WEEKLY INTELLIGENCE BRIEFING

Here is the signal for the week. The data holds, and the trends are clear. We have broken down the critical developments below.

Sequenxa Intelligence Agency

March 2–9, 2026

WEEKLY SYNC

AGENDA

01

MISSING PERSONS

We’re tracking 477 active cases. The data breaks down by age, identified movement corridors, and persistent reporting gaps.

02

EXPOSED INFRASTRUCTURE

Here’s the signal: 10,700+ internet-exposed devices. This includes critical ICS systems requiring immediate attention.

03

PROTEST ACTIVITY

The pattern holds with 522 global events logged. The US is leading volume, though cause attribution remains limited.

04

SANCTIONS & WATCHLISTS

Worth flagging: 4,637 designated entities and 1,191 subjects currently on the FBI watchlist.

05

WHAT TO WATCH

This week’s data shows key signals and structural patterns heading into the next operational cycle.

MISSING PERSONS

477 CASES THIS WEEK

Here's what we're seeing: Canada drives this figure, accounting for 296 cases. Within the domestic landscape, Ontario remains our primary focal point at 128 incidents, while British Columbia follows at 51.

MINORS DOMINATE THE DATA

The pattern holds: our high-volume cohorts are strictly under 18. 15-year-olds lead the count at 52 cases. Worth flagging: the 14, 17, and 16-year-old demographics follow closely with 40, 38, and 29 cases respectively.

HIGH-RISK CORRIDORS & DATA GAPS

1

DOMESTIC CORRIDORS

Flagged: Ontario, BC, Alberta, New Brunswick, Manitoba. Minors account for over 50% of missing counts across these zones.

2

INTERNATIONAL CORRIDORS

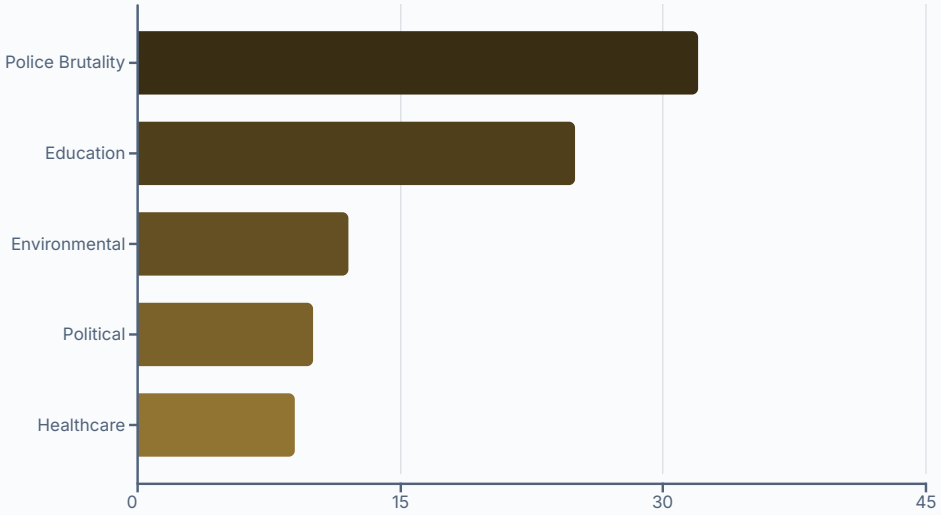
Flagged: Honduras, Ecuador, Guatemala, South Africa, and Slovakia. These are the active priority corridors.

3

DATA CAVEAT

Gap: Gender data is missing for 94% of cases. This severely limits our analysis and exposes systemic failures in upstream documentation.

PROTEST ACTIVITY SNAPSHOT



522 EVENTS GLOBALLY

Here’s the breakdown on global protest activity. We’ve tracked 522 events this week. The US accounts for 392 of those, with Canada logging 46 and Iran 12. Worth flagging: roughly 84% of all events remain unattributed, meaning this chart captures only the identified subset.

- Consider the 522 figure a floor; US volume is almost certainly understated.
- Attribution gaps continue to hinder our week-over-week trend analysis.
- The pattern holds: Iran appears across both protest and sanctions reporting this week.

EXPOSED INFRASTRUCTURE

SCALE OF EXPOSURE

Here's what we're seeing: our latest sweep identified over 10,700 internet-exposed devices this week. We've classified 35 as critical systems and 173 as high-risk.

Geography: The concentration is heaviest across the US Northeast and West Coast, with significant exposure in the South and Midwest as well. Canada East and West contribute approximately 700 units to that total.

ROOT CAUSES

This week's data shows roughly 1,000 devices remain reachable due to unchanged default credentials, while nearly 900 lack authentication entirely. A limited number of cases stem from firewall misconfigurations exposing internal systems.

