TINYg Quarterly Threat Report

Quarter: Q4 2025

Table of Contents

1. Letter from the Editor
2. Regional Threat Assessments
    a. QTR Feature Analysis: Latin America/Caribbean Threat Intelligence Desk
    b. Middle East and North Africa (MENA) Region Threat Intelligence Desk
    c. Sub-Saharan Africa (SSA) Threat Intelligence Desk
    d. Europe Threat Intelligence Desk
    e. North America Threat Intelligence Desk
    f. Asia Threat Intelligence Desk
3. Global Threat Analysis
    a. The Use of AI by Violent Non-State Actors in Cyber Operations
    b. Terrorist Financing
    c. Cartels and Narco Terrorists
4. QTR Spotlight: Barry Palmer
5. Meet Our Team

Letter from the Editor

This quarter was among the most violent and destabilizing periods we have tracked in recent years, both in North America and across the global threat landscape. From mass casualty violence, to sustained insurgent and terrorist activity, Q4 reinforced a reality many security professionals already feel daily: the threat environment is not only persistent, it is fragmenting, migrating, digitalizing, and increasingly personal. The boundaries between terrorism, organized crime, state conflict, and grievance driven violence continue to erode, creating a complex operating environment for governments, the private sector, and civil society alike.

Several trends cut across regions with troubling consistency. Antisemitism continued its sharp rise, manifesting not only as rhetoric and intimidation but as physical violence, vandalism, and credible plotting across multiple countries. This surge is not confined to one ideology or geography; it is amplified by online ecosystems that reward outrage, flatten context, and accelerate mobilization. At the same time, the global reach of jihadist narratives remained evident. The ISIS inspired, antisemitic shooting in Australia underscored how distant conflicts and propaganda ecosystems can converge and materialize into real world violence far from traditional theaters, reminding us that lone actor and small cell threats remain among the hardest to detect and disrupt.

In Latin America and the Caribbean, the arrest of Nicolás Maduro marked a historic inflection point, but not a clean break. As our feature analysis details, U.S. kinetic activity and expanded legal pressure against drug trafficking organizations have disrupted entrenched criminal networks while simultaneously introducing new risks. Maritime strikes, the use of terrorism designations against cartels, and a more muscular posture toward transnational crime may deter some actors, but they also create incentives for adaptation, convergence, and retaliation. The fallout from Venezuela is already rippling across migration routes, coastal economies, and regional diplomacy, with longer term consequences still unclear.

Elsewhere, familiar patterns intensified. In the Middle East and North Africa, maritime insecurity, terrorist financing innovation, and state intelligence activity continued to strain regional stability and global commerce. In Sub Saharan Africa, jihadist groups demonstrated how economic warfare, not just violence, can hollow out state authority and expand influence. Europe faced sustained hybrid sabotage and persistent extremist risk, underscoring how infrastructure and public trust have become primary targets. In Asia, unresolved insurgencies and cross border militancy kept pressure on fragile security balances.

North America, however, remained a sobering focal point for violent extremism. This quarter saw continued mass casualty violence, the expanding overlap between extremism and gun crime, and growing concern over how technology accelerates radicalization. These trends are not abstract. They play out in schools, workplaces, places of worship, and campuses.

It is with that reality in mind that we close this report with our spotlight interview with Barry Palmer. We spoke with Barry just weeks before the tragic shooting at Brown University. In hindsight, his reflections on campus safety, the evolving threat environment, and post-incident resilience now read differently and eerily prophetic. Not because he predicted a specific event, but because our discussion captured a truth many institutions struggle with: security failures are often not about intent alone, but about cumulative strain, perception, and preparedness. We include this interview not to sensationalize tragedy, but to ground this report in the human consequences of the threats we analyze.

As always, the purpose of the QTR is not to alarm, but to inform. Violence is not evenly distributed, nor is it inevitable. But ignoring the patterns emerging across regions, sectors, and communities would be a mistake. This quarter reminds us that vigilance, coordination, and honest assessment remain essential.

Deepest Regards,

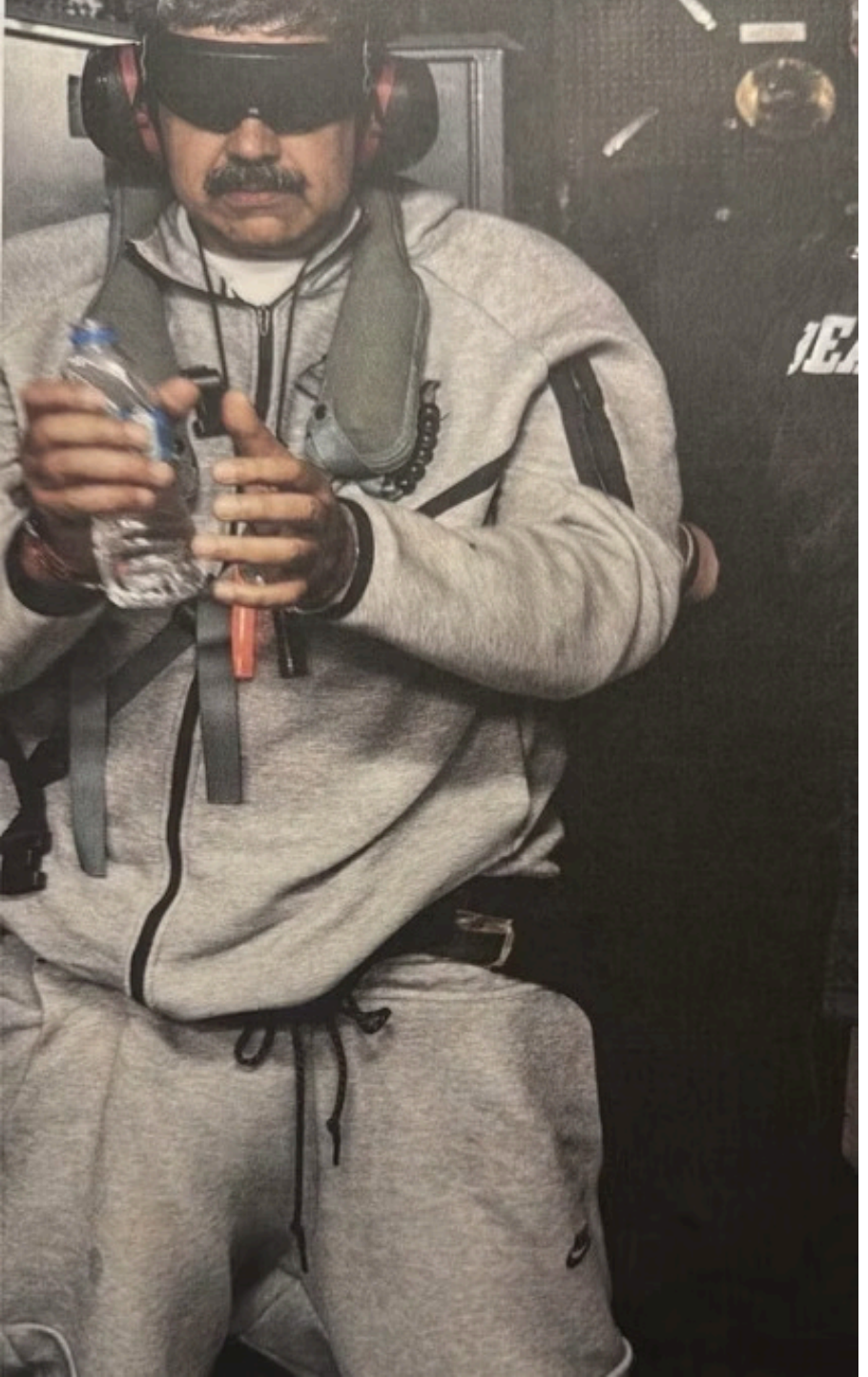
Dr. Donell Harvin
Editor, TiNYg Quarterly Threat Report

GLOBAL SECURITY

Global Security Landscape

Regional Threat Assessments

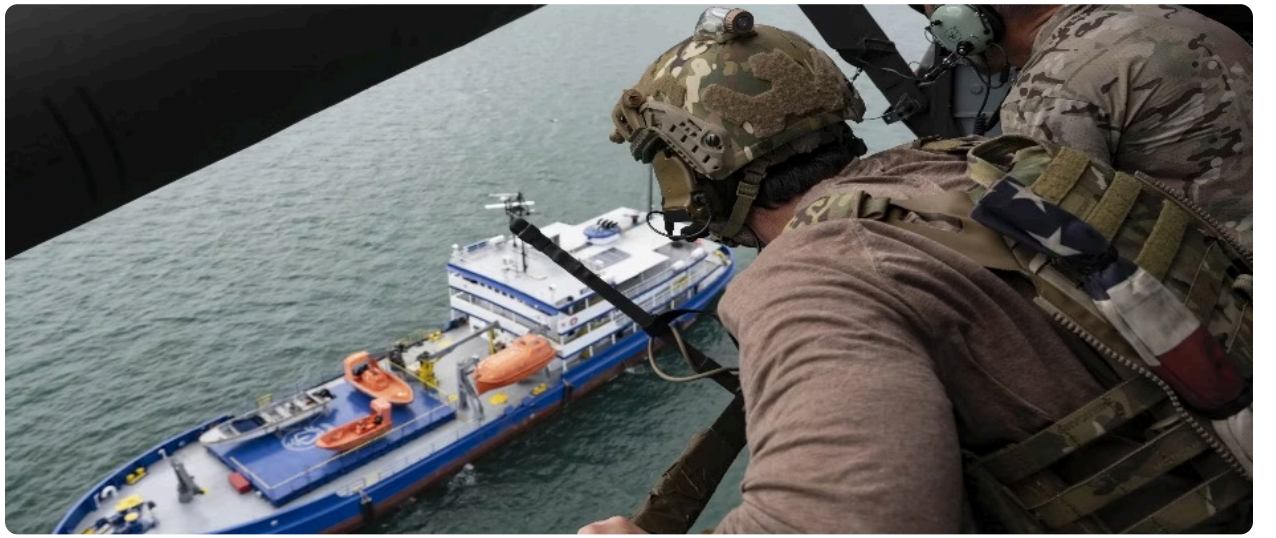
Comprehensive analysis of threat dynamics across six major regions, examining terrorism, organized crime, hybrid warfare, and emerging security challenges that define the current operational environment.



QTR Feature Analysis: Latin America/Caribbean Threat Intelligence Desk

Featured Regional Analysis

The Overthrow of Venezuelan President Nicolás Maduro, Transnational Maritime Escalation and Regional Fallout



Analysts: Aldair Campos, D. Harvin

BLUF (Bottom Line Up Front)

> The overthrow and arrest of Nicolás Maduro has triggered a volatile inflection point in Venezuela and the wider Caribbean Basin, increasing the risk of near-term instability as regime loyalists, armed militias, and transnational criminal organizations maneuver to fill the power vacuum. Concurrent U.S. kinetic operations at sea and the expanding use of terrorism designations against drug trafficking organizations are disrupting entrenched criminal networks such as Tren de Aragua, but also generating diplomatic backlash, potential retaliatory violence, and incentives for deeper convergence between foreign terrorist organizations and criminal groups. Taken together, the dynamic situation in Venezuela and the surrounding countries elevate risks to regional security, maritime safety, migration flows, and private-sector operations, while the long-term impact of Maduro's removal on the activities and behavior of FTOs and DTOs operating in the region remains uncertain.

Tren de Aragua (TDA) is a Venezuelan transnational criminal organization that originated within the country's prison system and has expanded across much of Latin America and into the United States. Intelligence and law enforcement assessments estimate its membership in the low thousands, supported by networks of facilitators and affiliates embedded in migrant smuggling routes across Colombia, Peru, Chile, Ecuador, Brazil, and Central America. The group is involved in extortion, human trafficking, drug trafficking, kidnappings, and contract killings, using extreme violence and intimidation to control territory and populations. Its decentralized structure, ability to exploit migration flows, and convergence with corrupt officials and armed actors make TDA a particularly dangerous threat that increasingly blurs the line between organized crime and terrorism-adjacent violence. **(DOJ, 2025)**

Key Judgments

Maduro's Arrest Creates a Power Vacuum

While still unfolding, the ouster and arrest of Maduro potentially marks a decisive rupture in Venezuela's political order, creating a high risk of short-term instability as competing military, militia, and criminal actors (many who are supporters of Maduro) move to fill the resulting power vacuum, with immediate implications for regional security, migration flows, and transnational criminal activity.

Tren de Aragua (TDA) Expands Amid Instability

Tren de Aragua's (TDA) maritime footprint and U.S. intervention indicate a dangerous cycle of provocation and potential retaliation. The group appears to be testing small-boat violence and sea-borne intimidation tactics. Confidence: Medium–High. (Al Jazeera, 2025; CBS News, 2025)

U.S. Maritime Strikes Escalate

U.S. authorities now treat TDA and other affiliated organizations such as Cartel de los Soles (with Maduro alleged as its leader) as a terrorist organization, applying Foreign Terrorist Organization (FTO) and Specially Designated Global Terrorists (SDGT) frameworks to prosecutions, deportations, and sanctions. Confidence: Medium. (DHS, 2025; CFR, 2025)

Cartel de los Soles Remains Embedded

The late night U.S. military operation to capture Maduro, and persistent lethal U.S. strikes in international waters have triggered protests from Venezuela and concerns from Colombia and Mexico over sovereignty and civilian casualties. Confidence: Medium-High. (WLRN, 2025; Le Monde, 2025)

- Cartel de los Soles is a Venezuela-based transnational drug trafficking network composed of current and former senior military and political officials that functions as a state-embedded facilitator of large-scale cocaine trafficking. While precise membership figures are not available due to its integration within government and security institutions, the network relies on a broad ecosystem of military officers, intelligence officials, logisticians, and criminal intermediaries who leverage control over airfields, ports, border crossings, and security forces to move narcotics through Venezuela toward Central America, the Caribbean, and the United States. The organization has historically favored corruption, protection, and selective violence over mass-casualty intimidation to secure trafficking routes and insulate operations from law enforcement pressure. Its combination of state sanctioning and criminal enterprise makes it uniquely dangerous. (Soufran Center, 2025, Department of State, 2025)

Key Judgments (Continued)

Regional Spillover is Likely

Instability in Venezuela may drive increased migration, smuggling, and criminal expansion into Colombia, Brazil, and Caribbean nations.
Confidence: Medium–High. (ACLED, 2025)

Humanitarian and Migration Pressure Will Intensify

Displacement, food insecurity, and violence are expected to worsen, straining neighboring countries and international organizations.
Confidence: High. (UNHCR, 2025)

Geopolitical Realignment is Underway

Regional and global powers are repositioning in response to Venezuela's instability, with implications for security cooperation and economic partnerships.
Confidence: Medium. (CFR, 2025)

Facts & Background

1. U.S. officials confirmed that a 10th maritime strike occurred in late October 2025, killing six aboard a small vessel near Venezuela (CBS News, 2025; Al Jazeera, 2025).
2. The campaign is framed as a "non-international armed conflict" targeting drug-terror organizations (Council on Foreign Relations, 2025).
3. The Department of Homeland Security (DHS) announced on October 24 the removal of multiple TDA-affiliated gang members from the U.S. (DHS, 2025).
4. The U.S. has expanded its naval presence in the southern Caribbean, deploying a carrier strike group and additional destroyers (Le Monde, 2025).
5. TDA remains active along migrant-smuggling routes into Colombia, Peru, Chile, and Brazil, where it profits from coercion, trafficking, and illicit mining.
6. Think-tank analyses describe the campaign as an evolving "war on cartels" conflict with uncertain outcomes (The Soufan Center, 2025).
7. The Venezuelan Armed Forces have shifted air-defense systems and maritime patrol units to eastern coastal states in response to U.S. naval strikes, raising tension across regional sea lanes. (Reuters, 2025)
8. Fishing cooperatives in Sucre and Nueva Esparta report major economic disruption as fishermen avoid zones where narco-boats and U.S. vessels have clashed, leading to reduced food supply and increased reliance on informal markets.
9. The Maduro regime has reportedly expanded the arming and training of civilian militias and loyalist groups, a move that increases internal militarization, complicates attribution in future security incidents, and heightens the risk of violence involving non-state actors.

