



LATIN AMERICA / ORGANISED CRIME / TECHNOLOGY RISK

Cartel Convergence in the Andes: Ecuador, Colombia, Venezuela and Drone-Enabled Organised Crime

Author: Benjamin Traunecker

Executive Summary

The Andean organised-crime environment is converging. Ecuador's prison gangs, Colombian armed groups, Venezuelan criminal networks and Mexican cartel partners do not operate as one command structure, but their routes, services and tactics increasingly overlap. That overlap is the risk.

Ecuador is the visible pressure point because ports, prisons and street violence have made the country a central node in cocaine logistics. Colombia remains the production and armed-group depth behind many routes. Venezuela provides criminal mobility, diaspora-linked extortion networks and the Tren de Aragua brand. Peru, Chile and Central America sit downstream. For companies, the threat is regional even when the incident is local.

Technology accelerates the pattern. Low-cost drones, encrypted messaging, remote surveillance and improvised explosive delivery allow criminal groups to test capabilities once associated mainly with insurgent or battlefield actors. The result is not a full military transformation of cartels. It is a lower barrier for surveillance, intimidation, prison support, smuggling and targeted violence.

Ecuador as the Visible Node

Ecuador's deterioration is tied to geography. Pacific ports, dollarised trade flows, prison networks and access to Colombian supply routes make the country useful to multiple criminal partners. Groups such as Los Choneros and Los Lobos have been reported in relation to prison control, extortion, trafficking and links to larger international cartels.

The practical issue is that Ecuador's violence is not only domestic crime. It reflects route competition and service provision inside a wider cocaine economy. A local assassination, prison riot or port seizure can therefore have implications for logistics, insurance, executive movement and contractor vetting.

Colombia and Venezuela as Depth

Colombia remains the strategic depth of the Andean criminal economy. Armed groups, dissident structures and drug corridors provide both supply and coercive capacity. Even when a company operates outside coca-producing areas, the influence of those routes can appear through roadblocks, extortion, informal taxes and contractor penetration.

Venezuela adds a different layer. Tren de Aragua and other networks have shown how a criminal brand can move with migration routes, prisons and diaspora communities. The group's exact structure varies by country, and local cells may operate with different levels of autonomy. The relevant point is that extortion, human trafficking, retail drug markets and migrant exploitation can travel along the same social pathways.

Drone-Enabled Organised Crime

Drones matter because they reduce cost and training barriers. A small commercial platform can observe police movement, track a convoy, test a prison perimeter, move contraband or deliver a small explosive payload. Groups do not need a sophisticated aviation branch to gain tactical value from that capability.

Colombian and Ecuadorian security reporting has increasingly treated drones as both a criminal instrument and a law-enforcement countermeasure. That dual use creates ambiguity. A drone near a mine, port, executive residence or police checkpoint may be reconnaissance, smuggling, intimidation or ordinary commercial use. Security teams need a local protocol before the first incident, not after it.

Business Exposure

Ports are the first exposure point. Container movement, fishing fleets, customs brokers and warehouse access all create opportunities for contamination, coercion and insider recruitment. Companies that treat port security as a compliance problem rather than a hostile-network problem will miss the risk.

Mining and energy sites face a different pattern: extortion, road access, contractor compromise and community pressure. Executive travel adds a third layer. The risk is not only kidnapping. It includes surveillance before arrival, hotel and driver compromise, route exposure, protest-crime overlap and reputational damage after a security incident.

Security Posture

Organisations should separate country risk from route risk. A capital city may remain functional while a port corridor, prison-adjacent district or border road carries a much higher threat. Contractor vetting should include ownership checks, driver history, vehicle substitution rules and links to local political or prison networks.

For physical security, the minimum posture is practical: detect surveillance, control vehicle changes, restrict unnecessary night movement, harden access to warehouses and check whether local guards understand drone reporting. For crisis management, the key question is whether a local incident is isolated or tied to a wider route contest.

Scenarios to Watch

Port pressure. Trafficking networks intensify contamination, coercion or intimidation around Pacific ports. This would affect logistics, insurers and export-facing companies first.

Drone escalation. Criminal groups use drones more visibly for reconnaissance, prison support or intimidation. This would force companies to add low-cost aerial detection and reporting procedures.

Cross-border enforcement shock. A major arrest, extradition or joint operation disrupts one route and shifts pressure to another. This can raise short-term violence even when the operation is strategically positive.

Indicators

Watch for prison violence, port seizures, drone seizures near criminal targets, attacks on prosecutors or police, new extraditions, public emergency decrees, threats against mining or logistics firms, and evidence that Tren de Aragua or Ecuadorian groups are appearing outside their usual operating areas.

Selected Sources

- InSight Crime reporting on Ecuadorian, Colombian and Venezuelan organised crime.
- UNODC and official reporting on drug routes and transnational trafficking.
- Public statements by regional law-enforcement and judicial authorities.
- Established regional media reporting on Ecuador, Colombia and Venezuela.
- Social-media reporting used only as unverified early warning unless corroborated.

Method Note

This report uses open-source information available up to 31 August 2026. It assesses network convergence and capability change, not formal alliance claims unless such claims are supported by official or established reporting.