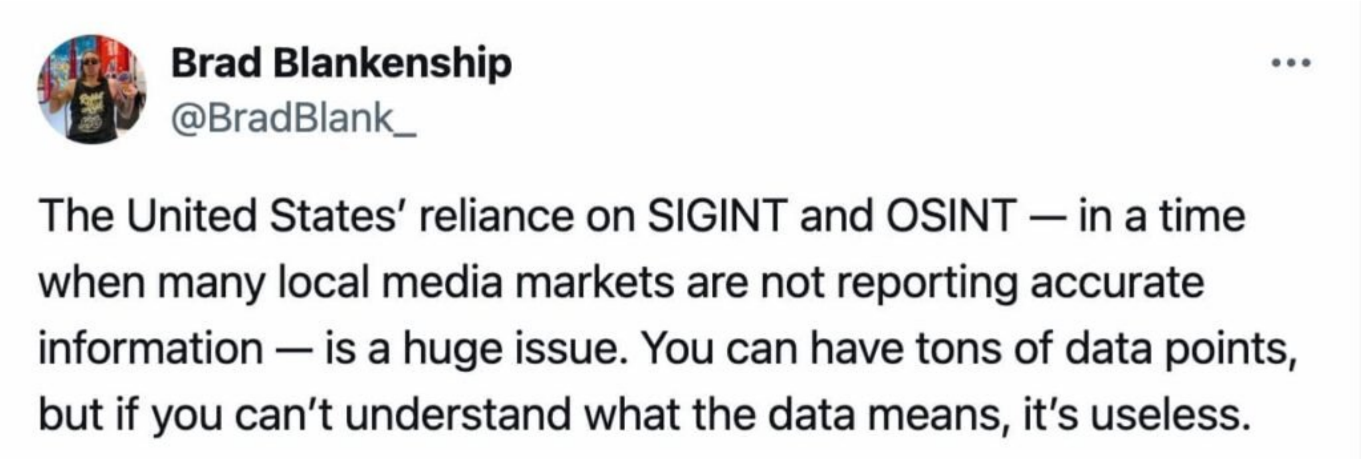
The Rise of OSINT and SIGINT: What Happens When Local Media Fails

Maria Cattini | 04/09/2025 | Open source intelligence

Brad Blankenship recently highlighted a critical trend: *Washington is increasingly leaning on open-source and signals intelligence because many local media outlets no longer provide reliable reporting*.
This is not a minor shift — it represents a structural transformation in how governments, journalists, and even citizens access and validate information.



Brad Blankenship
@BradBlank_

The United States' reliance on SIGINT and OSINT — in a time when many local media markets are not reporting accurate information — is a huge issue. You can have tons of data points, but if you can't understand what the data means, it's useless.

Why Open-Source Intelligence Became Central

OSINT (Open-Source Intelligence) refers to gathering and analyzing data that is publicly available — from social platforms and local news sites to commercial satellites and shipping trackers.

- **Ukraine (2014–2022):** Before the full-scale invasion, analysts mapped Russian troop buildups using satellite imagery from Maxar and TikTok videos geolocated by volunteers. Investigations by Bellingcat proved that OSINT could outpace NATO briefings in terms of speed and accuracy.
- **Gaza (2023–2024):** Civil drones and high-resolution commercial satellite images documented strikes, civilian casualties, and even humanitarian corridors before official statements from governments or NGOs.

- **Myanmar (2021):** TikTok and Facebook Live videos uploaded by citizens became admissible evidence in UN investigations on human rights abuses, illustrating OSINT’s judicial relevance.

OSINT has democratized intelligence gathering, but it comes with risks: manipulated footage, disinformation campaigns, and the “illusion of accuracy” when unverified data circulates as fact.

When Signals Intelligence Leaves the Shadows

SIGINT (Signals Intelligence) was once the exclusive domain of agencies like the NSA, GCHQ, or Mossad. That monopoly has eroded:

- **Sudan (2023):** Commercial radio scanners intercepted military chatter in Khartoum, later shared on OSINT channels.
- **Black Sea:** Civil AIS-spoofing monitors detected oil tankers bypassing sanctions by falsifying positions.
- **Baltic States:** Universities and private firms now deploy low-cost antennas to track satellite traffic — once an unthinkable capability for non-state actors.

This “privatization” of SIGINT blurs the lines between national security, journalism, and commercial surveillance. It also raises ethical and legal dilemmas that governments are not fully prepared to address.

The most alarming factor is not technological but societal: the decline of local, independent media. In **Ethiopia’s Tigray conflict**, journalists were expelled and censorship tightened. The result? Almost every verified report relied on OSINT (satellite photos of scorched villages) or SIGINT leaks.

Without strong reporters on the ground, the global narrative of wars, crises, or disasters risks becoming entirely dependent on digital traces — quick to spread, but fragile under scrutiny.

OSINT vs SIGINT: Strengths and Trade-Offs

Aspect	**OSINT (Open Source)**	**SIGINT (Signals)**
Accessibility	Open to NGOs, journalists, citizens.	Traditionally state-owned, but commercial tools are emerging.
Costs	Low to moderate: social data, commercial satellites.	High: antennas, satellites, classified infrastructure. Some costs are falling via COTS solutions.
Speed	Immediate: posts, drones, and live streams.	Often delayed: requires authorization, data is classified.
Risks	Fake news, propaganda, language bias, overload.	Legal breaches, espionage scandals, diplomatic fallout.
Opportunities	Exposing war crimes, illicit trade, disaster monitoring.	Tracking military activity, smuggling routes, clandestine networks.
Added Value	Transparency, accountability, public verification.	Access to non-public signals and technical depth.

Field Guide: 3 OSINT Investigations Anyone Can Replicate

1. **Verify the origin of a conflict video**
    - *Tools:* Google Earth, Sentinel Hub, Mapillary.
    - *Method:* Look for landmarks, shadows, signage → match with satellite maps → confirm coordinates.
    - *Use case:* Validate whether a viral war video truly comes from the reported location.
2. **Follow a suspicious tanker in the Mediterranean**
    - *Tools:* MarineTraffic, VesselFinder, OSINT Combine.
    - *Method:* Track movements → compare with embargo announcements → flag unusual route patterns.
    - *Use case:* Document sanction evasion or illegal trade.
    - **Spot military buildup with satellite imagery**
        - *Tools:* Planet Labs, Maxar, Copernicus Sentinel.

- *Method:* Analyze time-lapse imagery → detect repeated patterns of vehicles or makeshift runways.

- *Use case:* Monitor tensions near contested borders.

Beyond Technology: The Mirage of Transparency

The surge of OSINT and SIGINT creates a paradox. The more data is accessible, the stronger the belief that *everything is verifiable*.
In reality, every data point can be falsified or stripped of context. Without resilient local reporting and multi-layered verification, even the best intelligence risks becoming a **mirage of truth**.