Alternative Analysis

Alternative 1: Limited Regional Impact and Relative Stabilization

Despite the arrest of Nicolás Maduro, regional security dynamics may remain largely unchanged or marginally stabilize as entrenched criminal networks, trafficking routes, and corrupt security structures continue to operate independently of individual political figures. In this scenario, successor authorities focus on consolidation and risk reduction, reducing incentives for escalation, large migration surges, or rapid expansion of FTO–DTO cooperation.

Alternative 2: Return to Land Operations/Financial Operations

Facing heavy maritime pressure and legal designation, TDA may scale back sea operations and increase land-based extortion, cybercrime, blackmail, kidnappings, and migrant exploitation behind the coastlines.

Alternative 3: Hybrid Insurgent Orientation

TDA could partner with anti-U.S. or paramilitary factions within Venezuela, Colombia, Mexico, or establish relationships with Middle-East based groups, adopting insurgent branding and asymmetric tactics such as port bombings or ferry sabotage to resist U.S. operations and recruit on ideological grounds

Why This Matters

Maritime Safety

Boat bombings or retaliatory attacks endanger commercial shipping, ferry services, and coastal tourism.

Governance & Sovereignty

U.S. kinetic operations blur the line between counter-narcotics and undeclared warfare, pressuring regional governments.

Policy Precedent

Labeling TDA as both FTO and SDGT creates a template for broader extraterritorial counter-cartel campaigns.

Humanitarian Impact

Migrants traversing TDA-controlled corridors risk cross-fire, recruitment, and human-rights abuses.

Private-Sector Exposure

Port operators, fisheries, and logistics firms face heightened extortion, cargo delays, and sanctions-compliance risks.

Bounties on ICE Officials created by actors outside of the U.S.

Non-U.S.-based actors have reportedly placed bounties on U.S. Immigration and Customs Enforcement personnel, reflecting an escalation in transnational intimidation against U.S. officials, and a potential increased risk to U.S. officials operating domestically and abroad.

Recommendations for TiNYg Member Organizations & Possible Mitigations

1

Maritime Monitoring & Contingency Planning

- Expand Automatic Identification System (AIS) monitoring and anomaly detection for small, unregistered craft operating in known TDA corridor zones.
- Conduct red-team exercises simulating maritime explosions or vessel sabotage near logistics hubs.

2

Information Fusion & Incident Reporting

- Develop a shared database of maritime incidents, vessel-bombing cues, coastal recruitment indicators, and migrant-smuggling nodes.
- Coordinate with regional coast guards to escalate alerts when suspicions of vessel modification or bomb-load changes arise.

3

Legal/Compliance Posture for FTO/SDGT Exposure

- Review vendor and carrier contracts for links to flagged entities; update sanctions screening and internal reporting.
- Prepare communications templates for responding to incidents involving designated entities and U.S. enforcement actions.

4

Community & Migrant Resilience Efforts:

● Partner with NGOs to offer safe-relocation incentives for coastal/migrant populations vulnerable to TDA coercion or recruitment.
● Launch outreach to migrant workers in maritime logistics to raise awareness of recruitment and trafficking risks.

5

Community & Migrant Resilience Efforts:

● Partner with NGOs to offer safe-relocation incentives for coastal/migrant populations vulnerable to TDA coercion or recruitment.
● Launch outreach to migrant workers in maritime logistics to raise awareness of recruitment and trafficking risks.

6

Diplomatic/Norms Engagement:

● Advocate for greater multinational engagement (e.g., through Organization of American States or CARICOM) to define maritime interdiction norms, limit unintended civilian harm, and sustain intelligence sharing.

● Monitor for potential escalation into land-based strikes or broader “war on cartels” messaging that may reshape regional security frameworks.

Over the Horizon Threats

Instability in Venezuela and expanded U.S. counter-DTO operations may drive terrorist and criminal actors to further leverage the Tri-Border Area (TBA) as a permissive hub for financing, logistics, document fraud, and facilitation networks, increasing exposure for regional partners and multinational organizations.

The Tri Border Area (TBA) of Latin America remains a long standing permissive environment for terrorist facilitation and support activities, rather than a hub for overt militant operations. We assess with high confidence that the TBA continues to be exploited by transnational extremist and criminal networks for fundraising, logistics, procurement, and travel facilitation, with Hezbollah representing the most consistently documented foreign terrorist organization associated with the region. We assess with low confidence that there is an imminent attack threat originating directly from the TBA, but with moderate confidence that the area remains capable of supporting external terrorist operations should strategic conditions change. According to available intelligence, Hezbollah is the primary foreign terrorist organization assessed to have a historical and ongoing presence in the TBA.

Methodology

This assessment draws exclusively on open-source intelligence (OSINT) from U.S. government releases (DHS, State Department), major international media (AP, CBS, Al Jazeera, Reuters, Le Monde), and leading research institutions (CFR, The Soufan Center).

Confidence levels adhere to ODNI analytic tradecraft, reflecting corroboration strength, source reliability, and recency.

References

- Al Jazeera (2025, October 24). U.S. conducts 10th deadly boat strike as bombing campaign quickens. https://www.aljazeera.com/news/2025/10/24/us-conducts-10th-deadly-boat-strike-as-bombing-campaign-quickens
- CBS News (2025, October 24). New U.S. strike on alleged drug-smuggling boat kills 6. https://www.cbsnews.com/news/new-us-strike-alleged-drug-boat-kills-6-hegseth-says/
- Council on Foreign Relations (CFR) (2025, October). Global Conflict Tracker: Instability in Venezuela. https://www.cfr.org/global-conflict-tracker/conflict/instability-venezuela
- U.S. Department of Homeland Security (DHS) (2025, October 24). DHS deports Tren de Aragua gang members, sexual predators and violent criminals. https://www.dhs.gov/news/2025/10/24/dhs-deports-tren-de-aragua-gang-members-sexual-predators-and-violent-criminals
- Le Monde (2025, October 24). U.S. sends aircraft carrier to Latin America as military campaign escalates. https://www.lemonde.fr/en/international/article/2025/10/24/us-imposes-sanctions-on-colombia-s-president_6746755_4.html
- Reuters (2025, October 17). How many U.S. strikes on boats near Venezuela have there been? **https://www.reuters.com/world/americas/how-many-us-strikes-boats-near-venezuela-have-there-been-2025-10-17/**
- Reuters Venezuela to boost troops to tackle drug trafficking as US strengthens military in Caribbean", Reuters (2025, September 8) https://www.reuters.com/business/aerospace-defense/venezuela-boost-troops-tackle-drug-trafficking-us-strengthens-military-caribbean-2025-09-08
- The Soufan Center (2025, October 22). Is the United States Preparing for a War with Drug Cartels? https://thesoufancenter.org/intelbrief-2025-october-22/
- WLRN Public Radio (2025, October 24). Venezuela braces for a U.S. military strike — but will it change anything? https://www.wlrn.org/americas/2025-10-24/venezuela-braces-for-a-u-s-military-strike-but-will-it-change-anything
- KCRA News (2025, October 24). U.S. military expands anti-drug strikes into the Pacific Ocean. https://www.kcra.com/article/us-military-drug-trafficking-strikes-pacific/69180862

Middle-East and North Africa (MENA) Region Threat Intelligence Desk

Regional Analysis

Destabilizing MENA Trends: Yemeni Houthi Red Sea Threats, Islamic State Activity, Virtual Assets, Foreign Fighters, and Iranian Espionage

Analyst: Abigail Becker

BLUF

BLUF: Escalating security and intelligence challenges across the Middle East—including intensified Houthi attacks in the Red Sea, a renewed Islamic State campaign in Syria, and expanding Iranian espionage operations—are heightening risks to maritime trade, regional stability, and financial system resilience.

Key Judgments

Houthi Maritime Aggression

Houthi maritime aggression has escalated, with the group sinking two commercial vessels in the Red Sea since early July (OSINT, high confidence).

Islamic State Operations

Islamic State operations have intensified in eastern and central Syria, taking advantage of fragmented post-Assad security conditions (OSINT/HUMINT, high confidence).

Foreign Terrorist Fighters

Foreign Terrorist Fighters in Syrian camps are increasingly leveraging virtual assets and cash couriers to facilitate cross-border financial transfers (FININT/OSINT, moderate confidence).

Iranian Intelligence Activity

Iranian intelligence activity targeting Israel has expanded, evidenced by multiple disrupted plots and recent arrests (OSINT, high confidence).

Facts & Background

- Since July 6, Houthi forces have carried out eight attacks on commercial vessels in the Red Sea, sinking the Magic Seas and Eternity C. This represents the most sustained period of maritime disruption in the region since late 2024.
- From June to October, IS significantly increased its operational tempo around al-Busayrah, Jabal al-Bishri, and al-Sukhna. The group is estimated to maintain a force of 2,500–3,000 fighters, capitalizing on weak governance and fragmented security under Ahmed al-Sharaa's administration.
- Militant networks are increasingly routing funds through virtual assets before converting them into cash. On October 27, authorities in Korea detained an Uzbek national accused of raising $626,000 through digital wallets for militant activity. Additionally, American victims of Hamas's October 7 attacks have filed suit against cryptocurrency exchange Binance and its founder for allegedly facilitating financial transfers to Hamas.
- The al-Hol and Roj camps continue to pose security risks, with foreign fighters exploiting informal financial channels and encrypted communications to sustain external operations.
- Iranian intelligence activity has intensified since the 12-Day War. In September, an American-Israeli national was arrested for allegedly spying on senior Israeli officials, including a former IDF chief. Hundreds of Israeli citizens have also reported receiving recruitment-related phone calls.

Regional Analysis

Maritime Security

Houthi attacks in the Red Sea reflect renewed escalation and improved coordination, aligning with the group's broader regional strategy to maintain influence despite growing constraints on its conventional proxies.

Terrorism

IS cells in Syria continue to exploit weak governance and sectarian tensions, particularly following the March Coastal Events and the July unrest in Suwayda. Their expanding footprint in central Syria indicates a strategic shift toward a sustained, long-term insurgency.

Financing

Virtual assets are increasingly central to sustaining jihadist networks, enabling anonymous cross-border transfers that can be converted into cash within loosely governed environments, including Syrian refugee camps.

Espionage

Iran's intelligence activity against Israel signals a transition from overt logistical support to more covert influence and infiltration efforts. The growing use of dual nationals and insider recruitment highlights increasing operational sophistication.

Alternative Analysis

Alt-1: Houthi activity represents an independent campaign

Low confidence. The scale of weapons employed and the pattern of international responses indicate strong involvement by Iranian state-linked actors.

Alt-2: Islamic State remains weak and fragmented

Medium confidence. Intensified counterterrorism efforts by the U.S.-led Global Coalition may be constraining IS capabilities and limiting its operational coherence.

Alt-3: Recent espionage activity is unrelated to Iran

Low confidence. A substantial number of identified operatives have demonstrated direct ties to Iranian intelligence networks, making this alternative unlikely.

Why This Matters

Commercial operators transiting the Red Sea should expect sustained Houthi targeting of merchant vessels, with likely second-order effects on insurance premiums, routing choices, and delivery timelines. The threat also directly affects Gulf states, particularly Saudi Arabia, whose oil supply lines have already been struck, including the August 31 attack.

Companies operating in or near Syrian markets must factor in renewed IS activity, which threatens overland supply routes, energy infrastructure, and personnel movement across eastern and central Syria.

Banks, fintech platforms, and other financial intermediaries working with regional clients face heightened exposure to terrorist financing schemes involving virtual assets and informal cash couriers. This environment demands strengthened AML/CTF monitoring and enhanced due diligence procedures, particularly for cryptocurrency.

Public and private-sector entities should bolster counterintelligence measures, as Iranian espionage efforts increasingly target civilian, corporate, and government-linked personnel through both human sources and cyber-enabled intrusions.

Aid organizations and international contractors with staff near displaced persons camps in northeastern Syria should reassess operational risk. Extremist networks continue to use camp systems for fundraising, recruitment, and covert financial activities, raising the threat to personnel and programs.

Recommendations for TINYg Member Organizations & Possible Mitigations

1

Improve vessel affiliation and transit risk assessments for Red Sea shipping. Special attention should be paid to Houthi procurement networks and supply chains.

2

Engage with naval escort operations and private maritime security providers.

3

Expand counterterrorism efforts and border security in Syria.

4

Bolster counter-espionage and insider threat programs in Israel.

5

Enhance financial intelligence and counterterrorist financing measures.

Over The Horizon Threats

Drones

Terrorist groups such as IS, Hamas, and the Houthis are increasingly incorporating commercially available drones into their operations. These inexpensive devices are now routinely used for reconnaissance, targeted attacks, and battlefield adaptation. As drone technology becomes more advanced, affordable, and widely accessible, terrorist organizations will likely field more capable systems, improving their precision, range, and operational impact.

Artificial intelligence

While current terrorist use of AI remains limited, such as IS employing AI-assisted tools to translate content for its al-Naba publication, adoption is expected to grow. Future misuse may involve AI-driven operational planning, enhanced propaganda generation, automated targeting support, and other applications that could increase the scale, speed, and lethality of attacks.

Hezbollah rebuild

Despite being severely degraded by the September 2024 pager attack, Hezbollah is showing signs of recovery. The Lebanese government continues to extend political accommodation, including disability benefits to injured members. Recent warnings from senior Hezbollah figures, alongside indications of weapons smuggling through Syria, point to a slow but deliberate effort to rebuild capabilities in southern Lebanon. This poses renewed risks to regional stability.

Gaza

The trajectory of Gaza remains uncertain. Israel's November 20 decision to form a government committee responsible for overseeing phase two of the ceasefire framework, envisioning Hamas disarmament and the introduction of an International Stabilization Force, marks a critical inflection point. Approximately 200 Hamas fighters are believed to be sheltering in tunnels around Rafah, even as Hamas pledged to return the final two deceased Israeli captives by December 2. Continued Israeli strikes, including a November 19 response to Hamas fire near Khan Younis, underscore that kinetic activity will likely persist despite ongoing political negotiations.

Methodology

This assessment integrates open-source intelligence (OSINT), expert analyses, and publicly available reporting. Information was cross-referenced with multiple reputable sources to ensure accuracy, and analytic judgments were derived from corroborated data, historical patterns, and observable trends in regional security dynamics.

Confidence levels adhere to ODNI analytic tradecraft, reflecting corroboration strength, source reliability, and recency.

References

● "המודיעין האיראני מחפש סוכנים": השיחה שקיבלו ישראלים רבים – וההסבר. Ynet, 27 Sept. 2025, www.ynet.co.il/news/article/skilfmrhgx. Accessed 2 Dec. 2025.