Key Finding: Worth flagging that industrial control systems—including power grids, water treatment, and manufacturing hardware—are appearing in internet-wide scans. These assets were never designed for external exposure.

WATCHLISTS

SANCTIONS & WATCHLISTS

CONSOLIDATED WATCHLIST: 4,637 ENTITIES

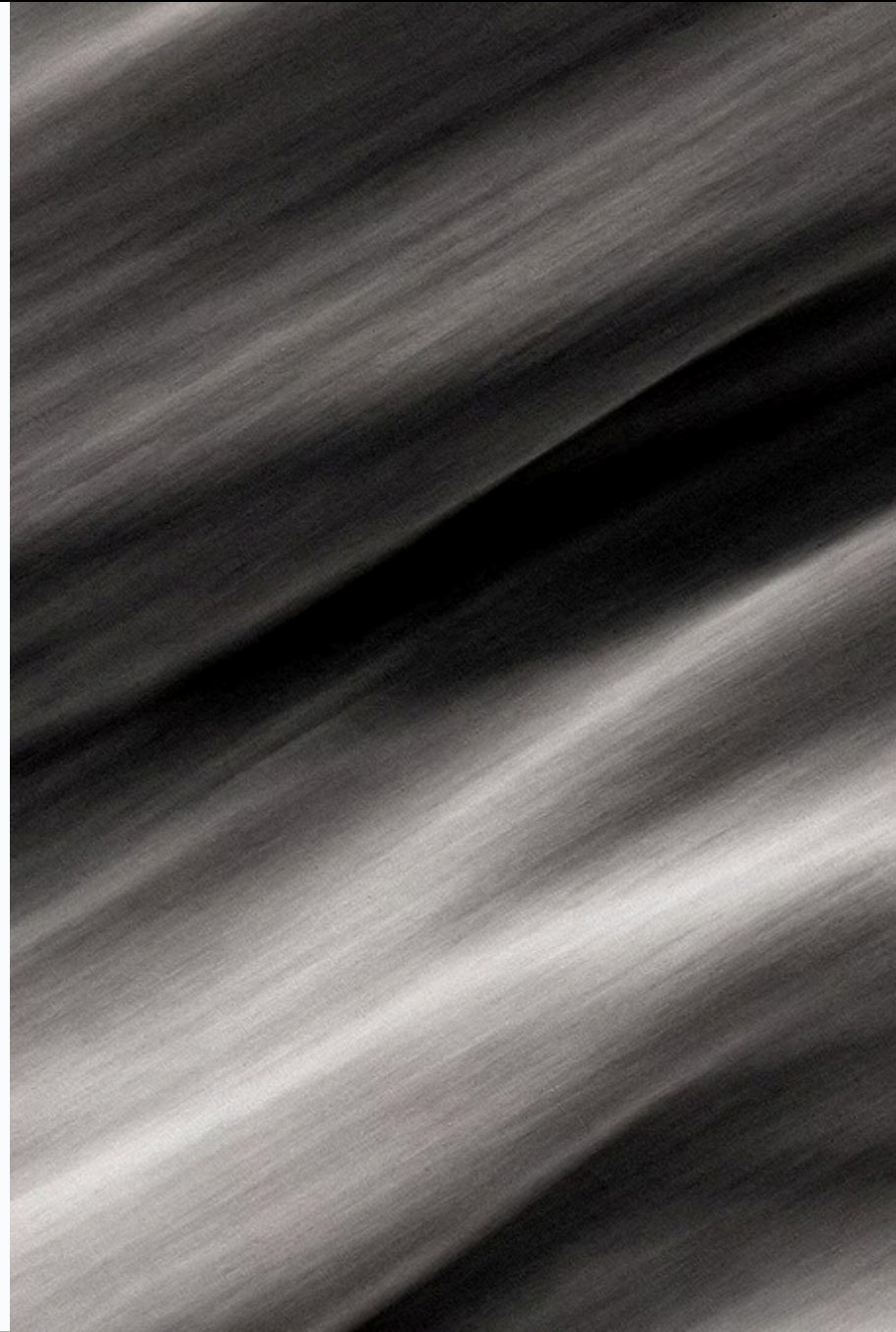
We’re currently tracking 4,637 entities. The majority carry terrorism-related designations, with a significant concentration tied to Iran. Operations remain heaviest in Iran, Pakistan, and Lebanon.

FBI WATCHLIST: 1,191 SUBJECTS

This week’s data shows 1,191 active subjects, with four additions. Flagging thirty as armed and dangerous. Outside of the broad "other" classification, violent crime and cybercrime remain our primary concerns.

IRAN CROSSOVER SIGNAL

Here’s what we’re seeing: Iran appears across multiple streams this week—spanning designated entities, operational areas, and protest activity. It’s worth flagging for potential convergence.



