

World Monitor: How One Engineer Built a Real-Time Conflict Intelligence System Using Only Open Data

Maria Cattini | 23/04/2026 | OSINT

On February 28, 2026, the United States and Israel launched strikes against Iran. Within hours, [commercial air traffic across the Persian Gulf](#) ground to a halt. Maritime shipping rerouted. Internet outages spread across nodes in the region.

What happened next revealed a structural gap in how information reaches the public during a crisis. News aggregators reported fragments. Social media amplified unverified claims. Professional OSINT platforms — the kind capable of correlating all these signals simultaneously — cost tens of thousands of dollars per year in licensing fees, placing them out of reach for independent analysts, journalists, and researchers.

By that evening, a platform that had attracted roughly one million registered users in several weeks doubled that figure in a single night. [It was called World Monitor](#). Its creator was not a defense analyst or intelligence professional. He was Elie Habib, CEO of Anghami — one of the largest music streaming platforms in the Middle East.

The case of World Monitor is not a story about viral success. It is a technical and methodological case study in how publicly available data streams can be combined, weighted, and correlated to produce something that previously required institutional infrastructure to achieve: real-time situational awareness at the geopolitical level.

Why News Aggregation Was Never the Answer

The standard response to information overload is aggregation. Pull more feeds, filter by keyword, sort by recency. Every major news platform works this way. The problem is structural: aggregation collects what sources have already published. It operates downstream of events.

Habib's diagnosis was precise. He did not need more headlines. He needed a system that showed how events were connected to each other in real time. The distinction matters operationally. An aggregator tells you that an airstrike occurred. A signal-correlation system tells you that a GPS jamming event, three flight reroutes, and an internet blackout occurred in the same 40-kilometer radius within six minutes — before any news outlet filed a report.

This is the core OSINT insight that World Monitor operationalizes: physical signals precede editorial signals. When you correlate the physical layer directly, you move upstream of the news cycle.

System Map: What Data World Monitor Actually Processes

The platform processes over 100 simultaneous data streams. Understanding what those streams are — and where they come from — is the first step toward replicating the methodology independently.

Layer 1: Positional tracking

- ADS-B transponders (Automatic Dependent Surveillance-Broadcast): Aircraft broadcast their position, altitude, speed, and heading in real-time via radio. Civilian aggregators like FlightRadar24

and ADS-B Exchange collect and publish this data. Military aircraft sometimes disable transponders, but deviations from standard routing patterns — or the sudden disappearance of transponder signals — are themselves informative signals.

- AIS signals (Automatic Identification System): Commercial vessels broadcast identity, position, course, and speed. Platforms like MarineTraffic and VesselFinder aggregate this publicly. Cargo ships that stop transmitting, divert from standard shipping lanes, or cluster in unexpected anchorages create detectable anomalies.

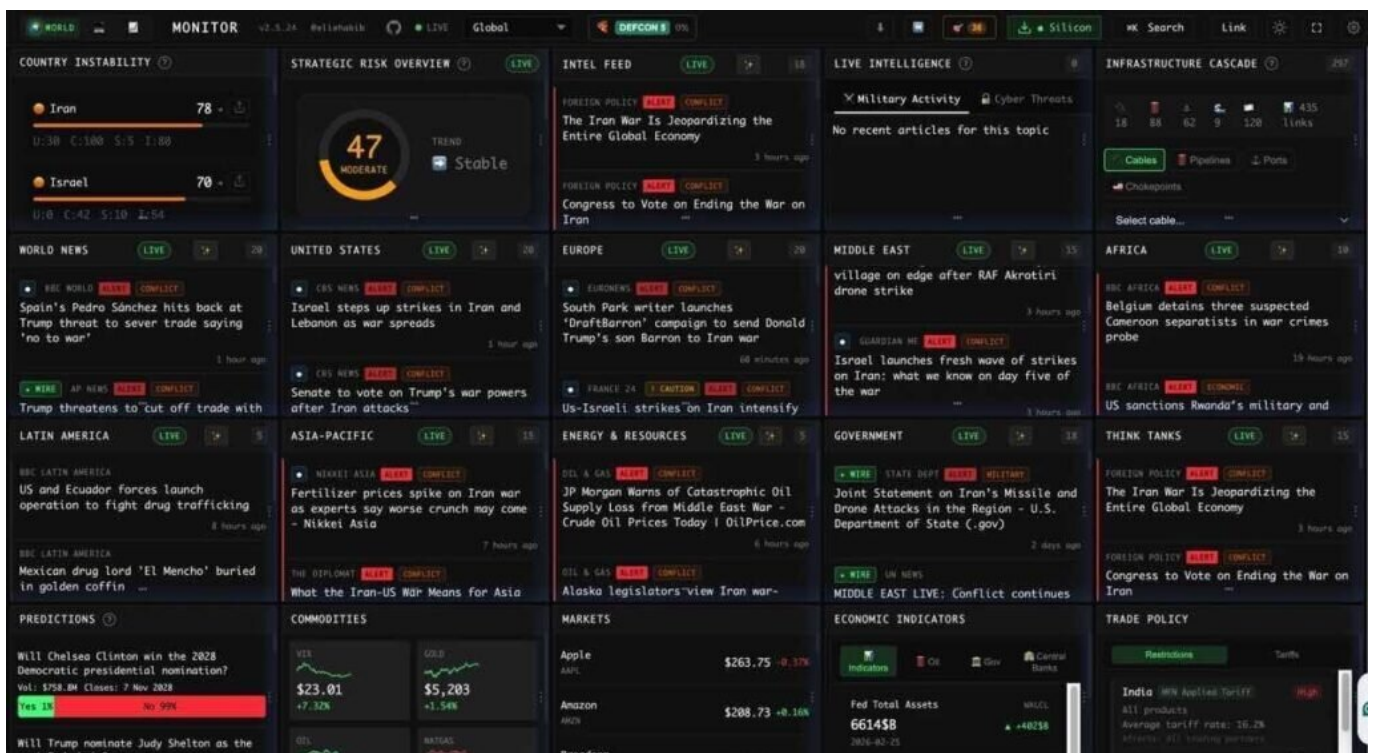
Layer 2: Infrastructure and environmental signals