● Dulligan, Jake, et al. "The Rising Threat of Non-State Actor Commercial Drone Use: Emerging Capabilities and Threats." CTC Sentinel, vol. 18, no. 3, Mar. 2025, pp. 40–44. PDF file, ctc.westpoint.edu/wp-content/uploads/2025/03/CTC-SENTINEL-032025_article-4.pdf. Accessed 2 Dec. 2025.

● "Mapping Terrorist AI Use: Identifying Factors Behind a Relatively Slow Adoption Rate." GNET, 17 Sept. 2025, gnet-research.org/2025/09/17/mapping-terrorist-ai-use-identifying-factors-behind-a-relatively-slow-adoption-rate/. Accessed 2 Dec. 2025.

● Badran, Tony. "A Year Later, Lebanon Still Won't Stand Up to Hezbollah." The Washington Institute for Near East Policy, 9 Oct. 2024, www.washingtoninstitute.org/policy-analysis/year-later-lebanon-still-wont-stand-hezbollah. Accessed 2 Dec. 2025.

● "October 7 Victims Sue Crypto Exchange Binance for Allegedly Facilitating Payments to Terror Groups." Foundation for Defense of Democracies, 25 Nov. 2025, www.fdd.org/analysis/2025/11/25/october-7-victims-sue-crypto-exchange-binance-for-allegedly-facilitating-payments-to-terror-groups/. Accessed 2 Dec. 2025.

● "The Zionists Should Be Worried: Hezbollah Mulls Response after IDF Strike Eliminates Key Commander." Foundation for Defense of Democracies, 24 Nov. 2025, www.fdd.org/analysis/2025/11/24/the-zionists-should-be-worried-hezbollah-mulls-response-after-idf-strike-eliminates-key-commander/. Accessed 2 Dec. 2025.

● "IDF Ramps Up Strikes against Hamas, Hezbollah Targets across Southern Lebanon." Foundation for Defense of Democracies, 19 Nov. 2025, www.fdd.org/analysis/2025/11/19/idf-ramps-up-strikes-against-hamas-hezbollah-targets-across-southern-lebanon/. Accessed 2 Dec. 2025.

● "IDF Eliminates 6, Apprehends 5 Hamas Terrorists Emerging from Rafah Tunnel." Foundation for Defense of Democracies, 21 Nov. 2025, www.fdd.org/analysis/2025/11/21/idf-eliminates-6-apprehends-5-hamas-terrorists-emerging-from-rafah-tunnel/. Accessed 2 Dec. 2025.

Reference (Continued)

● “Qatar Claims Israeli Strikes in Response to Gaza Shooting May Upend Ceasefire.” Foundation for Defense of Democracies, 20 Nov. 2025, www.fdd.org/analysis/2025/11/20/qatar-claims-israeli-strikes-in-response-to-gaza-shooting-may-upend-ceasefire/. Accessed 2 Dec. 2025.

● “Hezbollah Attempting to Smuggle Weapons through Syria, Rebuild in South Lebanon, IDF Says.” Foundation for Defense of Democracies, 12 Nov. 2025, www.fdd.org/analysis/2025/11/12/hezbollah-attempting-to-smuggle-weapons-through-syria-rebuild-in-south-lebanon-idf-says/. Accessed 2 Dec. 2025.

● “Houthi Maritime Threats and the Gaza Truce: Why Disrupting Supply Chains Is Indispensable.” The Washington Institute for Near East Policy, 2024, www.washingtoninstitute.org/policy-analysis/houthi-maritime-threats-and-gaza-truce-why-disrupting-supply-chains-indispensable. Accessed 2 Dec. 2025.

● Regan, Helen, et al. “Hundreds of Israelis Receive Recruitment Calls from Iranian Intelligence, Israel Police Says.” CNN, 27 Sept. 2025, www.cnn.com/2025/09/27/middleeast/israel-iran-phone-calls-intl. Accessed 2 Dec. 2025.

● Comprehensive Update on Terrorist Financing Risks 2025. Financial Action Task Force (FATF), 2025. PDF file, **www.fatf-gafi.org/content/dam/fatf-gafi/publications/Comprehensive-Update-on-Terrorist-Financing-Risks-2025.pdf.coredownload.inline.pdf**. Accessed 2 Dec. 2025.

● Operation Inherent Resolve Quarterly Report to Congress, Second Quarter Fiscal Year 2025. Office of Inspector General, U.S. Agency for International Development, May 2025. PDF file, oig.usaid.gov/sites/default/files/2025-05/OIR_Q2_FY25_Final_Report.pdf. Accessed 2 Dec. 2025.

● “Spy versus Spy: Iran’s Playbook for Espionage in Israel.” The Washington Institute for Near East Policy, 2024, www.washingtoninstitute.org/policy-analysis/spy-versus-spy-irans-playbook-espionage-israel. Accessed 2 Dec. 2025.

● “Syrian Citizenship, Foreign Fighters, U.S. Red Lines, and Nuances.” The Washington Institute for Near East Policy, 2024, www.washingtoninstitute.org/policy-analysis/syrian-citizenship-foreign-fighters-us-red-lines-and-nuances. Accessed 2 Dec. 2025.

Reference (Continued)

● “US Tells Koreans in Israel to ‘Leave Now.’” Chosun Biz, 27 Oct. 2025, biz.chosun.com/en/en-society/2025/10/27/MC6AH7RU4ZDXHCF2HEMQNOCAPM/. Accessed 2 Dec. 2025.

● Al-Ahmed, Samer, and Subhi Franjieh. “Will Syria Join the Global Coalition to Defeat ISIS?” Middle East Institute, 30 Oct. 2025, www.mei.edu/publications/will-syria-join-global-coalition-defeat-isis. Accessed 2 Dec. 2025.

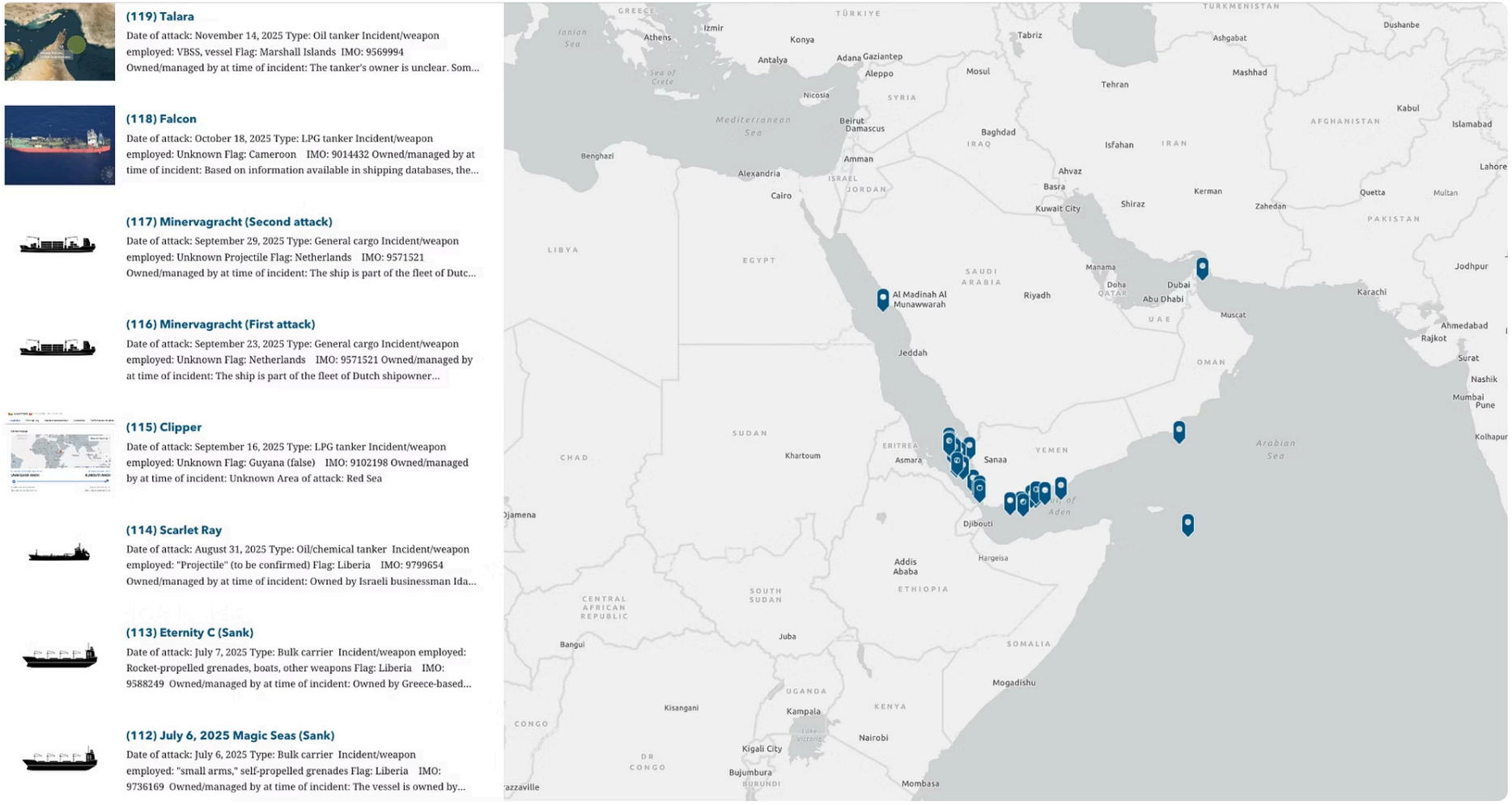
● “Will Syria Join the Global Coalition to Defeat ISIS?” Middle East Institute, **https://www.mei.edu/publications/will-syria-join-global-coalition-defeat-isis**. Accessed 2 Dec. 2025.

● The Global Coalition to Defeat ISIS [issue brief IF10328]. Congressional Research Service, Library of Congress, www.congress.gov/crs-product/IF10328. Accessed 2 Dec. 2025.

● “Israel to Receive Possible Hostage Remains from Gaza for Forensic Tests.” Reuters, 2 Dec. 2025, www.reuters.com/world/middle-east/israel-receive-possible-hostage-remains-gaza-forensic-tests-2025-12-02/. Accessed 2 Dec. 2025.

● “PM Rules Out Granting Safe Passage to 200 Hamas Gunmen Stuck in IDF-held Rafah.” The Times of Israel, 2 Dec. 2025, www.timesofisrael.com/pm-rules-out-granting-safe-passage-to-200-hamas-gunmen-stuck-in-idf-held-rafah/. Accessed 2 Dec. 2025.

MENA Regional Visualization



Source: The Washington Institute for Near East Policy, Noam Raydan and Farzin Nadimi

Interactive Story Map

Sub-Saharan African (SSA) Threat Intelligence Desk

Regional Analysis

JNIM's Economic Warfare in Mali: Blockades, State Erosion, and Escalating Spillover Risks Across West Africa

Analyst: Sam Rosenblum

BLUF

JNIM has imposed a new blockade in central Mali, cutting off key trade and transit routes and further undermining state authority. This tactic is likely to ripple into neighboring countries by disrupting cross-border commerce, straining food and fuel supplies, and creating openings for militant recruitment and expansion into Benin, Togo, and Ghana.

Key Judgments

JNIM Background

Jama'at Nusrat al-Islam wal-Muslimin (JNIM) is al-Qaeda's Sahel affiliate operating mainly in Mali, Burkina Faso, and Niger, with activity extending into Mauritania and Côte d'Ivoire. It emerged in 2017 from a merger of jihadist factions and maintains allegiance to al-Qaeda central and operational ties to AQIM.

Blockade undermines Malian junta authority

JNIM's ability to enforce a sustained blockade demonstrates operational strength and highlights the Malian state's weakening control (Africa Report, Sept 2025).

Regional spillover risk

Cross-border trade disruptions will likely drive economic hardship in coastal West African states, which may increase recruitment opportunities for JNIM and affiliates (Critical Threats, Sept 2025).

Economic warfare is a deliberate strategy

JNIM has shifted to targeting infrastructure and commerce, aiming to destabilize governance and expand influence (ACLED Update, Sept 2025).

Humanitarian strain exacerbates instability

Food and fuel shortages in Mali and neighboring states could worsen grievances against governments, feeding extremist narratives (Critical Threats, Sept 2025).

Facts & Background

- On September 11, 2025, JNIM established roadblocks in western and central Mali, restricting the movement of goods and people (Africa Report, OSINT, high reliability).
- ACLED reporting shows a surge in JNIM activity along strategic trade corridors, including routes toward Benin and Togo (ACLED, OSINT, medium reliability).
- Analysts assess JNIM's blockade as part of an "economic warfare" campaign designed to degrade state capacity and consolidate local legitimacy (Critical Threats, OSINT, high reliability).

Regional Analysis

Terrorism

JNIM's blockade marks an evolution toward economic coercion, amplifying instability across the Sahel and Gulf of Guinea.

- Sustained blockades undermine Malian state authority, force compliance from local populations, and extend militant influence.
- Regional spillover threatens Benin, Togo, and Ghana, where jihadist infiltration is already documented.
- Analysts assign a medium-to-high likelihood of expanded militant taxation schemes along southern trade corridors.

Homeland Security

Regional insecurity has implications for local governments and international stakeholders with personnel and assets in West Africa.

- Humanitarian consequences—food and fuel shortages—will strain already fragile public trust in governments, raising the risk of unrest.
- For foreign governments and companies, staff travel, NGO operations, and supply chains in Mali and its neighbors face an elevated risk of disruption or targeting.
- Western security services may face renewed calls for training and support to the Gulf of Guinea states, paralleling prior Sahel interventions.

Regional Analysis (Continued)

Emerging Threats

JNIM's economic blockade tactic may foreshadow wider adoption of "economic warfare" by regional militant networks.

- Rival groups, including ISIS-Sahel, could copy blockade and taxation strategies, potentially escalating violent competition over trade corridors.
- Expansion into coastal states may give JNIM access to new funding streams and recruitment bases.
- Analysts are tracking whether these tactics evolve into hybrid insurgency models that combine physical control with financial systems, resembling Taliban-style governance.

Alternative Analysis

Alt-1: Blockade is temporary and symbolic

Low. While militant groups sometimes stage symbolic actions, sustained trade disruptions suggest this is a strategic escalation.

Alt-2: Blockade reflects local banditry, not coordinated jihadist strategy

Medium-Low. Criminal groups are active in Mali, but the sophistication and alignment with JNIM's broader "economic warfare" strategy point to deliberate insurgent planning.

Why This Matters

Operational impact

Companies relying on regional trade routes face delivery delays, rising transport costs, and potential loss of access to Malian markets.

Financial risk

Commodity prices—especially fuel and food—are likely to spike, disrupting business continuity and local supply chains.

Security risk

JNIM expansion southward raises the threat environment for private-sector staff, logistics hubs, and infrastructure projects in the Gulf of Guinea.

Recommendations for TINYg Member Organizations & Possible Mitigations

1

Supply chain mapping

Identify dependencies on Malian transit routes; prioritize alternative corridors through Côte d'Ivoire and Senegal.

2

Regional monitoring

Establish regular intelligence checks on JNIM activity near Benin, Togo, and Ghana to anticipate spillover.

3

Stay informed through TINYg alerts

Ensure key staff subscribe to and actively monitor TINYg threat intelligence updates for rapid awareness of new blockades or spillover activity.

4

Business continuity planning

Prepare contingency fuel and food stockpiles for West African operations to mitigate disruption risk.

