unicri
United Nations
Interregional Crime and Justice
Research Institute

ISSUE Q1-Q2
January–June 2026

The Crime & Justice QUARTERLY

Published in August 2026
@UNICRI

DISCLAIMER

The opinions, findings, conclusions, and recommendations expressed in this publication do not necessarily reflect the views or positions of the United Nations, the United Nations Interregional Crime and Justice Research Institute (UNICRI), or any other national, regional, or international entity involved. The content of this publication may be quoted or reproduced, provided that the source is acknowledged. Neither UNICRI nor the authors bear responsibility for any use made of the information contained herein. The designations used and the presentation of material in this publication do not imply any opinion on the part of the United Nations Secretariat or UNICRI regarding the legal status of any country, territory, city, or area, or its authorities, nor regarding the delimitation of its frontiers or boundaries. Mention of specific institutions or companies does not constitute an endorsement or recommendation by the United Nations Secretariat or UNICRI over others of a similar nature.

ACKNOWLEDGMENTS

This publication is the product of an initiative led by UNICRI. It was written by Ms. Giordana Lucente, with editing by Marina Mazzini and design by Antonella Bologna.

The Quarterly draws on publicly available assessments, indices and analyses developed by international organizations, specialized agencies, think tanks and investigative networks which collectively form the evidence base for this publication.

It complements UNICRI's broader research agenda, in particular "UNICRI's Crime and Justice Trends Study", with its global report and nine regional analyses developed under this initiative. Where the Study provides an in-depth baseline of how crime and justice are evolving across and within regions, the Quarterly tracks how these trends develop quarter by quarter.

Table of **contents**

The Crime & Justice Quarterly is UNICRI flagship quarterly publication on emerging crime and justice trends globally and across regions, which acts as a quarterly newsletter to keep readers informed on trends and emerging research, operational and policy priorities.

This edition, being the first one of its kind, reviews crime and justice developments across the first half of 2026 (January to June 2026), drawing on threat assessments and indices published by international organizations, specialized agencies, think tanks and investigative networks. Some of the most recent trends are a continuation of earlier developments, which explains why a small selection of sources pre-date the reporting periods. This brief identified three global trends, four regional signals and emerging research gaps.

1. Executive Summary

During the reporting period, the center of gravity of transnational organized crime continued to shift from violent, commodity-based markets towards financie sustained enforcement, with criminal groups operating an increasingly professionalized "crime-as-a-service" model and adopting artificial intelligence to scale deception. Second, the global integrity framework that constrains these flows weakened further: the world's leading corruption index fell to a record low, while standard-setters intensified their focus on fraud, virtual assets and the offshore channels that launder criminal proceeds. Third, the structure of organized crime itself is changing, with non-violent financial and cyber-dependent markets now among the largest and least visible, and with state-embedded and foreign actors playing a growing role. Regionally, these dynamics take distinct forms: they include the displacement of scam operations across and beyond Southeast Asia, a militarized counter-narcotics reset in Latin America, and illicit economies financing armed groups across the Sahel. Together, these developments underscore that a single global trend often demands tailored regional responses.

What this means for responses.

For the international crime prevention and criminal justice community, these trends point to several priorities: treating fraud as a strategic, cross-cutting threat; strengthening capacities at the convergence of cybercrime, trafficking and money laundering rather than addressing each in isolation; investing in governance frameworks for artificial intelligence and virtual assets, including measures to enhance asset recovery; and sustaining a rule-of-law and crime-conflict lens in fragile settings. Across all of these, the binding constraint is evidence and cross-border cooperation, which are not keeping pace with the speed at which criminal markets adapt.

These findings this quarter reinforce an increasingly clear message for the criminal justice community: the crimes that now cause the greatest aggregate harm are the least visible, the most transnational, and the quickest to exploit emerging technologies. Aligning measurement, legal frameworks and operational cooperation with that reality is the central response challenge.

2. Global Strategic Trends

2.1 The industrialization and globalization of the cyber-enabled scam economy

What is happening? Industrial-scale online scam operations continued to expand and disperse during the reporting period despite intensifying crackdowns. Estimates cited by the Office of the UN High Commissioner for Human Rights (OHCHR) in February 2026 place global annual revenues of cyber-scam operations at around US$64 billion, of which more than US$43.8 billion is generated in the Mekong region alone, where roughly three-quarters of identified compounds are concentrated and at least 300,000 people — many trafficked from dozens of countries — are estimated to work in the industry.[1] Syndicates increasingly operate as criminal service providers, selling fraud tooling, money-laundering, recruitment and trafficking services to one another. Enforcement is scaling in parallel but unevenly: the International Criminal Police Organization (INTERPOL)-coordinated operations yielded significant results across multiple regions, including sixteen African countries, where Operation Red Card 2.0 led to 651 arrests;[2] and the Middle East and North Africa, where Operation Ramz, the first cybercrime operation of its kind in the MENA region, led to the arrest of 201 individuals.[3] Yet the dominant pattern is displacement rather than disruption: research published by the Global Initiative Against Transnational Organized Crime in March 2026 identifies displacement, diffusion and the embedding of scam operations in jurisdictions with weaker governance as the central forward risks, with Asian-led models now documented across Africa, Latin America, South Asia and the Pacific, and some countries drawn into the scam economy as laundering and service hubs rather than hosts.[4]

