**Letter from the Editor**

This quarter reflects a threat environment that is not only persistent, but increasingly adaptive, decentralized, and difficult to categorize. Across regions, we are observing the continued erosion of traditional boundaries between terrorism, organized crime, state conflict, and emerging technology driven risks. What once existed as distinct threat streams are now converging, creating a more complex and less predictable operating environment for governments, the private sector, and civil society.

Several trends emerged with notable consistency. First, instability is increasingly driven by fragmentation rather than consolidation. From cartel dynamics in Mexico to hybrid extremist ecosystems in North America and Europe, leadership disruption, decentralization, and digital connectivity are producing more diffuse and resilient threat actors. These are networks that are harder to attribute, harder to disrupt, and often more opportunistic in how they operate. For TiNYg members, this means that risk is less likely to present as a single, identifiable threat and more likely to emerge through localized disruption, insider risk, or rapidly evolving incidents that directly impact personnel, facilities, and operations.

Second, the role of technology continues to expand across the threat landscape. This is not limited to advanced capabilities, but includes the commodification of tools that lower the barrier to entry. Artificial intelligence, biometric systems, and digital platforms are simultaneously strengthening detection and prevention while also enabling surveillance, disinformation, identity exploitation, and operational planning by adversaries. As highlighted in this quarter's Emerging Technology assessment and our interview with Michael Bryan, the most immediate risk is not necessarily the creation of novel threats, but the amplification of existing ones. For private sector organizations, this translates into increased exposure to fraud, identity compromise, reputational risk, and the potential for adversaries to exploit corporate systems and data in ways that were previously limited to state actors.

Third, criminal and security dynamics are increasingly overlapping. In Latin America and the Caribbean, as well as in parts of Africa and Southeast Asia, transnational criminal organizations continue to expand influence through both violence and economic control. Their activities are no longer confined to illicit markets but are shaping governance, migration, and regional stability. Importantly, these actors remain primarily profit driven, which has implications for how they behave during high visibility events such as the upcoming 2026 FIFA World Cup. As our Mexico assessment underscores, the primary risk is not large scale attack, but exploitation, disruption, and localized violence. For TiNYg

members, this means elevated risk to supply chains, travel, logistics, and personnel safety, particularly in high traffic or economically significant environments.

Geopolitical tensions also continue to shape the broader environment. Escalation involving Iran and its regional proxies, persistent instability in Afghanistan, and strategic friction in East Asia all reinforce a global landscape where localized conflict can have cascading effects. These dynamics influence everything from maritime security and energy markets to domestic radicalization narratives and diaspora tensions. For organizations operating internationally, this creates volatility in operating environments, increased regulatory and compliance risk, and potential disruption to global business continuity.

At the same time, the threat environment is becoming more personal. Lone actor violence, grievance driven attacks, and localized extremist activity remain among the most difficult threats to detect and prevent. These incidents are often enabled by online ecosystems, amplified by real world events, and carried out with minimal coordination. The result is a form of violence that is both unpredictable and increasingly embedded within everyday environments. For the private sector, this reinforces the need to view security not only as a perimeter issue, but as a workforce and workplace issue that directly affects employees, customers, and brand exposure.

We close this quarter's report with a spotlight interview with Michael Bryan, whose experience across medicine, research, and counterterrorism offers a grounded perspective on the evolving intersection of artificial intelligence and biological risk. His insights reinforce a critical point: our greatest vulnerability is often not a lack of capability, but a failure to recognize emerging threats early and respond in a coordinated way. That observation is particularly relevant for organizations that must balance security, operations, and resource constraints in real time.

As always, the purpose of the QTR is not to alarm, but to inform. The trends outlined in this report do not point to a single defining threat, but rather to a landscape characterized by convergence, adaptation, and persistent uncertainty. Understanding these patterns is essential for anticipating risk, prioritizing resources, and strengthening resilience. For TiNYg members, this means maintaining situational awareness, investing in both physical and digital security measures, and ensuring that security considerations are integrated into operational and strategic decision making.

Deepest Regards,

Dr. Donell Harvin

Editor, TiNYg Quarterly Threat Report

**Q1 TINYg Quarterly Threat Report**

MENA Region Threat Intelligence Desk

**Title: Destabilizing MENA Trends: Iran Conflict, Energy Disruption, Great Power Competition, Hezbollah Reconstitution, and Gaza Diplomacy**

Analyst: Abigail Becker

## BLUF (Bottom Line Up Front)

Escalation involving Iran, Israel, and the United States has evolved into a multi front regional conflict characterized by retaliatory strikes, proxy engagement, and disruption to energy infrastructure. These dynamics are driving global economic instability, elevating security risks, and creating opportunities for both state and non state actors to expand influence.

## Key Judgments

### 1. U.S. and Israeli operations have degraded elements of Iran leadership structure

Targeted strikes against senior Iranian officials likely disrupted command and control; however, the regime retains sufficient capacity to sustain coordinated retaliation (high confidence).

**2. Iran is conducting a sustained regional retaliation campaign**

Iran has demonstrated intent and capability to target U.S. assets and partners across multiple theaters, indicating a coordinated response despite leadership losses (high confidence).

**3. Energy disruption is driving global economic instability**

Attacks on Gulf energy infrastructure and constraints on maritime transit through key chokepoints are contributing to sustained volatility in global oil and gas markets (high confidence).

**4. The conflict is creating strategic opportunities for Russia and China**

Both actors are positioned to exploit reduced U.S. focus and regional instability to expand economic and geopolitical influence (medium confidence).

**5. Diplomatic efforts in Gaza remain limited and fragile**

Parallel diplomatic activity continues, but progress toward durable agreements remains uncertain and vulnerable to broader regional escalation (medium confidence).

**Facts and Background**

Late February 2026 marked the onset of large scale hostilities involving Iran, Israel, and the United States. Multiple senior Iranian officials were reported killed in targeted strikes; reporting on specific individuals remains inconsistent across sources (OSINT, medium to high confidence).

Iran has conducted retaliatory strikes using drones and missiles against U.S. and partner assets across the region, including military installations and diplomatic facilities (OSINT, high confidence).

Disruptions to maritime transit through the Strait of Hormuz and attacks on regional energy infrastructure have contributed to significant volatility in global energy markets (OSINT, high confidence).

Energy infrastructure across the Gulf has been targeted, including facilities in Qatar, Kuwait, and the United Arab Emirates (OSINT, medium confidence).

Russia and China are leveraging the conflict environment to expand influence, including through energy market positioning and strategic engagement (OSINT, medium confidence).

Hezbollah has resumed large scale operations against Israel, launching sustained missile attacks and prompting significant Israeli counterstrikes in Lebanon (OSINT, high confidence).

Diplomatic efforts in Gaza continue, including proposals for ceasefire oversight and disarmament; outcomes remain uncertain (OSINT, medium confidence).

## Regional Analysis

### Iran Conflict

The escalation represents the most significant regional conflict in recent years. While leadership targeting has disrupted aspects of Iranian command and control, it has not resulted in regime collapse.

### Energy and Maritime Risk

Constraints on the Strait of Hormuz and attacks on energy infrastructure highlight the vulnerability of global supply chains.

### Great Power Competition

Russia and China are positioned to capitalize on the conflict by expanding influence in energy markets and regional diplomacy.

### Hezbollah Reconstitution

Hezbollah renewed operational tempo demonstrates resilience and continued reliance on Iranian support networks.

### Gaza Diplomacy

Ongoing diplomatic initiatives remain fragile and vulnerable to broader escalation.

## Alternative Analysis

Alt 1 The conflict de escalates and remains contained (low likelihood).

Alt 2 Energy markets stabilize in the near term (low likelihood).

Alt 3 Hezbollah becomes operationally constrained (medium likelihood).