Over The Horizon Threats

- JNIM may replicate the blockade model along new corridors toward Benin and Togo, potentially establishing sustained taxation systems that rival state authority.
- AQIM and ISIS-Sahel affiliates may adopt similar economic warfare tactics, raising the risk of competitive violence over control of trade nodes.
- **Islamic State–linked ADF insurgency in the eastern DR Congo** – The Allied Democratic Forces (ADF), a jihadist militia aligned with the Islamic State, is escalating its brutal campaign in the Great Lakes region. In November 2025, ADF fighters stormed a Catholic mission hospital in North Kivu (eastern D.R. Congo), massacring about 20 patients – including women in a maternity ward – and burning down the facility. This attack is part of a pattern of intensifying violence: ADF units regularly perpetrate gruesome village raids and massacres on both sides of the DRC–Uganda border, underscoring a growing jihadist threat to civilians in the region (Vatican News, Nov, 2025) (https://www.vaticannews.va/en/church/news/2025-11/drc-kivu-massacre-north-kivu-sisters-hospital.html#:~:text=Democratic%20Forces%29%E2%80%94aligned%20with%20the%20so,Beni)

Methodology and References

This assessment integrates open-source intelligence (OSINT), expert analyses, and publicly available reporting. Information was cross-referenced with multiple reputable sources to ensure accuracy, and analytic judgments were derived from corroborated data, historical patterns, and observable trends in regional security dynamics.

Confidence levels adhere to ODNI analytic tradecraft, reflecting corroboration strength, source reliability, and recency.

References

1. ACLED, Africa Overview: September 2025, https://acleddata.com/update/africa-overview-september-2025, OSINT.
2. The Africa Report, Al-Qaeda affiliate sets up blockade in western Mali to weaken junta, September 2025, OSINT.
3. Critical Threats, JNIM Economic Warfare – Africa File, September 11, 2025, OSINT.
4. "Mali shuts schools as fuel blockade imposed by fighters paralyses country," Al Jazeera, 27 Oct 2025
5. "US warns citizens in Mali to leave country immediately," Reuters, 28 Oct 2025

Europe Threat Intelligence Desk

Regional Analysis

Russian Hybrid Sabotage Pressure and Persistent Terrorism Risks

Analyst: D. Harvin

Source: The Economist https://www.economist.com/graphic-detail/2025/07/22/russian-sabotage-attacks-surged-across-europe-in-2024

BLUF

Europe faced a converging threat picture in Q4 2025 driven by intensifying Russia linked hybrid activity targeting critical infrastructure and sustained terrorism risks, including violent extremist mobilization and jihadist inspired plotting. A series of suspected sabotage incidents, including undersea cable disruption in the Baltic, reinforced the vulnerability of European energy and communications networks and increased operational risk for companies dependent on cross border logistics and connectivity.

Key Judgments

Hybrid sabotage pressure is rising

European officials assess Russia's destabilizing hybrid campaign is intensifying, with growing emphasis on sabotage, information manipulation, and cyber enabled disruption intended to strain European security resources and political cohesion. Confidence: High.

Critical infrastructure remains a primary target set

Recent Baltic cable incidents highlight a persistent risk to subsea infrastructure that supports regional communications and commerce, with spillover potential for financial services, maritime logistics, and energy markets. Confidence: Medium - High.

Terrorism risk remains multi vector

According to Europol, the EU threat environment continues to include jihadist, right wing, left wing, and ethno nationalist drivers, with lone actor and small cell dynamics remaining difficult to detect early and often enabled by online mobilization. Confidence: High.

Policy response is hardening but uneven

EU measures targeting Russian hybrid threats are expanding, but member state threat tolerance, legal thresholds, and operational capacity remain uneven, creating exploitable seams for hostile actors. Confidence: Medium.

Facts & Background

- **Baltic undersea cable disruption:** Finland seized a vessel on suspicion of damaging undersea telecommunications infrastructure between Finland and Estonia, underscoring continued concern about hybrid sabotage in the Baltic region.
- **Documented sabotage trendline:** Open source reporting compiled by major outlets indicates a sustained pattern of arson and sabotage incidents across Europe consistent with warnings from Western officials about a growing campaign.
- **EU sanctions and listings related to hybrid threats:** The EU Council expanded and used restrictive measures frameworks to target actors involved in information manipulation and cyber attacks tied to Russian destabilizing activity.
- **Terrorism baseline:** Europol's TE SAT provides a consolidated view of terrorism activity and arrests across EU member states, supporting continued assessment of a persistent, mixed threat landscape.

Regional Analysis

Cyber and Hybrid Threats

Russia linked hybrid activity is best understood as a blended campaign combining sabotage, cyber operations, and information manipulation to create uncertainty, degrade public confidence, and impose recurring costs on European governments and firms. The operational implication for the private sector is not only the probability of disruption, but also the compounding effect of repeated low level incidents on resilience, insurance, vendor reliability, and crisis communications.

Terrorism

Europe continues to face a persistent terrorism threat across ideological categories based on Europol's assessment, with the most acute near term risk often emerging from lone actors or small networks enabled by online ecosystems and opportunistic targeting. For multinational organizations, the highest exposure remains public facing sites, transportation nodes, and events where low complexity attacks can generate high strategic impact.

Homeland Security and Public Order

Hybrid disruption and terrorism risk interact with domestic polarization by elevating public anxiety, increasing demand on law enforcement, and amplifying disinformation narratives after incidents. These dynamics can accelerate protest activity, copycat attempts, and reputational risk for firms seen as linked to government policy, defense supply chains, or energy infrastructure.

Emerging Threats

The most concerning trajectory is the normalization of sabotage as a tool of state competition and ideological activism, with critical infrastructure and supply chain chokepoints increasingly treated as attractive targets because they enable outsized disruption with limited resources and ambiguous attribution.

Alternative Analysis and Why This Matters

Alternative Analysis

Alt 1: Hybrid incidents are mostly criminal and not strategically coordinated (Medium)

Some events may be opportunistic crime or activism rather than directed operations, and attribution can lag or remain inconclusive.

Alt 2: Deterrence and resilience measures materially reduce disruption in the near term (Medium Low)

Expanded sanctions, investigations, and infrastructure protection could raise costs and reduce frequency, but the current pattern suggests adversaries can adapt quickly with low cost tactics.

Why This Matters

- **Operational continuity:** Subsea cable and infrastructure disruptions can degrade communications, payments, shipping visibility, and safety systems.
- **Financial exposure:** Increased incident frequency raises costs for insurance, security, compliance, and contingency logistics.
- **Personnel risk:** Persistent terrorism and sabotage threats elevate risk for staff movement, public facing sites, and major events.

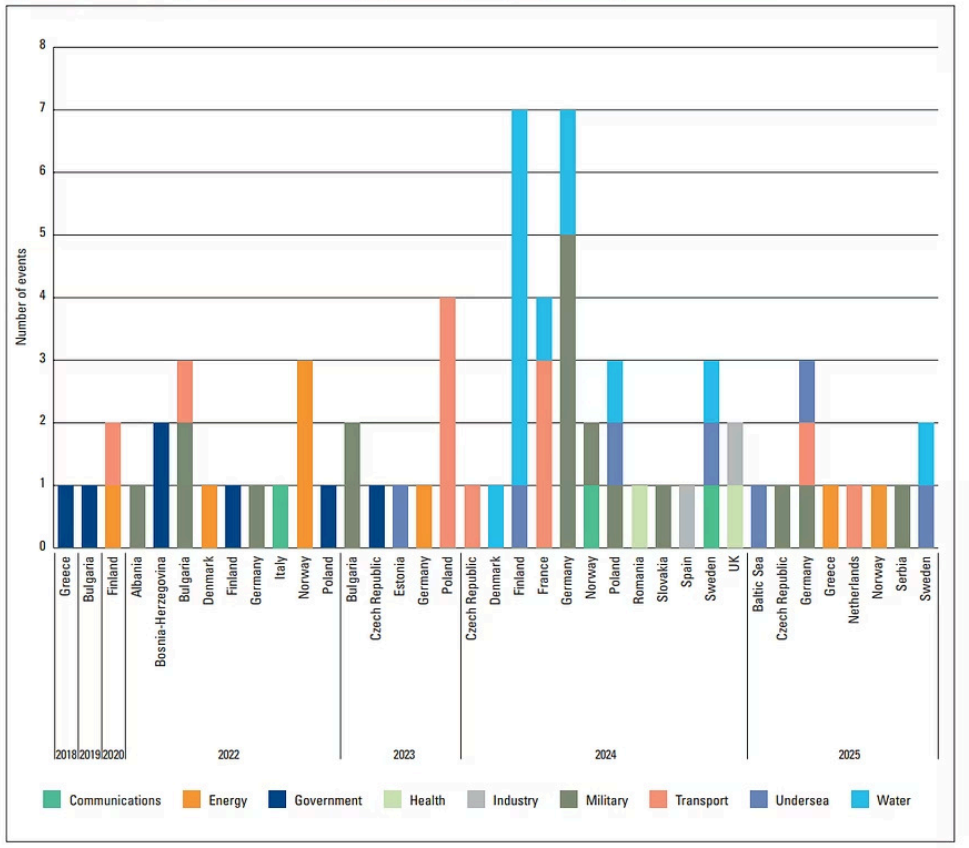
European Sabotage Analysis Visualizations

Note: Energy and communications categories exclude Russian efforts to sabotage undersea cables and pipelines; these actions are counted in the undersea category.

Source: IISS https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/

European Sabotage Analysis Visualizations

Figure 1.1: **Russian hybrid-warfare activity by country and year, January 2018–June 2025**



Notes: All hybrid attacks in 2022 occurred after the beginning of Russia's full-scale invasion of Ukraine. Energy and communications categories exclude Russian efforts to sabotage undersea cables and pipelines; these actions are counted in the undersea category.
Sources: IISS analysis; Armed Conflict Location & Event Data Project (ACLED), www.acleddata.com; Bart Schuurman, 'Russian Operations Against Europe Dataset', https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/TQ0FMQ

While the ECI landscape is broad and complex, IISS data suggests that Russian sabotage and covert opera- the sabotage of submarine cables[20] where failure cascades regionally; and sabotage of water-treatment

Source: IISS https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/

Recommendations for TINYg Member Organizations & Possible Mitigations

1

Critical Infrastructure Protection

- Conduct vulnerability assessments of undersea cables, energy facilities, and transportation networks
- Establish redundant communication systems and backup supply chains
- Coordinate with national authorities on threat intelligence sharing

2

Counterintelligence and Insider Threat Programs

- Enhance vetting procedures for personnel with access to sensitive systems
- Implement behavioral monitoring for indicators of recruitment or coercion
- Train staff to recognize and report suspicious approaches or requests

3

Cyber Resilience and Incident Response

- Deploy advanced threat detection for Russian-linked TTPs
- Conduct tabletop exercises simulating hybrid attack scenarios
- Maintain offline backups and recovery capabilities for critical data

4

Public Safety and Event Security

- Increase security postures for high-profile gatherings and symbolic targets
- Coordinate with local law enforcement on threat assessments
- Develop crisis communication protocols for hybrid incidents

Over The Horizon Threats

- **Escalating sabotage against logistics and communications:** Additional undersea cable incidents and arson or disruption events targeting transport nodes could increase, especially in Baltic and Nordic corridors.
- **Hybrid plus cyber sequencing:** Future campaigns may combine cyber intrusions with physical sabotage to extend downtime and complicate restoration.
- **Ideological spillover and copycat risk:** High visibility disruptions can inspire copycat attacks by extremists and opportunistic actors seeking impact and attention.

Methodology

This assessment integrates open-source intelligence (OSINT), expert analyses, and publicly available reporting. Information was cross-referenced with multiple reputable sources to ensure accuracy, and analytic judgments were derived from corroborated data, historical patterns, and observable trends in regional security dynamics.

Confidence levels adhere to ODNI analytic tradecraft, reflecting corroboration strength, source reliability, and recency.

References

- Reuters (2025-12-31). Finland seizes ship sailing from Russia after suspected cable sabotage in Baltic Sea. https://www.reuters.com/world/finland-suspects-ship-causing-undersea-cable-damage-president-says-2025-12-31/
- European Council (Consilium) (2025-12-15). Russian hybrid threats: Council sanctions twelve individuals and two entities over information manipulation and cyber attacks (PDF). https://www.consilium.europa.eu/en/press/press-releases/2025/12/15/russian-hybrid-threats-council-sanctions-twelve-individuals-and-two-entities-over-information-manipulation-and-cyber-attacks/pdf/
- European Council (Consilium). EU sanctions against Russia. https://www.consilium.europa.eu/en/policies/sanctions-against-russia/
- Associated Press (2025-12-18). Russian Europe sabotage project and incident database. https://apnews.com/projects/russian-europe-sabotage/
- Europol. EU Terrorism Situation and Trend Report (EU TE-SAT) landing page. https://www.europol.europa.eu/publications-events/main-reports/tesat-report
- Europol (2025-06-24). European Union Terrorism Situation and Trend Report 2025 (EU TE-SAT). https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2025-eu-te-sat
- International Institute for Strategic Studies (IISS): The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure. https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/
- UK House of Commons Library (2025-11-28). Sanctions against Russia: What has changed in 2025? (PDF). https://researchbriefings.files.parliament.uk/documents/CBP-10342/CBP-10342.pdf

North America Threat Intelligence Desk

Artificial Intelligence, Extremism, and the Expanding Boundaries of Terrorism in North America

Analysts: Isabella White, Sam Rosenblum

BLUF

BLUF: Extremists actors in North America are increasingly using artificial intelligence to spread ideological propaganda online, accelerating digital radicalization. At the same time, the overlap between extremist motives and gun violence, along with the expansion of terrorist designations, reflects a broader shift in how terrorism is defined and addressed across the region.

Key Judgments

Artificial intelligence is being used by extremists to promote a range of ideological and hate-based narratives - Extremists are experimenting with generative AI to produce and spread propaganda, deepfake content, and recruitment materials (OSINT, high confidence).

Gun violence is increasingly tied to extremist motives - Several shootings in North America have shown mixed personal and ideological elements, blurring the line between terrorism and gun crime (OSINT, medium confidence).

Terrorist designations are expanding - North American governments are increasingly labeling non-traditional groups, including violent extremist networks and gangs, as terrorist organizations (OSINT, medium confidence).

Lone actors remain a main threat in North America - Radicalized individuals continue to act independently, often influenced by online extremist content and mixed ideological motivations (OSINT, high confidence).

Facts & Background

- Artificially generated propaganda and hate content linked to multiple extremist ideologies have been found circulating mainstream and lightly moderated online platforms.
- DHS-FBI reporting continues to identify lone actors inspired by online extremist narratives as a domestic threat.
- August 27, 2025 a mass shooting occurred at Annunciation Catholic School, killing two and wounding 17. The shooter was a lone actor.
- Several mass-casualty shootings in 2025 included evidence of extremist and ideological influence.
- Governments in North America have expanded terrorist designations to include non-traditional entities. The Canadian government classified 764, Maniac Murder Cult and Terrorgram Collective as IMVE networks. Canada is the first country that has classified 764 as a terrorist entity.

Regional Analysis

1

Cyber:

Artificial intelligence is making it easier and faster for extremists to spread messages online. Extremist actors are using AI tools to generate propaganda, fake content, and manipulate media that appear realistic. This allows them to reach more people with less effort and makes it harder for platforms and analysts to identify harmful media before it spreads.

2

Terrorism:

The way terrorism is defined in North America is changing. Authorities are increasingly recognizing that modern terrorism does not only come from well-known organizations and groups. Hate-based movements, lone actors, and some criminal groups are now being treated as terrorist threats when their actions are ideologically motivated or intended to intimidate the public.