- Internet outage detection: Services like NetBlocks and IODA (Internet Outage Detection and Analysis, operated by Georgia Tech) monitor real-time BGP routing data and active probing to detect internet disruptions. A sudden BGP route withdrawal in a conflict-adjacent country is a verifiable physical event, not an editorial judgment.
- Satellite-based fire detection: NASA's FIRMS (Fire Information for Resource Management System) publishes near-real-time thermal anomaly data derived from MODIS and VIIRS satellite instruments. A heat signature in a geopolitically sensitive area that does not correspond to known agricultural burn patterns is a cross-checkable signal.
- Nuclear sites, undersea cables, spaceports: These are static infrastructure overlays that provide geographic context for the dynamic signals above.

Layer 3: Editorial and analytical signals

- Wire services: Reuters, AP, AFP
- Governmental sources: US Department of Defense, UN agencies
- Major broadcasters: BBC, Al Jazeera, France 24, CNBC, Bloomberg
- Investigative specialists: Bellingcat
- Telegram channel monitoring (added during the Iran conflict for near-real-time military reporting)
- Embassy alerts and airspace NOTAMs (Notices to Airmen, which document airspace restrictions)

The system processes approximately 190 sources total, each assigned a reliability score. The editorial layer does not drive the alert logic — it is weighted but secondary to physical signal convergence.



Operational Method: How the Alert Logic Works

The core algorithmic logic of World Monitor rests on a single principle: one signal is noise; three or four signals converging on the same geographic area within a compressed time window constitute an event worth flagging.

This is not a new concept in intelligence analysis. It mirrors the triangulation methodology used in traditional HUMINT and SIGINT workflows. What World Monitor does is apply it to open data at machine speed, across a global geographic scope, with no human editorial layer in the decision chain.

