



Contextual Resources: Navigating the Nexus of Crime, Terrorism, and Violent Extremism

September 2026

The following is a collection of Insights exploring the intersection of crime, terrorism, and violent extremism 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.

Emerging Threats & Technologies

[A Silent Escalation: Anti-Technology Violence Coming to the Fore](#)

Mauro Lubrano, 17 June 2026

This Insight investigates recent trends in anti-technology extremism, such as attacks on data centers and the firebombing of Sam Altman's house. It assesses this trajectory and the chances of further escalation, then focuses on potential responses and the dangers of over-securitizing legitimate concerns about technology in the wake of these events.

[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.

[Gen-Zs and Ghost Guns: Trends, Threats and Implications](#)

Rueben Dass, 24 September 2025

This Insight aims to shed light on the global trends pertaining to youth involvement with 3D-printed firearms.

Terrorist Financing

Europe

[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.



Middle East & Africa

[Propaganda as Financial Infrastructure: How Islamic State and al-Qaeda Media Ecosystems Enable Terrorist Finance](#)

Adam Roussele, 7 April 2026

This Insight argues that extremist propaganda ecosystems function as trust infrastructures that enable decentralized terrorist financing systems to operate outside.

[Inside Boko Haram's Wallet: Digital Pathways to Terrorist Financing in Nigeria](#)

Abraham Ename Minko, 30 May 2025

This Insight investigates how Boko Haram exploits digital platforms to finance its operations and analyzes the existing counter-terrorist financing framework in Nigeria, highlighting critical institutional and regulatory gaps that allow such illicit financial flows to persist.

[Cash Flow: Breaking Down the Houthis' Multibillion-Dollar Financial Networks](#)

Adam Roussele, 14 May 2025

This Insight explores the Houthis' financing mechanisms, including leveraging technology to evade sanctions and the involvement of foreign facilitators with demonstrable and plausible ties to foreign governments.

South East Asia

[Beyond Hawala: Emerging Online Financing Trends Among South Asian Violent Extremist Groups in 2025](#)

Ashreet Acharya, 5 September 2025

This Insight looks at the rapid evolution of fundraising tactics used by violent extremist groups across South Asia.

[Mapping the Money Trail: The Evolution of Terrorist Financing Networks in Indonesia](#)

Jose Akmal, 10 June 2025

This Insight explores how these groups exploit Indonesia's digital landscape to fund operations more securely and indirectly. The findings aim to help Indonesian and international authorities, along with tech companies, address the growing use of cryptocurrency to finance terrorism.

Latin America

[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.



Emerging Technologies in Terrorism Financing

[“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 Islamic State-Khorasan Province and pro-Hamas networks, and proposes actionable countermeasures for technology platforms and regulatory authorities.

[Closing the Enforcement Gap: AI, Illicit Liquidity, and the Next Phase of Counter-Terrorist Finance](#)

Adam Roussele, 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 toward proactive resilience.

[The Virtual Connection: Illicit Natural Resource Trade, Cryptocurrency, and Extremist Financing](#)

Dan Bruton, 23 April 2025

This Insight examines criminal networks that exploit virtual currencies to manage the proceeds of illicit natural resource exploitation and how extremist groups may achieve the same objective.

Online Ecosystems & Radicalisation Pathways

[From Reaction to Retaliation: How Islamic State Dark Web Ecosystems Processed the San Diego Mosque Shooting](#)

Muskan Sangwan, 15 June 2026

This Insight examines how Islamic State supporters on a dark web communication platform collectively processed and interpreted the San Diego attack in real time. It further explores how these early-stage reactions may offer insight into emerging retaliatory narratives, evolving internet-native forms of radicalization, and potential future threat trajectories following highly publicized religiously motivated attacks.

[Online Spousal Rape Networks: Advancing Violent Misogyny in Real Time](#)

Gazbiah Sans, 15 May 2026

This Insight analyzes how digital infrastructure can enable safe havens for coordinated spousal rape networks and the normalization of violent behavior towards women.

[Sovereign Solutions: Unpacking the Criminal History and Digital Footprint of an Extremist Seller](#)

Joseph Stabile, 13 August 2025

This Insight examines Sovereign Solutions – a Neo-Nazi-linked tactical equipment and training company operated by two military veterans. It explores how the company’s digital footprint reveals sophisticated cross-platform strategies to spread extremist content, evade automated moderation, and organize offline criminal behavior.



Nihilistic Violent Extremism (NVE)

[Distinctive Hallmarks: Investigations into Online Subcultures of Nihilistic Violence](#)

Calia Nocte and Ella Umbra, 26 May 2026

This Insight adopts a behavioral and psychological lens to better understand the dynamics underpinning NVE activity. It examines the defining characteristics of many NVE actors, including their offender profiles, patterns of victimization, pathways to radicalization, and operational methods, concluding with some preventing and countering violent extremism (P/CVE) recommendations to combat this type of threat actor.

[Ecofascist and Nihilistic Extremism: Taking Stock of Evolving Grievances in Targeted Violence Manifestos](#)

Daniel Madsen, 24 April 2026

This Insight investigates the rise (and fall) of eco-fascist grievances in targeted violence manifestos, and the extent to which terrorists may be shifting focus to other forms of grievance.

NVE in Latin America

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

Urszula Mrozowska, 23 June 2026

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 True Crime Community (TCC)-related social media content that glorifies local perpetrators.

[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.

NVE in Europe

[A Growing Global Threat: A Streamed Nihilistic Attack in Italy](#)

Manfredi Pozzoli, 7 May 2026

This Insight analyzes the Trescore Balneario attack and its placement within extremist subcultures online, particularly in non-English-speaking countries.

NVE in South East Asia

[Emerging Extremism Frameworks: Reexamining the 2023 Siam Paragon Attack in Context](#)

Munira Mustaffa, 29 June 2026

This Insight examines the Siam Paragon attack, tracing the conditions that produced the tragedy and situating it within the Participatory Memetic Violence and Misanthropic and Nihilistic Violent Extremism frameworks to inform responses to emerging regional incidents involving underage perpetrators.



Policies, Positive Interventions & Tooling

The 'True Crime Community Spotlight Model': Understanding Digital Pathways and Tumbler Ridge

Allizandra Herberhold, 1 May 2026

This Insight examines the recent Tumbler Ridge attack, explores the risks presented by the TCC, and introduces, in greater detail, a model designed to better identify potential harms at both the individual and community levels.

The Designation of 764 Network: Why Does it Matter?

Tanya Mehra, 16 March 2026

This Insight examines the implications of designating 764 as a terrorist organization in Canada, the European Union, the United Kingdom and the United States, analyzing designation procedures and consequences while assessing the merits and risks of applying this label and offering recommendations for responding to the network's growing threat.

Report | Beyond Extremism: Platform Responses to Online Subcultures of Nihilistic Violence

2 February 2026

This report examines the growing online threat posed by nihilistic violence subcultures, decentralized networks that promote violence, abuse, and exploitation without a clear political, ideological, or religious objective. Unlike traditional extremist movements, these communities are driven by a misanthropic worldview and operate across mainstream and fringe platforms to groom young people, coordinate harmful activities, and glorify violence. The report argues that platforms should move beyond terrorism-focused frameworks and adopt behavioral, ecosystem-wide approaches to prevention, moderation and disruption.

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 AI chatbot interventions, such as dialogue-based agents, to address gaps in the current online intervention landscape.

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). By integrating explainability, adaptability, and traceability, the platform aims to support P/CVE through linguistically and operationally contextualized tools designed for under-resourced environments.

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 →