3

Homeland Security:

Ideological motives are increasingly present in gun violence cases. Shootings linked to hate, conspiracy beliefs, or ideological grievances are harder to classify and prevent. This overlap complicates responses and challenges existing systems that separate terrorism from other forms of violent crime.

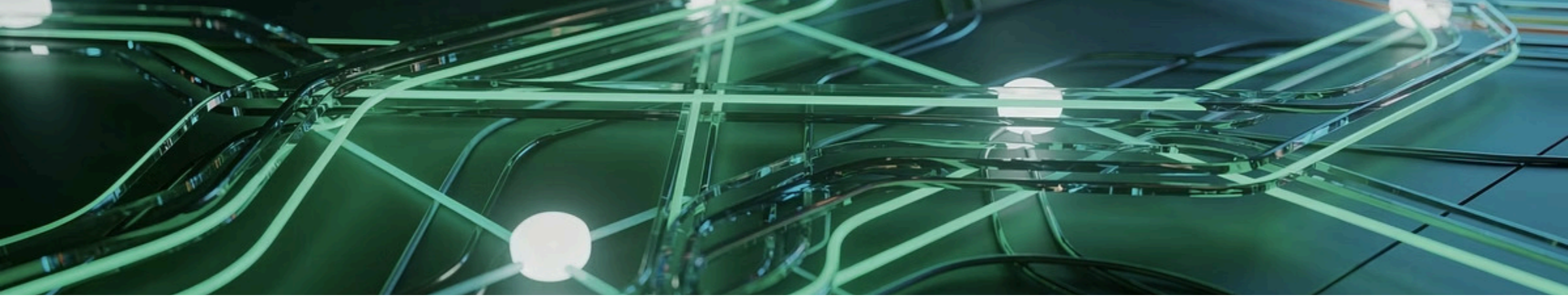
Emerging Threats:

Artificial intelligence-assisted radicalization is still developing but deserves concern. Extremists are beginning to use AI chatbots, automated messaging tools, and online personas to spread their views and engage users. While this activity is not yet widespread, it could increase the speed and scale of online radicalization in the future.

Alternative Analysis

Alt-1: AI's influence on extremism is overstated (Low): The consistency of AI generated material and extremist engagement suggests deliberate and growing use.

Alt-2: Gun violence is unrelated to ideology (Medium): While many incidents are non-ideological, extremist narratives appear with more frequency in attacker online behavior and communications.



Why This Matters

Policy Impact:

Expanded terror designations change how governments track and prosecute extremist activity.

Security Risk:

AI-generated disinformation could lead to increased online radicalization and expose organizations to reputational harm.

Community Safety:

The overlap between terrorism and gun violence complicate prevention and response measures, increasing public safety risks.

Recommendations for TINYg Member Organizations & Possible Mitigations

1

Increase monitoring of AI-generated extremist content. Track media, propaganda, and gate narratives on mainstream and lightly moderated platforms.

2

Improve digital literacy and awareness. Educate staff and communities on recognizing disinformation and extremist messaging generated by artificial intelligence.

3

Monitor updates to terrorist designation lists. Stay informed on newly designated groups that may pose operational or regional risks.

Over The Horizon Threats

1	Extremist actors are likely to expand their use of AI to create propaganda and media that appear increasingly realistic and harder to detect.
2	More extremist activity is expected to move to encrypted platforms.
3	The trend of attackers mixing personal grievances with extremist beliefs is expected to persist, complicating how future incidents are classified and prevented.

Methodology

This assessment integrates open-source intelligence (OSINT), expert analyses, and publicly available reporting. Information was cross-referenced with multiple reputable sources to ensure accuracy, and analytic judgments were derived from corroborated data, historical patterns, and observable trends in regional security dynamics.

Confidence levels adhere to ODNI analytic tradecraft, reflecting corroboration strength, source reliability, and recency.

References

- https://www.policeforum.org/trending13sep25
- https://www.canada.ca/en/public-safety-canada/news/2025/12/government-of-canada-lists-four-new-terrorist-entities0.html
- https://www.gunviolencearchive.org/reports/mass-shooting
- https://www.fbi.gov/news/speeches-and-testimony/worldwide-threats-to-the-homeland-121125
- https://www.fedagent.com/news/lone-offenders-pose-largest-threat-to-us-national-security
- https://www.dhs.gov/national-terrorism-advisory-system

Asia Threat Intelligence Desk

Pakistan and Tehrik-e Taliban Pakistan (TTP) Border Clashes

Analysts: Kushal Ganji, Isabella White

BLUF

Violence between Pakistan and the Tehrik-e Taliban (TTP) along the Afghan border has spiked, with recent raids and suicide attacks producing rising Pakistani military and civilian casualties. Indicators point to cross-border facilitation from Afghan territory, while Pakistan has intensified clearing operations and is publicly pressing the Afghan Taliban to stop TTP sanctuaries.

Key Judgments

TTP attacks will stay high in Khyber Pakhtunkhwa (KP)

Because fighters and helpers operate across the Afghan border, expect more complex strikes on security forces and convoys in the near term.

Pakistan's raids help, but won't fix the problem alone

Clearing operations kill or capture cells, but without Afghan Taliban cooperation, the cross-border pipelines (recruitment, staging, recovery) remain.

Roads, rail, and energy lines are at growing risk

TTP is likely to hit critical infrastructure to cause economic pain and stretch security resources, raising improvised explosive device (IED) ambush danger in KP/Balochistan.

Escalation along the Afghan border is likely

Public pressure on Kabul and a heavy security posture leave little room for de-escalation. One deadly incident or misread signal could trigger more attacks.

Facts & Background

1. From January 1st, 2021, to Sept 26th, 2025, TTP has conducted 862 violent events, most notably in the Pakistan region. This surge of violence has increased steadily since April 2023 (OSINT, high confidence). (ACLED)
2. 19 soldiers and 35-45 militants killed across Bajaur, South Waziristan, and Lower Dir (Pakistan's western border) (OSINT, high confidence). (Al Jazeera)
3. Three Afghan nationals were among five suicide bombers in the Bannu assault. Pakistan publicly blamed Afghan-based TTP/Hafiz Gul Bahadur networks (OSINT, high confidence). (Afghanistan International)
4. TTP operations increasingly use complex assaults (suicide + gunmen), roadside IEDs, and commercial drones for surveillance, complicating perimeter defense (OSINT, high confidence). (DNI)

Regional Analysis

Cyber:
The Chinese state-linked cyber espionage group, UNC3886, is running an ongoing campaign in Singapore, signaling an escalation in state-aligned cyber espionage operations across the Asia-Pacific region.

- These attacks reflect China's state-aligned groups, continued use of **advanced persistent threats** (APTs) to collect strategic intelligence, and weaken regional digital sovereignty. Singapore's public attribution demonstrates a rising concern over systemic cyber threats targeting national infrastructure.

Terrorism:
Lashkar-e-Tayyiba (LeT) and **Jaish-I-Mohammed** (JiM) pose India's most persistent cross-border terrorism threat, using Pakistan-occupied Kashmir as a base to infiltrate fighters, stage high-casualty attacks, and incite unrest in Jammu & Kashmir.

- Their continued access to training, funding, and logistical networks enables them to adapt to Indian counterterrorism measures, keeping the region in a cycle of violence and straining national security resources.

Alternative Analysis

- Alt-1 (Low): TTP violence will fade on its own.

o Assessment: the latest multi-district raids and suicide attacks show building momentum, not a brief spike. As long as support and safe routes from inside Afghanistan continue, the violence is unlikely to ease without cross-border changes.

- Alt-2 (Medium): Pakistan's intensified raids will substantially degrade TTP by the end of the year.

o Assessment: The raids are killing many fighters, but TTP can slip across the Afghan border, regroup, and recruit through scattered cells. Without cooperation from Kabul, a lasting, decisive defeat is unlikely.

Why This Matters

1. Expect more complex assaults on security posts and convoys in KP, raising casualties for officials, contractors, and NGOs operating nearby.
2. Critical infrastructure, such as roads, rail, and energy complexes, face elevated IED/ambush risk, threatening supply chains, project timelines, and costs.
3. With tensions high, a single mass-casualty event could trigger rapid escalation along the Afghan border. It could potentially lead to other countries getting involved.

Recommendations for TINYg Member Organizations & Possible Mitigations

Border Security Enhancements: Strengthening surveillance, rapid response, and intelligence operations along the Pakistan-Afghanistan border can limit insurgent movement.

Diplomatic and Economic Pressure: Collaboration with the Afghan Taliban, combined with leveraging regional partnerships, could incentivize Kabul to take action against TTP sanctuaries.

Regional Cooperation: Cooperation with the United States, Central Asian states, and China through combined security efforts could bolster counterterrorism efforts and stabilize border areas.

Stay up to date with news from TINYg

Over The Horizon Threats

● Over the next quarter, TTP is likely to pursue larger, coordinated attacks in Khyber Pakhtunkhwa, combining suicide teams, small arms, and roadside IEDs, to inflict higher military and political costs on Pakistan. Pakistan's raids will deliver only short pauses before rebound attacks. Expect critical infrastructure targeting (roads, rail, energy lines) to strain security resources and increase economic pressure.

Note: We are not specifically tracking any other developments in the region.

Methodology

This assessment integrates open-source intelligence (OSINT), expert analyses, and publicly available reporting. Information was cross-referenced with multiple reputable sources to ensure accuracy, and analytic judgments were derived from corroborated data, historical patterns, and observable trends in regional security dynamics.

Confidence levels adhere to ODNI analytic tradecraft, reflecting corroboration strength, source reliability, and recency.

References

● Afghanistan International. (2025). *Three Afghans Among Suicide Bombers In Deadly Attack On Pakistani Security Base.* https://www.afintl.com/en/202509082933

● Baruah, P. (2025). *Pakistan's Perilous Gambit: ISKP vs the Taliban and Baloch.* Observer Research Foundation. https://www.orfonline.org/expert-speak/pakistan-s-perilous-gambit-iskp-vs-the-taliban-and-baloch

· DNI. (2022). *Tehrik-e Taliban Pakistan (TTP).* https://www.dni.gov/nctc/groups/ttp.html

● Khan, N. (2025). *Security forces kill seven Pakistani Taliban militants in restive Balochistan province — military.* Arab News. https://www.arabnews.com/node/ 2617633/pakistan

· News Agencies. (2025). *Pakistani raids near Afghan border kill at least 19 soldiers, 35 fighters.* Al Jazeera. https://www.aljazeera.com/news/2025/9/13/pakistani-raids-near-afghan-border-kill-12-soldiers-35-fighters

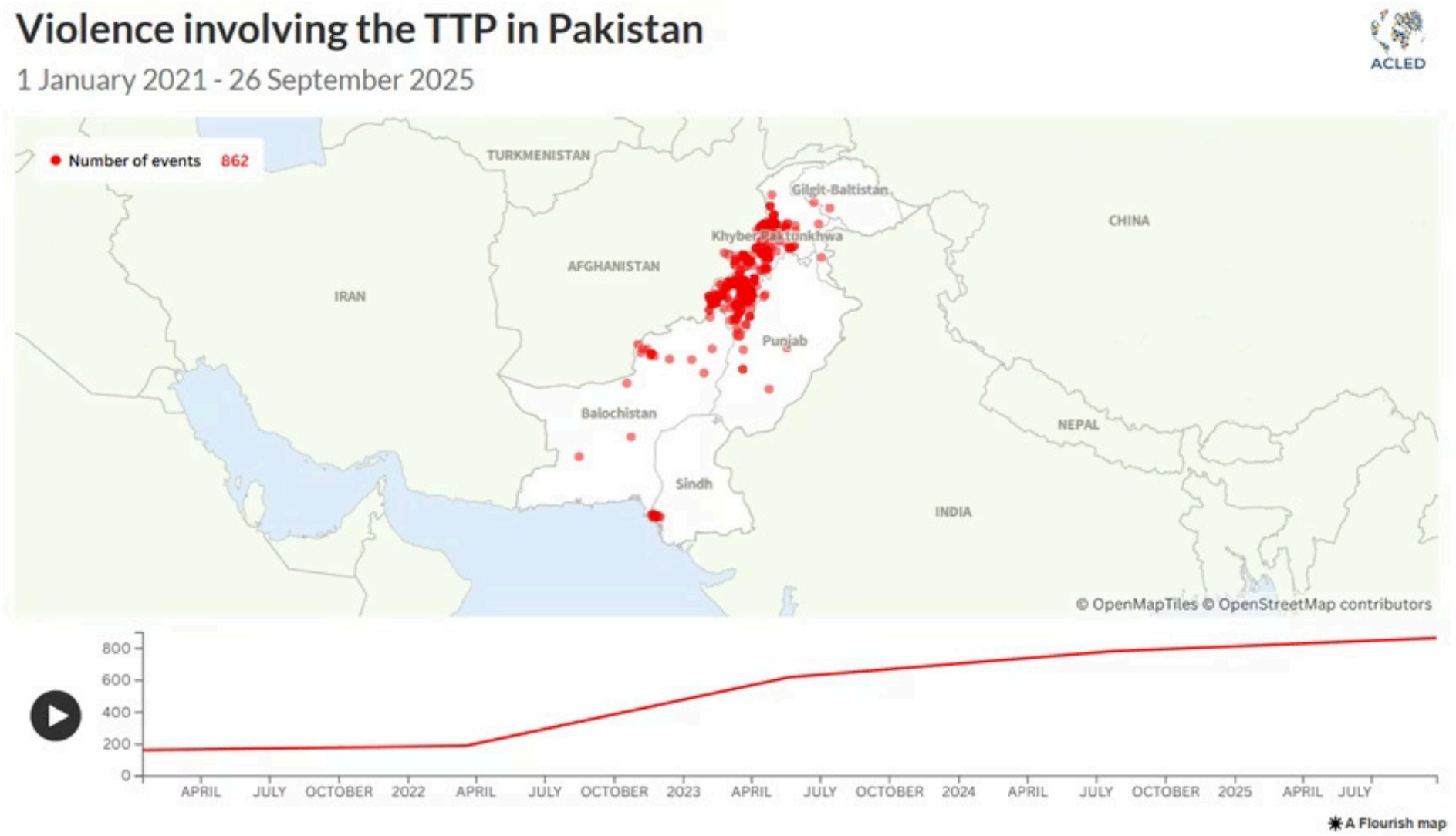
· Pearl, P. (2025). The battle for the borderlands: The Tehreek-i-Taliban Pakistan *challenges the state's control.* ACLED. https://acleddata.com/report/battle-borderlands-tehreek-i-taliban-pakistan-challenges-states-control

● Peltier, E., & ur-Rehman, Z. (2025). *Pakistan Fights Its Fiercest Taliban Insurgency in a Decade.* The New York Times. https://www.nytimes.com/2025/10/06/world/asia/Pakistan-taliban.html

