TINYg
Global Terrorism Information Network

TINYg Quarterly Threat Report Q3 2025

Table of Contents

Letter from the Editor

It is with great pride that we present the inaugural edition of the **TINYg Quarterly Threat Report**. This publication represents a new chapter in our ongoing effort to provide timely, relevant, and actionable counterterrorism and security insights to the global private sector.

Compiled by our talented team of interns, this report reflects the depth of research and analysis that TINYg is committed to fostering. By engaging the next generation of security professionals in meaningful analytic work, we not only enrich our community with fresh perspectives but also strengthen the pipeline of expertise that will carry this field forward.

The assessments that follow cover both regional threat landscapes and thematic areas shaping today's security environment, from terrorism financing to cyber-enabled propaganda. Each section is designed to help our members anticipate risks, adapt strategies, and ultimately make more informed decisions in protecting their organizations, assets, and people.

This initiative reflects TINYg's broader mission: to build a trusted, international network that shares intelligence, promotes collaboration, and strengthens resilience against terrorism and related threats. As outlined on our website, www.tinyg.info, our vision is to bring the very best in counterterrorism knowledge and practice to the private sector, free of cost, and to cultivate a global community where security leaders can learn from one another.

We are confident that this quarterly product will become a valuable resource for you and your teams. We welcome your feedback and look forward to refining and expanding future editions. Together, we can continue to raise the bar for counterterrorism preparedness across industries and geographies. We hope that you find this product insightful, and we welcome your feedback

Sincerely,

Dr. Donell Harvin

Editor, TINYg Quarterly Threat Report

Executive Summary

This quarter brought a mix of continuity and change across global security landscapes. Many of the risks our community has tracked for years remain present, yet several developments now demand fresh attention and urgent action.

In the Middle East and North Africa, Iranian cyber operators increased their focus on financial institutions and logistics firms in the Gulf. Their activity was characterized by credential theft and persistent network intrusions, underscoring the vulnerability of corporate systems that underpin critical trade. Libya once again saw protests disrupt its oil ports at Es Sider and Ras Lanuf, while southern Syria descended into heavy violence in Sweida and Daraa. A trilateral roadmap involving Jordan, Syria, and the United States offers some hope, but conditions on the ground remain volatile.

In Sub-Saharan Africa, Sudan's ongoing war spilled over into neighboring regions, driving illicit arms flows through the Red Sea corridor and raising the stakes for maritime trade and insurance providers. Europe, while relatively stable, experienced unsettling reminders of emerging tactics. Incidents of needle spiking at large events and the proliferation of 3D-printed firearms point to gaps in detection and response capacity.

Across North America, the evolution of domestic violent extremism continues, with online radicalization increasingly intersecting with organized crime networks. In Latin America and the Caribbean, cartels moved further toward hybrid insurgent-style operations. Weaponized drones, improvised explosives, and clandestine mass killings have transformed cartel violence into a destabilizing regional threat that fuels migration and drives fentanyl flows into the United States. Asia remains challenged by persistent separatist violence and transnational extremist networks, sustaining a climate of elevated risk.

Beyond these regional dynamics, several cross-cutting trends warrant urgent action. Terrorist financing increasingly relies on e-commerce platforms and mobile wallets, exploiting weak oversight to disguise illicit transactions as legitimate trade. Cartels are adopting hybrid tactics that blur the line between criminal enterprise and insurgency, with consequences for governance and public health. Extremists are experimenting with artificial intelligence to expand their reach and complicate attribution. Meanwhile, advances in consumer technology—from 3D-printed firearms to drones—are lowering the barrier to entry for violent actors.

For senior leaders, the immediate priorities are defenses against Iranian cyber campaigns, companies with exposure to Libyan oil or Red Sea shipping need

contingency plans to withstand sudden disruptions. Multinationals operating in Mexico and Central America should be preparing now for insurgent-style cartel attacks. Firms engaged in e-commerce and payments must enhance due diligence and tighten monitoring to stay ahead of terrorist financing risks. Event organizers in Europe and North America should ensure security protocols are ready for unconventional threats, from needle spiking to consumer drones.

The threat landscape is evolving quickly, and this quarter's developments highlight the importance of reimagining what we thought was unrealistic or impossible threats previously. Organizations that adapt their defenses and anticipate these shifts will be best positioned to safeguard their people, assets, and operations in the months ahead.

Regional Threat Assessments

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

Analyst: Dr. D. Harvin

BLUF

Iranian cyber campaigns against Gulf finance and logistics, recurring unrest around Libyan oil exports, and escalating violence in southern Syria continue to drive significant security and operational risks across the MENA region.

Key Judgments

- Iranian state-aligned cyber groups, such as APT34, continued to apply pressure on Gulf finance and logistics sectors. These operations focused on credential theft and long-term espionage against financial institutions and energy-linked networks. (High confidence).
- Libyan oil exports were threatened earlier in the year by protests near Es Sider and Ras Lanuf. Although the National Oil Company restored normal

operations, the political disputes that drive these disruptions remain unresolved. (Moderate confidence).

- Southern Syria saw large-scale violence and displacement. A new roadmap developed by Jordan, Syria, and the United States is intended to stabilize Sweida and Daraa, but border security and smuggling risks remain elevated. (Moderate confidence).
- Sudan's civil conflict continues to amplify regional arms flows. The involvement of external actors has increased risks to shipping and transshipment hubs in the Red Sea corridor. (Moderate confidence).
- Despite these recurring disruptions, Libya's National Oil Company is seeking new investment, including a memorandum of understanding with ExxonMobil. This may strengthen resilience in the medium term but does not remove the near-term risk of disruption. (Low to moderate confidence).

Facts & Background

- Multiple threat intelligence reports during June and July highlighted an increase in Iranian cyber campaigns. Groups such as APT34, APT35, and APT39 targeted financial institutions and energy-related logistics companies in the Gulf.
- On January 28, demonstrations in Libya threatened nearly 450,000 barrels per day of output at Es Sider and Ras Lanuf. Although the National Oil Company was able to negotiate a resumption of activity, revenue disputes continue to drive tension into the third quarter.
- Between July and September, violence in Sweida and Daraa displaced more than 160,000 people. On September 16, Syria, Jordan, and the United States announced a stabilization plan covering prosecutions, road security, and humanitarian assistance.
- At the United Nations Security Council, Sudan accused the United Arab Emirates of enabling foreign mercenaries fighting with the Rapid Support Forces. This underscores the continued risk of illicit arms flows affecting the Red Sea and Gulf of Aden.
- On August 4, Libya's National Oil Company signed a memorandum of understanding with ExxonMobil aimed at expanding upstream activity, despite the unstable security environment.

Analysis

Iranian Cyber Activity

These campaigns remain focused on espionage. They typically begin with credential harvesting and proceed through lateral movement to data theft. The tradecraft is

consistent with known Iranian groups such as APT34, APT35, and APT39. Banks, payment systems, and port logistics networks are particular targets. The activity aligns with Iran's strategy of applying pressure through non-kinetic means following regional tensions. For companies, the risk includes business email compromise, third-party exposure, and threats to the integrity of financial and operational data. (High confidence).

Southern Syria and Border Security

The fighting in Sweida and Daraa complicated an already fragmented militant landscape. Claims of an Islamic State resurgence are inconsistent, but smuggling pipelines and cross-border pressures in Jordan remain a serious concern. The new trilateral roadmap is a constructive development, yet road closures and checkpoint volatility are still likely. (Moderate confidence).

Libya's Energy and Political Risk

Disruptions at Libya's ports continue to be used as political leverage. While the National Oil Company managed to keep exports flowing after negotiations in January, similar episodes can be expected. The recent ExxonMobil memorandum suggests longer-term investment interest, but near-term volatility is still a realistic possibility. (Moderate confidence).

Red Sea Supply Chains

The Sudan conflict sustains arms trafficking and opaque private military supply networks. This increases the risk of inspection delays and insurance complications for traffic transiting Egypt, Saudi Arabia, and Djibouti. These risks compound wider maritime insecurity in the Red Sea and Gulf of Aden. (Moderate confidence).

Alternative Analysis

- It is possible that some of the activity observed in the Gulf is criminal rather than state-sponsored. This assessment is considered unlikely, as the tactics, targeting, and telemetry are consistent with known Iranian groups. (Low confidence).
- The Libyan port disruptions could be interpreted as isolated events. However, their recurrence over many years and the persistence of revenue disputes suggest that the risk is ongoing. (Low to moderate confidence).
- The violence in southern Syria may not spill across borders. The new roadmap provides some grounds for optimism, although conditions on the ground remain volatile. (Medium confidence).

Why This Matters for TINYg Members

- Financial institutions and payment systems in the Gulf should expect continued phishing and supplier compromise attempts.
- Energy markets remain vulnerable to sudden interruptions in Libyan exports caused by political protests or armed groups.
- Personnel working along the Jordanian-Syrian frontier face increased unpredictability at checkpoints and along key travel routes.
- Maritime operators should anticipate possible inspections, delays, and higher insurance premiums linked to arms trafficking through the Red Sea.

Recommendations for Q3

1. Enforce multi-factor authentication across all Gulf banking and logistics operations. Review conditional access policies and protect privileged accounts. Strengthen defenses against phishing and conduct exercises simulating Iranian tactics. (Immediate).
2. Reassess third-party risk exposure. Require service providers, particularly fintech firms and port IT contractors, to provide evidence of recent security exercises. (30 days).
3. Monitor the status of Libyan ports, especially Es Sider and Ras Lanuf, before scheduling shipments. Prepare contingency plans and coordinate with insurers regarding force majeure clauses. (Ongoing).
4. Update travel and security protocols for operations near Jordan and Syria. Ensure that staff receive timely alerts on border closures and security escalations. (Immediate).
5. Review Red Sea shipping routes regularly. Pre-clear documentation to minimize inspection delays and track advisories from international maritime organizations. (Ongoing).