Alt 4 Gaza disarmament efforts succeed (medium likelihood).

## Why This Matters

Global economic risk is elevated due to sustained disruption in energy markets and maritime transit routes.

Private sector entities face increased exposure to supply chain disruption, security threats, and regional instability.

Expanded proxy warfare increases risk to personnel, infrastructure, and operations.

Strategic competition between major powers is intensifying.

## Recommendations for TINYg Member Organizations and Possible Mitigations

Diversify logistics and energy supply routes where feasible.

Enhance cyber and insider threat defenses against state and proxy actors.

Update contingency planning for operations in high risk regions.

Strengthen physical security at ports and logistics hubs.

Coordinate with partners operating near conflict zones.

## Over the Horizon Threats

Sustained use of low cost drone systems may create long term cost imbalance for defensive systems.

Environmental and infrastructure damage may contribute to secondary crises.

Prolonged conflict may increase radicalization and recruitment.

Reduced focus in secondary theaters may enable extremist resurgence.

## Methodology

This assessment draws on open source intelligence, expert analysis, and publicly available reporting. Information was cross validated across multiple sources.

**Q1 TINYg Quarterly Threat Report**

Sub Saharan Africa Threat Intelligence Desk

**Title: Al Shabaab and Houthi Alliance in East Africa and the Red Sea**

Analyst: Callie Mitchell

**BLUF (Bottom Line Up Front)**

Increased collaboration between Somalia based Al Shabaab and Yemen based Houthis in the Red Sea is generating heightened threats to maritime security and commercial shipping, while also expanding Houthi influence into East Africa.

**Key Judgments**

**1. Al Shabaab Houthi Collaboration Increases Regional Instability**

a. Both groups gain operational advantages from this partnership, including access to training and weapons. These capabilities increase lethality and strengthen insurgent operations, contributing to regional instability.

**2. Domestic Unpopularity in Yemen Driving Strategic Realignment**

a. Yemeni civilians are increasingly war fatigued and resentful of Houthi governance due to prolonged sanctions, humanitarian conditions, violence, and infrastructure degradation. This environment likely incentivizes the Houthis to expand operations externally to justify continued mobilization.

**3. US Israel Iran Conflict Contributing to Shipping Disruptions in the Red Sea**

a. The Houthis and Al Shabaab were primary threats to regional shipping prior to the escalation of the US Israel Iran conflict on February 28, 2026. Iran, as a state sponsor of the Houthis, has restricted access to both the Strait of Hormuz and the Bab al Mandeb Strait, which are critical commercial and energy transit routes.

**Facts and Background**

1. Since 2023, the Houthis have conducted attacks on vessels transiting the Red Sea in response to Israel's war in Gaza.

2. The Houthis are expanding engagement in East Africa to gain operational advantages, including the transfer of weapons, technical expertise, and small arms to Al Shabaab (OSINT, high confidence).

3. Despite sectarian differences, the Houthis and Al Shabaab share common adversaries, including the United States, Israel, and Gulf states aligned with Western interests (OSINT, high confidence).

4. The Houthis are training Al Shabaab in drone operations and improvised explosive device manufacturing, increasing precision strike capability and operational effectiveness. This knowledge transfer is likely informed by Iranian backed Hezbollah practices (OSINT, medium confidence).

5. The Houthis are exploiting structural vulnerabilities in East Africa, including porous coastlines, weak central governance, established smuggling networks, and proximity to Red Sea shipping corridors (OSINT, medium confidence).

**Regional Analysis**

Al Shabaab is a Somalia based Sunni Islamist terrorist organization founded in 2004 during a period of political instability. It remains the most capable militant group in Somalia and is affiliated with Al Qaeda. The group conducts transnational attacks, particularly in Kenya, and seeks to establish an Islamic state in Somalia by overthrowing the current federal government.

The Houthis are a Zaydi Shia movement based in Yemen that emerged in opposition to the central government and perceived Saudi influence. In 2014, tensions escalated into civil

war, resulting in Houthi control of Sanaa. Historically confined to Yemen, the group is now expanding its operational reach through collaboration with Al Shabaab.

This emerging collaboration represents a shift in the regional threat environment, indicating a growing willingness among militant organizations to deprioritize ideological differences in favor of operational and strategic gains.

**Alternative Analysis**

Alt 1: Limited impact on shipping networks (medium likelihood) due to competing regional conflicts. To date, both groups have reduced visible activity following escalation involving Iran.

Alt 2: Increased collaboration and operational tempo (low likelihood) driven by broader regional conflict involving Iran, Israel, and the United States.

Alt 3: Enhanced Al Shabaab capabilities, including drone and IED integration, could enable renewed insurgent campaigns against the Somali government with indirect Houthi support (low likelihood). Current indicators suggest focus remains on capability development.

**Why This Matters**

**1. Shipping Security and Economic Impact**

a. Maritime security remains the primary concern due to persistent threats along key Red Sea chokepoints.

b. Elevated risk has increased shipping costs, with rerouting required around the African continent.

**2. Maritime Safety**

a. Attacks on vessels increase risk to commercial operators, local fishing communities, and coastal populations.

**3. Human Rights Implications**

a. A more capable Al Shabaab increases the likelihood of complex, high casualty attacks in Somalia and Kenya.

**4. Governance and Regional Stability**

a. Cross ideological militant collaboration presents a broader destabilization risk to regional governments and security frameworks.

**Recommendations for TINYg Member Organizations**

1. TINYg members should avoid maritime transit through the Red Sea and adjacent waterways.

2. TINYg members should avoid non essential travel to East Africa and the Middle East due to elevated security risks and potential disruptions.

3. TINYg members should continue monitoring developments through TINYg reporting and updates.

**Over the Horizon Threats**

Sunni Shia militant collaboration across regions represents a notable evolution in transnational extremist behavior.

Sunni Shia insurgent group collaboration is historically rare and indicates a shift toward pragmatic alliances focused on operational effectiveness rather than ideology.

Represents cross regional coordination across East Africa and the Red Sea.

Activity is likely to expand in areas of geographic and operational convergence.

Intelligence gaps remain regarding the scale and durability of this collaboration, requiring continued monitoring.

**Methodology**

This product draws on open source intelligence, threat assessments, and media reporting. Information was cross validated across multiple reputable sources.

**References**

Blitz (2026, February 25). Yemeni Houthis are expanding the battlefield into East Africa. https://weeklyblitz.net/2026/02/25/yemeni-houthis-are-expanding-the-battlefield-into-east-africa/

The New York Times (2026, March 1). US Israeli Attacks on Iran Disrupt Shipping in the Red Sea. https://www.nytimes.com/2026/03/01/world/middleeast/maersk-red-sea-iran-war.html

Africa Defense Forum (2025, November 25). UN Report Shows Increasing Collaboration of Houthis, Al Shabaab. https://adf-magazine.com/2025/11/u-n-report-shows-increasing-collaboration-of-houthis-al-shabaab/

Council on Foreign Relations (2022, March 31). Al Shabaab in East Africa. https://www.cfr.org/timelines/al-shabaab-in-east-africa

Australian Parliament House of Representatives Committees (2012, October 10). Appendix C Statement of Reasons Al Shabaab. https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Completed_Inquiries/pjcis/five_terrorist/report/appendixc

**Q1 TINYg Quarterly Threat Report**

Central Asia Threat Intelligence Desk

**Title: Central Asia Threat Report**

Analyst: Bianca Thompson, Callie Mitchell

**BLUF (Bottom Line Up Front)**

Terrorist activity within Central Asia remains low; however, cross border militant movement linked to the Islamic State Khorasan Province continues to pose a credible external threat, requiring sustained border security and counter radicalization efforts.

**Key Judgments**

**1. Terrorist Attacks in Central Asia Remain Limited**

a. There have been no confirmed domestic terrorist attacks in Central Asia in 2026.