Step-by-step: how an escalation alert is generated

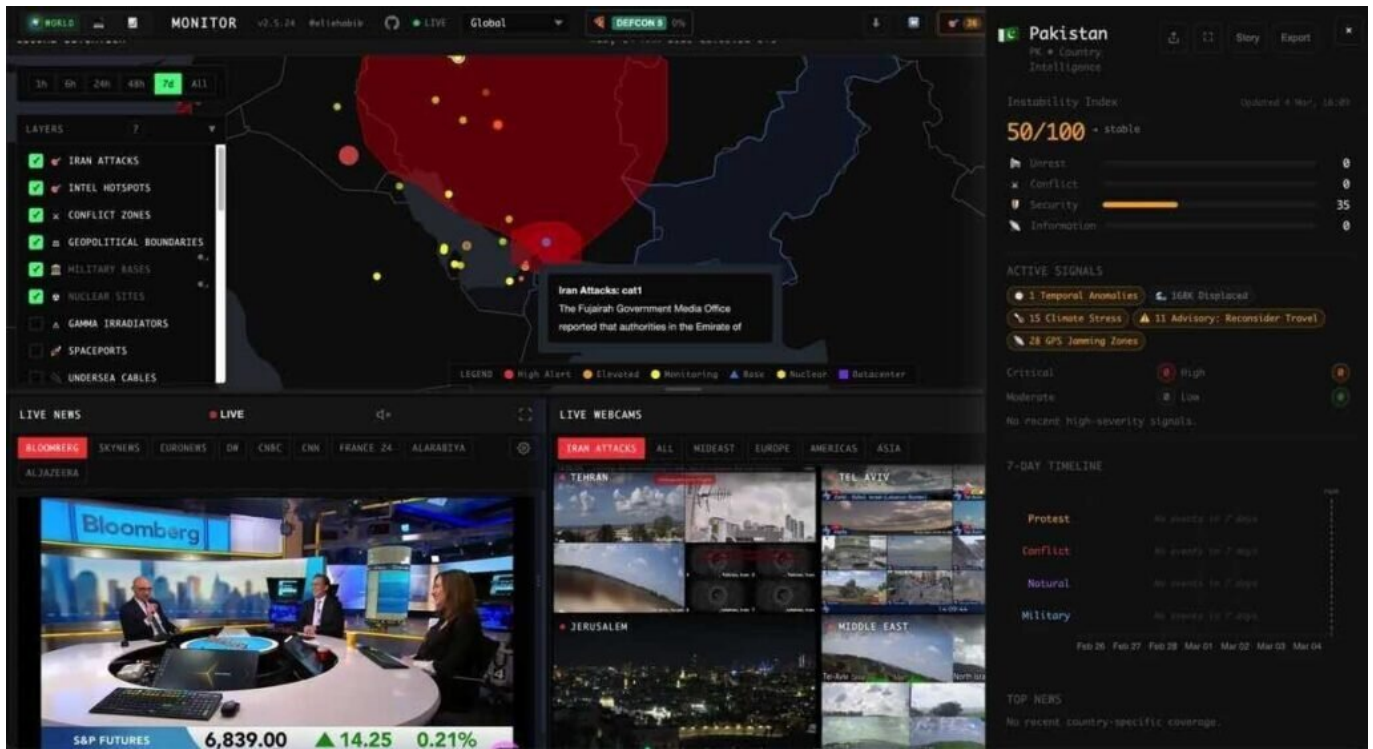
1. Signal ingestion: Continuous API polling and feed parsing across all 190+ sources. Data is normalized — timestamps converted to UTC, locations geocoded, event types categorized.
2. Geospatial binning: Events are assigned to geographic cells. The granularity is not public, but the system must operate at sub-100km resolution to distinguish, for example, a flight deviation near Tehran from one near Tabriz.
3. Cross-layer correlation: The algorithm checks how many distinct signal types — from different layers (positional, infrastructure, editorial) — activate within the same geographic bin within a defined time window. Habib's stated threshold: three or four simultaneous, distinct signal types trigger a high-visibility marker on the map.
4. Reliability weighting: Not all signals carry equal weight. A Reuters dispatch and a Telegram post from an unverified channel are both ingested, but their contribution to the escalation score differs. The weighting schema is not published, but the hierarchy — wire services and government sources at the top, followed by major broadcasters and investigative outlets — is documented.
5. Visualization: Events are rendered on a WebGL globe capable of rendering thousands of simultaneous markers without performance degradation. Escalation zones are color-coded by severity score.

What was added during the Iran conflict (February-March 2026)

The platform's architecture had to adapt in real time. Habib added, under operational pressure:

- Siren alerts translated from Hebrew to English (sourced from Israeli Home Front Command systems)
- GPS jamming detection layers
- Flight cancellation tracking (cross-referenced against standard schedules)
- Telegram channel integration for near-real-time military reporting
- New map layers for rapidly evolving ground situations

The ability to add these features quickly reflects the underlying architecture: a modular data ingestion pipeline, similar to what Habib had built for high-volume music streaming at Anghami and OSN+.



How to Replicate This Methodology Independently

World Monitor is a single integrated platform. The methodology it embodies, however, is replicable using free and open tools. The following stack approximates the core logic:

Positional layer

- ADS-B Exchange (adsbexchange.com) — unfiltered ADS-B data, no military suppression
- MarineTraffic (marinetraffic.com) — AIS ship tracking, free tier available
- FlightAware (flightaware.com) — commercial aviation tracking

Infrastructure layer

- IODA (ioda.live) — real-time internet outage visualization by country and AS number
- NetBlocks (netblocks.org) — publishes outage reports, active on social media
- NASA FIRMS (firms.modaps.eosdis.nasa.gov) — satellite fire/thermal anomaly data, free API

Editorial layer

- GDELT Project (gdeltproject.org) — real-time global news event database, free, machine-readable
- Bellingcat (bellingcat.com) — open source investigative journalism
- LiveUA Map (liveuamap.com) — conflict mapping, crowdsourced with moderation

