



Contextual Resources: Unpacking the Links Between Terrorism, Violent Extremism, and Crime

Mexico City, October 2026

The following is a collection of Insights exploring the links between terrorism, violent extremism, and crime produced by the Global Network on Extremism and Technology (GNET). GNET is the academic research arm of the Global Internet Forum to Counter Terrorism (GIFCT). GNET's mission is to publish actionable research to better understand and prevent terrorist and violent extremist exploitation of digital platforms. GNET is convened by the Centre for Statecraft and National Security based within the Department of War Studies at King's College London.

Latin America Insights

Regional Context

[From Columbine to Teotihuacán: The Rise of Nihilistic Violence in Latin America](#)

Urszula Mrozowska, 23 June 2026

Building on the attack in Teotihuacán, this Insight examines a selection of recent attacks associated with nihilistic violence across Latin America, adopting a broader regional perspective on the phenomenon and analyzing the circulation of TCC-related social media content that glorifies local perpetrators.

[Shock and Awe: Geopolitical Disruption and Terrorist Narrative Opportunism Online](#)

Sam David, 4 February 2026

Using the Maduro capture as an empirical anchor, this Insight analyzes a trend in which geopolitical events are used as symbolic reinforcement and ideological advancement within TVE narratives online, specifically within jihadist ecosystems. This is indicative of a second-order effect that should be taken into greater account: tactical successes strategically weaponized by militant non-state actors to signal legitimacy in online communities with overlapping areas of grievance.

Global Networks in Latin America

[Reconceptualising Makarenko's Continuum in the Digital Age: The Case of Hezbollah](#)

Adriana Marin, 1 October 2026

This Insight argues that technological innovation is transforming the contemporary crime-terror nexus by enhancing the adaptability, resilience, and transnational reach of Hezbollah's illicit financial networks. In doing so, it argues that the existing crime-terror nexus theory should be expanded to account for the growing role of digital technologies. This expansion would shift analysis beyond traditional forms of criminal-terrorist interaction to consider how digital technologies enable new forms of financial, operational, and transnational convergence.



Hezbollah's Latin American Networks: Stablecoins, Smuggling, and Sanctions Evasion

Adam Roussele, 21 July 2025

This Insight explores how Hezbollah's networks in Venezuela and the Tri-Border Area are adapting to new financial realities, how they exploit regional instability and permissive crypto markets, and what this means for fintech firms, compliance professionals, and policymakers trying to stay ahead of this evolving threat.

Sonic Hate: Examining Brazil's NSBM Scene and Its Global Networks

Ricardo Cabral Penteado, 10 February 2025

This Insight discusses the Brazilian National Socialist Black Metal (NSBM) scene and its role in propagating extremist ideologies, with a focus on transnational connections. Drawing on a dataset of over 100 identified Brazilian bands (active between 1993–2024) and more than 1,000 songs, this study employs network analysis and Natural Language Processing (NLP) to understand how these groups disseminate narratives of hate and reinforce global neo-Nazi networks.

Emerging Threats & Technologies

Cloned Voices and Synthetic Recruiters: Generative AI at the Cartel–Far-Right Nexus

Debaarjun Dasgupta

This Insight discusses the operational overlap in generative AI use between newly designated extremist organizations in Latin America and far-right violent extremist movements. This overlap is treated as tactical convergence within the broader crime-terrorism nexus, rather than as a general survey of AI misuse in the region.

From Kyiv to Culiacán: How Mexican Cartels Are Adapting Drone Warfare Lessons from Ukraine by Gamba Matilde

Matilde Gamba, 28 September 2026

By analyzing specific examples of cartel drone operations alongside emerging evidence of tactical learning from the Ukrainian conflict, this Insight investigates how Mexican drug cartels are adapting drone tactics that have emerged from the Russo-Ukrainian War beyond their traditional use. The Insight further considers what this adaptation reveals about the increasing overlap between criminal and violent extremist approaches to technology-enabled violence. Based on these findings, the Insight puts forward recommendations to mitigate the misuse of commercial drone technologies and disrupt the spread of emerging violent tactics.