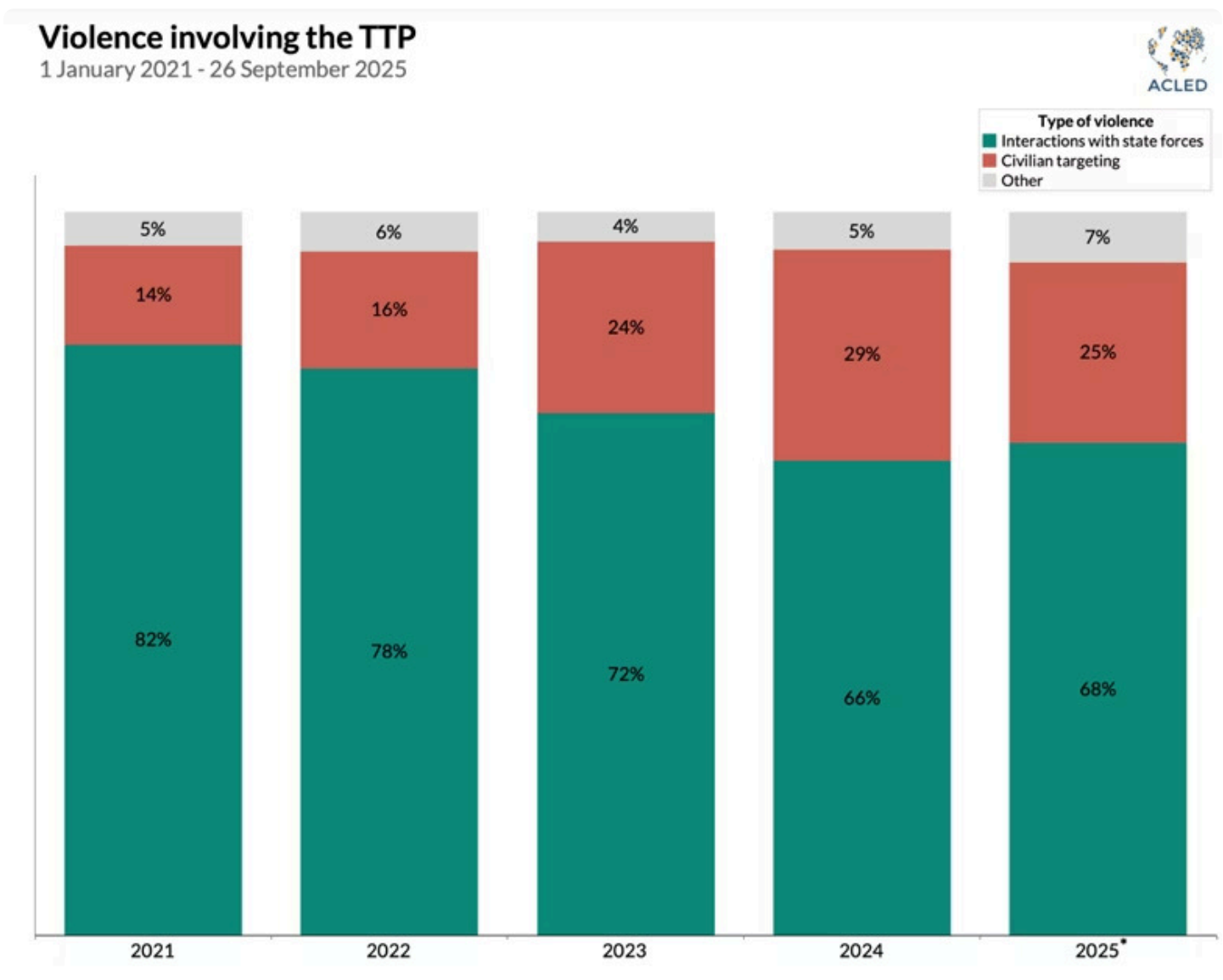
● SpecialEurasia OSINT Team. (2025). *Pakistani Security Forces and TTP Militants Clash at the Afghan Border.* SpecialEurasia. https://www.specialeurasia.com/2025/09/14/*pakistan*-ttp-clash-afghan-border

· ur-Rehman, Z. (2025). Quietly, Pakistan Wages a Deadly Drone Campaign Inside Its Own *Borders.* The New York Times. https://www.nytimes.com/2025/06/19/world/asia/pakistan-drones-militants.html

Graphics

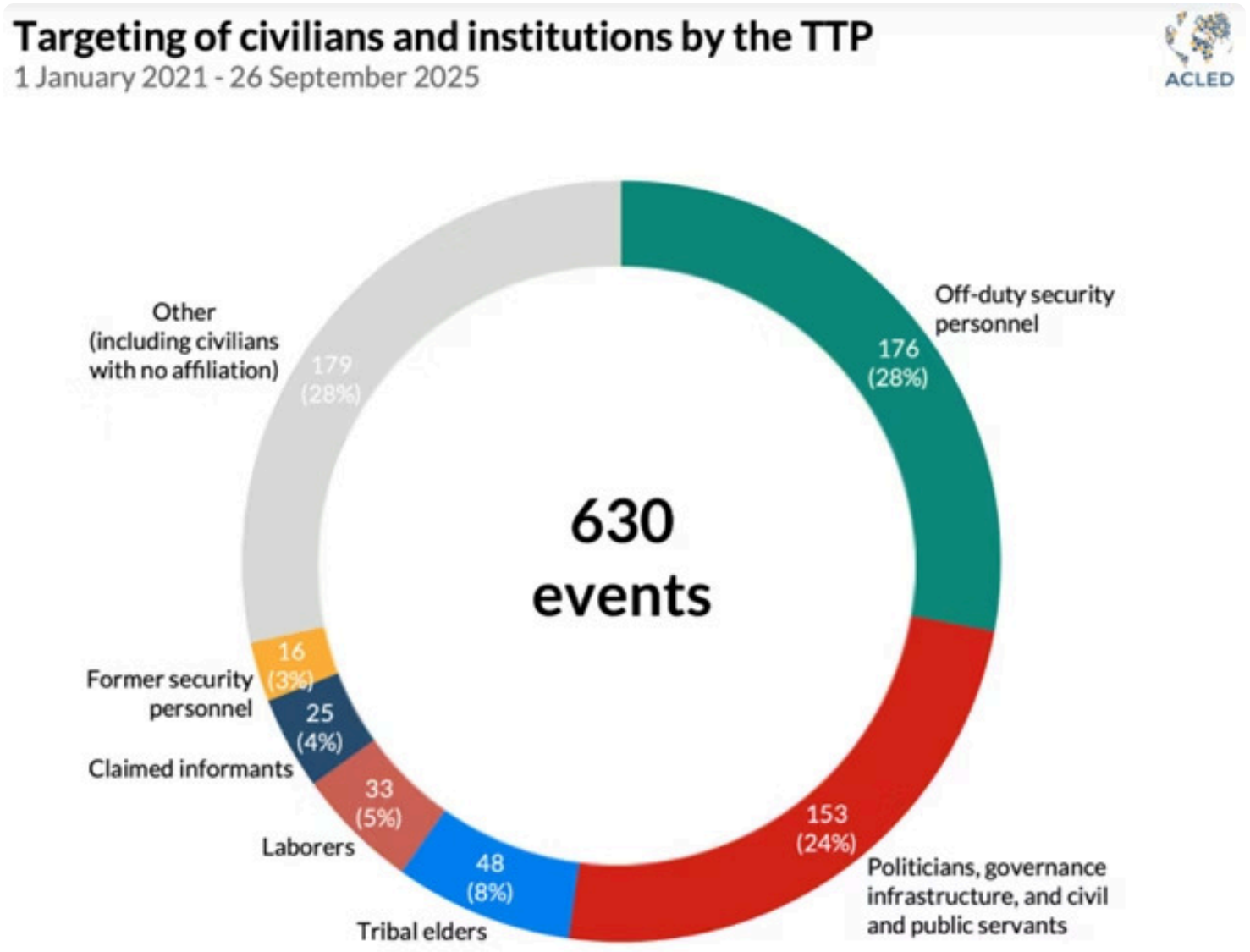


https://acleddata.com/report/battle-borderlands-tehreek-i-taliban-pakistan-challenges-states-control

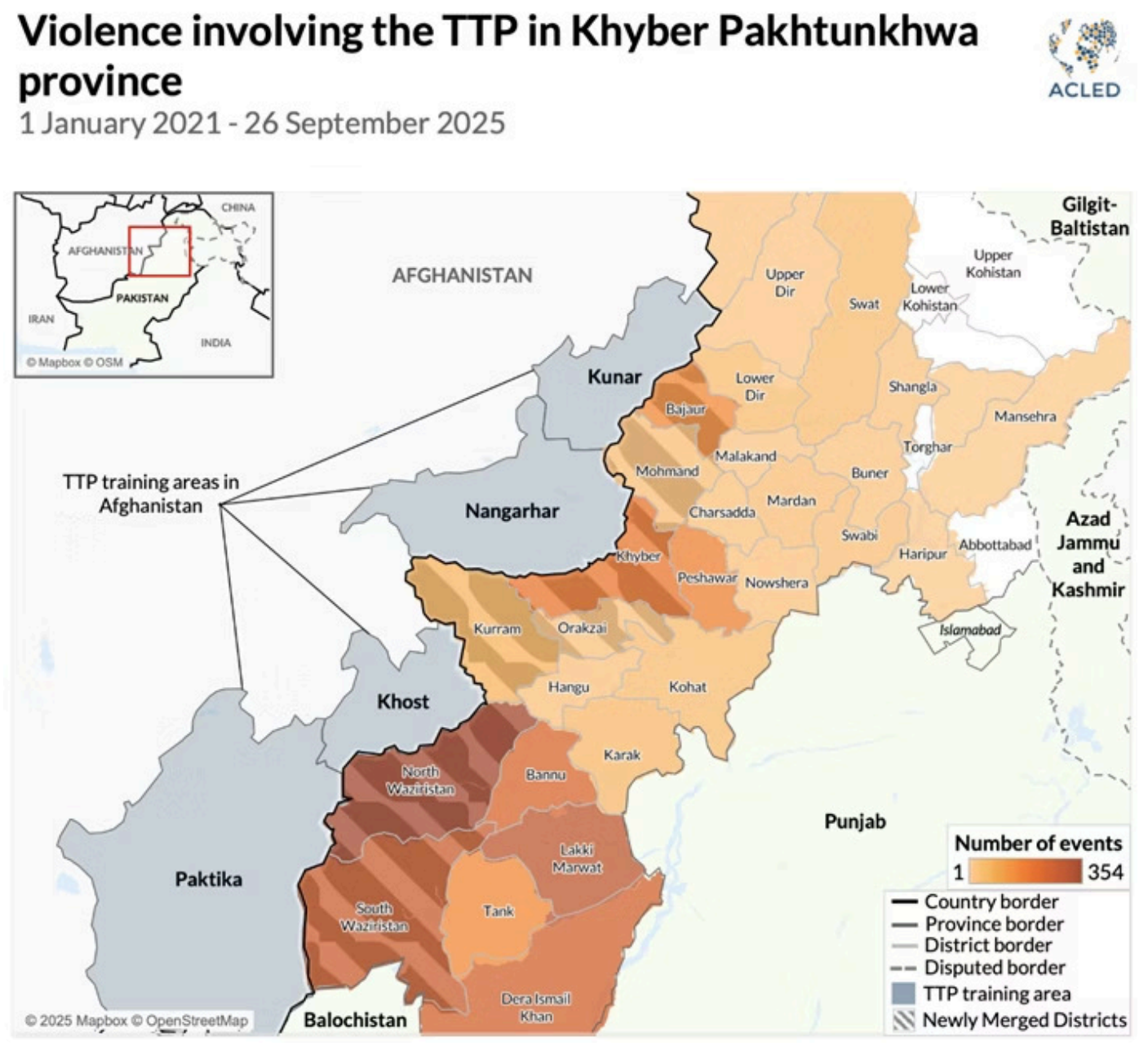


https://acleddata.com/report/battle-borderlands-tehreek-i-taliban-pakistan-challenges-states-control

Graphics (Continued)



Source: https://acleddata.com/report/battle-borderlands-tehreek-i-taliban-pakistan-challenges-states-control



Source:https://acleddata.com/report/battle-borderlands-tehreek-i-taliban-pakistan-challenges-states-control

Global Threat Analysis

The Use of AI by Violent Non-State Actors in Cyber Operations

Nexus between artificial intelligence and violent maligned actors.

Analysts: Kushal Ganji, Bianca Thompson

BLUF

Criminals, hostile actors and terrorists are using generative artificial intelligence (AI) to write better phishing emails, fake voices/videos, and speed up hacking tasks. This makes attacks more frequent and convincing, giving defenders less time to react.

Key Judgments

1. AI will make hacks happen more often and faster Generative AI improves phishing, impersonation, and code customization, so more intrusions with less warning are likely. (**NCSC**)
2. A widening digital divide is coming Some orgs will keep pace with AI-enabled threats; many won't, creating a digital divide that attackers can exploit at scale. (**NCSC**)
3. More actors will gain AI intrusion capability As AI tools spread, criminals will be able to run more capable and efficient operations. (**NCSC**)
4. Greater attack surface in critical infrastructure As AI models/systems are embedded across information technology/operational technology and critical national infrastructure, there's more to attack and more ways in. (**NCSC**)

Facts & Background

1. AI supercharges social engineering. CrowdStrike reports a 442% increase in voice phishing (vishing) from the first half of 2024 to the second half of 2024, as GenAI deception rose. (**Crowdstrike**)
2. AI-assisted phishing is far more clickable. A Microsoft-cited dataset shows AI-automated phishing had a 54% click-through rate vs. 12% for non-AI lures. Additionally, 50% of critical infrastructure security professionals say they faced an AI-powered attack in the past year. (**Axios**)
3. Law-enforcement warning. FBI San Francisco division flags rising use of AI for **business email compromise (BEC) scams**, cloned voice/video, and sophisticated social engineering against businesses and the public. (**FBI**)
4. First documented **agentic-AI** cyber campaign. Anthropic describes a state-linked operation where AI handled ~80–90% of the intrusion workflow across ~30 global targets, executing thousands of requests (multiple per second) before disruption. (**Anthropic**)

Analysis

Use of AI by Terrorist Organizations

Terrorist and extremist groups are adopting generative AI primarily to scale propaganda and recruitment, auto-producing multilingual texts, images/videos, and deepfake audio that mimic trusted voices or witnesses. They use AI tools to target specific audiences (e.g., tailoring narratives by language, grievance, or platform), to automate outreach via chatbots, and to evade moderation by spawning near-duplicate content after takedowns. Beyond influence, AI assists with open-source reconnaissance (translation and summarization of public data), while still relying on humans for execution. The result is faster radicalization pipelines, broader reach across demographics (including minors), and shorter warning windows for defenders, even though fully autonomous "AI attacks" are not the norm today, but could very well be in the future.

Examples of AI usage by terrorist organizations

ISIS and aligned outlets: Generative AI to mass-produce propaganda posters/text and recycle variants across channels.

AI-Qaeda and aligned outlets: Pro-AQ media nodes have circulated posters/images highly likely generated with AI tools.

Hamas/Israel–Gaza conflict propaganda: Multiple actors involved in or commenting on the conflict have pushed AI-generated imagery to influence narratives.

Hezbollah: Included in broader analyses of terrorist/extremist generative-AI exploitation (visuals, translation, and voice cloning).

Neo-Nazi/extreme-right networks (e.g., Terrorgram): Documented early adopters of generative AI for memes and manifestos at scale.

Legislation/guardrails

Executive Order 14110 on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

● Addresses balancing possible benefits and harms of AI usage.

● Used by DHS for interagency cooperation, risk evaluation, and auditing framework.

● Calls for action by the National Institute of Standards and Technology (NIST) and the DHS Chief Data Officer Council

S.299, 118th Congress Artificial Intelligence and Biosecurity Risk Assessment Act

● Addresses the risk of AI use to develop biological and chemical weapons.

● Calls for risk assessment and strategic initiatives by the Assistant Secretary of Preparedness and Response.

Take It Down (TID) Act (2025)

Criminalizes publishing or threatening to publish AI-generated deepfakes (specifically non-consensual intimate imagery)

Requires platforms to remove flagged content within 48 hours and prevent reuploads.