Verification and cross-check

- Google Earth Engine — for satellite imagery cross-reference
- Sentinel Hub EO Browser (browser.dataspace.copernicus.eu) — free Copernicus satellite imagery
- Radio Free Europe / Reuters / AP — primary editorial cross-check layer

Correlation workflow (manual version)

1. Set a geographic area of interest.

2. Monitor ADS-B and AIS for anomalies (route deviations, transponder gaps, vessel clustering).
3. Cross-check IODA for internet disruption events in the same area.
4. Pull FIRMS data for thermal anomalies in a 24–72 hour window.
5. Search GDELT for editorial coverage in the same geographic cluster.
6. If three or more distinct signal types activate in the same area within a 6–12 hour window: document, timestamp, and escalate for further investigation.

This is not automated. Running it manually requires analyst time and tool familiarity. But the logic is identical to what World Monitor executes algorithmically.

Critical Issues: What the System Does Not Solve

Habib acknowledges the core risk explicitly: removing human editorial judgment creates structural blind spots.

Blind spot 1: Novel event types

The convergence algorithm is trained — implicitly — on historical conflict patterns. An escalation that does not fit established signal patterns (a cyberattack with no physical signature, a covert infiltration, a political crisis without kinetic activity) may not trigger the alert threshold. The system flags what matches the model; it has no mechanism for flagging what it does not recognize.

Blind spot 2: Signal manipulation

ADS-B and AIS data can be spoofed. GPS jamming — which the platform now tracks — can create phantom aircraft positions or obscure real ones. A sophisticated actor aware of how the platform's alert logic works could, in theory, generate or suppress signals to manipulate the convergence score. This is not a theoretical concern: GPS spoofing in the Black Sea and Eastern Mediterranean has been documented by aviation authorities for several years.

Blind spot 3: Reliability scoring under pressure

The weighting system assigns higher scores to established outlets. But during fast-moving events, established outlets are frequently wrong or slow. The speed advantage of the platform — flagging events before mainstream coverage — partly depends on ingesting lower-reliability sources like Telegram channels. The tension between speed and accuracy is not resolved by the architecture; it is embedded in it.

Blind spot 4: Geopolitical bias in source coverage

The source hierarchy reflects the English-language and Western media ecosystem. Events in regions with thin coverage from Reuters, AP, or BBC will generate fewer editorial signals, reducing the convergence score even if physical signals are present. This creates systematic underreporting of escalations in areas with weak international media presence.

Analytical Layer: What World Monitor Reveals About OSINT's Structural Shift

The user base breakdown is instructive. At the point of reporting: Asia accounted for approximately 35% of traffic; Europe, 20%; Middle East and North Africa, 18%; United States, 10%. These are not the demographics of a professional intelligence tool. They are the demographics of a global public that has lost confidence in the editorial layer's ability to provide timely situational awareness.

The platform's rapid adoption — 216,000 concurrent users on peak days — reflects a structural demand that existing media and intelligence products were not meeting. Professional OSINT platforms charge institutional prices for institutional access. Newsrooms aggregating and filtering content operate too slowly during fast-moving crises. The gap between these two product categories is exactly where World Monitor sits.

What makes this significant for practitioners is not the platform itself, but the demonstration effect. A six-day build — by someone who explicitly had no intelligence background — produced a tool that outperformed, in speed and multi-signal correlation, the products that governments and large corporations pay tens of thousands of dollars per year to access. The primary input was methodological clarity: understand which data streams are publicly available, understand the correlation logic, build the ingestion and visualization layer.

The Bellingcat model proved that open source investigation could match or exceed classified intelligence for specific verification tasks. World Monitor's emergence suggests the same dynamic is now operating at the infrastructure level — not for individual event verification, but for continuous, real-time geopolitical monitoring.

The system's next stated direction is predictive: from monitoring events after they occur to detecting convergence patterns before they become news. Habib's stated goal is identifying where signals are clustering before the escalation becomes visible to editorial coverage.

This is a different problem than reactive monitoring. Predictive signal detection requires baseline modeling — establishing what normal looks like for a given region across all signal layers, so that deviations can be detected against that baseline rather than against a news cycle. It requires longer time-series data, more sophisticated anomaly detection, and a clearer framework for distinguishing genuine pre-escalation signals from noise patterns that happen to cluster geographically.

The tools to build this exist. The methodology is established in academic conflict early-warning research. The open data streams are accessible. What World Monitor demonstrates is that the barrier to assembling these components is lower than the institutional OSINT market has historically suggested.

The constraint is not data. The constraint is the analytical framework for what to look for before you know what you are looking for.