Why it matters and what it means for responses. INTERPOL's March 2026 Global Financial Fraud Threat Assessment positions fraud among the top five global crime threats, citing estimates of $442 billion in global losses for 2025, and reports a 54 per cent rise in fraud-related notices and diffusions from 2024.[5] The harm is both financial and human: hundreds of thousands of people from dozens of countries have been trafficked into compounds and forced to commit fraud under coercive, sometimes violent conditions.[6] The assessment also points to a step-change in capability, with AI-enhanced fraud reported to be substantially more profitable than traditional methods and "agentic"

1 **Office of the United Nations High Commissioner for Human Rights (OHCHR)**, A Wicked Problem: Seeking Human Rights-Based Solutions to Trafficking into Cyber Scam Operations in South-East Asia, February 2026.

2 **INTERPOL,** *Major Operation in Africa Targeting Online Scams Nets 651 Arrests, Recovers USD 4.3 Million, February* 2026.

3 **INTERPOL,** *201 Arrests in First-of-Its-Kind Cybercrime Operation in MENA Region*, May 2026.

4 **K. Amerhauser and A. Goodwin**, *A World of Deceit: Mapping the Landscape of the Global Scam Centre Phenomenon*, March 2026.

5 **INTERPOL,** Global Financial Fraud Threat Assessment, March 2026.

6 **UN News,** *Report Exposes Torture, Rape in Southeast Asia's Multi-Billion-Dollar Scam Centres,* February 2026.

systems increasingly able to automate entire campaigns from targeting to extraction. Because fraud now sits at the intersection of cybercrime, trafficking and money laundering, responses designed around individual offences will continue to lag behind the threat. The priority is to treat the scam economy as a convergence problem, by combining enforcement with prevention, victim identification and protection, and the disruption of enabling infrastructure such as recruitment networks, money-laundering services and hosting infrastructure. As operations migrate to jurisdictions with weaker governance, durable progress depends on cross-border coordination and capacity-building in transit and destination countries rather than on isolated national crackdowns.

2.2 Eroding integrity: corruption, illicit finance and the laundering of criminal proceeds

What is happening? The environment that should constrain illicit flows weakened over the period. Transparency International's 2025 Corruption Perceptions Index, released in February 2026, recorded a global average of 42 out of 100, its lowest level since the comparable index began and the first decline in more than a decade, with 122 of 182 countries scoring below 50 and the number of high-performing countries (those scoring above 80) shrinking from twelve to five over the decade.[7] In parallel, at its April 2026 Ministerial Meeting, the Financial Action Task Force (FATF) made fraud an explicit priority and called for risk-based implementation of its standards,[8] following reports published earlier in 2026 on the misuse of stablecoins and on offshore virtual asset service providers used to launder scam-compound proceeds.[9]

Why it matters, and what it means for responses. Corruption and weak financial oversight are the enabling layer beneath nearly every trend in this brief, allowing scam economies to take root, criminal proceeds to be laundered and organized crime to infiltrate institutions. The virtual-asset dimension is now central: analysis cited by FATF attributes the vast majority of illicit virtual-asset transaction volume in 2025 to stablecoins, frequently moved through unhosted wallets that sit outside conventional oversight. Enforcement gains against individual networks will therefore be offset unless this integrity and financial-oversight layer is strengthened in parallel. In practice that means prioritizing asset recovery, closing offshore and virtual-asset supervision gaps, and embedding anti-corruption and integrity safeguards within justice institutions themselves, supported by credible, non-partisan analysis that connects corruption, illicit finance and organized crime and can inform both international standard-setting and day-to-day operational practice.

> “ **Corruption and weak financial oversight are the enabling layer beneath nearly every trend in this brief**

7 **Transparency International,** Corruption Perceptions Index 2025, February 2026.