Youth, Recruitment & Online Exploitation

Blurred Lines: The Child Safety Gap in the Crime–Terror Nexus by Cecilia Polizzi

Cecilia Polizzi, 29 September 2026

This Insight maps the specific mechanisms – linguistic, cultural, audiovisual, and infrastructural – through which cartel content evades existing tech platform moderation. It explores what this misalignment means for minors, and the broader implications for platforms. The Insight also highlights the shared patterns of the crime-terror nexus, including evasion techniques and pathways of youth engagement.



[Not Just Copycat: Digital Ecology of School-Targeted Violence in Lázaro Cárdenas](#)

Ricardo Cabral Penteado, 5 May 2026

This Insight examines the Lázaro Cárdenas attack not as an isolated tragedy, but as a case that helps illuminate how school-targeted violence is shaped by contemporary digital environments. Rather than presenting a new form of violence, the case shows how familiar elements – including pre-attack leakage in the form of a video posted by the perpetrator hours before the attack, misogynistic signaling, and post-attack recirculation – can converge across platforms in ways that make violent content and symbolic repertoires more visible, recognizable, and reusable.

[From TechHaven to Telegram: How Latin American Youth Are Being Drawn into Jihadist Networks](#)

Maria Zuppello, 11 November 2025

This Insight examines the radicalization transformation that has occurred, focusing particularly on Brazil, and shows how the decentralized web is cultivating an online ecosystem that inspires new lone actors in Latin America.

[Guerrillas Online: Recruitment, Propaganda, and Control by Colombia's FARC-EP Dissidents and ELN](#)

Urszula Mrozowska, 28 July 2025

This Insight analyzes how these two far-left guerrilla groups use social media to improve their digital communication and youth recruitment tactics. It examines their online presence and platform use to maintain territorial influence.

Positive Interventions, Tooling & Practice

[Introducing BR-ECHO: A Tool to Fight Online Extremism in Brazilian Portuguese](#)

Ricardo Cabral Penteado, 11 August 2025

This Insight introduces the BR-ECHO (Brazilian Extremist Content Hashing Observatory), a modular pipeline created to fill this gap. By integrating explainability, adaptability, and traceability, the platform aims to support preventing and countering violent extremism (P/CVE) through linguistically and operationally contextualized tools designed for under-resourced environments.

Global Crime x Terror Nexus Insights

Crime, Terrorism & Violent Extremism Overlaps

[HAYI and State-Cover Networks: The Changing Landscape of Terrorist Financing in Europe](#)

Fabrizio Minniti, 10 June 2026

This Insight examines how terrorist financing in Europe is changing in practice, as organized crime and state-backed violent extremism increasingly overlap, and explores the financial logic of what this Insight terms state-cover networks: deniable, modular structures that use criminal intermediaries to fund and carry out attacks across European jurisdictions.



The Virtual Connection: Illicit Natural Resource Trade, Cryptocurrency, and Extremist Financing

Dan Bruton, 23 April 2025

This Insight examines evidence of criminal networks exploiting virtual currencies to manage the proceeds of illicit natural resource exploitation and illustrates their potential as a powerful tool for extremist groups to achieve the same objective. It also underlines the confluence in the financing methods used by criminal networks and extremist groups.

Emerging Threats & Technologies

Innovation in AI-Enabled Harms: The Transference of AI Knowledge from Cybercriminals to Extremists

Yuri Neves & Emily Klein, 8 June 2026

This Insight argues that an accelerating convergence between cybercriminals and violent extremists is enabling the transference of AI capabilities into extremist spaces. This occurs through shared membership in both communities and the development of AI-powered tools for doxxing, harassment, and extortion specifically marketed to extremist communities.

