnológicas y autoridades reguladoras.

[Mapping Terrorist AI Use: Identifying Factors Behind a Relatively Slow Adoption Rate \(Mapeo del uso de la IA en el terrorismo: razones de la tasa de adopción relativamente lenta\)](#)

David Wells, 17 de septiembre de 2025

Este informe pone de relieve la lenta y gradual adopción de la IA generativa por parte de agentes terroristas y extremistas violentos, e intenta describir los efectos relativamente limitados de dicha adopción. Evalúa las razones de esta tasa de adopción, por ejemplo, comparándola con la tasa de adopción de IA generativa por parte de la delincuencia grave organizada (SOC, por sus siglas en inglés) y explorando los factores que influyen en la adopción de nuevas tecnologías por parte de grupos terroristas.

Juventud, reclutamiento y explotación en línea

[Gen-Zs and Ghost Guns: Trends, Threats and Implications \(La generación Z y las armas de fuego de fabricación privada: tendencias, amenazas y consecuencias\)](#)

Rueben Ananthan Santhana Dass, 24 de septiembre de 2025

Este artículo examina las tendencias globales en la relación de jóvenes con armas hechas mediante impresión 3D y pone al día el informe de su autor sobre las tendencias mundiales de proliferación de dichas armas. Estudia la relación de jóvenes con armas de fuego de impresión 3D y los entornos en línea en los cuales circulan conocimientos, archivos y comunidades.



Intervenciones positivas, herramientas y prácticas

[Warning Behaviors for Right-Wing Violent Radicalization on Online Platforms: Conceptual Challenges and Empirical Findings \(Conductas que alertan de una radicalización ultraderechista violenta en plataformas en línea: desafíos conceptuales y resultados empíricos\)](#)

Robert Pelzer, Tobias Weidmann y Sina Weickgenannt, 20 de febrero de 2026

Este artículo presenta los resultados de un amplio estudio empírico sobre Telegram y la aplicación de «señales conductuales de alarma» en la comunicación aceleracionista de ultraderecha en servicios de mensajería. Con base en estos resultados exponemos las implicaciones en la supervisión de las plataformas, la identificación de cúmulos de riesgos, la regulación y la ejecución de las leyes.

[The Exploration of Dialogue-Based AI Interventions in P/CVE: Opportunities, Limits, and Lessons \(Exploración de las intervenciones de IA basada en diálogos en la prevención y lucha contra el extremismo violento: oportunidades, límites y lecciones\)](#)

Kevin Marc Blasiak, 12 de enero de 2026

Este informe parte de anteriores observaciones de un programa de investigación en curso para explorar el potencial de las intervenciones de chatbots de inteligencia artificial (IA), por ejemplo, con agentes basados en diálogo, para abordar las lagunas que existen en el actual panorama de la intervención en línea.

[OSINT: The Digital Force-Multiplier for Extremist Violence \(OSINT: la fuerza multiplicadora digital de violencia extremista\)](#)

Tim Kappler, 3 de octubre de 2025

Este artículo explora el fenómeno en evolución del extremismo impulsado por inteligencia de fuentes abiertas (OSINT), sus efectos estratégicos en el panorama de amenazas, y un conjunto de recomendaciones orientadas a la actuación que van desde la mejora en la moderación de contenidos hasta el intercambio de inteligencia entre plataformas para dificultar la instrumentalización de los datos abiertos por parte de extremistas.

Medidas políticas y regulatorias

[Neither Terrorist nor Criminal: How Hybrid Actors Fall Through Platform Moderation \(Ni terrorista ni delincuente: cómo los agentes híbridos esquivan la moderación en las plataformas\)](#)

Rebecca Fainberg, 30 de septiembre de 2026

Este artículo parte de un estudio de caso de la política de Meta sobre personas y organizaciones peligrosas para explorar cómo al separar la aplicación de políticas contra el terrorismo y contra la delincuencia se crean lagunas que pueden ser explotadas por esos grupos. Se aduce que las plataformas deberían prestar más atención a indicadores conductuales y funcionales de daños en vez de centrarse en la aplicación de políticas con base en la denominación.

Closing the Enforcement Gap: AI, Illicit Liquidity, and the Next Phase of Counter-Terrorist Finance (Cerrar la brecha de aplicación de las leyes: IA, flujos financieros ilícitos y la próxima fase de financiamiento antiterrorista)

Adam Roussele, 24 de octubre de 2025

Este informe explora las nuevas tendencias tecnológicas y regulatorias dirigidas a cerrar la brecha global de aplicación de las leyes. Expone cómo la aplicación de las leyes facilitada por la IA, el mapeo sistémico de flujos financieros ilícitos, y la síntesis multidominio pueden transformar el financiamiento antiterrorista para que pase de la respuesta reactiva a la resiliencia proactiva.

Analysing the FATF's 2025 Global Review of Terrorism Financing for the GNET Community (Análisis de la actualización de 2025 del GAFI sobre financiamiento del terrorismo para la Comunidad de la GNET)

Stephen Reimer, 10 de septiembre de 2025

Este artículo presenta al Grupo de Acción Financiera Internacional (GAFI) y explica su función como autoridad para la creación de herramientas y medidas de lucha contra el financiamiento del terrorismo. Explica también por qué sus preceptos son importantes para profesionales, responsables políticos, investigadores y demás personas que trabajen en la lucha contra el financiamiento del terrorismo.

"Sovereign Solutions" Arrests Raise Questions About Uneven Moderation Policies Across Online Platforms (Los arrestos en Sovereign Solutions plantean preguntas sobre políticas de moderación desiguales en plataformas en línea)

Joseph Stabile, 13 de agosto de 2025

Este informe examina la actividad en línea de sospechosos en tres plataformas: una página de Instagram, una cuenta de YouTube y un sitio web de Sovereign Solutions. Con el análisis, se observa cómo los dueños de las cuentas parecen adaptar sus publicaciones y mensajes en las distintas plataformas a fin de evadir las herramientas de moderación automáticas.

Información Adicional

Sigue a continuación más información sobre GNET:

Pónganse en contacto con GNET: mail@gnet-research.org

Escriban para GNET: <https://gnet-research.org/write-for-us/>

Para suscribirse a la lista de correo de GNET, escaneen el código QR →