Outlook for Q4

- Iranian cyber activity against financial and logistics networks is likely to continue or intensify in the coming quarter.
- Political disputes in Libya will likely trigger further disruptions, although they may remain short-lived rather than prolonged.
- The roadmap for southern Syria may reduce levels of violence, but smuggling and checkpoint volatility are expected to persist.
- The Sudan conflict will continue to drive arms trafficking and elevate risks to shipping in the Red Sea corridor.

References

1. "Threat Brief: Escalation of Cyber Risk Related to Iran" — Unit 42, Palo Alto Networks. Unit 42
2. "Libya's NOC says oil loadings normal following protests" — *Reuters*, Jan 28, 2025. Reuters
3. "Syria, Jordan, US agree on plan to restore stability in Sweida after deadly clashes" — *AP News*, Sept 16, 2025. AP News+1
4. "Protests in Libya disrupt oil loadings at 2 ports" — *Arab News* (reporting Reuters data), Jan 28, 2025. Arab News
5. "Libya Protests Halting Oil Shipments From Key Eastern Ports" — *Bloomberg*, Jan 28, 2025. Bloomberg.com
6. "U.S. Agencies Warn of Rising Iranian Cyber Attacks on Middle Eastern Networks" — *The Hacker News*, Jun 30, 2025. The Hacker News

Sub-Saharan Africa (SSA) Threat Intelligence Desk

Title: Fallout of USAID Withdrawal: Heightened Terror Threat in Sub-Saharan Africa
Analyst: Sam Rosenblum

BLUF (Bottom Line Up Front)

The abrupt withdrawal of USAID from Sub-Saharan Africa in early 2025 has degraded regional stability by creating vetting gaps and halting essential services, contributing to a rise in extremist recruitment and security risks.

Key Judgments

- Vetting Gaps Have Heightened Risk of Terror Finance – Furloughed USAID staff could no longer vet implementing partners, creating blind spots through which extremist-linked NGOs may have received funds (OSINT, medium confidence).
- Service Collapses are Fueling Recruitment – Termination of health, water, and agricultural programs in Mali and DR Congo worsened humanitarian crises, increasing vulnerability to jihadist narratives promising stability and income (OSINT, high confidence).

- Security Vacuums lead to possible removal of vital intelligence– The loss of USAID field staff removed a vital source of ground intelligence, possibly delaying detection of jihadist activity and weakening local government response(OSINT, Low Confidence)
- Strain on Other U.S. Assets Risks Strategic Drift – U.S. military and diplomatic assets are now overstretched, leading to over-reliance on kinetic solutions while long-term stabilization lags behind (OSINT, medium confidence).

Facts & Background

- As announced by the U.S. government, major development missions were shut down across Sub-Saharan Africa (OSINT, confirmed by multiple news sources).
- Projects Canceled in High-Risk Zones – Mali's agriculture and health programs, and DR Congo's water infrastructure projects were halted, cutting aid access to thousands (OSINT, Al Jazeera).
- UN: Livelihood Loss Drives Extremist Recruitment – A 2023 UNDP study found loss of income as a primary motivator for joining extremist groups (OSINT, high confidence).

Regional Analysis

Terrorism:

BLUF: The current lack of international support creates an environment where critical stabilizing functions are absent, reducing access to basic services that previously helped suppress jihadist recruitment. In regions like northern Mali and eastern DRC, militants are exploiting service gaps and public discontent, presenting themselves as alternative providers in the absence of effective state presence.

Homeland Security:

BLUF: Reduced U.S. civilian presence has degraded regional threat visibility. Without USAID's ground-level situational awareness, terrorist movements are harder to track, delaying U.S. and partner responses. This poses increased homeland security risks, particularly through transnational networks with West African roots (e.g., AQIM, ISGS) that may pivot toward targeting Western interests.

Emerging Threats:

BLUF: Aid gaps create an environment that risks radicalizing new demographics. Youth populations previously insulated from recruitment pipelines by international aid are now more exposed. Analysts assess a moderate probability that disillusioned

youth in coastal states (e.g., Senegal, Ghana) could be drawn into radical networks in the next 6–12 months.

Alternative Analysis

- **Alt-1: Aid Withdrawal Not Directly Causing Terror Recruitment (Low)** – UN data and field reports consistently tie aid loss to increased radicalization risk; local communities explicitly cite collapsed services as recruitment motivators.

- **Alt-2: Security Deterioration Due to Local Factors (Medium)** – While regional instability predates USAID's departure, the sudden aid void accelerated the decline in local government legitimacy and worsened conflict dynamics.

Why This Matters for TINYg Members

- **Terror Finance Risks** → Foreign entities conducting business in SSA may face legal and reputational damage if funds reach sanctioned entities due to vetting failures.

- **Operational Risk for Foreign Investors** → Security deterioration in Mali, Niger, and DRC may disrupt extractive industries and logistics corridors.

- **Public Perception and CSR Exposure** → Western firms may be seen as complicit in withdrawal consequences, raising reputational and ESG-related risks.

- **Overburdened Diplomatic Missions** → Lack of development partners forces U.S. embassies and military attachés to divert bandwidth toward humanitarian gaps.

Recommendations for TINYg Member Organizations

1. Reassess partner risk profiles in light of reduced U.S. vetting.
2. Prepare Contingency Plans. For corporate actors, develop business continuity strategies that factor in extremist disruption scenarios in newly unstable areas.

3. Maintain vigilance by continuing to monitor TINYg alerts.

Over The Horizon Threats

Radicalization in Coastal West Africa – Analysts are tracking early indicators of increased jihadist messaging and recruitment efforts and activity in countries like Togo, Ghana, and Senegal. This represents a new operating theatre where extremist groups may seek to expand influence beyond their traditional strongholds.

Methodology

This report is based on OSINT.

References

1. "Negotiating With Terrorists: Somalia's Double-Edged Sword," *Foreign Affairs Review*, October 24, 2022 — by Sofia Sanz-kimura
2. "Ivory Coast Is Losing US Aid as al-Qaida and Other Extremist Groups Are Approaching," AP News, March 16 2025
3. "Trump's Funding Cuts Will Hurt South Africa and the Region," The Washington Post, June 8 2025
4. A Powerful, Opaque al-Qaeda Affiliate Is Rampaging across West Africa," The Washington Post, June 8 2025
5. "Ghana Sahel Jihadis Find Refuge, Supplies, Sources Say," Reuters, October 24 2024
6. "Militants Inflict Heavy Losses on Benin's Armed Forces in an Attack in the North," AP News, April 2025
7. "Trump's Aid Cuts Are Fueling Terrorism, Warns Bank Chief," The Telegraph, 2025
8. "Why West Africa Is Now the World's Terrorism Hotspot," Reuters, 2025
9. "How Jihadists Struck Gold in Africa's Sahel," Reuters, 2025
10. "Lack of Jobs, the Main Driver of Violent Extremism in Sub-Saharan Africa: UNDP," UN News, 2023
11. "Sahel Crisis Goes Coastal as Insurgents Push Toward the Atlantic," The New York Times, 2025

Europe Threat Intelligence Desk

Rising Threats to European Security: Shadow Networks, Right-wing Extremism, and Online Ecosystems

Analyst: Bianca Thompson, Kushal

BLUF (Bottom Line Up Front)

Europe faces the mounting threat of Iranian and Russian-commissioned criminal 'shadow networks' carrying out hybrid attacks, while online communities are shortening pathways to ideological violence, especially within youth populations.

Key Judgments

- Both Russia and Iran have increasingly outsourced sabotage campaigns to criminal proxies across Europe, marking a new trend in state-sponsored terrorism. (OSINT, High confidence)
- Right-wing extremism remains a persistent and increasingly transnational threat in Europe, driven by anti-migrant sentiment, conspiracy ideology, and digital propaganda networks. (OSINT, High confidence)
- Online radicalization is becoming increasingly effective with shorter incubation times, especially with minors. (OSINT, Moderate confidence)

Facts & Background

- Drug traffickers Umit B. and Naji Zindashti have allegedly received sanctuary in Iran in exchange for the utilization of criminal networks to carry out attacks on behalf of the government. Similarly, criminal organizations like Foxtrot, Hell's Angels, and Rumba have been leveraged against Israeli and Jewish targets in Europe.
- On behalf of Iran, two rival Swedish gangs, Foxtrot and Rumba, attempted several attacks against the Israeli embassy in Stockholm in the last year.
- Lithuanian prosecutors confirmed that the two Ukrainian citizens convicted for setting fire to a Vilnius shopping center were hired by a member of the Russian military intelligence services.
- Data recently published by the German Federal Office for the Protection of the Constitution (BfV) showed a 32.4% increase in right-wing politically motivated crime in 2024.
- In France, 11 minors have been charged with terrorism offences, projecting a 50% increase from 2024 by the end of the year. 1 in 5 people arrested on terrorism charges in the UK are under 18.

Analysis

Criminal Proxies

BLUF: Russia and Iran's use of criminal proxies is not a new phenomenon, but one that should continue to be monitored.

> Of the 102 Iran-linked plots recorded in Europe since 1972, 54 occurred between 2021 and 2024, marking a significant increase in the pace of Iranian external operations since the events of October 7th. Russia demonstrated an adjacent trend of escalation since the beginning of the invasion of Ukraine. This suggests a strategic shift toward deniable hybrid action, allowing both countries to project influence and conduct targeted violence during periods of international scrutiny.

Right-Wing Extremism:

BLUF: Right-wing extremist ideologies are gaining consistent momentum due to mounting social tensions resulting from migration, global conflicts, and the return of fascism in mainstream politics.