Generative AI Terrorism Risk Assessment Act (Bill)

● Requires DHS and ODNI to submit annual assessments (to Congress) on GenAI misuse by terrorist/violent extremist organizations/individuals

o Requires recommendations for countermeasures

● Analysis focuses on the use or attempted use of GenAI for:

o Propagation and messaging

o Recruitment and radicalization

o Enhancement of CBRN capabilities

Alternative Analysis

Alt-1: AI is hype and does not need to be taken seriously (Low)

Evidence from the FBI/NCSC shows clear gains in realism and volume, especially in phishing and fraud cyberattacks. According to a report by Darktrace, 84% of companies in the Asia-Pacific and Japan (APJ) region believe AI will play a significant role in future cyber threat scenarios. Yet only 42% have formal governance policies for AI use.

Alt-2: Fully autonomous AI attacks are imminent (High)

Currently, people, not machines, are the ones who drive the attacks to use AI to work faster, which is referred to as human-in-the-loop. However, technology, programs, and tools are advancing rapidly, so more automation is expected in the future.

Why This Matters

● Generative AI supercharges phishing and impersonation (including deepfakes), lowering detection/response time and raising compromise rates of secured systems.

● Deepfakes and data leaks hurt trust among stakeholders.

● **Cost:** Recovery, legal, downtime, and supplier impacts add up quickly and are very costly.

● Propaganda and recruitment remain the main cyber use cases. AI speeds up radicalization and widens reach, especially to youth.

● AI lowers the barrier to better targeting and social engineering, raising the risk of disruptive incidents against soft targets and vulnerable third-party networks.

Recommendations for TINYg Member Organizations & Possible Mitigations

1. Continuously conduct security assessments
2. Develop an incident response planDocument that outlines an organization's procedures, steps, and responsibilities in the event of a cyberattack.
3. Employee awareness training
4. Implement AI-powered solutionsLeverage AI-enabled tools to automate security-related tasks, including monitoring, analysis, patching, prevention, and remediation.
5. Stay up to date with news from TINYg

Over The Horizon Threats

● Singapore named China-linked APT UNC3886 for targeting Singapore's critical infrastructure and long-term persistence. (**Reuters**)

● Australia’s spy chief warned Chinese groups are probing Australia’s national telecoms and critical systems, likely pre-positioning for disruption. (**Reuters**)

Methodology

This product draws from open-source intelligence (OSINT), threat assessments, and media reporting. Sources were cross-validated across reputable sources and publicly disclosed information.

References

Anthropic. (2025). *Disrupting the first reported AI-orchestrated cyber espionage campaign.*

https://www.anthropic.com/news/disrupting-AI-espionage

Axios. (2025). *AI is about to supercharge cyberattacks.*

https://www.axios.com/2025/10/25/ai-is-

about-to-supercharge-cyberattacks

Church, Z. (2025). *AI cyberattacks and three pillars for defense.*

https://mitsloan.mit.edu/ideas-

made-to-matter/ai-cyberattacks-three-pillars-defense

FBI. (2024). *FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial*

Intelligence.

https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-

of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence

NCSC. (2025). *Impact of AI on cyber threat from now to 2027.*

https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027

Nelu, C. (2024). *Exploitation of Generative AI by Terrorist Groups.*

https://icct.nl/publication/exploitation-generative-ai-terrorist-groups

Saini, K. (2025). *20 Emerging Cybersecurity Trends to Watch Out in 2026.*

https://www.simplilearn.com/top-cybersecurity-trends-article

Schuster, J. (2025). *2025 CrowdStrike Global Threat Report: China's Cyber Espionage Surges*

150% with Increasingly Aggressive Tactics, Weaponization of AI-powered Deception

Rises.

https://www.crowdstrike.com/en-us/press-releases/crowdstrike-releases-2025-

global-threat-report/

Senate. (2025). *H.R.1736 - Generative AI Terrorism Risk Assessment Act.*

https://www.congress.gov/bill/119th-congress/house-bill/1736/text

Stalinsky, S. (2025). *Artificial Intelligence And The New Era Of Terrorism: An*

Assessment Of How Jihadis Are Using AI To Expand Their Propaganda, Recruitment,

And Operations And The Implications For National Security.

https://www.memri.org/

reports/artificial-intelligence-and-new-era-terrorism-assessment-how-jihadis-are-using-

ai-expand

Stanham, L. (2025). AI-Powered Cyberattacks.

https://www.crowdstrike.com/en-

us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/?__cf_chl_tk=e._

P6D9smmIxAjGtPehrGnWx34JX6gMRnVeSzmWbF9k-1764280793-

1.0.1.1-_SZCMhAa8NXhWm.YzUZKpiwwGRiykI9RqHWUqknz41E

UNCCT. (2021). Algorithms and Terrorism: The Malicious Use of Artificial Intelligence

For Terrorist Purposes. **https://unicri.org/sites/default/files/2021-**

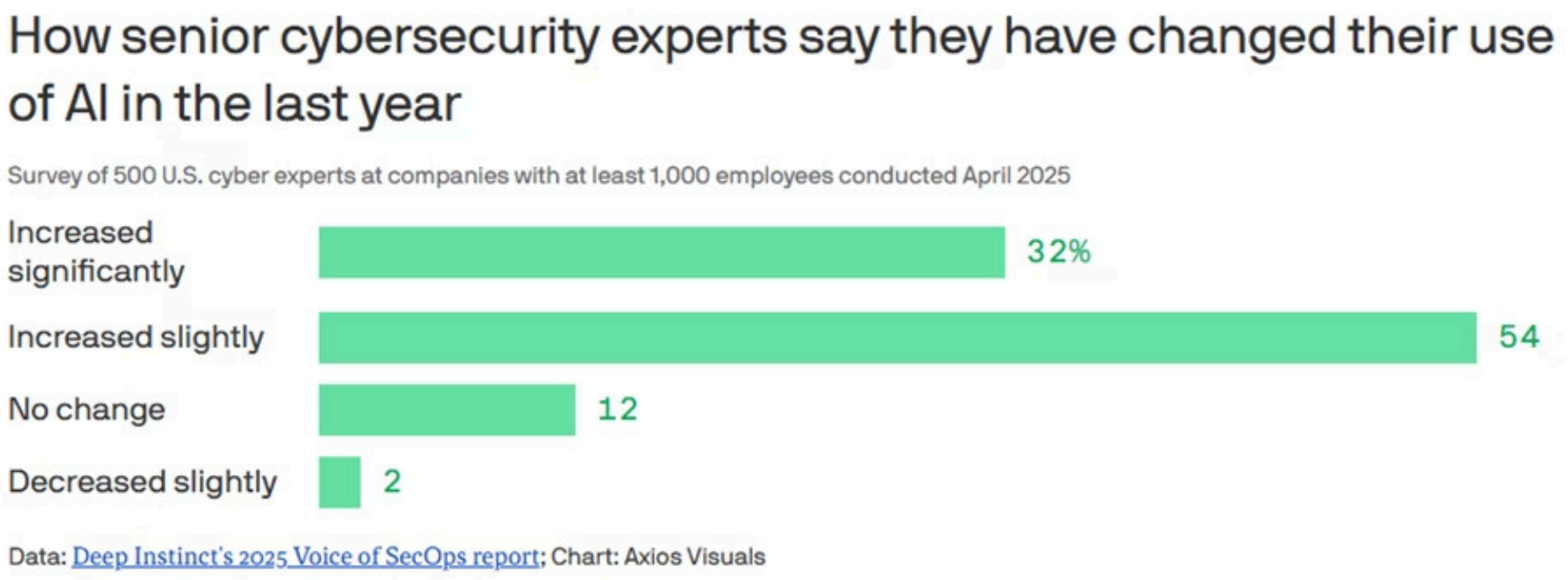
06/Malicious%20Use%20of%20AI%20-%20UNCCT-UNICRI%20Report_Web.pdf

Weimann, G., Pack. A. T., Sulciner, R., Scheinin, J., Rapaport, G., & Diaz, D. (2024).

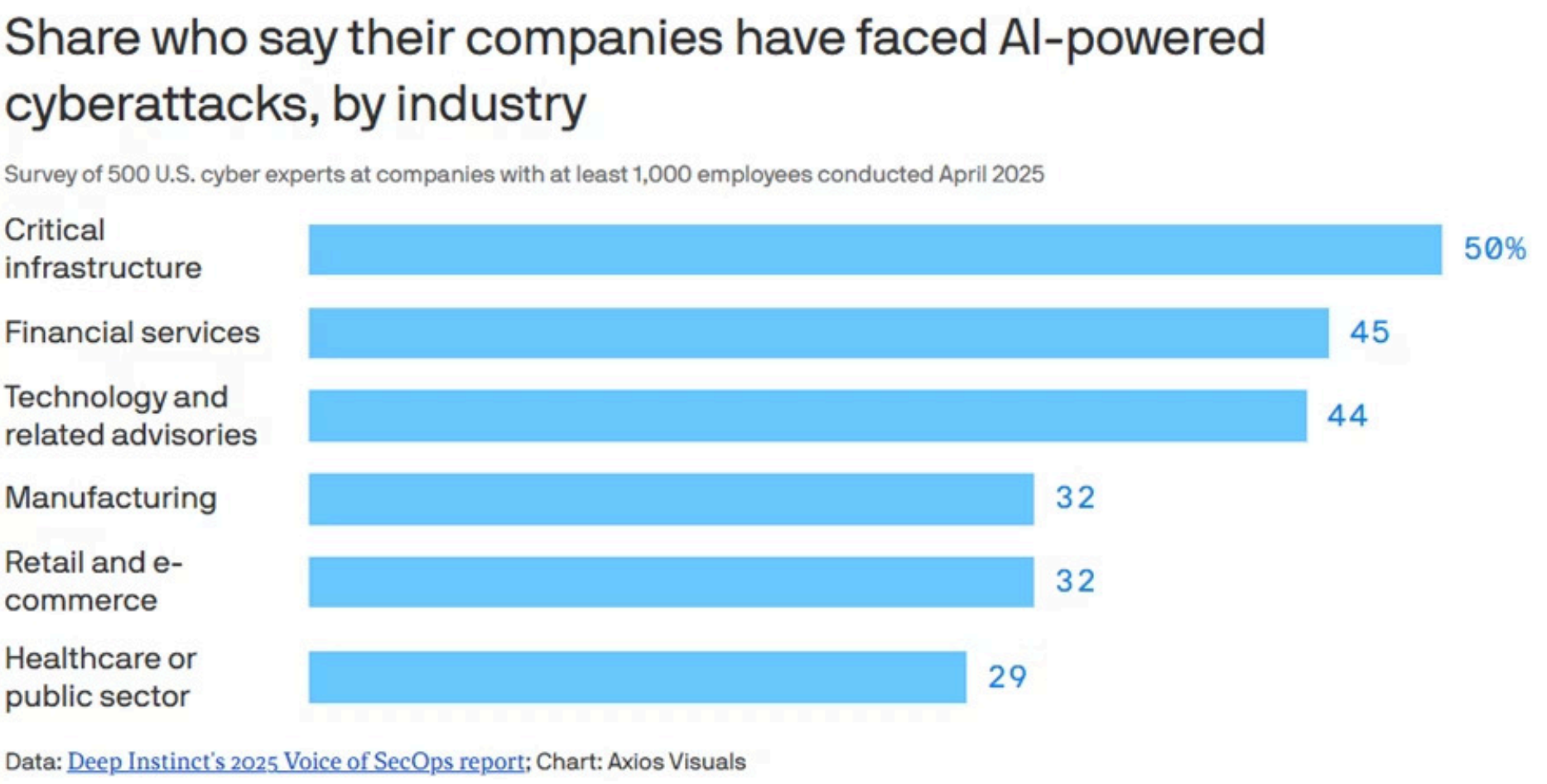
Generating Terror: The Risks of Generative AI Exploitation.

https://ctc.westpoint.edu/generating-terror-the-risks-of-generative-ai-exploitation/

Graphics



Source: https://www.axios.com/2025/10/25/ai-is-about-to-supercharge-cyberattacks



Terrorist Financing

Regional Analysis

AI-Enhanced Crypto Laundering and Terrorist Financing

Analyst: Sam Rosenblum

Screenshot from the Qassam Brigade's Telegram channel asking for donations in bitcoin

Source: CipherTrace https://cointhinktank.com/upload/CipherTrace-CAML-2019-Q3.pdf

BLUF

Terrorist groups are actively experimenting with cryptocurrencies for fundraising, and the integration of AI tools is enhancing money laundering operations. Autonomous AI systems and generative tools can accelerate cross-chain obfuscation, create synthetic identities, and evade compliance controls, escalating the risk of undetected terrorist financing flows.

Key Judgments

1. Terrorist groups are turning to crypto for financing – CTED reports highlight the increasing use of virtual assets by terrorist actors to raise and transfer funds outside formal banking systems (CTED).
2. AI enables new laundering capabilities – TRM Labs assesses that AI-driven autonomous agents can automate laundering pathways, probe weak compliance points, and reduce detection rates in crypto ecosystems (TRM Labs).
3. AI-powered laundering is a growing systemic risk – GlobalRadar notes criminals are using AI to optimize money-laundering strategies, with crypto as a prime vector, signaling future adoption by terrorist financiers (GlobalRadar).
4. Corporate exposure is rising – Organizations that touch crypto — directly or via suppliers — risk reputational and sanctions fallout if terrorist-linked funds move through their networks.

Facts & Background

- In 2025, the TRM Labs 2025 Crypto Crime Report found that sanctioned entities, including known terrorist and extremist-linked wallets, accounted for 33 % of illicit crypto volume. The report specifically notes that terrorist financing via cryptocurrency has “expanded,” with groups increasingly using unhosted wallets, mixers, and privacy coins such as Monero (OSINT, high confidence – TRM labs, 2025)

- In 2025, Islamic State Khorasan Province (ISKP), the Afghanistan-linked affiliate of Islamic State (ISIS), continued to use cryptocurrency to finance its operations (OSINT, high confidence – TRM labs, 2025).

- Reports document how autonomous AI agents are already being tested to launder funds across blockchains and exchanges (OSINT, high confidence – TRM Labs, 2025).

- Generative AI is powering new laundering schemes — including document forgery, transaction layering, and synthetic identity creation — that directly threaten the financial sector’s integrity (OSINT, medium confidence – GlobalRadar, 2024).

Alternative Analysis

Alt-1: AI use in crypto laundering by terrorists is overstated (Medium)

Adoption may remain experimental, with cybercriminal groups leading innovation rather than terrorist financiers.

Alt-2: Regulatory tightening limits growth (Low)

Rapid regulatory action could mitigate risks, though uneven enforcement across jurisdictions makes this unlikely in the near term.

Why This Matters

Operational: Increased potential for undetected terror financing through crypto undermines AML/CFT programs.

Regulatory: Exposure to terrorist-linked crypto flows can trigger sanctions and compliance failures.

Reputational: Corporations risk brand damage if inadvertently linked to terror financing networks.

Recommendations for TINYg Member Organizations & Possible Mitigations

1

Review suppliers and partners for ties to high-risk wallets, mixers, or weakly regulated exchanges.

2

Continue monitoring TINYg intelligence updates for early indicators of AI-crypto laundering threats.