**2. ISIS K Remains the Primary Threat Actor**

a. The group maintains operational capability in Afghanistan, and recruitment pipelines remain active.

**3. Cross Border Militant Activity Persists Along the Afghan Border**

a. Central Asia continues to face regional spillover risk, contributing to persistent security concerns.

**Facts and Background**

Regional security services report a low incidence of domestic terrorism, with minimal successful attacks or credible attempts (OSINT, high confidence).

A January 2026 bombing in Kabul that killed seven individuals was claimed by ISIS K, demonstrating continued operational capability and the potential for cross border influence (OSINT, high confidence).

Five individuals were killed in December 2025 during a clash between Tajik security forces and militants attempting to enter Tajikistan. While no group claimed responsibility, the Tajik government assessed the incident to be linked to instability in Taliban controlled Afghanistan, though this attribution remains unconfirmed (OSINT, medium confidence).

**Regional Analysis**

Despite the absence of major domestic attacks, Central Asia's proximity to Afghanistan creates ongoing exposure to militant infiltration. ISIS K's demonstrated ability to conduct attacks in Kabul and surrounding areas indicates a sustained threat environment.

Regional governments continue to prioritize border security, intelligence sharing, and counter radicalization programs to mitigate these risks.

**Alternative Analysis**

Alt 1: Militants are primarily criminal actors (low likelihood). While some border incidents involve smuggling networks, ISIS K's established presence and attack history make this unlikely.

Alt 2: Central Asia may become a near term target zone (medium likelihood). A northward shift in ISIS K operational focus could increase domestic attacks, though current trends do not indicate imminent targeting.

**Why This Matters**

**1. Potential for Rapid Threat Escalation**

a. Demonstrated regional operability indicates the potential for increased attacks if ISIS K strategy shifts.

**2. Cross Border Instability**

a. Instability in Afghanistan remains the primary driver of spillover risk into Central Asia.

**3. Economic and Resource Implications**

a. Regional instability could disrupt production and export of energy and natural resources.

**4. Transnational Threat Linkages**

a. Central Asian nationals have been identified in international ISIS related attacks, indicating continued relevance to global threat networks.

**Recommendations for TINYg Member Organizations and Possible Mitigations**

1. TINYg members should continue monitoring regional developments, as increased activity may indicate a shift in ISIS K strategy.

2. TINYg members should exercise caution in travel and workforce vetting, given the potential for spillover activity and ongoing radicalization pipelines.

**Over the Horizon Threats**

Potential northward expansion of ISIS K operations into Central Asia

Increased cross border infiltration as instability persists in Afghanistan

Continued foreign fighter mobilization involving Central Asian nationals

**Methodology**

This product draws from open source intelligence, threat assessments, and media reporting. Information was cross validated across multiple reputable sources.

**Q1 TINYg Quarterly Threat Report**

Southeast Asia Threat Intelligence Desk

**Title: Terror in Southeast Asia**

Analyst: Lamont Pyykkonen

**BLUF (Bottom Line Up Front)**

Continued terrorist activity and cross border tensions between Pakistan and Afghanistan, combined with evolving counterterrorism measures in India and persistent transnational criminal activity in Southeast Asia, are contributing to a complex and evolving regional threat environment. Escalation between Pakistan and Afghanistan may create conditions that enable terrorist organizations such as Al Qaeda and ISIS K to expand operational capability as state security resources are diverted.

**Key Judgments**

**1. Pakistan cross border strikes may degrade TTP but require Taliban cooperation**

Pakistan military operations may reduce Tehrik e Taliban Pakistan presence near its border; however, sustained success is unlikely without cooperation from Taliban authorities in Afghanistan (medium confidence).

**2. Regional crackdown on scam centers is disrupting transnational criminal activity**

Multiple Southeast Asian governments are intensifying enforcement actions against large scale scam operations, resulting in arrests, facility closures, and victim repatriation (high confidence).

**3. India counterterrorism posture may reduce attack success rates**

India PRAHAAR policy emphasizes proactive disruption of terrorist financing, misinformation, and radicalization, which may reduce the likelihood of successful attacks over time (medium confidence).

## Facts and Background

1. The Balochistan Liberation Army conducted a coordinated attack across Balochistan province.

2. Pakistan conducted cross border strikes against suspected Tehrik e Taliban Pakistan positions along the Afghanistan border, claiming to have killed at least 70 fighters (OSINT, high confidence).

3. A February 2026 suicide bombing at a Shia mosque in Islamabad resulted in casualties (OSINT, high confidence).

4. Pakistan conducted additional strikes targeting alleged militant positions in Afghanistan; reporting on outcomes remains inconsistent (OSINT, low confidence).

5. Pakistan reported significant Taliban casualties from strikes, while Taliban sources reported substantially lower figures, indicating conflicting claims (OSINT, low confidence).

6. A November 2025 vehicle borne explosion in New Delhi caused multiple fatalities and injuries.

7. Investigations indicate involvement of educated individuals radicalized through extremist networks (OSINT, high confidence).

8. India introduced its PRAHAAR counterterrorism policy in February 2026, emphasizing prevention, response, capacity aggregation, rule of law, counter radicalization, international alignment, and recovery (OSINT, high confidence).

## Regional Analysis

### Terrorism Dynamics

Tehrik e Taliban Pakistan militants remain active along the Pakistan Afghanistan border, conducting cross border movement and attacks. Pakistan has responded with cross border strikes targeting suspected militant positions, increasing tensions with Taliban authorities.

Pakistan also faces persistent domestic terrorism in Balochistan, where militant groups continue attacks on government infrastructure and state assets.

India has increased focus on identifying and mitigating domestic radicalization, particularly among educated populations, following recent attacks.

**Regional Trend Scam Centers**

Southeast Asia continues to face widespread human trafficking linked to scam centers, particularly in Cambodia, Myanmar, and Thailand. Individuals are recruited under false pretenses and forced into conducting large scale fraud operations targeting victims globally.

Reporting indicates significant financial impact, with billions of dollars lost annually. Increased international pressure and economic impacts have prompted regional crackdowns, resulting in arrests, facility closures, and repatriation of victims.

**Why This Matters**

Terrorism Risk Escalation between Pakistan and Afghanistan may create permissive conditions for terrorist organizations to expand while state resources are diverted.

Criminal Risk Scam centers present significant financial and cyber risk to organizations through fraud, extortion, and data exploitation.

Regional Stability Continued cross border tensions and uneven enforcement environments increase overall instability across interconnected regions.

**Alternative Analysis**

Alt 1 Pakistan and Afghanistan reach a limited agreement on managing TTP presence (low likelihood). While de escalation is possible, enduring ties between TTP elements and Taliban structures make full removal from border areas unlikely.

Alt 2 Pakistan continues sustained cross border operations (medium likelihood). Continued strikes may degrade militant positions but are unlikely to eliminate TTP capability entirely.

**Recommendations for TINYg Member Organizations and Possible Mitigations**

1. Enhance cybersecurity awareness and employee training to mitigate scam related risks.

2. Monitor regional security developments, particularly along the Pakistan Afghanistan border.

3. Exercise increased caution in travel and operations in affected regions.

4. Continue monitoring official travel advisories and TINYg reporting.

**Over the Horizon Threats**

Continued clashes between Pakistan and militant groups along the Afghanistan border

Potential escalation in Pakistan Afghanistan tensions impacting regional stability

Expansion of scam center operations into new geographic areas if enforcement pressure shifts

Possible movement of foreign fighters or militant elements in response to broader geopolitical instability

**Methodology**

This product draws from open source intelligence, threat assessments, and media reporting. Information was cross validated across multiple reputable sources.

