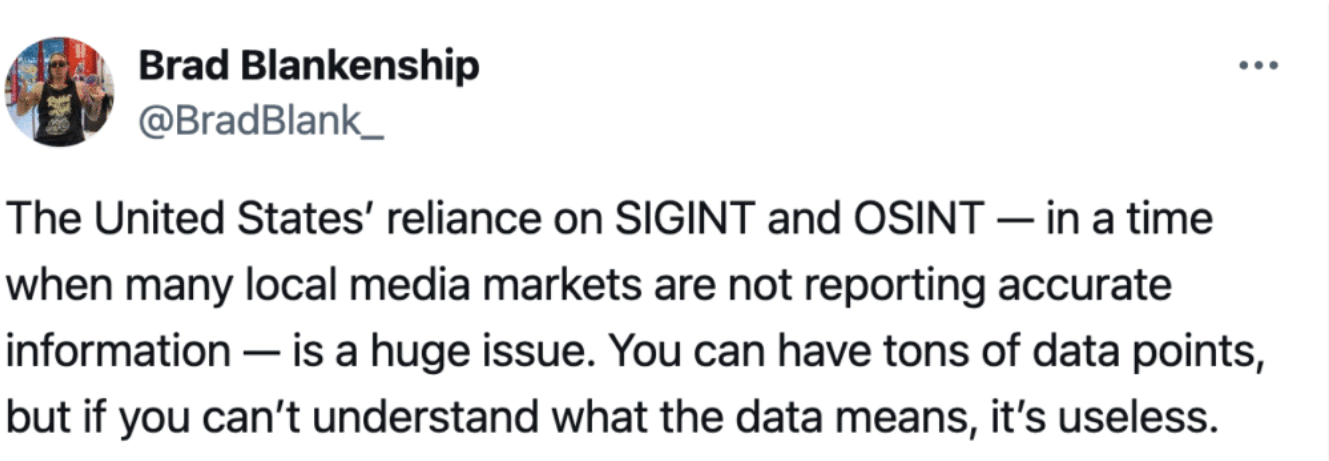
Quando OSINT e SIGINT diventano essenziali

Maria Cattini | 26/08/2025 | Open source intelligence

La fragilità dell'informazione locale e la new-normal della raccolta intelligence



Il tweet di Brad Blankenship sottolinea un passaggio epocale: *gli Stati Uniti — e non solo loro — fanno sempre più affidamento su OSINT e SIGINT in un'epoca in cui i media locali non garantiscono più accuratezza e copertura completa*.
È un cambio di paradigma che non riguarda solo le guerre ibride o i teatri di crisi, ma l'intero ecosistema dell'informazione globale.OSINT sul campo: casi pratici

Ucraina: Twitter e Telegram al posto dei giornalisti embedded

Dal 2014 al 2022, fino all'invasione su larga scala, l'analisi di foto e video pubblicati su Telegram**, TikTok e Twitter** è diventata cruciale per mappare movimenti di truppe, identificare armi e verificare attacchi.
Gruppi come **Bellingcat** hanno dimostrato che una foto satellitare gratuita di Maxar o un video girato con uno smartphone potevano confermare la presenza di sistemi missilistici russi ben più rapidamente dei briefing ufficiali della NATO.

Gaza: droni civili e satelliti commerciali

Nel conflitto tra Israele e Hamas, giornalisti e ricercatori indipendenti hanno usato immagini da **Planet Labs** e video di droni civili per documentare bombardamenti, localizzare ospedali colpiti e persino monitorare corridoi umanitari. Questo tipo di OSINT ha spesso anticipato le dichiarazioni ufficiali di governi e ONG.

Myanmar: TikTok come fonte di prova

Dopo il colpo di stato del 2021, la repressione è stata documentata da cittadini attraverso **Facebook Live e TikTok**. Molti video, geolocalizzati con metodi OSINT, sono entrati nei dossier delle Nazioni

Unite come **evidenze di violazioni dei diritti umani**, segnalando un ribaltamento: l'open source come fonte giudiziaria.