> Right-wing extremist rhetoric is seemingly evolving into a fluid, digitally networked movement with cross-border ideological linkages due to online communities.

Online radicalization:

BLUF: The online radicalization of minors is accelerating due to algorithmic exposure and unregulated encrypted ecosystems (Telegram, Discord, etc.), reducing detection timeframes and increasing the risk of ideologically motivated violence.

> An American report by the NCJRS in 2016 showed that the timeframe from indoctrination to action in youths had decreased from 15 months pre-2010 to 6.25 months post-2010–a downward trend that has likely continued. The shorter incubation period, combined with the increased sophistication of handbooks accessible on these online platforms, is likely why lone actor plots have increased.

Alternative Analysis

Alt-1: Plots aligning with Iranian and Russian interests are not state-directed (Low): Intelligence overwhelmingly suggests a link.

Alt-3: Right-wing extremism is a localized national issue rather than a cross-border threat (Medium): Evidence of shared symbolism, manifestos, and tactical references suggests the presence of a transnational ideological network influencing actors across Europe

Alt-4: Youth radicalization via encrypted media is an overstated threat (Medium): 93% of terrorism fatalities in Europe come from lone actors, who can find increasingly sophisticated handbooks online. Youth populations are particularly vulnerable to improved online propaganda and recruitment frameworks.

Why This Matters for TINYg Members

Deniability created by proxy sabotage operations by Russia and Iran complicates governmental response, and alleged assistance by the government to criminal organizations hinders intelligence capabilities to stop them.

The rise of conservatism in global politics has emboldened right-wing extremists, and cross-border cooperation increases the complexity of tracking and disrupting plots.

Lone actor plots have a much higher rate of success [61% compared to 18% for group attacks] because they are far more challenging to track. Accelerated online radicalization, especially among minors, reduces that window for intervention.

Recommendations

1. **Tracking criminal proxies:** Expand intelligence-sharing on state-linked gangs; monitor financial flows and suspicious procurement.
2. **Monitoring online forums:** Employ OSINT on Telegram, Discord, and fringe forums to identify emerging threats.
3. **Preventing youth radicalization:** Help schools learn to detect online grooming and radicalization in their students.
4. **Stay up to date with TiNYg news.**

Over The Horizon Threats

Criminal proxies leveraged by Iran may expand their target set beyond Israeli and Jewish institutions or activate on a larger scale.

As Russia faces further strategic pressure, expect coordinated cyber intrusions paired with physical disruptions. These may coincide with winter energy demand.

Extremist groups are likely to deploy AI-generated content to more effectively radicalize and prepare minors online to execute larger, more fatal attacks.

Christmas markets, New Year celebrations, and large public gatherings across major European cities may be at elevated risk from lone actors seeking maximum symbolic and media impact.

Methodology

This report is based on open-source intelligence (OSINT), corroborated by independent analysis.

References

1. "Iranian External Operations in Europe: The Criminal Connection," ICCT, October 16, 2024 (OSINT)
2. "Recruited by gangs, exploited by Iran," CNN, April 7, 2025 (OSINT)
3. " Lithuania accuses Russia over Ikea store fire in Vilnius," BBC, May 17, 2025 (OSINT)

4. “2024 Report on the Protection of the Constitution,” German Federal Ministry of the Interior, 2025 (OSINT)
5. “Violent videos draw more French teens into ‘terror’ plots, say prosecutors,” The Straits Times, July 29, 2025 (OSINT)
6. “Number of young people arrested for terrorism offences hits record high,” UK Counter Terrorism Policing, March 15, 2024 (OSINT)
7. “A Behavioral Study of the Radicalization Trajectories of American “Homegrown” Al Qaeda-Inspired Terrorist Offenders,” NCJRS, November 2016 (OSINT)

North America Threat Intelligence Desk

Title: Terrorism Trends in North America: Digital Radicalization and Lone Actor Violence
Analyst: Isabella White

BLUF (Bottom Line Up Front)

Lone actor violence remains the most persistent and unpredictable terrorism threat to North America. Fueled by digital radicalization, grievance-based ideologies, and global conflict spillover, lone actors have increasingly targeted civilians, public spaces, and enforcement personnel, including DHS and ICE, across the U.S. and Canada in 2025. This threat cuts across ideological lines and challenges traditional prevention models.

Key Judgments

- Lone actors have conducted or attempted at least four major attacks in North America this year, driven by jihadist, anti-government, eco-extremist, and anti-enforcement motives (OSINT, High Confidence).
- The diversity in motives and lack of formal group affiliation among lone actors complicates efforts in early detection and intervention (OSINT, High Confidence).

- Online spaces like encrypted chat apps, social media, and fringe forums are making it easier for people, especially young or socially isolated individuals, to become radicalized(OSINT, High Confidence).
- Recent attacks on ICE and DHS personnel suggest that law enforcement is an emerging symbolic threat across extremist ideologies (OSINT, Moderate Confidence).

Facts & Background

- Alberta, Canada - May 2025: A teenage suspect was arrested on suspicion of planning a terrorism-related attack. Authorities have linked the 15 year old to having ties with the COM/764 terrorism network (OSINT)
- Prairieland ICE Facility, Texas - July 2025: An organized group of individuals ambushed officers at a DHS facility. The attackers left anti-ICE slogans showing growing hostility toward enforcement agencies(OSINT).
- Coeur d'Alene Firefighters Ambush - June 2025: 20 year old suspect set a brush fire to lure in first responders and then opened fire from a concealed position. Investigators have not linked his motives with any extremist affiliation(OSINT).

Regional Analysis

- Grievance-based violence is overtaking traditional ideologies: Many recent attackers do not align directly with established terrorist groups or ideologies. Instead, they act on personal grievances combined with hybrid ideologies.
- Digital radicalization and youth vulnerability are growing threats: Extremist online spaces serve as echo chambers where young and often isolated individuals find ideological reinforcement and social validation for violence. Many recent attackers have been under 25, with some as young as 16. Extremist groups, such as The Order of Nine Angels and the 764 Network for example, use online platforms to exploit emotional vulnerabilities.
- Law enforcement is emerging as a symbolic target: The attack on ICE officers in Texas and the shooting at a Border Patrol station in McAllen represent the trend that federal law enforcement agencies are being targeted by actors often with retaliatory motives.

Alternative Analysis

- Alt 1: Recent incidents reflect isolated criminal behavior, not terrorism. (Low confidence)

While some attackers may have overlapping grievances, the recurring presence of ideological themes and targeting patterns suggests a wider extremist trend rather than random acts of violence.

- Alt 2: Online spaces are overestimated in radicalization. (Medium confidence)
  Some analysts suggest that mental health challenges are the primary motivators of violence, rather than online content. While these factors are significant, evidence increasingly shows that digital spaces play a significant role in furthering radicalization and shaping attackers' ideologies.

Why This Matters for TINYg Members

- Public Safety Risks: Lone Actors often target public gatherings where attendance is high with little to no operational warning.
- Law Enforcement Vulnerability: Officers at federal enforcement agencies face growing risks from actors who view them as targets for ideological or retaliatory reasons.
- Digital Monitoring Challenges: Encrypted apps and anonymity prevent early detection. Behavioral intervention and reporting are becoming more critical.
- Community Education and Resilience: Schools, parents, and other community leaders must be educated and equipped to recognize and respond to early signs of radicalization.

Recommendations for TINYg Members

1. Enhance behavioral threat assessment training within TINYg member organizations, ensuring partners can identify early warning signs of planned acts of targeted violence.

2. Invest in digital counter-radicalization efforts, including partnerships with technology platforms to monitor emerging online extremist trends.
3. Increase physical and cyber protection at targets vulnerable to Lone Actor style attacks.
4. Improve intelligence sharing across the TINYg network and US and Canadian law enforcement to better detect and track non-traditional threats.

Over The Horizon Threats

Digital radicalization will likely continue to lower the barrier to entry for violence, particularly among youth. Encrypted chat groups and artificially generated propaganda will likely make early detection even more difficult.

Extremist communities will likely keep sharing tactics, narratives, and online content across borders, which could contribute to a broader pool of grievance based violence across North America.

Methodology

Open source Intelligence, including regional and national reports, local law enforcement incident reports, and government press releases.

References

1. "American Nazis: The Aryan Freedom Network is riding high in Trump era," Reuters, https://www.reuters.com/investigations/american-nazis-aryan-freedom-network-is-riding-high-trump-era-2025-08-08/
2. "DHS Statement on Violent Extremist Involved in Prairieland Attack on ICE Agents," Department of Homeland Security https://www.dhs.gov/news/2025/07/16/dhs-statement-capture-violent-extremist-involved-prairieland-attack-ice-agents
3. "Order of Nine Angels: What is this obscure Nazi Satanist Group," BBC https://www.bbc.com/news/world-53141759
4. "National Terrorism Advisory System Bulletin," Department of Homeland Security https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-june-22-2025
5. "Terrorism News and Press Releases," FBI News pagehttps://www.fbi.gov/investigate/terrorism/news
6. "Terrorism," FBI https://www.fbi.gov/investigate/terrorism
7. "Leaders of 764 Arrested and Charged for Operating Global Child Exploitation Enterprise," United States Department of Justice https://www.justice.gov/usao-dc/pr/leaders-764-arrested-and-charged-operating-global-child-exploitation-enterprise
8. "Suspect Identified in the Fatal Ambush of 2 firefighters in Idaho," NPR https://www.npr.org/2025/06/30/g-s1-75267/idaho-gunman-firefighters-shooting-what-we-know
9. "Edmonton-area teen, 15, allegedly connected to violent online network intent on causing 'as much suffering as possible," City News https://edmonton.citynews.ca/2025/05/29/edmonton-teenager-terrorism-charges-violent-network/

Latin America/Caribbean Threat Intelligence Desk

Title: CJNG Expansion Beyond Violence: Terror, Scams, and Societal Disruption
Analyst: Aldair Campos

BLUF (Bottom Line Up Front)

BLUF: Two recent violent events in Mexico show that the Jalisco New Generation Cartel (CJNG) is using both public attacks and covert killings to spread fear and control territory. Its recent designation as a terrorist organization by the United States highlights the growing threat to regional stability.