**Q1 TINYg Quarterly Threat Report**

East Asia and Oceania Threat Intelligence Desk

## Title: Rising Social Tensions in Australia and Strategic Friction Between China and Japan

Analyst: Naomi Horner, Julia Hammerschlag

### BLUF (Bottom Line Up Front)

The December 2025 attack in Australia has contributed to increased antisemitic and Islamophobic incidents, elevating risks to communities and soft targets. At the same time, worsening China Japan relations are contributing to economic pressure and maritime tension. While escalation risks remain elevated, near term kinetic conflict between China and Japan is unlikely.

### Key Judgments

#### 1. China Japan relations are unlikely to normalize in the near term

Ongoing political positioning and strategic competition suggest tensions will persist, particularly in relation to Taiwan and regional security dynamics (high confidence).

#### 2. Houses of worship in Australia face elevated threat levels

Increased antisemitic and Islamophobic incidents following the December 2025 attack have heightened risks to religious institutions and gatherings (high confidence).

**3. Extremist groups in Australia are likely to adapt rather than diminish**

In response to new legislation, extremist actors are likely to decentralize and adjust tactics rather than disengage from activity (high confidence).

**4. Government responses may contribute to domestic tension**

New legislation targeting hate speech and extremist activity may generate legal and social friction, particularly regarding civil liberties and differing community perceptions of protection (medium confidence).

## Facts and Background

Japan signaled potential support for Taiwan in the event of a conflict, prompting economic and political responses from China, including export restrictions and pressure campaigns (OSINT, high confidence).

China has applied economic measures, including restrictions on key materials and influence operations targeting tourism and public perception (OSINT, medium to high confidence).

A maritime incident involving a Chinese vessel and Japanese authorities highlighted ongoing friction in contested areas (OSINT, high confidence).

In December 2025, a mass casualty attack at a religious gathering in Australia contributed to a significant increase in reported antisemitic incidents (OSINT, high confidence).

Reporting indicates a substantial rise in Islamophobic incidents following the attack, including threats directed at religious institutions (OSINT, high confidence).

The Australian government introduced legislation targeting hate groups, extremist content, and recruitment, including enhanced penalties and expanded enforcement authority (OSINT, high confidence).

Extremist groups have demonstrated adaptive behavior, including modifying online presence and continuing offline activity (OSINT, medium to high confidence).

## Regional Analysis

### Australia Domestic Security Environment

The attack has intensified social tensions and increased the threat environment for religious communities. Legislative responses aim to address extremist activity but may also generate concerns related to civil liberties and uneven application.

**Extremist Adaptation**

Restrictions on organizations and symbols are likely to reduce overt activity but encourage decentralized and less visible forms of organization and communication.

**China Japan Strategic Friction**

Economic pressure, maritime incidents, and political signaling continue to drive tension between China and Japan. These dynamics increase the risk of miscalculation, though both states retain incentives to avoid direct conflict.

**Emerging Trend Technology Enabled Exploitation**

Illicit activities such as covert recording and digital exploitation highlight broader challenges related to privacy, cyber risk, and regulatory enforcement in parts of East Asia.

**Alternative Analysis**

Alt 1 China Japan relations stabilize more rapidly than expected (low likelihood). Historical patterns suggest tensions may plateau, but structural drivers make near term normalization unlikely.

Alt 2 Government measures significantly reduce extremist activity (low likelihood). While enforcement may disrupt visible networks, underlying drivers of radicalization are likely to persist.

**Why This Matters**

Increased threat to soft targets, including religious institutions and public gatherings.

Elevated reputational and operational risks for organizations operating in affected environments.

Economic and geopolitical tension may impact trade, tourism, and regional stability.

Legal and regulatory changes may introduce compliance risks for international organizations.

**Recommendations for TINYg Member Organizations and Possible Mitigations**

Enhance security awareness for personnel and facilities, particularly in high visibility or sensitive environments.

Monitor evolving legal frameworks in Australia to ensure compliance with new restrictions.

Strengthen partnerships with local stakeholders and security entities where appropriate.

Increase awareness of regional geopolitical developments affecting operations and supply chains.

**Over the Horizon Threats**

Continued social tension and potential for copycat or opportunistic attacks

Persistent China Japan friction with risk of maritime incidents

Expansion of technology enabled exploitation and cyber related risks

Potential shifts in regional trafficking or illicit activity patterns

**Methodology**

This product draws from open source intelligence, threat assessments, and media reporting. Information was cross validated across multiple reputable sources.

**Q1 TINYg Quarterly Threat Report**

Europe Threat Intelligence Desk

**Title: Expansion of Russian Linked Criminal Networks, Organized Crime, and Violent Extremism**

Analyst: Manuel Del Valle

**BLUF (Bottom Line Up Front)**

Europe faces a persistent and evolving threat environment characterized by hybrid activity, organized crime expansion, and ideologically diverse violent extremism. Russian linked criminal activity and hybrid tactics are increasing pressure on state and private sector security systems, while organized crime and extremist actors continue to expand operational reach across the region.

**Key Judgments**

**1. Russian linked criminal activity is increasing across Europe**

The use of intermediaries and low visibility operatives suggests a strategy focused on maintaining plausible deniability while gradually degrading the security capacity of targeted states (high confidence).

**2. Hybrid tactics represent a primary threat vector**

Cyber activity, disinformation campaigns, and exploitation of extremist networks are being used to target critical infrastructure and generate sustained disruption (high confidence).

**3. Policy responses face implementation challenges**

New security frameworks have been introduced to counter hybrid threats; however, declining political cohesion across European states may limit consistent implementation (medium confidence).

**4. Organized crime networks are expanding and adapting**

Growth in cyber enabled crime, cocaine trafficking, and synthetic drug markets highlights increasing sophistication and cross border coordination among criminal actors (medium confidence).

## Facts and Background

In December 2025, cyber activity targeted elements of Poland energy sector, including renewable energy and industrial systems. Polish authorities assessed the activity as linked to Russian actors with moderate confidence (OSINT, medium confidence).

In January 2026, the European Commission identified a cyber incident affecting its mobile device management system. While no devices were confirmed compromised, potential exposure of staff information was reported (OSINT, high confidence).

A total of 151 incidents linked to Russian activity have been documented between February 2022 and early 2026, including 41 additional cases identified in late 2025 and early 2026 (OSINT, high confidence).

In February 2026, German authorities indicted an individual in connection with a suspected parcel device plot assessed as linked to Russian intelligence activity (OSINT, medium confidence).

In March 2026, Europol supported the disruption of a cocaine trafficking network linked to external criminal organizations, highlighting ongoing transnational criminal activity (OSINT, high confidence).

## Regional Analysis

### Hybrid Threat Environment

Russian linked activity continues to combine cyber operations, disinformation, and limited physical disruption, including sabotage and arson. This approach is designed to erode public trust and create cumulative pressure on security systems.

**Organized Crime**

Organized criminal networks are expanding, with foreign linked groups playing a significant role in drug trafficking and associated violence. These dynamics contribute to localized insecurity and may generate secondary effects, including increased political and social tensions.

**Terrorism**

The terrorist threat environment remains persistent and diverse. Risks include self radicalized individuals, digitally enabled extremist networks, and potential indirect support from foreign actors. Likely targets remain public spaces, transportation infrastructure, and symbolic locations.

**Alternative Analysis**

Alt 1 Overestimation of coordinated hybrid activity (low likelihood). Some incidents may be opportunistic or criminal in nature rather than part of a coordinated campaign; however, broader patterns support a structured hybrid approach.

Alt 2 Polarization driven primarily by domestic factors (medium likelihood). Political polarization may be driven largely by internal dynamics rather than external influence; however, foreign actors are likely amplifying these trends.

**Why This Matters**

Disruption to critical infrastructure presents operational risk to both public and private sector entities.

Increasing frequency and complexity of attacks will likely drive higher security and compliance costs.