SIGINT e geopolitica: da monopolio statale a "mercato privato"

Il **Signals Intelligence**, un tempo esclusiva di NSA, GCHQ o Mossad, oggi è "democratizzato". Alcuni casi:

• Sudan, 2023: durante i combattimenti a Khartoum, agenzie private hanno usato radio-scanners commerciali per monitorare le comunicazioni militari. Alcuni dati sono trapelati su canali OSINT, fornendo prove sugli spostamenti dei generali.
• Mar Nero: flotte commerciali di AIS spoofing detection (Automatic Identification System) hanno rivelato manovre sospette di petroliere russe che aggiravano le sanzioni, un compito tradizionalmente riservato a satelliti militari.
• BaltiTech in Lituania ha sviluppato sistemi di intercettazione low-cost per monitorare traffico satellitare LEO. Questi strumenti, accessibili anche a università e centri civili, dimostrano come il SIGINT sia ormai parte di un mercato aperto.

Quando i media sul campo sono deboli o controllati dal potere politico, **l'intelligence open source diventa la principale lente sul reale**.
Un esempio lampante è l'**Etiopia durante la guerra nel Tigray**: mentre i giornalisti indipendenti erano espulsi, OSINT e SIGINT hanno fornito quasi tutte le informazioni sulla crisi umanitaria.
Il problema: senza corrispondenti e fact-checking radicati, l'ecosistema si affida a **fonti digitali**, più rapide ma anche più manipolabili.

OSINT + SIGINT integrati

• All-Source Analysis (ASA): metodologia che integra OSINT, SIGINT, HUMINT e GEOINT per compensare i limiti delle singole fonti.
• AI e NLP (Natural Language Processing): usati per scandagliare milioni di post sui social in tempo reale. Ad esempio, software come Palantir Gotham o Dataminr filtrano segnali da rumore con algoritmi di machine learning.
• COTS Satellites (Commercial Off-The-Shelf): immagini satellitari di alta qualità acquistabili sul mercato (Planet, Maxar, Capella Space) che hanno rivoluzionato la sorveglianza strategica.
• AIS e ADS-B tracking: sistemi civili per monitorare navi e velivoli, oggi sfruttati da analisti OSINT per studiare traffici sospetti (armi, petrolio, contrabbando).

C'è però un paradosso: **più OSINT e SIGINT diventano accessibili, più rischiamo di credere che "tutto sia verificabile"**.
In realtà, ogni dato aperto può essere manipolato, falsificato o decontestualizzato. Senza media locali robusti e senza un ecosistema di verifica multilivello, persino la migliore intelligence open-source rischia di diventare un **miraggio di accuratezza**.

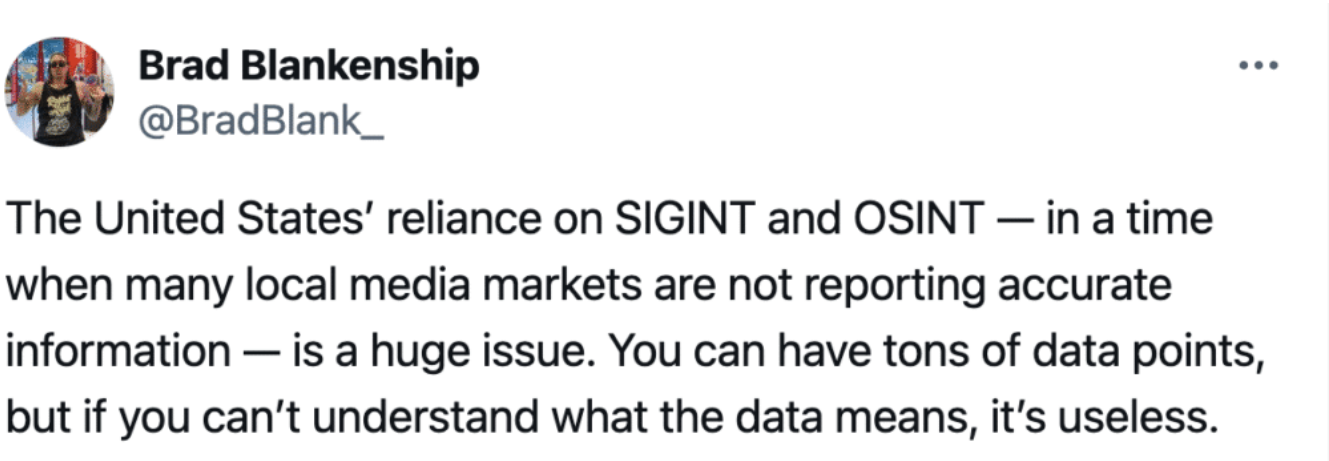
Caratteristica	OSINT (Open Source Intelligence)	SIGINT (Signals Intelligence)
Accessibilità	Aperto e disponibile a ricercatori, ONG, cittadini, media.	Tradizionalmente riservato a governi e militari, ma sempre più disponibile tramite soluzioni commerciali.
Costi	Relativamente bassi: accesso a dati social, piattaforme open, satelliti commerciali (Planet, Maxar).	Elevati: antenne dedicate, satelliti, infrastrutture di intercettazione. Alcuni sistemi COTS hanno abbattuto i costi.
Velocità	Immediata: i social e i droni civili permettono verifiche in tempo reale.	Dipende da capacità tecniche e autorizzazioni. I dati sono spesso classificati.
Rischi	Manipolazione di fonti, fake	Violazioni legali/etiche, cyber