Key Judgments

- **Multi-Dimensional Tactics:** CJNG combines violence, financial scams, cyber extortion, and social coercion to dominate local populations and rival criminal networks.
  Confidence: High

- **Public Intimidation and Media Influence:** High-profile attacks, coupled with online dissemination of threats and propaganda, aim to shape public perception

and suppress resistance.
Confidence: Medium-High

- **Economic Disruption:** Extortion of businesses, fraudulent "protection" schemes, and manipulation of local supply chains are destabilizing regional commerce.
  Confidence: Medium

- **Regional Spillover Risk:** CJNG's diversified operations—including scams, coercion, and logistics control—may extend influence into Querétaro, San Luis Potosí, and northern Central America, creating complex security challenges.
  Confidence: Medium

- **Threat to Governance and Civil Society:** The cartel's tactics erode trust in law enforcement, corrupt local institutions, and disrupt daily life in affected municipalities.
  Confidence: High

Facts & Background

- **CJNG Terrorist Designation (Feb 2025):** U.S. State Department labeled CJNG a Foreign Terrorist Organization and SDGT, reflecting its use of extreme violence, terror tactics, and fentanyl trafficking (OSINT, high confidence).
- **June 24 Mass Shooting, Irapuato:** Attack killed 12 and injured over 20 during a crowded religious festival, demonstrating CJNG's continued use of high-visibility violence (AP News, Reuters, OSINT, high confidence).
- **August Mass Graves Discovery:** 32 bodies found near Irapuato, signaling clandestine terror operations targeting rivals and civilians (AP News, CBS News, OSINT, high confidence).
- **Financial Scams & Extortion:** CJNG has reportedly expanded extortion schemes targeting small businesses and logistics companies. Reports indicate "protection" rackets, fraudulent online payment scams, and coercive micro-lending operations affecting local economies (InSight Crime, OSINT, medium confidence).
- **Social Coercion:** Forced recruitment of youth, school intimidation, and control over local political actors are shaping community behavior and suppressing opposition (El País, OSINT, medium confidence).

- **Cyber and Logistics Exploitation:** CJNG uses encrypted messaging and social media to coordinate operations, threaten competitors, and control distribution networks, creating new vulnerabilities for law enforcement and businesses (Small Arms Survey, Janes, OSINT, medium confidence).
- **Paramilitary Infrastructure:** Training camps, torture sites, and recruitment facilities remain active across Guanajuato and surrounding states, supporting both violent and non-violent control mechanisms (El País, OSINT, medium confidence).

Regional Analysis

BLUF: CJNG's operations are increasingly hybrid, combining terror, economic coercion, cyber enabled schemes, and social manipulation to dominate central Mexico.

Analysis: CJNG's integration of non-violent tactics amplifies instability. Public attacks serve as a psychological anchor, while scams, extortion, and coercion disrupt commerce, weaken governance, and create a climate of fear that extends beyond traditional cartel violence. These activities compound regional instability, impede legitimate business, and threaten migration and border security. The central Mexican corridor remains a hub for both physical violence and multi layered criminal influence, with potential spillover into northern Central America.

Emerging Trends:

1. CJNG may expand online scams targeting cross border transactions, increasing financial exposure in Mexico and the U.S.

2. Social coercion through forced recruitment, school intimidation, and local political influence is likely to deepen territorial control.

3. Diversified operations may create new challenges for law enforcement, combining traditional counter narcotics approaches with anti-terrorism, cybercrime, and economic crime measures.

Alternative Analysis

- Alternative 1: Opportunistic Economic Exploitation (Medium Confidence): Some scams may be opportunistic rather than strategic. However, coordinated patterns suggest intentional territorial control.
- Alternative 2: Violence as Primary Motive (Low Confidence): CJNG may prioritize narcotics profits, using terror and scams as secondary tools.

Evidence of multi-tiered operations indicates a broader strategy than pure financial gain.

Why This Matters for TINYg Members

Civilian Safety: Public gatherings, schools, and residential areas are increasingly vulnerable to both violence and social coercion.

Economic Impact: Businesses face extortion, fraud, and supply chain disruptions, which may affect regional trade and cross-border commerce.

Governance and Rule of Law: Corruption and intimidation hinder state authority, compromising law enforcement and civil institutions.

Regional Stability: The multi-dimensional nature of CJNG operations magnifies migration pressures and complicates counter-narcotics and counter-terrorism efforts.

Recommendations for TINYg Member Organizations

1. Strengthen Regional Threat Monitoring
- Track CJNG's public attacks, online propaganda, and extortion schemes.
- Share intelligence on emerging scams, recruitment efforts, and coercion with law enforcement and NGOs.

2. Harden Business and Community Resilience
- Review security protocols for small businesses, logistics hubs, and schools.
- Implement fraud detection and financial reporting systems to mitigate CJNG scams.

3. Support Civil Society and Anti-Coercion Measures
- Partner with NGOs to provide community education on recruitment risks, financial scams, and social coercion.
- Engage local authorities to strengthen governance and reduce corruption vulnerabilities.

4. Prepare Multi-Dimensional Contingency Plans
- Develop emergency response protocols that address both violent attacks and economic/cyber threats.
- Conduct scenario-based drills for staff safety, financial continuity, and rapid reporting of criminal activities.

Over The Horizon Threat Assessment

- **Expansion of Scams and Extortion:** CJNG may increase cyber-enabled scams, fraudulent business schemes, and coerced local "taxation" of communities.
- **Multi-State Territorial Consolidation:** Violence, coercion, and scams are likely to spread into Querétaro, San Luis Potosí, and Michoacán.
- **Regional Influence on Central America:** CJNG tactics could shape criminal networks in northern Central America, increasing migration pressures and illicit trade flows.
- **Hybrid Operational Threat:** Combining violence, financial exploitation, social coercion, and cyber tactics creates complex, multi-layered threats that are difficult to counter using conventional methods.

Methodology

Analysis is based entirely on OSINT, including media reports, investigative outlets, think tank assessments, and open government sources. Confidence levels follow ODNI analytic standards, emphasizing cross-verification, temporal relevance, and consistency with known regional patterns. No classified sources were used.

References

1. AP News. (2025, June 25). "12 Killed During Shooting at Festival in Irapuato." https://apnews.com/article/2ca392537f979bc85b777bd105fd13eb

2. Reuters. (2025, June 25). "Festival Attack Leaves 12 Dead." https://www.reuters.com/world/americas/least-12-killed-shooting-mexico-street-celebration-2025-06-25/

3. El País. (2025, July 5). "La Paradoja de Guanajuato." https://elpais.com/mexico/2025-07-05/la-paradoja-de-guanajuato.html

4. AP News. (2025, Aug 5). "32 Bodies Found in Graves in Central Mexico." https://apnews.com/article/e85d7096b1705f1061c9cff8809b1eb5

5. CBS News. (2025, Aug). "Bodies Discovered in Plastic Bags." https://www.cbsnews.com/news/dismembered-bodies-found-home-

guanajuato-mexico-missing-people/

6. U.S. Department of State. (2025, Feb). “Designation of CJNG as a Foreign Terrorist Organization.” https://www.state.gov/

7. InSight Crime. (2025, April). “CJNG’s Expanding Influence: Violence, Scams, and Social Coercion.” https://insightcrime.org/news/cjng-multi-dimensional-threats/

8. Small Arms Survey. (2024). “Emerging Threats in Mexican Criminal Networks.” https://smallarmssurvey.org/

9. Department of the Treasury. (2025). Public Sanctions on CJNG. https://home.treasury.gov/

Asia Threat Intelligence Desk

Title: China-Linked APT Group UNC3886 Targets Singapore's Critical Infrastructure
Analyst: Kushal Ganji, Bianca Thompson

BLUF (Bottom Line Up Front)

A Chinese state-linked cyber espionage Advanced Persistent Threat (APT) group has been targeting Singapore's critical infrastructure by exploiting zero-day vulnerabilities in advanced threat detection systems, posing a potential strategic threat to national resilience across Southeast Asia.

Key Judgments

- UNC3886 is conducting sophisticated cyber espionage targeting critical infrastructure. The group used zero-day vulnerabilities in major systems (Fortinet, VMware, Juniper) to access and persist in sensitive operational networks across energy, water, finance, and telecom sectors (OSINT).

- Fortinet, VMware, and Juniper are technology companies providing solutions for network security, virtualization, and networking infrastructure
- Singapore formally attributed the attacks to UNC3886, marking a rare public identification. Authorities identified the group without directly attributing it to the Chinese government, likely to balance geopolitical sensitivities (OSINT).
- UNC3886's tactics align with state-level intelligence operations – The use of highly tailored malware and targeting of non-monetary assets suggests a focus on intelligence collection and strategic disruption (OSINT).

Facts & Background

- UNC3886 exploited Fortinet, VMware, and Juniper zero-days to penetrate critical systems (OSINT).
- Singapore's Cyber Security Agency confirmed impacts to 13 sectors and launched incident response protocols (OSINT).
- Malware strains such as MOPSLED and RIFLESPINE are used for long-term credential harvesting and lateral movement (OSINT).
- Malware Strains: https://cloud.google.com/blog/topics/threat-intelligence/uncovering-unc3886-espionage-operations
- UNC3886 operates with stealth, disabling logging features and residing in hardware with limited endpoint detection (OSINT).