State linked activity complicates attribution and response for intelligence and law enforcement agencies.

Persistent instability may impact investment environments and key economic sectors across Europe.

**Recommendations for TINYg Member Organizations and Possible Mitigations**

Strengthen cybersecurity and infrastructure resilience measures.

Increase monitoring of online platforms to identify indicators of radicalization or emerging threats.

Enhance financial monitoring to identify suspicious transaction patterns linked to criminal or extremist activity.

Maintain awareness through TINYg reporting and regional updates.

**Over the Horizon Threats**

Escalation in the Middle East may contribute to increased extremist activity or polarization within European states.

Previously compromised data from cyber incidents may be leveraged for future operations or targeting.

Increasing cooperation among transnational criminal groups may expand operational reach and diversify activities across the region.

**Methodology**

This product draws from open source intelligence, threat assessments, and media reporting. Information was cross validated across multiple reputable sources.

**Q1 TINYg Quarterly Threat Report**

South America Threat Intelligence Desk


**Title: Early 2026 Indicators of Regional Instability: Armed Non State Actor Opportunity and Escalating Transnational Criminal Organization Violence**

Analyst: Sam Rosenblum

**BLUF (Bottom Line Up Front)**

Escalating violence in corridor economies, particularly Ecuador, persistent sanctuary dynamics, and online extremist narrative opportunism signal growing instability across key transit states and border regions in South America. These conditions create opportunities for terrorist organizations and transnational criminal organizations to expand operational influence and diversify illicit revenue streams, increasing operational, compliance, and personnel security risks for private sector organizations.

**Key Judgments**

**1. Regional instability is creating exploitable conditions for armed non state actor expansion**

Political volatility and weakening state control in high friction zones increase the likelihood that insurgent and terrorist aligned groups will expand territorial influence and revenue generation (medium high confidence).

**2. Transnational criminal organizations are shifting toward more violent competition in strategic transit hubs**

Fragmentation and competition over trafficking corridors and port infrastructure increase the likelihood of sustained high intensity violence in 2026 (high confidence).

**3. Hybrid convergence between TCOs and armed actors is likely to deepen**

Expansion into illegal mining, environmental crime, and cyber enabled financial activity increases overlap between criminal and politically motivated violence networks (medium confidence).

**4. Geopolitical shocks are accelerating extremist narrative mobilization online**

Disruption events are being leveraged by extremist ecosystems to amplify grievance framing and recruitment messaging across multiple platforms (medium confidence).

**5. Structural security drivers are unlikely to reverse in the near term**

Institutional responses are increasing, but entrenched trafficking incentives and corruption dynamics suggest violence levels will remain elevated through at least Q2 2026 (medium confidence).

**Facts and Background**

Ecuador violence metrics elevated (OSINT, high confidence): Reporting indicates Ecuador entered the top ten most violent countries globally in early 2026 due to escalating gang violence. ACLED reporting identifies widespread organized crime related violence in 2025 that continues into 2026. Coastal cities such as Guayaquil and Duran have become key export hubs for cocaine shipments, with homicide rates exceeding 100 per 100000 in contested zones.

Rising homicide and trafficking linked violence (OSINT, high confidence): UNODC reporting documents expanding cocaine markets and sustained homicide increases along trafficking corridors in Latin America.

Criminal diversification trends (OSINT, medium confidence): IISS analysis indicates political disruption is reshaping criminal activity, including expansion into illegal mining, environmental crime, and cyber enabled fraud.

Cross border armed group activity (OSINT, medium confidence): Crisis Group reporting identifies ELN recruitment and operational movement between Venezuela and Colombia.

Extremist narrative opportunism (OSINT, medium confidence): GNET analysis assesses that geopolitical disruption generates increased online narrative exploitation by extremist ecosystems. Claims regarding the 2026 capture of Nicolas Maduro are contested and inconsistently reported; however, related information activity demonstrates how geopolitical narratives are leveraged to reinforce anti US messaging.

Citizen security investment ongoing (OSINT, high confidence): IDB reporting outlines continued multi year security programming across Latin America and the Caribbean.

**Regional Analysis**

Regional governments are expanding militarized crackdowns, anti corruption reforms, financial enforcement, and cross border coordination to counter rising organized crime and violence. Effectiveness is likely to remain limited through Q2 2026 due to structural constraints and adaptive adversaries.

States of emergency and military deployments in countries such as Ecuador and El Salvador may generate short term reductions in visible violence but risk displacement effects and lack sustainability without broader judicial and economic reforms.

Efforts to target illicit financial flows and diversify enforcement beyond narcotics are challenged by criminal groups shifting into less regulated sectors such as illegal mining and cyber enabled fraud.

Persistent corruption and uneven institutional capacity, particularly in border and extractive regions, continue to enable cross border sanctuary dynamics, allowing armed groups and criminal networks to sustain operations despite increased regional coordination.

**Alternative Analysis**

Alt 1: Intensified security operations reduce violence rapidly (low medium likelihood). Enforcement surges may disrupt specific networks but are more likely to displace rather than eliminate violence.

Alt 2: TCOs reduce overt violence to avoid scrutiny (medium likelihood). This scenario is less likely as territorial competition and weak enforcement incentivize continued use of violence as a control mechanism.

**Why This Matters**

Operational Risk: Increased kidnapping, extortion, and supply chain disruption in port and transit corridors.

Personnel Security: Elevated threat environment in border regions, maritime ports, and gang controlled urban areas increases risk of kidnapping, extortion, armed robbery, and collateral exposure to violence.

Reputational Risk: Online extremist narratives may increase harassment and targeting of individuals, NGOs, and companies with perceived ties to Western governments or activities.

**Recommendations for TINYg Member Organizations and Possible Mitigations**

1. Implement corridor based risk monitoring focused on Ecuadorian ports and border adjacent regions.

2. Strengthen third party due diligence, including beneficial ownership screening and extortion risk assessment in high violence environments.

3. Continue monitoring through TINYg alerts and reporting.

**Over the Horizon Threats**

Increased financing through illegal gold mining represents a growing risk vector. Organized armed groups are expanding operations across Colombia, Peru, and Venezuela to fund activities, secure territorial control, and launder proceeds.

If commodity prices rise or enforcement weakens, these mechanisms are likely to expand, increasing capability and longevity of both criminal and politically motivated armed actors.

**Methodology**

This product draws from open source intelligence, threat assessments, and media reporting. Information was cross validated across multiple reputable sources.

**Q1 TINYg Quarterly Threat Report**

Latin America and Caribbean Threat Intelligence Desk


**Title: Destabilization in the Northern Triangle and Caribbean: Organized Crime, Maritime Risk, and Humanitarian Pressures**

Analyst: Julia Hammerschlag

## BLUF (Bottom Line Up Front)

Persistent violence, organized crime activity, humanitarian pressures, and economic instability are driving a complex and deteriorating security environment across the Northern Triangle and Caribbean. Transnational criminal organizations, gang networks, and maritime trafficking routes continue to expand, increasing regional instability and elevating operational and security risks.

## Key Judgments

### 1. Organized crime and gang activity are primary drivers of instability

Transnational criminal organizations and local gangs continue to expand operations across Central America and the Caribbean, leveraging weak governance and maritime access to sustain trafficking and illicit activity (high confidence).

**2. Maritime trafficking networks remain critical to regional criminal operations**

Ports and coastal routes serve as key transit points for narcotics, smuggling, and human trafficking, increasing risk to maritime operations and regional security (high confidence).

**3. Humanitarian conditions are worsening and driving migration pressures**

Violence, economic hardship, and environmental factors are contributing to increased displacement, migration, and vulnerability to exploitation (high confidence).

**4. State responses are reducing some violence but introducing secondary risks**

Emergency measures and large scale incarceration efforts have reduced visible gang activity in some areas but are associated with human rights concerns and long term governance challenges (medium confidence).