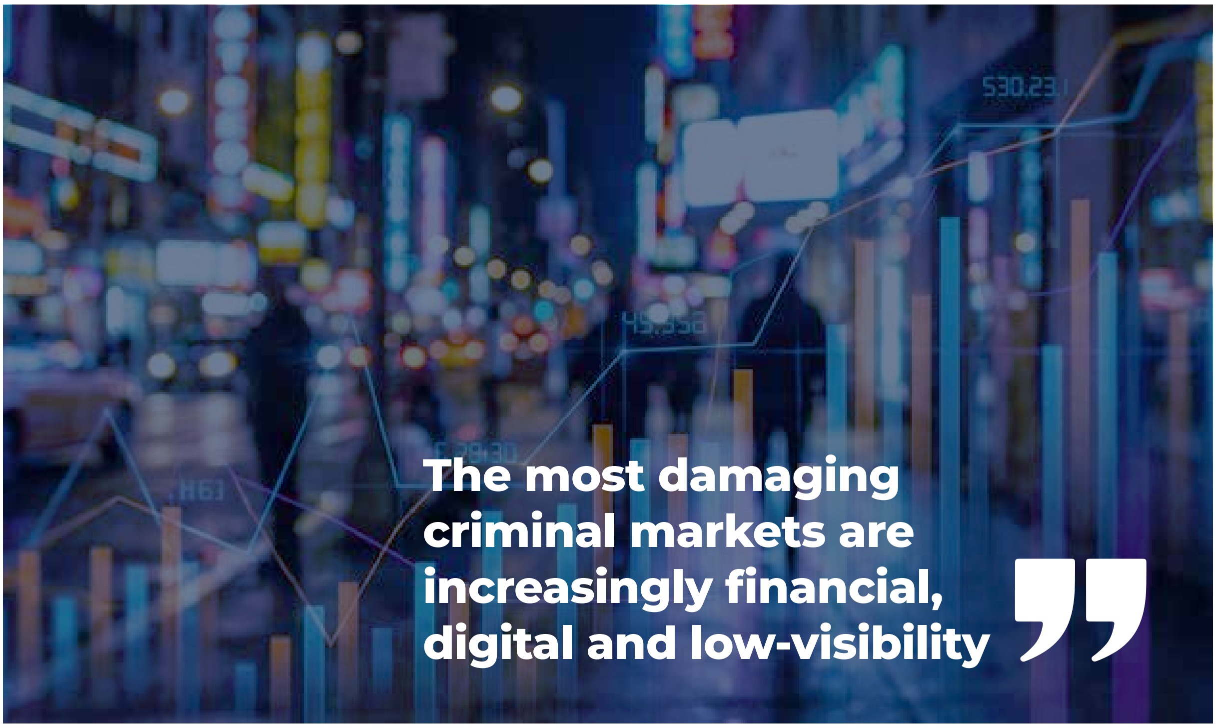
8 **FATF,** Ministerial Declaration, April 2026.

9 **FATF,** Targeted Report on Stablecoins and Unhosted Wallets; - Peer-to-Peer Transactions, March 2026.

2.3 The structural transformation of organized crime: networked, service-based and technology-driven

What is happening? The most recent edition of the Global Initiative Against Transnational Organized Crime (GI-TOC) Global Organized Crime Index, published in late 2025, documents a significant and rapidly growing shift toward non-violent financial and cyber-dependent crime. These "invisible" markets are deeply embedded in transnational financial and digital systems and harder to detect.[10] The Index also finds that state-embedded actors remain the most prevalent criminal actor type, while foreign actors registered the sharpest increase, and that criminal groups are typically the first to exploit disruption, whether from geopolitical competition, technological change, conflict, or economic stress. Traditional markets persist and adapt, with synthetic drugs and cocaine increasingly dominating drug markets and counterfeiting rising amid economic insecurity, but the organizing logic is now networked and service-based rather than hierarchical and territorial.

Why it matters, and what it means for responses. If the most damaging criminal markets are increasingly financial, digital and low-visibility, frameworks built around violent, commodity-based crime will systematically under-detect them. The service-based model also lowers barriers to entry and accelerates the diffusion of capability, including AI tooling, across otherwise unconnected groups. For the field this raises the premium on data, cross-border intelligence and resilience over seizure-based metrics alone, and it argues for reframing how organized crime is conceptualized and measured, complementing index-based monitoring with applied research on criminal business models, professional enablers, and the interface between licit and illicit economies.



10 **GI-TOC,** Global Organized Crime Index 2025: Crime at a Crossroads, November 2025.

3. Regional Signals

The following region-specific signals complement the global trends above and are deliberately kept brief; they highlight developments not addressed elsewhere in Section 2.