Regional Analysis

Cyber:
BLUF: UNC3886's campaign in Singapore signals an escalation in state-aligned cyber espionage operations across the Asia-Pacific.

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

Terrorism:

- BLUF: Lashkar-e-Taiba (LeT) and Jaish-e-Mohammed (JeM) 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: Attacks are financially motivated (Low confidence)** – No signs of ransom or financial theft. Targets were strategic, not commercial.
- **Alt-2: A non-state actor mimicking UNC3886 (Low confidence)** – Toolsets and tactics are consistent with prior UNC3886 operations validated by multiple cybersecurity firms (Trend Micro, Mandiant).

Why This Matters for TINYg Members

- **Operational risk:** Persistent access to infrastructure systems threatens continuity of essential services.
- **Strategic vulnerability:** Espionage may provide adversaries with leverage over national policy or crisis response.
- **Brand/regulatory:** Failure to mitigate these threats could result in the loss of public trust and regulatory penalties across affected sectors.
- Blueprint for non-state cyber actors to operate with no impunity in other regions

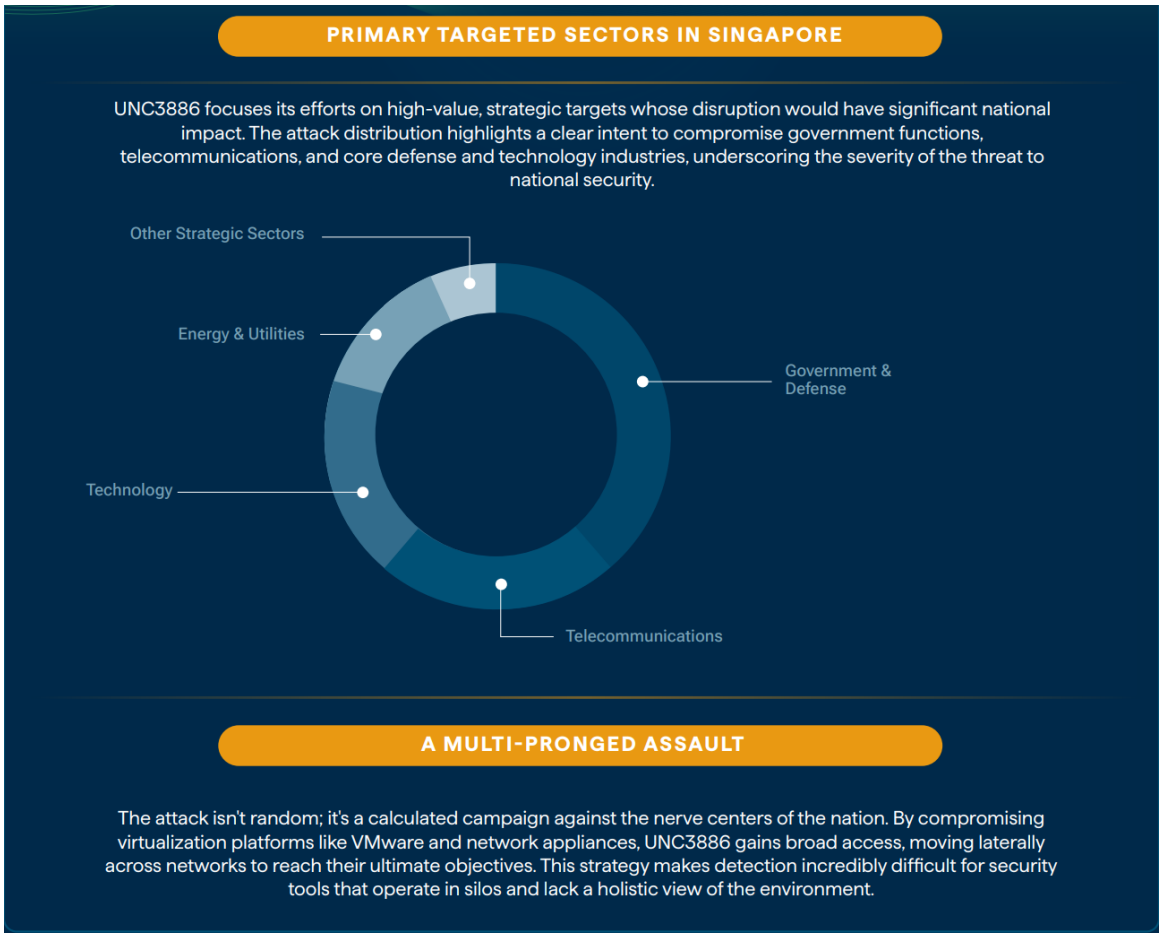
Recommendations for TINYg Member Organizations

1. Apply available patches for Fortinet, VMware, and Juniper systems immediately.
2. Audit logs and network traffic for signs of malware such as MOPSLED, RIFLESPINE, and SSH manipulation.
3. Isolate high-value assets and enforce strict access controls and multi-factor authentication.
4. Engage in tabletop exercises simulating supply chain or IT hybrid compromise scenarios.
5. Stay up to date with news from TINYg

Over The Horizon Threats

UNC3886 or similar groups may target network vulnerabilities within Southeast Asian defense and aerospace sectors

Increased reconnaissance activity targeting maritime logistics systems in the region.



Methodology

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

References

1. "OT-ISAC warns Singapore critical infrastructure of UNC3886 exploiting zero-days in Fortinet, VMware, Juniper systems," Industrial Cyber, July 24 2025 (OSINT).

2. “Advanced Persistent Threats (APT) Explained,” Crowdstrike, March 4, 2025 (OSINT).
3. “Revisiting UNC3886 Tactics to Defend Against Present Risk,” Trend, July 28 2025 (OSINT).
4. “What is UNC3886, the group that attacked Singapore’s critical information infrastructure?,” The Straits Times, July 18 2025 (OSINT).
5. “Singapore says cyber espionage group targeting critical infrastructure,” Reuters, July 18 2025

Global Threat Analysis

Analysis: Terrorist Financing

Title: Global/E-Commerce Threat Landscape
Analyst: Sam Rosenblum

BLUF (Bottom Line Up Front)

Terrorist groups increasingly exploit e-commerce platforms and online marketplaces to raise, launder, and move funds under the guise of legitimate trade. Online retail, integrated payment systems, and global logistics create a “triple blind spot” for regulators, heightening the risk that private firms become conduits for terrorist financing.

Key Judgments

- Terrorists are leveraging e-commerce for covert fundraising – Small, routine online sales conceal illicit activity, making them unlikely to trigger Anti-money laundering/Counter Terrorist Financing(AML/CFT) alerts (OSINT, FATF 2025)
- Integrated payment systems and virtual assets facilitate cross-border transfers – Mobile wallets and crypto enable rapid, low-visibility movement of funds (OSINT, FATF 2025)

- Logistics networks obscure final recipients – Parcel delivery services mask ultimate beneficiaries, creating gaps in oversight between online retailers, payment providers, and shippers (OSINT, FATF 2025)
- Regulatory frameworks remain fragmented –The Financial Action Task Force (FATF) warns that the convergence of online retail, social media marketing, and alternative payments undermines traditional financial monitoring (OSINT, FATF 2025)

Facts & Background

- FATF's 2025 comprehensive update highlights terrorist exploitation of lightly regulated e-commerce platforms and payment processors (OSINT, high confidence)

- Europol Serious and Organised Crime Threat Assessment (SOCTA) 2021 identified the use of online marketplaces as a laundering vector for organized crime, now extended to terrorist entities (OSINT, medium confidence)

- Transactions are often low-value and routine, evading traditional AML thresholds (OSINT, high confidence)

Regional Analysis

Cyber:

BLUF: Terrorist networks exploit integrated digital payment ecosystems. Mobile wallets and crypto exchanges, combined with weak "Know Your Customer" (KYC) rules in certain regions, allow funds to bypass traditional monitoring. FATF identifies this as a systemic blind spot, with a high likelihood of persistence through 2026.

Terrorism:

BLUF: Online retail operations provide terrorists with a sustainable source of micro-financing. The cumulative effect of these small transactions enables steady resourcing for recruitment, propaganda, and small-scale attacks.

Emerging Threats:

BLUF: Cross-platform coordination (e-commerce + social media marketing) magnifies reach. Terrorist groups increasingly advertise through social platforms

while transacting via online marketplaces, complicating attribution and enforcement.

Alternative Analysis

Alt-1: Primarily criminal, not terrorist, exploitation (Medium). Some online laundering may stem from criminal networks rather than terrorist groups. However, FATF evidence explicitly notes terrorist adaptation of these methods.

Alt-2: Overestimation of scale (Low). Regulatory blind spots could be narrower than described. Consistent OSINT across FATF and Europol reports suggests this is a widespread, durable trend.

Why This Matters for TINYg Members

Operational risk: Companies risk unknowingly enabling terrorist financing through online platforms.

Regulatory risk: Firms face penalties for AML/CFT lapses if transactions link to sanctioned entities.

Reputational risk: Association with terrorist-linked activity could cause significant brand damage.

Recommendations for TINYg Member Organizations

1. Enhance vendor due diligence – Implement stronger KYC/AML screening for e-commerce sellers, particularly those operating cross-border.
2. Audit payment flows – Monitor mobile wallet and virtual asset transactions for suspicious patterns of small, repetitive transfers.
3. Integrate logistics oversight – Cross-check shipping data with payment and vendor records to identify potential mismatches or anomalies.
4. Coordinate with regulators – Share suspicious e-commerce activity with Financial Intelligence Units (FIUs) to reduce systemic blind spots.