**5. Terrorist activity remains limited, though violence levels are high**

The region continues to experience high homicide rates driven by criminal violence, with limited evidence of sustained terrorist activity (medium confidence).

**Facts and Background**

Operations targeting Cartel Jalisco Nueva Generacion leadership have resulted in significant casualties; however, reporting on leadership status and internal dynamics remains inconsistent (OSINT, medium confidence).

The cartel continues to operate through established trafficking and alliance networks, facilitating cocaine movement from South America to North America (OSINT, high confidence).

In February 2026, Cuban authorities reported an armed maritime incident involving individuals attempting to enter the country; official claims characterized the incident as having terrorist intent, though independent verification is limited (OSINT, low to medium confidence).

In Haiti, gang control remains extensive in Port au Prince, contributing to displacement, insecurity, and humanitarian crisis conditions (OSINT, high confidence).

Regional data indicates high levels of displacement and vulnerability, particularly among children in gang controlled areas (OSINT, high confidence).

Gang activity across Haiti, Jamaica, and other Caribbean locations continues to drive elevated homicide rates and instability (OSINT, high confidence).

States of exception in El Salvador and Honduras have resulted in large scale arrests and reduced visible gang activity, alongside concerns regarding due process and detention conditions (OSINT, high confidence).

## Regional Analysis

### Organized Crime and Gangs

Criminal networks dominate the regional threat environment, engaging in narcotics trafficking, extortion, and human smuggling. Their ability to exploit weak governance structures enables sustained operations and geographic expansion.

### Maritime and Trafficking Risk

Ports and maritime routes are critical nodes in regional criminal networks. Increased trafficking activity elevates risks to shipping, port operations, and maritime personnel.

### Humanitarian Pressures

Economic instability, violence, and environmental challenges are contributing to large scale displacement and migration. These dynamics increase vulnerability to exploitation and strain regional and international systems.

### State Response and Governance

Government measures, including states of exception, have demonstrated short term reductions in violence but raise concerns regarding long term sustainability, institutional integrity, and human rights.

## Alternative Analysis

Alt 1 Expansion of criminal terrorist linkages (low likelihood). While historical reporting suggests limited interaction between criminal and terrorist actors, there is insufficient evidence to assess sustained collaboration across the region.

Alt 2 Emergence of hidden extremist networks (low likelihood). Current reporting indicates minimal terrorist activity; however, latent radicalization risks cannot be fully discounted.

## Why This Matters

Maritime and transportation systems face increased exposure to criminal activity and associated violence.

Humanitarian conditions are driving migration pressures that impact regional and international stability.

Organized crime activity increases operational, financial, and security risks for private sector organizations.

Governance challenges and instability may affect investment environments and long term economic conditions.

**Recommendations for TINYg Member Organizations and Possible Mitigations**

Increase maritime and port level monitoring to detect trafficking and smuggling activity.

Strengthen coordination with local and regional security partners where appropriate.

Enhance organizational awareness of human trafficking indicators and reporting mechanisms.

Continue monitoring developments through TINYg reporting and updates.

**Over the Horizon Threats**

Continued migration pressures driven by violence, economic instability, and environmental factors

Expansion of maritime trafficking routes and associated criminal activity

Ongoing evolution of transnational criminal organizations and leadership structures

Potential shifts in cartel leadership impacting trafficking dynamics

**Methodology**

This product draws from open source intelligence, threat assessments, and media reporting. Information was cross validated across multiple reputable sources.

**Q1 TINYg Quarterly Threat Report**

North America Threat Intelligence Desk


**Title: Hybrid Extremism, Lone Actor Violence, and Cartel Driven Instability in North America**

Analyst: Lauren Paolozzi

## BLUF (Bottom Line Up Front)

North America faces a complex threat environment characterized by lone actor violence, persistent extremist activity, cartel driven instability, and emerging technological and biosecurity risks. These threats are shaped by political polarization, transnational criminal dynamics, and global conflict narratives, increasing risks to public safety, law enforcement, and critical infrastructure.

## Key Judgments

### 1. Lone actor violence remains a persistent and adaptive threat

Political polarization, online radicalization, and grievance driven motivations continue to contribute to sporadic but high impact violent incidents targeting soft targets, public officials, and symbolic locations (high confidence).

### 2. Cartel activity is increasing tactical risk along the U.S. Mexico border

Reporting indicates increased willingness by cartel actors to target law enforcement and adopt new tactics, including weaponized drone usage, elevating operational risk in border regions (high confidence).

**3. Cartel leadership disruption may increase short term instability**

Reported leadership targeting within CJNG may contribute to fragmentation, retaliation, and localized violence; however, long term structural impact remains uncertain due to inconsistent reporting (medium confidence).

**4. Global conflict narratives are influencing domestic threat dynamics**

International conflict developments are likely contributing to radicalization narratives and may increase risk of ideologically motivated or inspired incidents, though direct coordination remains limited (medium confidence).

**5. Emerging technology and biosecurity risks are expanding the threat landscape**

The convergence of cyber, AI enabled influence operations, and potential biosecurity vulnerabilities highlights increasing overlap between digital and physical security risks (medium confidence).

## Facts and Background

Multiple violent incidents across the United States and Canada reflect continued lone actor and small scale attack patterns; motivations vary and include personal grievances, ideological drivers, and opportunistic violence (OSINT, high confidence).

Reporting indicates increased cartel related threats toward U.S. border personnel and evolving tactics, including drone enabled capabilities (OSINT, high confidence).

Claims regarding the death of CJNG leader Nemesio Oseguera Cervantes are inconsistent across sources; however, reporting indicates increased cartel activity and retaliatory violence (OSINT, medium confidence).

Global conflict escalation involving Iran and U.S. aligned actors has contributed to heightened concern regarding potential retaliatory or inspired activity domestically (OSINT, medium confidence).

A previously identified unauthorized biological laboratory in the United States highlights ongoing biosecurity concerns and regulatory vulnerabilities (OSINT, medium confidence).

## Regional Analysis

### Extremism and Lone Actor Violence

The threat landscape continues to be defined by decentralized actors motivated by a mix of ideological, political, and personal grievances. Online ecosystems facilitate exposure to extremist narratives, contributing to radicalization and mobilization.

**Cartel Activity and Border Security**

Cartel organizations remain highly adaptive, with increasing use of technology and willingness to confront law enforcement. Leadership disruptions may intensify short term violence as groups compete for control.

**Geopolitical Influence**

International conflicts and narratives are shaping domestic threat perceptions and may contribute to isolated incidents of violence. However, evidence of coordinated foreign directed activity remains limited.

**Technological and Biosecurity Risk**

The intersection of AI driven influence operations, cyber threats, and biological vulnerabilities presents a growing hybrid risk environment that extends beyond traditional threat categories.

**Alternative Analysis**

Alt 1 Perceived increase in violence is driven by visibility rather than actual frequency (medium likelihood). Increased media coverage and information circulation may amplify perception of threat without corresponding systemic increase in incidents.

Alt 2 Violence trends are episodic and event driven (high likelihood). Violence levels may fluctuate based on major political or global events rather than reflecting a sustained upward trajectory.

Alt 3 Extremism is evolving into hybridized forms (high likelihood). The blending of ideological, political, and global narratives may produce more complex and less predictable threat actors.

