Sub-national composite risk - darker = higher. Source: GeoBit.

Paraguay dataset (CSV) - events, per-region risk, cyber & sources

1 Day - $5

1 Week - $15

1 Month - $39 - best value

function gbBuyCsv(s,dt,range){var u='/api/data-checkout?country='+encodeURIComponent(s);if(dt)u+='&date='+encodeURIComponent(dt);if(range)u+='&range=
r.json();}).then(function(d){if(d&&d.url){location.href=d.url;}else{alert((d&&d.error)||'Dataset download is not available yet.');}}).catch(function(){alert('Could not start checkout.');});}

Threat Trajectory

Threat Breakdown

Each category 0-100, scored from live conflict, insurgency, crime, protest & Cloudflare Radar cyber feeds. See the full threat matrix

Cyber & Internet Disruption

Layer-7 DDoS attack intensity (0-100, normalized) & internet outages over the last 28 days - Source: Cloudflare Radar.

Situation Summary

Paraguay faces a compounding cyber-security crisis overlaid on persistent traditional organized-crime and street-crime threats in specific regions. A 7.4-million-record citizen-data breach, confirmed presence of Chinese state-sponsored cyber-espionage (Flax Typhoon) in government networks, and a wave of intrusions into judicial, health, and political systems have created a cascading confidentiality and operational-continuity risk for both government and private sector. While Paraguay ranks #107 globally on composite threat, the concentration of cyber and governance risk in Asuncion and critical infrastructure, combined with elevated violent-crime corridors in border departments, warrants elevated duty-of-care posture for corporate operations and personnel.

Key Developments

- Asuncion - Nationwide citizen-data breach (7.4M records): Names, ID numbers, and addresses circulating on criminal forums; identity-theft and phishing risk escalating across the country.

- Asuncion - Chinese cyber-espionage in state systems: U.S. Southern Command and Paraguayan government joint review confirmed Flax Typhoon PRC-linked actor embedded in government networks, threatening classified and operational data.

- Asuncion - Judicial and health-sector breaches: Ministry of Justice and Ministry of Health databases compromised; judges', prosecutors', and HIV/AIDS program data publicly disclosed.

- Asuncion - Political-institution website wave and presidential-account hijack: 30+ government websites defaced; President Pena's X account hijacked to post false Bitcoin-legalization

announcement; disinformation and reputational risk at executive level.

- Nationwide telecom infrastructure - Tigo ransomware attack: Paraguay's largest mobile and internet operator hit; internal systems disrupted; communications and connectivity reliability compromised.

- Eastern border departments (Amambay, Alto Parana, Canindeyu): Transnational criminal organizations drive arms/narcotics trafficking and violent crime; overland travel and commercial movements carry heightened risk.

- Urban centers (Asuncion, major cities): Street crime (pickpocketing, armed robbery on motorcycles, home-invasion impersonation) remains endemic; high baseline risk for expatriates and business travelers.

Highest-Risk Areas

Presidente Hayes Department's disproportionate risk score (31.4) reflects organized-crime activity and remote-area governance gaps; however, the operational concentration of cyber and political risk lies in Asuncion (central government and judiciary). Itapua Department (3.9) and the eastern tri-border corridor (Amambay, Alto Parana, Canindeyu) face persistent transnational-crime and violent-crime drivers. For corporate operations, Asuncion presents acute cyber and data-breach exposure; for field operations and border commerce, eastern departments and overland routes present acute physical-security and trafficking-disruption risk.

How GeoBit Would Assist

Security teams should deploy OSINT Sweep and X/Telegram intelligence to monitor evolving breach disclosures, phishing campaigns, and criminal-forum activity targeting exposed citizen data and corporate entities. AOI Monitoring & Early Warning on Asuncion government networks, telecom infrastructure, and eastern border crossing points would provide real-time alerting on intrusion activity, ransomware incidents, and organized-crime movement. Network & Actor Analysis focused on Flax Typhoon TTPs and local criminal networks, combined with Routing & Network Analysis for personnel movement in high-crime and border zones, enables proactive duty-of-care and incident-response planning.

7-Day Outlook

Government and private-sector cyber-hardening measures are underway, but the scale of the citizen-data breach and persistence of Flax Typhoon suggest continued exploitation risk over the near term. Street crime and border-area organized-crime activity will remain stable but elevated. Monitor telecom-provider recovery timelines and any secondary breach announcements in judicial or health systems.

Highest-Risk Areas - Ranked

#State / RegionRisk1Presidente Hayes Department31.42Itapua Department3.93Caazapa Department2.64Concepcion Department1.45San Pedro Department1.46Guaira Department1.47Amambay Department1.48Canindeyu Department1.49Caaguazu Department1.410Alto Parana Department1.411Boqueron1.412Alto Paraguay Department1.4

Sources

- occrp.org
- theparaguaypost.com
- smartraveller.gov.au

- travel.state.gov
- py.usembassy.gov
- travel.gc.ca
- resecurity.com
- risky.biz
- gordoninstitute.fiu.edu

Download PDF

Email me the PDF

Subscribe to Paraguay daily

See Paraguay live.GeoBit maps Paraguay - every region, event, and risk layer - on demand.Request a live demo

Automated by GeoBit AI from publicly reported events and open-source research. Context only; not a risk advisory. Recognized by Deloitte - NVIDIA Inception - Geospatial World Forum.

REPORTED EVENTS (MOST-CITED)

No high-confidence events in the current window.