Over The Horizon Threats

Terrorist groups could increasingly pair e-commerce fundraising with AI-driven marketing and automation tools, allowing them to scale operations globally with minimal human oversight. Monitoring this evolution will be a priority for Q4 2025.

Methodology

This report is based on open-source intelligence (OSINT), including FATF's *Comprehensive Update on Terrorist Financing Risks 2025* and Europol's *SOCTA 2021*, corroborated by independent analysis.

References

1. FATF, Comprehensive Update on Terrorist Financing Risks 2025 (OSINT)
2. Europol, Serious and Organised Crime Threat Assessment (SOCTA 2021) (OSINT)

Analysis: Narco-Terrorism Highlight: Developments Over the Last Six Months

Analyst: Aldair Campos

BLUF (Bottom Line Up Front)

BLUF: Cartels across Mexico and Central America are evolving into hybrid narco terror actors, deploying insurgent tactics like weaponized drones, IEDs, and targeted killings. Coupled with innovations such as 3D printed drones and firearms and rising ideological elements, these methods intensify regional destabilization, drive migration, and amplify threats to U.S. security and public health.

Key Judgments

- **Escalation in Tactics:** Cartels are deploying weaponized drones, car bombs, and mass graves to instill terror.

Confidence: Moderate

- **Regional Spillover:** Violence is expanding into Guatemala, Honduras, and El Salvador, aided by weak governance and cartel gang ties.
  Confidence: Moderate

- **Migration Pressure:** Violence is accelerating migration and fueling the fentanyl crisis, heightening the U.S. border and public health threats.
  Confidence: High

- **Direct U.S. Impact:** Mexican cartels are the primary suppliers of fentanyl driving the U.S. opioid crisis. Expansion of insurgent-style methods raises the risk of these tactics eventually targeting U.S. interests.
  Confidence: High

- **Hybrid Threat:** Organized crime and insurgency tactics are combining into a new form of narco terrorism that undermines governance and regional stability.
  Confidence: Moderate

Facts & Background

- Cartel Tactics Escalate: Mexican and Central American cartels are using weaponized drones, improvised explosive devices (IEDs), and targeted killings to intimidate rivals and control territory **(OSINT, medium confidence)**.

- Mass Casualty Operations: Authorities have discovered mass graves and dismembered bodies in central Mexico, reflecting deliberate terror strategies by criminal groups **(OSINT, high confidence)**.

- Technological Innovation: Cartels are experimenting with 3D printed drones and firearms, increasing accessibility to lethal capabilities **(OSINT, medium confidence)**.

- Regional Spillover: Violence and cartel influence are expanding beyond Mexico into Guatemala, Honduras, and El Salvador, exploiting weak governance, corruption, and porous borders **(OSINT, medium confidence)**.

- U.S. Public Health Threat: Mexican cartels remain the primary suppliers of fentanyl, driving the U.S. opioid crisis and elevating border security risks

(OSINT, high confidence).

- Hybrid Narco-Terrorism: Organized crime and insurgency-style tactics are merging, creating a new form of regional threat that undermines governance and stability **(OSINT, medium confidence)**.

Regional Analysis

BLUF: Narco terrorism in the region is shifting into a hybrid format, operating like insurgent forces that combine territorial control, lethal tactics, and technological innovation.

Analysis: Violence is spreading beyond traditional cartel strongholds, destabilizing neighboring countries including Guatemala, Honduras, and El Salvador. This expansion exacerbates weak governance, undermines law enforcement, and creates conditions for transnational criminal networks to thrive. The flow of fentanyl and other illicit drugs into the United States underscores the threat to U.S. public health and national security. Clandestine killings, mass graves, and highly visible attacks indicate a deliberate strategy to instill fear and disrupt both local and regional stability. Porous borders and corruption further enable operational expansion, making coordinated countermeasures challenging.

Emerging Threats: Cartels may continue to adopt technology-enabled tactics such as drones and improvised explosive devices to target rivals or law enforcement, while expanding influence into less secure regions of Central America. Spillover violence may increase migration pressures northward and create new challenges for border security and regional intelligence operations.

Alternative Analysis

Alternative 1: Violence may be extending beyond Mexico into Central America due to weak governance and porous borders. Cartel alliances in Guatemala, Honduras, and El Salvador could create new transnational criminal corridors. **Confidence: Medium.**

Alternative 2: Cartels' use of drones, explosives, and clandestine killings may reflect tactical innovation rather than a full shift toward insurgency. These groups remain primarily motivated by profit rather than ideology. **Confidence: Medium-High.**

Why This Matters for TINYg Members

This is not "more of the same" cartel violence. The adoption of insurgent tactics and regional expansion represents a **strategic evolution** in narco-terrorism. Monitoring

these shifts is critical for anticipating how criminal groups may increasingly operate like non-state armed actors, posing direct and indirect threats to the U.S.

This is important to track because narco-terrorism is no longer confined to isolated violence. It is evolving into a regional insurgent-style challenge that undermines governance, accelerates migration, and directly impacts U.S. security and public health.

Recommendations for TiNYg Member Organizations & Possible Mitigations:

1. Strengthen Threat Detection and Monitoring

- Implement geospatial monitoring of low-altitude drone activity and integrate AI-enabled imagery analysis to detect emerging narco-terror tactics.
- Prioritize surveillance in regions identified as high-risk operational zones, including border areas and known cartel strongholds.

2. Harden Facilities and Critical Infrastructure

- Upgrade security protocols to detect 3D printed or improvised weapons and train personnel to recognize drone-enabled or small explosive threats.
- Conduct periodic physical security audits of supply chains, transport routes, and personnel movement in Mexico and Central America.

3. Support Regional Cooperation and Information Sharing

- Participate in multi-stakeholder forums connecting law enforcement, policy, and private sector actors to exchange emerging threat indicators and operational trends.
- Coordinate with NGOs to counter ideological recruitment and messaging pipelines among youth in vulnerable communities.

4. Enhance Emergency Preparedness and Contingency Planning

- Develop continuity, evacuation, and rapid response plans that account for asymmetric attacks, including drone strikes, explosives, and targeted killings.
- Test emergency response protocols regularly to ensure personnel safety and operational resilience.

Over the Horizon Threats

- **Drone-Enabled Attacks:** Cartels are likely to expand the use of weaponized or autonomous drones against rival groups, law enforcement, and potentially civilian targets **(prospective, medium confidence)**.

- **Transnational Expansion:** Narco-terror networks may further extend into northern Central America, creating new criminal corridors that increase regional instability and migration pressures toward the U.S. **(prospective, medium confidence)**.

- **Weapon Innovation:** Continued adoption of 3D printed firearms and improvised explosive devices may empower smaller cells to conduct high-impact attacks with minimal detection **(prospective, medium confidence)**.

- **Ideological Radicalization:** Emerging ideological elements among cartel-affiliated groups could shift some operations beyond profit-driven motives, although evidence is limited **(prospective, low confidence)**.

- **Operational Spillover:** Expansion into previously stable regions could challenge law enforcement and intelligence operations, increasing the risk of unforeseen violence **(prospective, medium confidence)**.

- **Evolving Threat:** Potential cross-border attacks targeting U.S. interests using hybrid narco-terror tactics remain under-monitored due to insufficient data **(evolving threat, low confidence)**.

Methodology

This assessment is based solely on **open-source intelligence (OSINT)**, including international media, regional outlets, investigative reporting, and security think tanks. Sources were cross-checked for reliability and corroboration, with preference given to recent reporting within the last six months. Confidence levels were assigned using **ODNI analytic standards**, weighing source credibility, consistency across outlets, and alignment with historical patterns. No classified information was used.

References

1. AP News. (2025, June 25). 12 Killed During Shooting at Festival in Irapuato. https://apnews.com/article/2ca392537f979bc85b777bd105fd13eb

2. Reuters. (2025, June 25). Festival Attack Leaves 12 Dead. https://www.reuters.com/world/americas/least-12-killed-shooting-mexico-street-celebration-2025-06-25/

3. El País. (2025, July 5). La Paradoja de Guanajuato. https://elpais.com/mexico/2025-07-05/la-paradoja-de-guanajuato.html

4. AP News. (2025, Aug 5). 32 Bodies Found in Graves in Central Mexico. https://apnews.com/article/e85d7096b1705f1061c9cff8809b1eb5

5. CBS News. (2025, Aug). Bodies Discovered in Plastic Bags in Guanajuato. https://www.cbsnews.com/news/dismembered-bodies-found-home-guanajuato-mexico-missing-people/

6. InSight Crime. (2025, April). Cartel Drone Attacks and Expanding Criminal Governance in Mexico. https://insightcrime.org/news/cartel-drone-attacks-mexico/

7. AP News. (2025, July). Guatemalan Officials Warn of Rising Cartel Presence Along Border. https://apnews.com/article/guatemala-cartel-border-violence-2025

8. U.S. Drug Enforcement Administration (DEA). (2025). National Drug Threat Assessment Update: Fentanyl Flows from Mexico. https://www.dea.gov/reports

9. Borderland Beat. (2025). Cartel Alliances Expanding into Honduras and El Salvador. http://www.borderlandbeat.com/

10. International Crisis Group. (2025). Central America's Criminal Dynamics and Regional Spillover. https://www.crisisgroup.org/latin-america-caribbean

11. Council on Foreign Relations (CFR). (2025). The Fentanyl Challenge: Cross-Border Implications for U.S. Security. https://www.cfr.org/

12. Small Arms Survey. (2024). 3D Printed Firearms: Emerging Threats and Criminal Use in Latin America. https://smallarmssurvey.org/

13. Janes Defence Weekly. (2025). Cartels Experiment with 3D Printed Drones and Improvised Explosives. https://www.janes.com/

14. United Nations Office on Drugs and Crime (UNODC). (2024). Criminal Governance and the Evolution of Non-State Armed Actors in Central America. https://www.unodc.org/

15. ACLED. (2025). Political Violence and Organized Crime in Mexico and Central America. https://acleddata.com/

Analysis: AI-Powered Propaganda & Extremist Recruitment

Analysts: Kushal Ganji, Isabella White

BLUF (Bottom Line Up Front)

Extremist actors are weaponizing generative AI to mass-produce multilingual propaganda, automate one-to-one recruitment, and evade moderation, shortening the path from online exposure to real-world violence, particularly among minors.