Join the community:

- Newsletter → <https://projectosint.substack.com/>
- Telegram → <https://t.me/osintprojectgroup>

On February 28, 2026, the United States and Israel launched strikes against Iran. Within hours, [commercial air traffic across the Persian Gulf](#) ground to a halt. Maritime shipping rerouted. Internet outages spread across nodes in the region.

What happened next revealed a structural gap in how information reaches the public during a crisis. News aggregators reported fragments. Social media amplified unverified claims. Professional OSINT platforms — the kind capable of correlating all these signals simultaneously — cost tens of thousands of dollars per year in licensing fees, placing them out of reach for independent analysts, journalists, and researchers.

By that evening, a platform that had attracted roughly one million registered users in several weeks doubled that figure in a single night. [It was called World Monitor](#). Its creator was not a defense analyst or intelligence professional. He was Elie Habib, CEO of Anghami — one of the largest music streaming platforms in the Middle East.

The case of World Monitor is not a story about viral success. It is a technical and methodological case study in how publicly available data streams can be combined, weighted, and correlated to produce something that previously required institutional infrastructure to achieve: real-time situational awareness at the geopolitical level.

Why News Aggregation Was Never the Answer

The standard response to information overload is aggregation. Pull more feeds, filter by keyword, sort by recency. Every major news platform works this way. The problem is structural: aggregation collects what sources have already published. It operates downstream of events.

Habib's diagnosis was precise. He did not need more headlines. He needed a system that showed how events were connected to each other in real time. The distinction matters operationally. An aggregator tells you that an airstrike occurred. A signal-correlation system tells you that a GPS jamming event, three flight reroutes, and an internet blackout occurred in the same 40-kilometer radius within six minutes — before any news outlet filed a report.

This is the core OSINT insight that World Monitor operationalizes: physical signals precede editorial signals. When you correlate the physical layer directly, you move upstream of the news cycle.

System Map: What Data World Monitor Actually Processes

The platform processes over 100 simultaneous data streams. Understanding what those streams are — and where they come from — is the first step toward replicating the methodology independently.

Layer 1: Positional tracking

- ADS-B transponders (Automatic Dependent Surveillance-Broadcast): Aircraft broadcast their position, altitude, speed, and heading in real-time via radio. Civilian aggregators like FlightRadar24 and ADS-B Exchange collect and publish this data. Military aircraft sometimes disable transponders, but deviations from standard routing patterns — or the sudden disappearance of transponder signals — are themselves informative signals.
- AIS signals (Automatic Identification System): Commercial vessels broadcast identity, position, course, and speed. Platforms like MarineTraffic and VesselFinder aggregate this publicly. Cargo ships that stop transmitting, divert from standard shipping lanes, or cluster in unexpected anchorages create detectable anomalies.

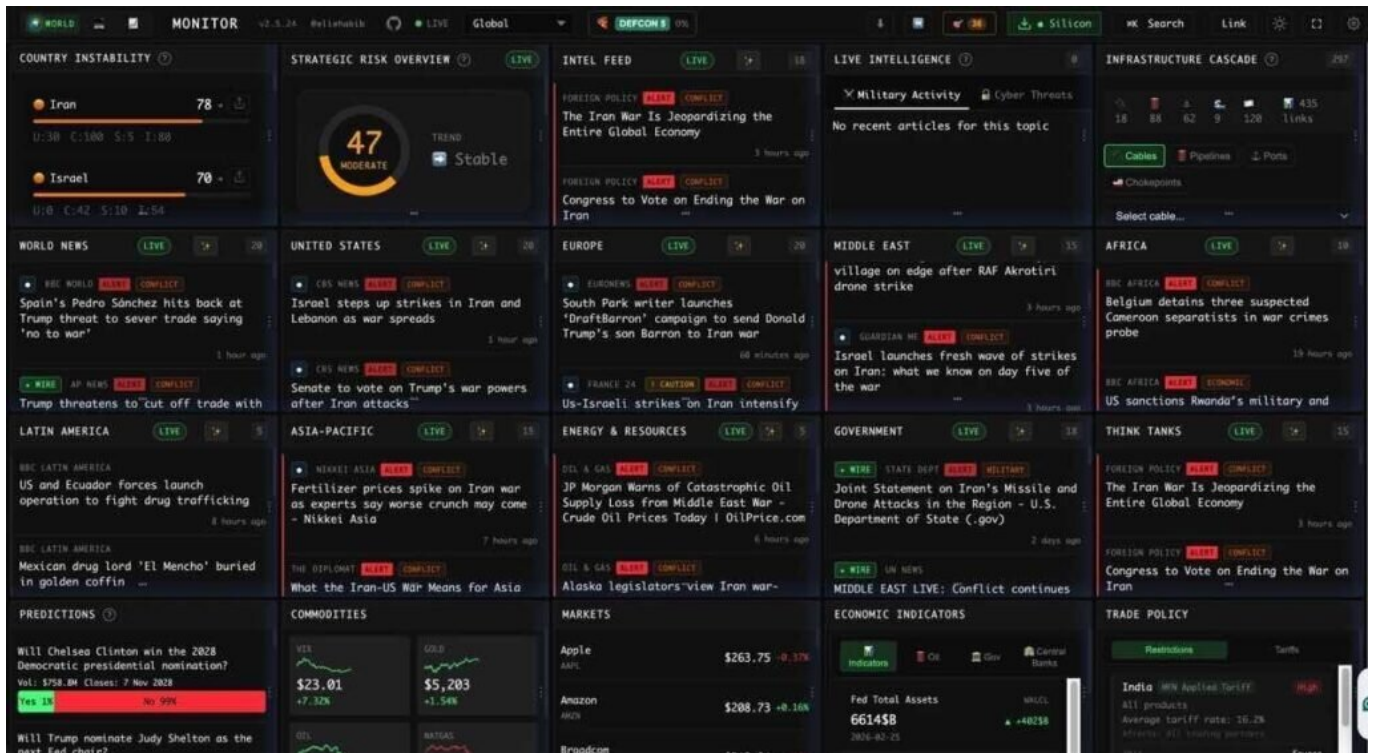
Layer 2: Infrastructure and environmental signals