**Why This Matters**

Elevated risk to soft targets, public gatherings, and critical infrastructure

Increased operational risk for law enforcement and security personnel, particularly in border regions

Growing convergence of criminal, ideological, and technological threats

Expanding cyber and information security risks affecting both public and private sector organizations

**Recommendations for TINYg Member Organizations and Possible Mitigations**

Enhance monitoring for insider threat indicators and grievance driven behaviors

Strengthen physical and digital security posture for personnel, facilities, and events

Expand training on identifying extremist indicators, cyber threats, and misinformation

Implement robust cybersecurity measures, including access controls and network monitoring

Continue monitoring developments through TINYg reporting and intelligence updates

**Over the Horizon Threats**

Continued evolution of digitally enabled extremism and recruitment networks

Expansion of hybrid ideological motivations among lone actors

Potential instability linked to cartel leadership dynamics

Persistent cyber and influence operations by state and non state actors

Ongoing biosecurity and regulatory vulnerabilities

**Methodology**

This product draws from open source intelligence, threat assessments, and media reporting. Information was cross validated across multiple reputable sources.

**Q1 TINYg Quarterly Threat Report**

Special Assessment

**Title: Cartel Violence in Mexico and Security Implications for the 2026 FIFA World Cup**

Analysts: Julia Hammerschlag, Lauren Paolozzi

## BLUF (Bottom Line Up Front)

Recent reporting on potential leadership disruption within the Cartel de Jalisco Nueva Generacion has coincided with increased cartel violence and instability in parts of Mexico. While reporting on leadership status remains inconsistent, heightened violence, territorial competition, and retaliatory activity are contributing to an elevated threat environment. These dynamics may increase operational and security risks surrounding the 2026 FIFA World Cup, particularly in key host cities.

## Key Judgments

### 1. Cartel leadership disruption may increase short term instability

Conflicting reporting regarding the status of CJNG leadership complicates assessment; however, perceived disruption is likely contributing to localized violence, fragmentation, and increased cartel competition (medium confidence).

**2. World Cup host cities face elevated security risks from criminal activity**

Guadalajara, Mexico City, and Monterrey are likely to experience increased crime related risks, including violence, extortion, and transportation disruption, rather than coordinated large scale attacks (high confidence).

**3. Cartel activity is likely to remain profit driven during the World Cup**

Cartels are unlikely to conduct large scale attacks that could disrupt revenue generating opportunities, instead prioritizing narcotics trafficking, extortion, and illicit market expansion (high confidence).

**4. Cartel violence may create indirect risk to World Cup operations**

Road blockades, localized violence, and law enforcement strain may disrupt transportation, logistics, and event security operations (high confidence).

**5. Information operations are emerging within cartel activity**

Reporting indicates increased use of disinformation and AI generated content by cartel actors to influence public perception and spread fear (medium confidence).

**Facts and Background**

Reporting on the status of CJNG leadership remains inconsistent across sources; however, security operations targeting cartel leadership have coincided with increased violence in affected regions (OSINT, medium confidence).

Multiple incidents of retaliatory violence, including road blockades, vehicle burnings, and clashes with security forces, have been reported following recent operations (OSINT, high confidence).

U.S. Department of State travel advisories identify elevated crime risks in multiple Mexican regions, including World Cup host cities, with varying threat levels (OSINT, high confidence).

Guadalajara is currently assessed at a higher risk level relative to Mexico City and Monterrey due to cartel activity and recent violence (OSINT, high confidence).

Cartel use of digital platforms and disinformation campaigns has increased, including the spread of AI generated content to influence public perception and amplify fear (OSINT, medium confidence).

## Regional Analysis

### Cartel Instability

Perceived or actual leadership disruption within CJNG is likely contributing to fragmentation and increased competition among cartel factions and rival groups.

### Operational Spillover Risk

Increased cartel activity raises the potential for spillover effects, including heightened violence near transportation corridors and border regions.

### FIFA World Cup Security Environment

The 2026 FIFA World Cup will introduce large volumes of international visitors, increasing the complexity of security efforts. While cartels are unlikely to target the event directly, increased economic activity may create opportunities for criminal exploitation.

### Cartel and Terrorism Dynamics

Cartels remain financially motivated organizations with limited incentive to collaborate with terrorist groups, particularly during high visibility events.

## Alternative Analysis

Alt 1 Cartel fragmentation leads to longer term weakening (medium likelihood).

Alt 2 Increased violence is temporary and stabilizes before the World Cup (medium likelihood).

Alt 3 Security posture significantly improves prior to the World Cup (low likelihood).

## Why This Matters

Elevated risk of crime, violence, and disruption in major urban centers hosting international events

Increased operational challenges for transportation, logistics, and event security planning

Expanded opportunities for criminal exploitation during high visibility global events

Potential reputational and safety risks for organizations operating in or traveling to affected regions

**Recommendations for TINYg Member Organizations and Possible Mitigations**

Conduct location specific risk assessments for World Cup host cities

Monitor transportation routes and plan for potential disruption

Enhance traveler awareness and security protocols

Coordinate with local security partners and monitor official advisories

**Over the Horizon Threats**

Continued cartel fragmentation and localized violence

Expansion of digital influence and disinformation tactics by criminal actors

Increased trafficking and criminal activity tied to large scale international events

Potential shifts in cartel leadership and territorial control dynamics

**Methodology**

This product draws from open source intelligence, threat assessments, and media reporting. Information was cross validated across multiple reputable sources.

**Q1 TINYg Quarterly Threat Report**

Emerging Technology Threat Intelligence Desk

**Title: Biometric Systems and Emerging Identity Security Risks**

Analyst: Bianca Thompson, Donnell Harvin

## BLUF (Bottom Line Up Front)

The expansion of biometric identification systems across commercial and government sectors is introducing high impact vulnerabilities that may be exploited by state and non state actors for identity compromise, surveillance, coercion, and unauthorized access to sensitive systems and infrastructure.

## Key Judgments

### 1. Biometric data collection lacks consistent regulatory oversight

Private sector adoption of biometric technologies continues to expand in the absence of standardized federal frameworks, increasing exposure to misuse, breach, and inconsistent data protection practices (high confidence).

### 2. Compromise of biometric data creates persistent identity risk

Unlike traditional credentials, biometric identifiers cannot be reset, increasing long term vulnerability if data is exposed or stolen (high confidence).

**3. Biometric systems have demonstrated vulnerability in conflict environments**

Past reporting indicates that biometric systems and devices have been accessed or exploited in conflict settings, highlighting potential misuse of identity data (medium confidence).

**4. Biometric access controls introduce new security risks for critical infrastructure**

Reliance on biometric authentication may increase susceptibility to spoofing, insider threat, and unauthorized access if systems are compromised (medium confidence).

## Facts and Background

Biometric technologies, including facial recognition, fingerprints, iris scans, voice recognition, and gait analysis, are increasingly integrated into authentication systems across public and private sectors (OSINT, high confidence).

Reporting indicates that biometric identification devices were obtained in Afghanistan in 2021 and may have been used to identify individuals associated with coalition forces, demonstrating potential misuse in conflict environments (OSINT, medium confidence).

Large scale data repositories, including international organizations, have experienced cyber intrusions, highlighting vulnerabilities in centralized identity data systems (OSINT, medium confidence).

Commercial entities, including major retailers and technology firms, continue to deploy biometric technologies in consumer environments, often with varying levels of transparency and oversight (OSINT, high confidence).

## Alternative Analysis

Alt 1 Biometric systems enhance overall security (medium likelihood). Multi factor authentication incorporating biometrics may reduce certain forms of fraud; however, compromise consequences are more severe and less recoverable.

Alt 2 Threat severity is overstated (medium likelihood). Large scale exploitation remains limited; however, advances in AI and synthetic media may reduce barriers to misuse.

Alt 3 Risk remains primarily within government systems (low likelihood). Private sector adoption continues to expand rapidly, increasing exposure beyond government controlled environments.