Africa: the crime-conflict nexus in the Sahel. Illicit economies continue to sustain armed and extremist groups across the Sahel, which accounted for more than half of global terrorism-related deaths in 2025.[11] Gold is central to this nexus: artisanal mining sites are a critical revenue source for groups such as Jama'at Nusrat al-Islam wal-Muslimin (JNIM) and Islamic State Sahel Province (ISSP), which impose taxes and protection fees on miners and communities as a governance strategy — with JNIM involved in over 40 per cent of all mining-adjacent conflict events recorded in the central Sahel over the past decade, and ISSP in more than a quarter.[12] More broadly, the Africa Organised Crime Index 2025 rates the influence of state-embedded criminal actors, the most prevalent criminal actor type on the continent, as severe in nearly half (48 per cent) of African countries.[13]

Latin America: a militarized counter-narcotics reset. A pronounced shift toward a militarized, enforcement-heavy posture, including maritime interdiction and the terrorist designation of several criminal groups, reshaped the regional landscape; analysts caution that such measures displace rather than reduce flows.[14] In parallel, the migrant-smuggling market contracted sharply as the United States became a less viable destination, while criminal adoption of cryptocurrency and AI-enabled fraud, including voice-cloning extortion, expanded.[15]

Southeast Asia: displacement, not disruption. Enforcement pressure intensified during the period, yet scam operations continued to relocate and re-embed rather than shut down. Research published during the reporting period identifies displacement, diffusion and entrenchment in weaker-governance jurisdictions as the central forward risks.[16] The trafficking dimension remains acute: an estimated 300,000 people, trafficked from at least 66 countries, are forced to work in operations concentrated in the Mekong region.[17]

Europe: organized crime embedded in legitimate sectors. European signals point to networked, service-based crime exploiting legitimate platforms and economic sectors, including large-value fraud against public revenue such as multi-million-euro VAT carousel schemes disrupted by European judicial and financial authorities.[18] In the neighboring MENA region, INTERPOL-coordinated action against phishing-as-a-service infrastructure is consistent with the service-based model operating on Europe's periphery.[19]

11 **Institute for Economics & Peace (EIP)**, *Global Terrorism Index 2026*, March 2026.
12 **ACLED**, *Extraction under fire: How mining reshapes conflict in the central Sahel*, July 2026.
13 **ENACT**, Africa Organised Crime Index 2025, November 2025.
14 **InSight Crime**, GameChangers 2025: A Decade of Tectonic Shifts in Criminal Markets, December 2025.
15 **InSight Crime,** *Organized Crime and AI: 5 Topics We Are Monitoring in 2026*, January 2026.
16 **K. Amerhauser and A. Goodwin,** *A World of Deceit: Mapping the Landscape of the Global Scam Centre Phenomenon*, March 2026.
17 **OHCHR**, *A Wicked Problem: Seeking Human Rights-Based Solutions to Trafficking into Cyber Scam Operations in South-East Asia*, February 2026.
18 **EPPO**, Investigation Emily: EPPO strikes against criminal network behind multimillion VAT fraud involving sales of luxury cars, March 2026.
19 **INTERPOL**, 201 arrests in first-of-its-kind cybercrime operation in MENA region, May 2026.

4. Emerging Research Gaps

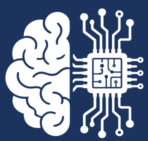
Three questions recur across this period's evidence and remain inadequately answered, which are flagged here as priorities for the wider research and policy community.

The first concerns the criminal adoption of artificial intelligence. Assessments increasingly cite agentic fraud systems, deepfakes and voice cloning as force multipliers,[20] yet there is no systematic, comparable evidence on how rapidly or how widely these tools are being used, or on the uplift they actually provide. Policy is being shaped largely by striking individual cases, because reporting is incident-led and law-enforcement and victim data are not structured to capture AI use. Until a shared measurement approach exists, responses risk being calibrated to anecdote rather than to evidence at scale.

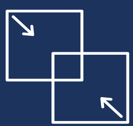
The second is the convergence of trafficking and fraud in scam compounds. Hundreds of thousands of people are implicated as both coerced perpetrators and victims,[21] which raises unresolved questions for justice systems, victim protection and the treatment of compelled offences. The evidence remains fragmented across trafficking, cybercrime and labour-exploitation silos, victims are dispersed across many nationalities and jurisdictions, and trauma-sensitive data are difficult to gather. A coherent, justice-centred framework that joins these strands is still missing.

The third is the measurement of the "invisible" financial and cyber-dependent economy. The markets now identified as among the largest are also the least reliably quantified, including the laundering of proceeds through stablecoins and unhosted wallets.[22] Loss figures rest on heavy under-reporting and inconsistent definitions, and virtual-asset flow analysis is concentrated in a handful of private providers and rarely integrated with official crime statistics. So long as resourcing tracks violent and commodity-based crime, responses will remain misaligned with where aggregate harm now concentrates.

Artificial Intelligence



Trafficking and fraud convergence



Invisible financial and cyber-dependent economy

20 **INTERPOL,** Global Financial Fraud Threat Assessment, March 2026.

21 **UN News**, *Report Exposes Torture, Rape in Southeast Asia's Multi-Billion-Dollar Scam Centres,* February 2026.

22 **FATF,** *Targeted Report on Stablecoins and Unhosted Wallets; - Peer-to-Peer Transactions* (citing Chainalysis), March 2026.

unicri
United Nations
Interregional Crime and Justice
Research Institute

www.unicri.org