- Internet outage detection: Services like NetBlocks and IODA (Internet Outage Detection and Analysis, operated by Georgia Tech) monitor real-time BGP routing data and active probing to detect internet disruptions. A sudden BGP route withdrawal in a conflict-adjacent country is a verifiable physical event, not an editorial judgment.
- Satellite-based fire detection: NASA's FIRMS (Fire Information for Resource Management System) publishes near-real-time thermal anomaly data derived from MODIS and VIIRS satellite instruments. A heat signature in a geopolitically sensitive area that does not correspond to known agricultural burn patterns is a cross-checkable signal.
- Nuclear sites, undersea cables, spaceports: These are static infrastructure overlays that provide geographic context for the dynamic signals above.

Layer 3: Editorial and analytical signals

- Wire services: Reuters, AP, AFP
- Governmental sources: US Department of Defense, UN agencies
- Major broadcasters: BBC, Al Jazeera, France 24, CNBC, Bloomberg
- Investigative specialists: Bellingcat
- Telegram channel monitoring (added during the Iran conflict for near-real-time military reporting)
- Embassy alerts and airspace NOTAMs (Notices to Airmen, which document airspace restrictions)

The system processes approximately 190 sources total, each assigned a reliability score. The editorial layer does not drive the alert logic — it is weighted but secondary to physical signal convergence.



Operational Method: How the Alert Logic Works

The core algorithmic logic of World Monitor rests on a single principle: one signal is noise; three or four signals converging on the same geographic area within a compressed time window constitute an event worth flagging.

This is not a new concept in intelligence analysis. It mirrors the triangulation methodology used in traditional HUMINT and SIGINT workflows. What World Monitor does is apply it to open data at machine speed, across a global geographic scope, with no human editorial layer in the decision chain.

Step-by-step: how an escalation alert is generated

1. Signal ingestion: Continuous API polling and feed parsing across all 190+ sources. Data is normalized — timestamps converted to UTC, locations geocoded, event types categorized.
2. Geospatial binning: Events are assigned to geographic cells. The granularity is not public, but the system must operate at sub-100km resolution to distinguish, for example, a flight deviation near Tehran from one near Tabriz.
3. Cross-layer correlation: The algorithm checks how many distinct signal types — from different layers (positional, infrastructure, editorial) — activate within the same geographic bin within a defined time window. Habib's stated threshold: three or four simultaneous, distinct signal types trigger a high-visibility marker on the map.
4. Reliability weighting: Not all signals carry equal weight. A Reuters dispatch and a Telegram post from an unverified channel are both ingested, but their contribution to the escalation score differs. The weighting schema is not published, but the hierarchy — wire services and government sources at the top, followed by major broadcasters and investigative outlets — is documented.
5. Visualization: Events are rendered on a WebGL globe capable of rendering thousands of simultaneous markers without performance degradation. Escalation zones are color-coded by severity score.