**Why This Matters**

Increased risk of unauthorized access to facilities, systems, and sensitive infrastructure

Long term identity exposure due to inability to reset biometric credentials

Potential for coercion, surveillance, and targeting using compromised biometric data

Expanded attack surface as biometric systems integrate with digital and physical security frameworks

**Recommendations for TINYg Member Organizations and Possible Mitigations**

Conduct risk assessments for systems utilizing biometric authentication

Limit storage of biometric data where feasible and ensure strong encryption and access controls

Integrate biometric systems within multi factor authentication frameworks rather than standalone use

Monitor for anomalous authentication behavior and potential spoofing indicators

**Over the Horizon Threats**

Increased use of synthetic media and AI to replicate biometric identifiers

Expansion of digital identity manipulation and long term infiltration tactics

Growing intersection of biometric data with smart infrastructure and surveillance systems

Potential targeting of biometric databases by state and non state actors

**Methodology**

This product draws from open source intelligence, threat assessments, and media reporting. Information was cross validated across multiple reputable sources.

QTR Spotlight: Michael Bryan

Written by: Lara Connor

*On AI, Bioterrorism, and the Risk We Might Miss*

Bio

Michael Bryan's career spans medicine, research, and counterterrorism. A former officer with London's Metropolitan Police, he is now an MD-PhD researcher focused on early cancer detection and personalized vaccines, with experience at institutions including Harvard and Oxford.

That dual lens of scientific and security experience shapes how he approaches the convergence of artificial intelligence and biology. While public attention often focuses on futuristic fears of AI-designed pathogens, Bryan points to a more immediate shift. Existing threats are becoming easier to scale, harder to detect, and more accessible to those already intent on acting.

In this conversation, he breaks down where AI is genuinely changing the risk landscape—and where the real vulnerabilities lie.

---

Interview

**QTR:** Everyone hears AI, and I'm not quite sure they know what it is. My question is, what is AI to you, Michael? Can you define it?

**Bryan:** AI is essentially a set of statistical approaches that allow you to define rules from sets of data. That can be putting in a set of features and getting it to learn what you're trying to predict. There's also unsupervised learning, where it identifies patterns or clusters. And reinforcement learning, which is the idea that if you can show the actions and costs of a specific course, the model can learn what is good and what is bad. The way tools like ChatGPT work is by predicting the next sequence based on probability.

**QTR:** When people hear "AI and bioterrorism," it sounds like science fiction. How real is this right now?

**Bryan:** I'd split AI and bioterrorism into two sides: prevention and perpetration. On the prevention side, AI allows us to take in masses of disease outbreak information and identify trends from media reports and case reports. It lets us see if something looks unnatural. On the perpetration side, it takes someone with a high school knowledge—or even no knowledge of biology—and gives them an amplified threat.

**QTR:** Concerning AI and bioterrorism, is the greater risk today misuse or creation?
**Bryan:** With my experience working with UK counterterrorism policing, a lot of the threats that we see are using conventional pathogens or agents like ricin, and groups think, *Okay, how do I take what I currently have my hands on and amplify it further?* So, for instance, *how do I choose a vector that is likely to be even more dangerous?* I think the scenario that is far more dangerous is mutating a pathogen to the point it has autoimmunity effects like HIV, for example. That is a really frightening scenario.
**QTR:** Do advances in early detection, such as identifying cancer or risks years in advance, have parallels in detecting emerging biological threats or engineered pathogens?
**Bryan:** [AI] has made detection technologies better, so it means that now we can do whole genome sequencing on pathogens within, like, an hour or two, when before you'd have to send it to a lab. And so that is valuable, because if I'm in London and receive mail with a white powder in it, we might have to send that biological risk to a lab for bio-testing. Whereas if detection technologies are better and faster,

enabled by AI, then you could do that potentially within hours, and you could do that at the scene. One of the examples of where I've seen that be really effective in the UK has been with airports.

**QTR:** You've worked in both medicine and policing—does that change how you think about risk?
**Bryan:** From a policing side, I naturally think, *What is the worst possible thing that a perpetrator could do, and how do we prevent it?* But I think both the police and the medical side make me think about the practicality. There are several safety measures that I think would be important to implement, but then there's a resource allocation issue. The opportunity cost of running hundreds of biological security investigations is that organized crime, for instance, investigations, or drug crime investigations, may then get less priority. And defining what you count as terrorism and how much you investigate and pursue each lead.

**QTR:** Do you worry about the US or the UK's response time to bioterrorism incidents?
**Bryan:** Absolutely. When something is announced as a crisis, with a confirmed bioterrorism link, someone claiming responsibility, and a targeted group, I think the response is world-class, especially in the US. The issue is actually recognizing a crisis as bioterrorism and that something is deliberate. If a person has walked into a New York hospital with Ebola, or if there's FMD in our cows, someone must consider, *Why is that, and could that be deliberate?* Either some people genuinely haven't thought about the deliberate side from a public health angle, or people are just too busy—having a direct method of communication between concerned public health officials and law enforcement is an example of a better response.

**QTR:** If you were advising policymakers, what would you prioritize?
**Bryan:** Three things. First, better reporting systems, especially around suppliers. We already do this for things like explosives, where retailers flag suspicious purchases. We should be doing something similar for biological materials and related tools. Second, broadening how we think about who poses a threat—a bioterrorist isn't just someone in a lab that's trying to end the world. It could be a disgruntled scientist, it could be someone who is a part of a terrorist group, and is thinking, *How do I expand my reach?* Or it could be someone who's just, like, playing around with pathogens, looking to use them maliciously for one purpose, and it gets out of hand. Third, is having the CDC co-train, co-investigate, and co-located in some cases, with the FBI. I think that it is one of the single biggest benefits in peacetime to have both public health officials, epidemiologists, in the same room as law enforcement, so that they understand what each other are doing.

**QTR:** Many AI company executives in the U.S. have asked Congress to regulate AI, seemingly concerned about the lack of guardrails. Is this just people being alarmists? Should we really be concerned about AI?
**Bryan:** I think what they're concerned about is the fact that people who are already capable, for example, virologists can do things never previously thought possible. We've seen this, sort of, in the UK, as Al-Qaeda has tried to encourage the recruitment of people who are already scientists to try to join their ranks.
**QTR:** With that, are you aware of any international guardrails going up?
**Bryan:** I think there's a balance, because the reason why AI companies are perpetuating this alarm is partly to encourage more regulation, and I wonder to what extent that's anti-competitive as well, since it's

in the AI company's interest for there to be great regulation that means that they're the only ones left in the market. With Anthropic, for example, they've actively put in lots of safeguards to the point where if you ask a virology question, it would just say, *Sorry, I cannot answer you.* Whereas OpenAI is taking a far more liberal approach.

# Meet Our Team

**Aldair Campos – TiNYg Senior Fellow**
Georgetown University
Master of Professional Studies in Applied Intelligence Masters

**Kushal Ganji – TiNYg Senior Fellow**
Georgetown University
School of Continuing Studies, Applied Intelligence Masters

**Julia Hammerschlag – TiNYg Senior Fellow**
Georgetown University
School of Continuing Studies, Applied Intelligence Masters

**Lauren Paolozzi – TiNYg Fellow**
Georgetown University
School of Continuing Studies, Applied Intelligence Masters

**Lamont pyykkonen – TiNYg Fellow**
George Mason University

**Manuel Del Valle – TiNYg Fellow**
George Mason University

**Abigail Becker – TiNYg Intern**
Georgetown University
School of Foreign Service, International Security

**Lara Connor – TiNYg Intern**
Georgetown University
Walsh School of Foreign Service, International Security

Naomi Horner **– TiNYg Intern**
Georgetown University
Walsh School of Foreign Service, International Security

Callie Mitchell **– TiNYg Intern**
Georgetown University
Walsh School of Foreign Service, International Security

**Sam Rosenblum – TiNYg Intern**
Georgetown University
Walsh School of Foreign Service, International Security

**Bianca Thompson – TiNYg Intern**
Georgetown University
School of Foreign Service International Security