3

Build a response plan for flagged crypto or AI-linked laundering cases

Over The Horizon Threats

The fusion of AI with crypto laundering creates a scalable, low-cost pathway for terrorist financiers to bypass compliance regimes. Terrorist actors are already moving beyond simple Bitcoin donations toward more complex tactics involving privacy coins, mixers, and cross-chain transfers, which AI can further optimize for obfuscation. Generative AI tools allow near-instant creation of synthetic KYC documents and fake identities, enabling rapid account openings at smaller exchanges and DeFi protocols that lack strong oversight. These tactics are especially likely to proliferate in jurisdictions with uneven or permissive regulatory enforcement, creating fertile ground for AI-driven laundering schemes to expand in Q4 and beyond.

References

1. UN CTED, Latest Trends in the Use of Cryptocurrency by Terrorist Groups, Insight Briefing, 2023. **Link**
2. TRM Labs, The Rise of AI-Enabled Crime, 2025. **Link**
3. GlobalRadar, AI-Powered Money Laundering: A Growing Threat to Financial Integrity, 2024. **Link**
4. U.S. Department of Justice, "Justice Department Disrupts Hamas Terrorist Financing Scheme Through Seizure," Press Release, 2023. **Link**
5. TRM Labs, "Category Deep Dive: Use of Crypto in Terrorist Financing Expanded in 2024," Blog Post, 2024. **Link**

Cartels and Narco Terrorists

Regional Analysis

Radicalization Pathways: Tactics, Techniques and Procedures (TTPs) of Latin American Cartels Recruitment and Indoctrination of Minors and Migrants

Analyst: Aldair Campos

Source: Daily Mail
https://www.dailymail.co.uk/news/article-7923611/Mexico-sees-rise-gangs-vigilantes-recruiting-children.html

BLUF

Cartels across Latin America are fusing criminal enterprise with identity-based recruitment, luring vulnerable youth and migrants through social media, false job offers, and "protector" narratives. This evolution reflects a hybrid radicalization model that mixes economic incentives, belonging, and coercion, eroding governance and blurring the line between organized crime and insurgency. The trend presents long-term risks for U.S. and regional partners managing counter-crime and migration operations.

Key Judgments

01

Hybrid Recruitment Model:

Cartels now blend financial incentives with social and moral framing, portraying participation as a way to defend family or community against state neglect. **Confidence: High.** (CSIS, 2025)

02

Youth and Migrant Recruitment:

Minors and displaced migrants remain prime targets. Investigations document children as young as 12 being groomed through gaming chats and social platforms. **Confidence: Medium–High.** (Reuters, 2025)

03

Manpower Demand:

Mexican cartels require roughly 350 new recruits per week to maintain manpower, sustaining a continuous recruitment pipeline. **Confidence: High.** (Prieto-Curiel et al., 2023)

04

Digital Facilitation:

Recruitment and coordination increasingly occur through social-media algorithms, encrypted messaging apps, and video platforms that amplify reach and concealment. **Confidence: Medium.** (CSIS, 2025)

05

Regional Convergence:

Colombian, Venezuelan, and Brazilian groups—such as PCC and Tren de Aragua—are replicating Mexican tactics in border economies and migrant corridors. **Confidence: Medium.** (Atlantic Council, 2025)

Facts & Background

- **Scale of Recruitment:** Estimates place cartel membership between 160,000–185,000, necessitating constant replenishment. (Prieto-Curiel et al., 2023)
- **Digital Pathways:** Cartels advertise false "security" or "driver" jobs via Facebook, Telegram, and TikTok to lure recruits. (CSIS, 2025)
- **Child Exploitation:** Documented cases show minors forcibly trained and indoctrinated after online recruitment. (Reuters, 2025)
- **Economic Drivers:** Chronic youth unemployment remains a primary vulnerability in recruitment zones. (Oxford QEH, 2024)
- **Regional Spread:** Organized criminal networks in Colombia and Brazil use similar recruitment methods to sustain territorial control. (Atlantic Council, 2025)

Analysis

Cartel recruitment increasingly mirrors insurgent mobilization. Economic collapse, migration pressure, and weak governance create ideal conditions for groups to present themselves as employers and protectors. Online propaganda normalizes violence and portrays membership as community service. Migrants and youth in Mexico, Venezuela, and Colombia are particularly susceptible, deepening state fragility and social dependency on criminal structures. (UNICEF LACRO, 2024)

Beyond Mexico, similar dynamics appear in Colombia, Venezuela, and Brazil, where networks like PCC and Tren de Aragua leverage migrant flows and border instability to expand control. In Colombia's frontier regions, these groups now regulate trade and enforce order where the state is absent (Atlantic Council, 2025). UNICEF reporting shows migrant and youth populations facing rising coercion and recruitment risks across Central America and the Caribbean (UNICEF LACRO, 2024). This fusion of crime, protection, and social identity is eroding state legitimacy and entrenching criminal networks as alternative systems of governance.

Emerging Threats

- **Surge in encrypted "job-offer" recruitment via social-media apps.** (CSIS, 2025)
- **Child grooming through gaming and streaming platforms.** (Reuters, 2025)
- **Border-zone hubs linking smuggling logistics with forced enlistment.** (UNICEF LACRO, 2024)
- **Narratives of protection and justice gaining traction in marginalized areas.** (Atlantic Council, 2025)

Alternative Analysis

Transactional Recruitment:

Most join for money or coercion; ideological framing is secondary. (Oxford QEH, 2024)

Proto-Insurgency:

Certain networks intentionally cultivate ideology and loyalty to secure governance functions and legitimacy. (AP News, 2025)

Why This Matters for TiNYg Members

- **Security:** Radicalized recruits resist demobilization and escalate violence. (Reuters, 2025)
- **Governance:** Cartels supplant state authority in underserved regions. (UK Home Office CPIN, 2025)
- **Policy:** Recruitment prevention is more effective than attrition or arrests. (Prieto-Curiel et al., 2023)
- **Humanitarian:** Migrants and minors face severe exploitation and trafficking risks. (UNICEF Innocenti, 2024)

Recommendations for TINYg Member Organizations & Possible Mitigations

1

Expand digital-monitoring and platform partnerships

to identify recruitment posts and coded job ads. (CSIS, 2025)

2

Coordinate with NGOs in migrant corridors

to identify and assist at-risk youth. (UNICEF LACRO, 2024)

3

Incorporate ideological indicators

—loyalty, belief, belonging—into risk assessments.

4

Enhance cross-border intelligence sharing

on facilitators and recruitment networks. (ACLED, 2025)

5

Invest in prevention programs

targeting youth employment and education gaps. (Oxford QEH, 2024)

Outlook for Next Quarter

- Emergence of **cartel training compounds** disguised as legitimate job centers. (AP News, 2025)
- **Micro-recruitment via gaming and social platforms**, reaching beyond Latin America. (CSIS, 2025)
- Growth of **"narco-nationalist" narratives** portraying cartels as social defenders. (Atlantic Council, 2025)

Methodology

This assessment draws on open-source intelligence (OSINT) from investigative journalism, think-tank research, and academic modeling. Confidence levels adhere to ODNI analytic standards, reflecting corroboration strength, recency, and reliability.

References

1. Al Jazeera. (2025, October 24). U.S. conducts 10th deadly boat strike as bombing campaign quickens. https://www.aljazeera.com/news/2025/10/24/us-conducts-10th-deadly-boat-strike-as-bombing-campaign-quickens
2. AP News. (2025). CJNG lures recruits with fake jobs via social platforms. https://apnews.com/article/99f755b7173f101d74e6a1eac333cd38
3. Atlantic Council. (2025, August 7). Five charts that show how criminal organizations in Colombia work and grow. https://www.atlanticcouncil.org/blogs/new-atlanticist/five-charts-that-show-how-criminal-organizations-in-colombia-work-and-grow
4. Center for Strategic and International Studies (CSIS). (2025, May 28). The Role of Social Media in Cartel Recruitment. https://www.csis.org/analysis/role-social-media-cartel-recruitment
5. Courthouse News. (2023, November 2). The recruitment tactics Mexican cartels use to lure victims. https://www.courthousenews.com/getting-in-is-easy-getting-out-is-hard-the-recruitment-tactics-mexican-cartels-use-to-lure-victims
6. El País (Chile). (2025, July 28). Chile reporta la cifra más alta de secuestros en una década: 868 en 2024. https://elpais.com/chile/2025-07-28/chile-reporta-la-cifra-mas-alta-de-secuestros-en-una-decada-868-en-2024.html
7. Oxford Department of International Development, Queen Elizabeth House (QEH). (2024, May 31). Mexican government failing to provide decent jobs for vulnerable youth – leaving door open to cartel recruitment. https://www.qeh.ox.ac.uk/blog/mexican-government-failing-provide-decent-jobs-vulnerable-youth-leaving-door-open-cartel
8. Prieto-Curiel, R., Campedelli, G. M., & Hope, A. (2023). Reducing cartel recruitment is the only way to lower violence in Mexico. arXiv. https://arxiv.org/abs/2307.06302
9. Reuters. (2025, May 28). How Mexico's cartels recruit children and groom them into killers. https://www.reuters.com/world/americas/how-mexicos-cartels-recruit-children-groom-them-into-killers-2025-05-28
10. United Kingdom Home Office. (2025, March). Country Policy and Information Note: Organised Criminal Groups, Brazil. https://www.gov.uk/government/publications/brazil-country-policy-and-information-notes/country-policy-and-information-note-organised-criminal-groups-brazil-march-2025-accessible
11. United Nations Children's Fund (UNICEF) Latin America and the Caribbean Regional Office (LACRO). (2024, December). Children on the Move and Other Crises – Mexico and Central America, Year-End 2024 Humanitarian Situation Report No. 2. https://www.unicef.org/media/168781/file/LACRO-Humanitarian-SitRep-No.2-%28Children-on-the-Move-and-other-Crises---Mexico-and-Central-America%29-Year-End-2024.pdf.pdf
12. United Nations Children's Fund (UNICEF) Innocenti Research Centre. (2024). Children's Involvement in Organized Violence: Regional Trends and Risks. https://www.unicef.org/innocenti/media/9736/file/UNICEF-Innocenti-Child-Violence-Recruit-2024.pdf
13. Armed Conflict Location & Event Data Project (ACLED). (2025, September). Latin America & Caribbean Regional Overview: September 2025. https://acleddata.com/update/latin-america-and-caribbean-overview-september-2025
14. Armed Conflict Location & Event Data Project (ACLED). (2025, February). Latin America & Caribbean Regional Overview: February 2025. https://acleddata.com/update/latin-america-and-caribbean-overview-february-2025
15. Armed Conflict Location & Event Data Project (ACLED). (2025, August). Latin America & Caribbean Regional Overview: August 2025. https://acleddata.com/update/latin-america-and-caribbean-overview-august-2025
16. Armed Conflict Location & Event Data Project (ACLED). (2025, May 30). Violence Targeting Local Officials: 2024 Annual Report. https://acleddata.com/system/files/2025-06/violence-targeting-local-officials-2024-annual-report-30-may.pdf
17. United States Department of Justice, Drug Enforcement Administration (DEA). (2025, July). 2025 National Drug Threat Assessment. https://www.dea.gov/sites/default/files/2025-07/2025NationalDrugThreatAssessment.pdf
18. Latinoamérica21. (2025, July). Dangerous Influencers: Organized Crime on Social Media. https://latinoamerica21.com/en/dangerous-influencers-organized-crime-on-social-media

QTR Spotlight: Barry Palmer

Barry Palmer, BEM is a senior security professional with more than three decades of leadership experience across the protective security sector. His career began in the armed forces, where he served during the conflict in Northern Ireland and the First Gulf War, before moving into a wide-ranging security career spanning the luxury hotel industry, global health organisations, media, and the arts.

Barry has held influential positions on domestic and international boards and committees, and has delivered specialist training and workshops throughout Asia, Africa, Europe, and the United States. In recognition of his significant contributions to counter-terrorism and community security partnerships, he was awarded the British Empire Medal in 2023.

He currently works within the university sector and serves as Chairman of TiNYg UK, where he continues to promote innovation, collaboration, and excellence in global security practice.

> Note From the Editor: We interviewed Mr. Palmer several months before the tragic shooting at Brown University in the United States. The discussion we had around campus safety, while prophetic, is not intended to trigger the reader, nor dishonor the memories of the students killed and injured at Brown.

Interview with Barry Palmer

QTR: How does terrorism impact your industry and profession?

Palmer: Terrorism affects universities in multiple ways, especially in large cities like London. Universities are businesses as well as academic institutions, and attacks directly influence student mobility, recruitment, and perceptions of safety. When incidents occur on public transport or near campuses, it affects attendance, travel patterns, and the willingness of international students and their families to engage with institutions in the UK.

QTR: What are the downstream impacts on international students?

Palmer: International students are often the most affected. Terrorism can influence visa decisions, travel confidence, and whether students feel comfortable studying abroad at all. Even when attacks are isolated, the perception of risk can linger, which impacts enrollment and creates uncertainty for universities that depend heavily on global student populations.

Interview with Barry Palmer (Continued)

QTR: How has the threat environment changed over time from your perspective?

Palmer: The threat feels more persistent and less predictable. Past attacks in London, such as those targeting transport systems, have made people more conscious of everyday vulnerability. That awareness shapes how institutions think about resilience, communication, and student welfare, not just physical security.

QTR: What challenges do universities face in responding to these risks?

Palmer: Universities are open environments by nature. Balancing openness with security is difficult, especially when campuses are integrated into city life. There is also a responsibility to avoid creating fear among students while still acknowledging real risks and preparing for disruption.

QTR: What do you see as an overlooked issue in counterterrorism discussions?

Palmer: The secondary effects often get less attention. Even when universities are not direct targets, terrorism affects transport, housing, staffing, and mental well being. These indirect impacts shape long term institutional stability and student experience more than any single incident.

Interview with Barry Palmer (Continued)

QTR: How do universities balance transparency with the need to avoid panic after an incident?

Palmer: Communication is critical. Universities have to acknowledge incidents quickly and honestly, but they also need to contextualize risk so students and staff do not assume every disruption signals imminent danger. Clear messaging about what is known, what is being done, and where to get support helps maintain trust without amplifying fear.

QTR: What role should universities play in broader resilience and preparedness efforts?

Palmer: Universities are part of the surrounding community, not isolated entities. They should coordinate with local authorities, transport providers, and emergency services, and they should prepare students and staff for disruption without framing everyday life as inherently unsafe. That kind of preparedness supports continuity and reinforces confidence rather than undermining it.

> (Interview edited for length and clarity.)

Meet Our Team

Aldair Campos

TiNYg Senior Fellow, Latin America/Caribbean Desk Analyst

Georgetown University

Master of Professional Studies in Applied Intelligence
Masters

Kushal Ganji

TiNYg Senior Fellow, Asia Desk Analyst

Georgetown University

School of Continuing Studies, Applied Intelligence
Masters

Abigail Becker

TiNYg Intern, Middle East/North Africa (MENA) Desk Analyst

Georgetown University

School of Foreign Service, International Security

Elizabethe Bogrette

TiNYg Intern, Oceana Desk Analyst

Georgetown University

School of Foreign Service, International Security

Meet Our Team (Continued)

Sam Rosenblum

TiNYg Intern, Sub-Saharan Africa (SSA) Desk Analyst

Georgetown University

Walsh School of Foreign Service, International Security

Bianca Thompson

TiNYg Intern, Europe Desk Analyst

Georgetown University

School of Foreign Service International Security

Isabella White

TiNYg Intern, North America Desk Analyst

Randolph-Macon College

Cybersecurity Major

Join Our Team

Interested in TiNYg?

Explore opportunities to contribute to our global analysis.