BY THE NUMBERS

1

MISSING PERSONS

- 477 total cases tracked.
- Canada accounts for 296 cases.
- The data skews young; top four age groups are under 18.
- Missing gender data in 94% of records—a clear intelligence gap.

2

INFRASTRUCTURE & WATCHLISTS

- We've identified 10,700+ exposed devices.
- The threat profile includes 35 critical and 173 high-risk systems.
- Consolidated watchlists track 4,637 designated entities.
- FBI records list 1,191 subjects; 30 are flagged as armed and dangerous.

WHAT TO WATCH

Three key indicators demand attention as we transition into the next reporting period. Here is what we're seeing.

MINOR-TO-ADULT RATIO IN MISSING PERSONS

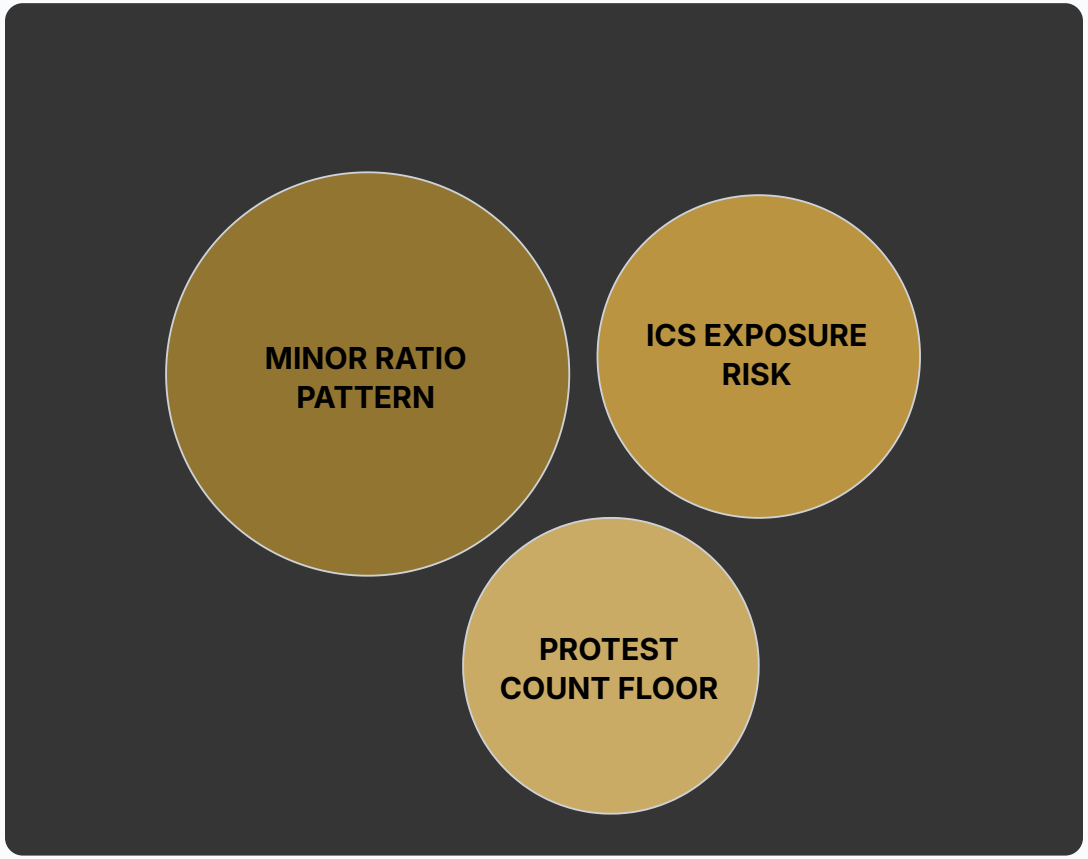
The ratio remains consistently high week over week.

Assessment: This isn't a data anomaly. It's a structural pattern within monitored corridors.

INDUSTRIAL CONTROL SYSTEMS IN EXPOSURE DATA

ICS presence in internet scans warrants a distinct tracking protocol separate from general enterprise devices.

Assessment: The risk profile is fundamentally different. Treat this as a separate category.



REPORT PERIOD CLOSE

- **PROTEST VOLUME CAVEAT**

  Treat 522 events as a floor, not a ceiling. With 84% of events lacking clear attribution, actual activity—especially in the US—is likely significantly higher than what we have recorded.

- **DATA QUALITY WATCH**

  We see a 94% gender data gap in missing persons cases. This signals an upstream documentation failure. We need to flag this to source agencies immediately for the next cycle.

- **NEXT REPORT PERIOD**

  Our focus for 2026-03-09 to 2026-03-16 is clear: monitor Iran crossover signals, verify ICS exposure stability, and confirm the pattern in minor corridor ratios.