Key Judgments

- AI supercharges propaganda. Extremists can rapidly create fake videos/audio and push multiple language versions; even when removed, the content quickly reappears.
- Recruitment is partly automated. Chatbots/Large Language Models (LLMs) tailor messages and keep people engaged. Jailbreaks can bypass safety rules to support recruitment narratives.

- Moderation can't keep up. Tactics such as mass-producing variants, auto-translating, recycling posts, personalizing content, and evading filters can overwhelm simple hash/keyword tools.
- Youth risk is growing. More minors are active in online extremist spaces, where hybrid ideologies make violence seem normal.

Facts & Background

1. Record levels of generative AI propaganda/hate speech. More minors are involved. National Coordinator for Counterterrorism and Security (NCTV) warns of rapid online radicalisation among youth with Level-4 ("substantial") threat posture
2. Online communities blend jihadist, accelerationist, and other currents. (OSINT)
3. Extremists are experimenting with generative AI for propaganda, misinformation/disinformation campaigns, and interactive recruitment. "How-to" guides are circulating. (OSINT)
4. Researchers show LLM jailbreaks can get restricted outputs across several models, useful for recruitment, tactics, and attack planning. (OSINT)
5. A review of 5,000 AI-generated items maps tradecraft, media spawning, translation, variant recycling, personalization, and moderation subversion. (OSINT)

Regional Analysis

Cyber: Burst posting, cross-platform cloning, and multilingual spikes are outpacing platform defenses.

- Burst posting: Publishing a large number of posts in a short, concentrated period of time.
- Cross-platform cloning: The creation of an application that functions similarly or identically across different operating systems (like Android, iOS, Windows) and device types (like desktops, mobiles, tablets)

Terrorism: AI speeds up lone-actor pathways as mixed online communities promote simple, high-impact violence.

Homeland Security: Shorter warning windows for schools and local authorities as minors are pulled into AI-amplified propaganda.

Emerging Threats: Chatbot "mentors" and jailbreakable LLMs lower barriers to radicalization and learning.

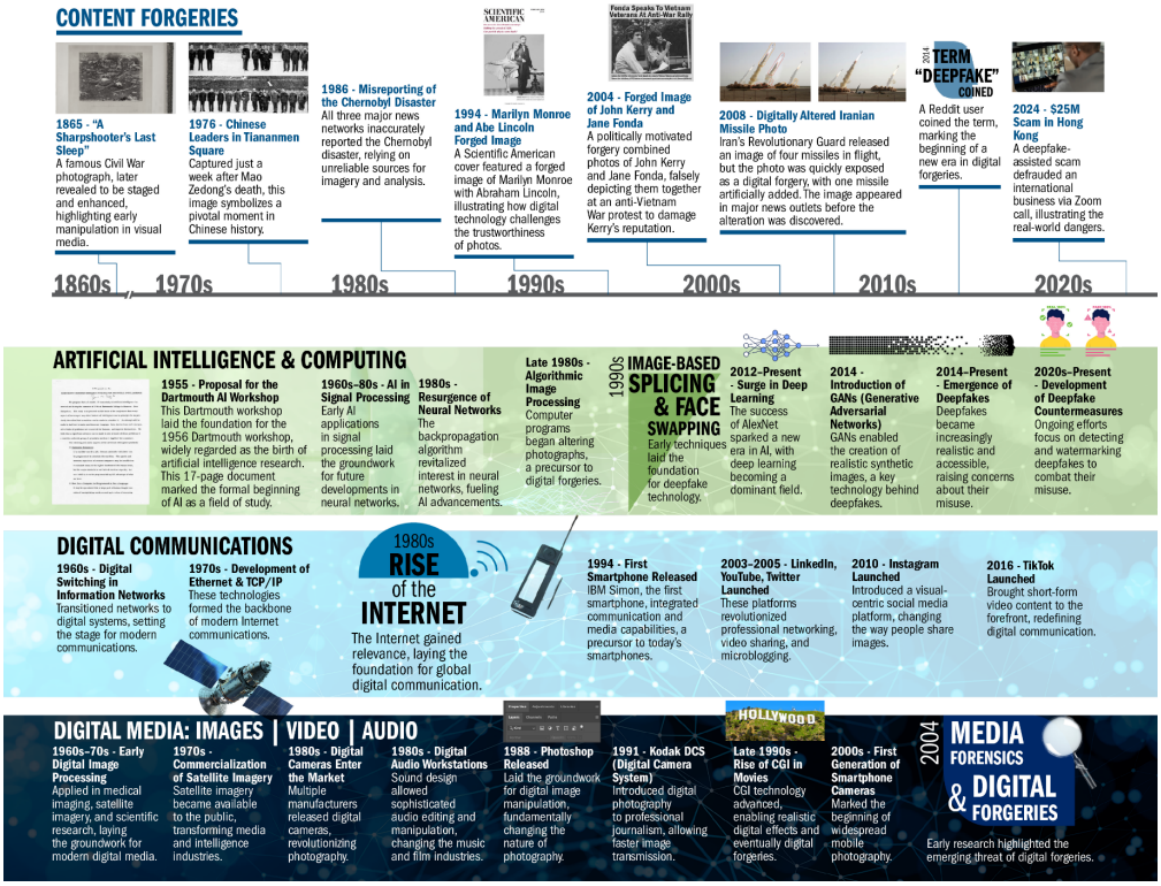


Figure 1.1. Infographic on the Evolution and Convergence of Technologies Forming the Basis of the Digital Content Forgeries

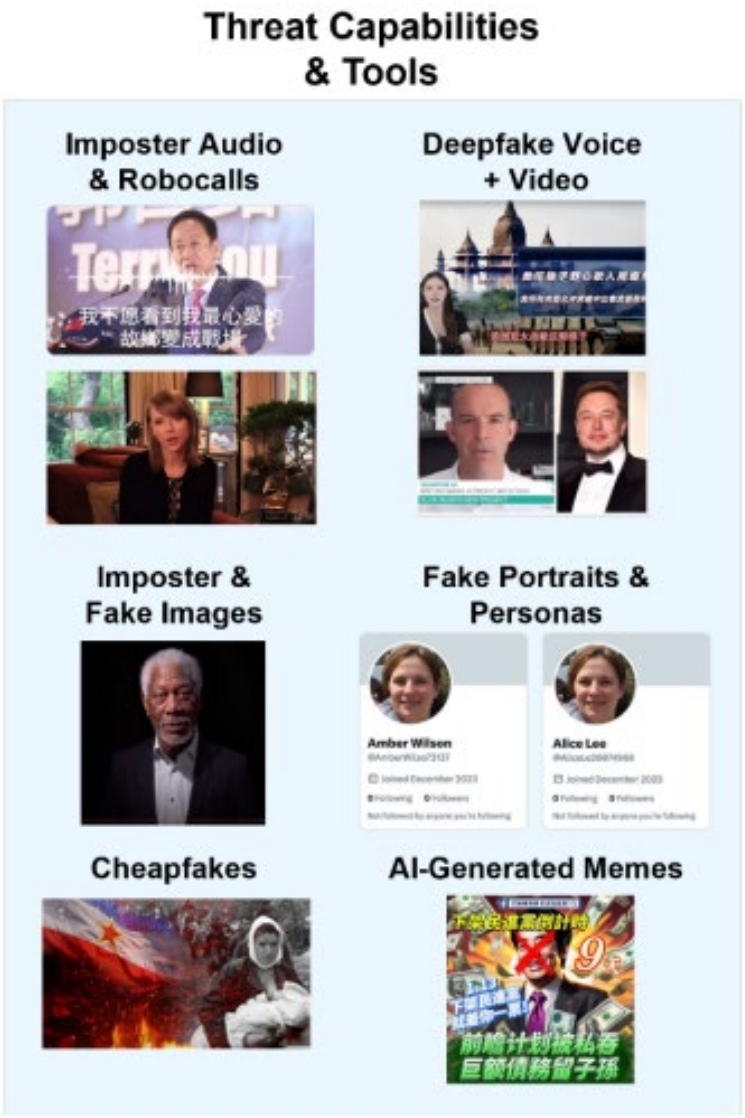


Figure 3.2. AI-generated news bulletin on IS's deadly Moscow concert hall attack.[138]

This incident underscores the ease with which deepfake technology can be used to create realistic forgeries that can deceive the public and authorities, resulting in potential dangers posed by deepfake technology exploited by terrorists to achieve malicious purposes, such as in a coordinated terrorist attack. The commonality between this example and a potential terrorist scenario lies in the exploitation of deepfake technology to manipulate public perception and create chaos, maximizing human casualties and damages.

Figure 3.4. A False Report of Explosion at Pentagon[140]

This incident highlights the growing threat of AI-generated deepfakes in spreading disinformation and manipulating public perception. The fake image was circulated by several Twitter accounts (now known as X), some of which had blue checkmarks — previously a symbol of verified accounts, but later obtainable by any user who subscribes to Twitter Blue. The hoax briefly impacted financial markets and demonstrated how easily deepfakes can be created and disseminated, raising concerns about the potential for future misuse of this technology.[141]

Alternative Analysis

AI's impact is overstated. Most content is still manual. - Low confidence

EU/NGO reporting reveals unprecedented volumes of AI-generated variants (including those for spawning and translation) that humans alone would struggle to produce at the same speed.