What was added during the Iran conflict (February-March 2026)

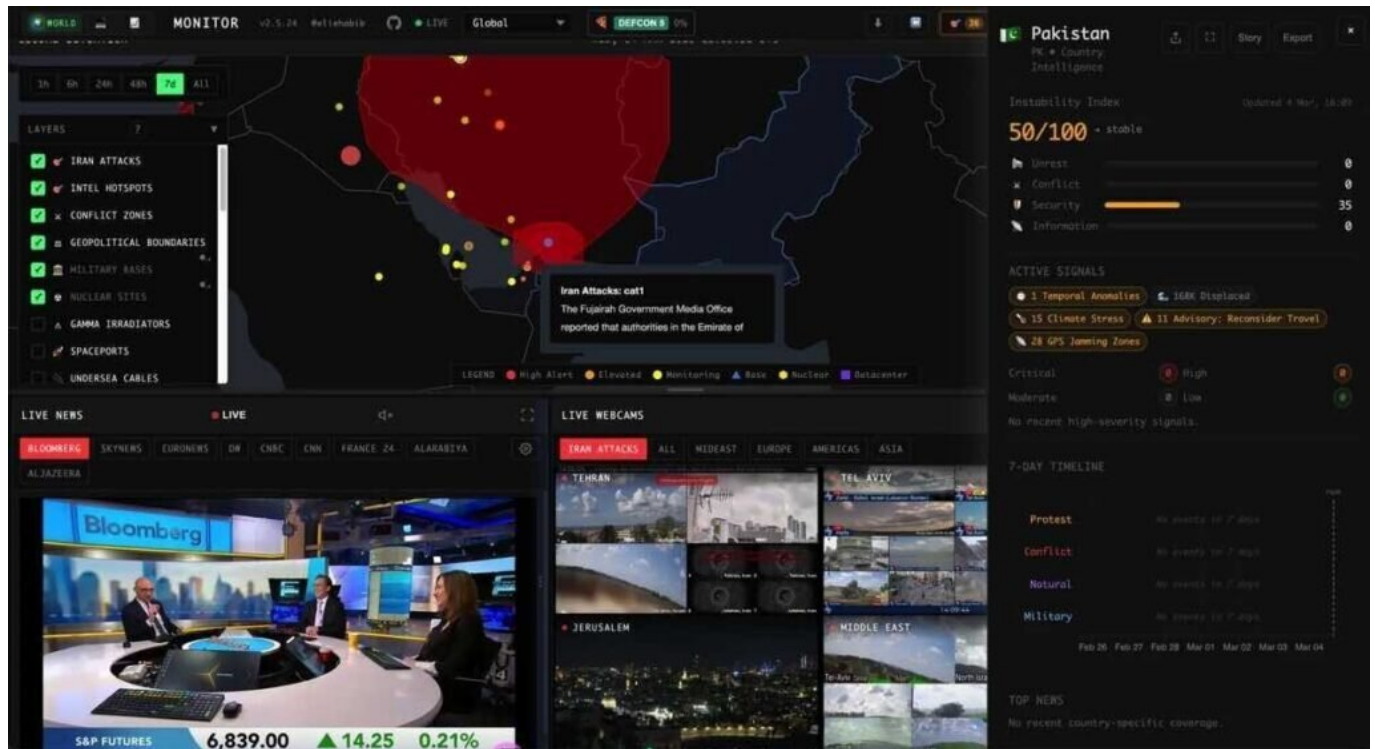
The platform's architecture had to adapt in real time. Habib added, under operational pressure:

- Siren alerts translated from Hebrew to English (sourced from Israeli Home Front Command)

systems)

- GPS jamming detection layers
- Flight cancellation tracking (cross-referenced against standard schedules)
- Telegram channel integration for near-real-time military reporting
- New map layers for rapidly evolving ground situations

The ability to add these features quickly reflects the underlying architecture: a modular data ingestion pipeline, similar to what Habib had built for high-volume music streaming at Anghami and OSN+.



How to Replicate This Methodology Independently

World Monitor is a single integrated platform. The methodology it embodies, however, is replicable using free and open tools. The following stack approximates the core logic:

Positional layer

- ADS-B Exchange (adsbexchange.com) — unfiltered ADS-B data, no military suppression
- MarineTraffic (marinetraffic.com) — AIS ship tracking, free tier available
- FlightAware (flightaware.com) — commercial aviation tracking

Infrastructure layer

- IODA (ioda.live) — real-time internet outage visualization by country and AS number
- NetBlocks (netblocks.org) — publishes outage reports, active on social media
- NASA FIRMS (firms.modaps.eosdis.nasa.gov) — satellite fire/thermal anomaly data, free API

Editorial layer

- GDELT Project (gdeltproject.org) — real-time global news event database, free, machine-readable
- Bellingcat (bellingcat.com) — open source investigative journalism
- LiveUA Map (liveuamap.com) — conflict mapping, crowdsourced with moderation