“Agentic Smurfing”: How AI-Autonomous Micro-Laundering is Outpacing Traditional Terrorist Financing Detection

Daria Alexe, 28 January 2026

This Insight analyzes the technical mechanics underpinning agentic laundering, examines its adoption by ISKP and pro-Hamas networks, and proposes actionable countermeasures for technology platforms and regulatory authorities.

Mapping Terrorist AI Use: Identifying Factors Behind a Relatively Slow Adoption Rate

David Wells, 17 September 2025

This Insight outlines the slow, piecemeal adoption of Gen AI by TVE actors, and tries to characterize the relatively limited impact of this adoption. It assesses the factors behind the rate of adoption, including by contrasting this with Gen AI adoption by Serious and Organized Crime (SOC), and exploring factors that affect terrorist adoption of new technologies.

Youth, Recruitment & Online Exploitation

Gen-Zs and Ghost Guns: Trends, Threats and Implications

Rueben Ananthan Santhana Dass, 24 September 2025

This Insight examines global trends in youth involvement with 3D-printed firearms and updates the author’s report on global proliferation trends of 3D-printed firearms. It surveys youth involvement with 3D-printed firearms and the online environments through which knowledge, files, and communities circulate.



Positive Interventions, Tooling & Practice

Warning Behaviors for Right-Wing Violent Radicalization on Online Platforms: Conceptual Challenges and Empirical Findings

Robert Pelzer, Tobias Weidmann & Sina Weickgenannt, 20 February 2026

This Insight presents findings from extensive empirical research on Telegram and an operationalization of “warning behavior” in accelerationist right-wing communication on messaging services. Building on these findings, we outline implications for platform monitoring, identifying risk clusters, regulation, and law enforcement.

The Exploration of Dialogue-Based AI Interventions in P/CVE: Opportunities, Limits, and Lessons

Kevin Marc Blasiak, 12 January 2026

This Insight draws on early observations from an ongoing research program to explore the potential of artificial intelligence (AI) chatbot interventions, such as dialogue-based agents, to address gaps in the current online intervention landscape.

OSINT: The Digital Force-Multiplier for Extremist Violence

Tim Kappler, 3 October 2025

This Insight explores the evolving phenomenon of OSINT-driven extremism, its strategic effects on the threat landscape, and a set of action-oriented recommendations ranging from enhanced content moderation to cross-platform intelligence sharing to raise the costs for extremists who weaponize open data.

Policy & Regulatory Responses

Neither Terrorist nor Criminal: How Hybrid Actors Fall Through Platform Moderation

Rebecca Fainberg, 30 September 2026

Drawing upon Meta’s Dangerous Organizations and Individuals policy as a case study, this Insight explores how separating terrorist and criminal enforcement creates gaps that these groups can exploit and argues that platforms should place greater emphasis on behavioral and functional indicators of harm rather than designation-based enforcement.

Closing the Enforcement Gap: AI, Illicit Liquidity, and the Next Phase of Counter-Terrorist Finance

Adam Rousselle, 24 October 2025

This Insight explores emerging regulatory and technological trends aimed at closing the global enforcement gap, showing how AI-enabled enforcement, systemic liquidity mapping, and multi-domain synthesis can shift counter-terrorist financing from reactive disruption to proactive resilience.

Analysing the FATF’s 2025 Global Review of Terrorism Financing for the GNET Community

Stephen Reimer, 10 September 2025

This Insight introduces the Financial Action Task Force and explains its authoritative role in shaping CFT tools and measures, including why what it says really matters for practitioners, policymakers, researchers, and others concerned with terrorism financing.



Sovereign Solutions” Arrests Raise Questions About Uneven Moderation Policies Across Online Platforms

Joseph Stabile, 13 August 2025

This Insight examines suspects’ online activity across three platforms: an Instagram page, a YouTube account, and a website for “Sovereign Solutions.” As part of this analysis, it explores how the account owners appear to have tailored posts to evade automated moderation tools, including by adapting their messages across platforms.

Further Information

For additional information about GNET, please see below:

Contact GNET: mail@gnet-research.org

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

To sign up for GNET’s mailing list, scan the QR code →