What would change our view: a sustained drop in near-duplicate AI-generated content and multilingual bursts after significant events. Forensic signs of manual-only pipelines.

Gen AI misuse is limited to fringe actors. - Low confidence

Adoption appears in right-wing and jihadist spaces, with AI voices/avatars/PDFs showing up on large channels, not just obscure forums. Certain right-wing groups that utilize AI include, Terrorgram, Britain First, and The American Futurist, among others. Also found among pro Al-Qaeda outlets, ISIS, Hamas, and Hezbollah.

ISIS/ISIS-K deepfake "news anchors."

ISIS and ISIS-Khorasan have pushed AI-generated anchor videos to claim or frame attacks, illustrating credible-looking propaganda at speed.

What would change our view: AI artifacts disappear from mainstream platforms and persist only on small, fringe sites.

Why This Matters for TINYg Members

- Quicker radicalization + tougher takedowns = higher risk. When people are radicalized faster and content is harder to trace and remove, the likelihood of incidents increases.
- Old filters miss new AI content. Traditional hash/keyword tools do not reliably catch synthetic, constantly modified, multi-variant media.
- More youth exposure → bigger long-term problem. Increased contact among minors with extremist content raises long-term security risks and makes prevention harder.

Recommendations for TINYg Member Organizations

1. Track patterns, not just posts. Flag sudden surges in activity, duplicate content appearing on multiple platforms, and the same message popping up in different languages.
2. Partner with schools/platforms for age-appropriate controls, digital literacy, and simple reporting
3. Test how easily your AI can be tricked into breaking safety rules regularly, and record any cases where it produces content that could help with recruitment, tactics, or attack planning.
4. Turn on tools that label and verify where images/videos come from, and have a ready-made communications and legal plan for how to respond if a deepfake appears.
5. Stay up to date with news from TINYg

Over The Horizon Threats

- AI “recruiter” bots operating inside encrypted messaging platforms.
- Large bursts of near-identical posts/videos (often across platforms and languages) right after high-profile events.
- Continued growth in teen/young-adult radicalization across EU member states.

Methodology

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

References

1. “Exploitation of Generative AI by Terrorist Groups,” ICCT, June 10 2022 (OSINT).
2. “Terrorism Situation and Trend Report,” Europol, 2025 (OSINT).
3. “Generating Terror: The Risks of Generative AI Exploitation,” CTC, January 2024 (OSINT).
4. “Terrorist Use of Generative AI,” Tech Against Terrorism, 2025 (OSINT).
5. “AI Chatbots Accelerate Youth Radicalisation and Terror Threat in Singapore,” OECD, 2025 (OSINT).
6. “The Convergence of Artificial Intelligence and Terrorism: A Systematic Review of the Literature,” Studies in Conflict and Terrorism, July 14 2025 (OSINT).
7. “Impacts of Adversarial Use of Generative AI on Homeland Security,” DHS, January 2025 (OSINT).

Analysis: Emerging Technology and Tactics -Lowering the Barrier to Entry: 3DPFs and Needle Spiking

Analyst: Bianca Thompson

BLUF

3D-printed firearms (3DPF) and needle spiking represent low-barrier, rapidly evolving threats that challenge detection, prevention, and law enforcement response.

Key Judgments

1. Improving open-source designs and consumer-grade printers for 3D-printed firearms presents a growing security gap. (OSINT, high confidence).
2. The success of needle spiking incidents in Europe raises concerns that it could be used as a delivery mechanism for a biological agent or toxin (OSINT, medium confidence).

Facts & Background

1. In July, New York authorities busted a “ghost gun kingpin” for making and selling firearms and accessories with 3D printers out of his home. Cops seized more than 110 guns, 67 suppressors, and 12 3D printers upon his arrest.
2. On June 21st, 2025, nearly 150 people were randomly pricked by syringes at a music festival in France. Perpetrators were not identified or arrested.

Analysis

3D-printed weapons: Accessibility of blueprints and cheap hardware lowers the barrier to entry, making 3DPFs increasingly attractive to extremist cells, organized crime, and lone actors who seek untraceable firearms or to circumvent gun laws.

The online 3DPF development communities and channels have demonstrated a significant presence of right-wing extremists and white-supremacists, meaning the continuous advancement of this technology is an inherent security risk.

Needle spiking: A needle spiking attack was successfully executed at a large scale, with little forensic evidence and no immediate arrests.

While incidents of needle spiking have thus far been limited to sedatives and other drugs, the injection method could potentially be utilized in a motivated attack as a delivery mechanism for a biological agent or toxin.

Alternative Analysis

Alt-1: 3DPFs are no more dangerous than regular firearms, and do not present any unique threat (Medium likelihood).

3DPFs increase the number of arms available to traffickers, gangs, terrorist organizations, etc., while limiting law enforcement's capability to solve crimes; 3DPFs could also eventually pose detection concerns.

Alt-2: Since the development of biological agents and toxins has a much higher barrier to entry, the threat of their utilization in a terrorist attack can not be considered a high likelihood. (Medium likelihood).

Some biological toxins do not require sophisticated labs to produce, meaning that they are theoretically accessible to lone actors. The aerosolization of toxins or agents is one of the most complicated parts of development, an obstacle avoided by an injection delivery.

Why This Matters for TINYg Members

Security Risk: The possibility of creating 3DPFs out of primarily plastic or non-metal materials, thus making them less detectable, is a significant security risk. Non-metal skeletons are not currently viable, but the online development community is rapidly evolving with the intent to improve the power and subtlety of 3DPFs. If the technology were to develop, it would render security measures like metal detectors inadequate.

Absence of protocol: If a needle-spiking attack employed the use of biological agents or toxins, emergency response services currently lack the protocol to identify and aid victims effectively. Since needle spiking attacks have so far been limited to date-rape drugs like GHB, responders would be unprepared to perform a comprehensive toxin screening and respond appropriately. Organizations managing large venues or events should be aware that needle-spiking attacks have the potential to escalate to something drastically more threatening.

Recommendations for TINYg Member Organizations

1. **Monitor 3DPF ecosystems:** Law enforcement and security agencies should monitor online design communities and extremist forums propagating weapon blueprints. Flag designs that subvert traditional security measures.
2. **Enhance venue security:** Security agencies should invest in superior detection technology (e.g., advanced imaging scanners) to potentially identify non-metal firearms that may bypass traditional metal detectors.
3. **Develop response protocols for needle spiking:** Train security and medical staff at venues to recognize symptoms, collect forensic evidence quickly, and coordinate rapid medical response.
4. **Prepare for bioterrorism scenarios:** Educate frontline personnel on how to escalate protocol in the event of a biological agent or toxin being employed.
5. **Stay tuned to TiNYg alerts.**

Over The Horizon Threats

Slaughter bots: The weaponization of unmanned vehicles (self-driving cars, UAS) through hacking.

Access Bypass: RFID/NFC cloning of ID badges and keycards can be used to duplicate access to private/restricted facilities.

Methodology

This report is based on open-source intelligence (OSINT), corroborated by independent analysis.

References

1. “Print and shoot: How 3D-printed guns are spreading online,” BBC, Jun 18, 2025 (OSINT)
2. “The emergence of 3D-printed firearms: An analysis of media and law enforcement reports,” NIH, March 28, 2025 (OSINT)
3. “Daniel Probeck Made, Sold 100+ Ghost Guns: Suffolk DA,” Daily Voice, July 10, 2025 (OSINT)
4. “Teen victim of mass festival ‘syringe stabbing’ tells of her terror as 145 attacked in assault ‘planned on social media’,” The Sun, June 23, 2025 (OSINT)
5. “Bioweapons,” NIH, October 5, 2002 (OSINT)

QTR Spotlight: Patrick Cumba

Patrick Cumba supports multiple Counterterrorism and Counterintelligence programs with his talented team at Patrick Cumba, LLC. He is a DOD-recognized SME in Police Operations and Protective Security. Since 2009, Patrick has served as a Liaison Officer and delegate to the UK, representing the US Government and Law Enforcement.

QTR: Among the most pressing threats, what do you think is an issue that is overlooked?

Cumba: In terms of US counterterrorism, it's online radicalization. It's been especially effective since October 7. Social media has created this big impact - it has no borders and anyone can reach this information. It's effective, borderless, and educational to this generation. They provide open-source information for TTP (tactics, techniques and procedures).

QTR: How has the national security landscape changed in recent years?

Cumba: We've gone from explosives and active shooters to virtual attacks or "cyber jihad." Instead of dying for an extremist cause, would-be terrorists can simply hack into infrastructure to create more impactful attacks.

QTR: What emerging technologies are creating new challenges in security?

Cumba: It's more about mitigation and defense, not technology itself. You have to keep up with emerging technology through network assessment and penetration testing. It's continuously changing, and there's no easy fix.

QTR: What new strategies and techniques have the most potential to combat terrorism?

Cumba: Rapid screening quickens the throughput of people but it's not always effective. There's also evolving technology and equipment that can listen in to special key words and specific names, which makes it less disruptive but maintains effectiveness. It's important to keep the combination of highly trained people and high-end tech.

QTR: Follow-up question on that: how do we best protect soft targets?

Cumba: We should be trying to give grants to police agencies to support counterintelligence, and as AI progresses, it will be cheaper and simpler. The best is to be in front of the attack or mitigate before the attack happens.

QTR: What is an ethical issue in intelligence and security that you think requires more attention?

Cumba: People retiring out of government and then going to a foreign country on contract.

(Interview has been 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 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

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