Verification and cross-check

- Google Earth Engine — for satellite imagery cross-reference
- Sentinel Hub EO Browser (browser.dataspace.copernicus.eu) — free Copernicus satellite imagery
- Radio Free Europe / Reuters / AP — primary editorial cross-check layer

Correlation workflow (manual version)

1. Set a geographic area of interest.
2. Monitor ADS-B and AIS for anomalies (route deviations, transponder gaps, vessel clustering).
3. Cross-check IODA for internet disruption events in the same area.
4. Pull FIRMS data for thermal anomalies in a 24–72 hour window.
5. Search GDELT for editorial coverage in the same geographic cluster.
6. If three or more distinct signal types activate in the same area within a 6–12 hour window: document, timestamp, and escalate for further investigation.

This is not automated. Running it manually requires analyst time and tool familiarity. But the logic is identical to what World Monitor executes algorithmically.

Critical Issues: What the System Does Not Solve

Habib acknowledges the core risk explicitly: removing human editorial judgment creates structural blind spots.

Blind spot 1: Novel event types

The convergence algorithm is trained — implicitly — on historical conflict patterns. An escalation that does not fit established signal patterns (a cyberattack with no physical signature, a covert infiltration, a political crisis without kinetic activity) may not trigger the alert threshold. The system flags what matches the model; it has no mechanism for flagging what it does not recognize.

Blind spot 2: Signal manipulation

ADS-B and AIS data can be spoofed. GPS jamming — which the platform now tracks — can create phantom aircraft positions or obscure real ones. A sophisticated actor aware of how the platform's alert logic works could, in theory, generate or suppress signals to manipulate the convergence score. This is not a theoretical concern: GPS spoofing in the Black Sea and Eastern Mediterranean has been documented by aviation authorities for several years.

Blind spot 3: Reliability scoring under pressure

The weighting system assigns higher scores to established outlets. But during fast-moving events, established outlets are frequently wrong or slow. The speed advantage of the platform — flagging events before mainstream coverage — partly depends on ingesting lower-reliability sources like Telegram channels. The tension between speed and accuracy is not resolved by the architecture; it is embedded in it.

Blind spot 4: Geopolitical bias in source coverage

The source hierarchy reflects the English-language and Western media ecosystem. Events in regions with thin coverage from Reuters, AP, or BBC will generate fewer editorial signals, reducing the convergence score even if physical signals are present. This creates systematic underreporting of escalations in areas with weak international media presence.

Analytical Layer: What World Monitor Reveals About OSINT's Structural Shift

The user base breakdown is instructive. At the point of reporting: Asia accounted for approximately 35% of traffic; Europe, 20%; Middle East and North Africa, 18%; United States, 10%. These are not the demographics of a professional intelligence tool. They are the demographics of a global public that has lost confidence in the editorial layer's ability to provide timely situational awareness.

The platform's rapid adoption — 216,000 concurrent users on peak days — reflects a structural demand that existing media and intelligence products were not meeting. Professional OSINT platforms charge institutional prices for institutional access. Newsrooms aggregating and filtering content operate too slowly during fast-moving crises. The gap between these two product categories is exactly where World Monitor sits.

What makes this significant for practitioners is not the platform itself, but the demonstration effect. A six-day build — by someone who explicitly had no intelligence background — produced a tool that outperformed, in speed and multi-signal correlation, the products that governments and large corporations pay tens of thousands of dollars per year to access. The primary input was methodological clarity: understand which data streams are publicly available, understand the correlation logic, build the ingestion and visualization layer.

The Bellingcat model proved that open source investigation could match or exceed classified intelligence for specific verification tasks. World Monitor's emergence suggests the same dynamic is now operating at the infrastructure level — not for individual event verification, but for continuous, real-time geopolitical monitoring.

The system's next stated direction is predictive: from monitoring events after they occur to detecting convergence patterns before they become news. Habib's stated goal is identifying where signals are clustering before the escalation becomes visible to editorial coverage.

This is a different problem than reactive monitoring. Predictive signal detection requires baseline modeling — establishing what normal looks like for a given region across all signal layers, so that deviations can be detected against that baseline rather than against a news cycle. It requires longer time-series data, more sophisticated anomaly detection, and a clearer framework for distinguishing genuine pre-escalation signals from noise patterns that happen to cluster geographically.

The tools to build this exist. The methodology is established in academic conflict early-warning research. The open data streams are accessible. What World Monitor demonstrates is that the barrier to assembling these components is lower than the institutional OSINT market has historically suggested.

The constraint is not data. The constraint is the analytical framework for what to look for before you know what you are looking for.

Join the community:

- Newsletter → <https://projectosint.substack.com/>
- Telegram → <https://t.me/osintprojectgroup>