Caratteristica	OSINT (Open Source Intelligence)	SIGINT (Signals Intelligence)
	news, overload informativo, bias linguistici.	intrusion, rischi diplomatici.
Opportunità	Documentazione indipendente (guerre, disastri, traffici illeciti). Supporto a giornalismo investigativo e giustizia internazionale.	Tracciamento di reti militari, traffico marittimo/aereo sospetto, attività clandestine.
Valore aggiunto	Democratizzazione dell'intelligence, trasparenza, verifiche open.	Profondità tecnica e capacità di intercettare segnali non pubblici.

3 casi OSINT replicabili da un analista indipendente

1. Geolocalizzare un video di conflitto • Strumenti: Google Earth Pro, Mapillary, Sentinel Hub.• Processo: analisi dei dettagli (cartelli stradali, ombre, architettura) → confronto con mappe satellitari → verifica di coordinate.• Applicazione: confermare la provenienza di un filmato di guerra o di proteste civili.
2. Tracciare una nave sospetta nel Mediterraneo Strumenti: MarineTraffic (AIS), VesselFinder, OSINT Combine tools.
3. Processo: seguire i movimenti di una petroliera con flag di comodo → confrontare con news di embargo → incrociare rotte e attività sospette.
4. Applicazione: documentare triangolazioni di carburante o violazioni di sanzioni.
5. Verificare la presenza di sistemi militari in un'area Strumenti: immagini satellitari commerciali (Planet, Maxar, Copernicus Sentinel).
6. Processo: analisi di immagini a intervalli → rilevamento di pattern (veicoli corazzati, piste d'atterraggio improvvisate).
7. Applicazione: monitoraggio indipendente di buildup militari vicino a confini contesi.

La fragilità dell'informazione locale e la new-normal della raccolta intelligence



Il tweet di Brad Blankenship sottolinea un passaggio epocale: *gli Stati Uniti — e non solo loro — fanno sempre più affidamento su OSINT e SIGINT in un'epoca in cui i media locali non garantiscono più accuratezza e copertura completa*.
È un cambio di paradigma che non riguarda solo le guerre ibride o i teatri di crisi, ma l'intero ecosistema dell'informazione globale.OSINT sul campo: casi pratici

Ucraina: Twitter e Telegram al posto dei giornalisti embedded

Dal 2014 al 2022, fino all'invasione su larga scala, l'analisi di foto e video pubblicati su Telegram**, TikTok e Twitter** è diventata cruciale per mappare movimenti di truppe, identificare armi e verificare attacchi.

Gruppi come **Bellingcat** hanno dimostrato che una foto satellitare gratuita di Maxar o un video girato con uno smartphone potevano confermare la presenza di sistemi missilistici russi ben più rapidamente dei briefing ufficiali della NATO.

Gaza: droni civili e satelliti commerciali

Nel conflitto tra Israele e Hamas, giornalisti e ricercatori indipendenti hanno usato immagini da **Planet Labs** e video di droni civili per documentare bombardamenti, localizzare ospedali colpiti e persino monitorare corridoi umanitari. Questo tipo di OSINT ha spesso anticipato le dichiarazioni ufficiali di governi e ONG.

Myanmar: TikTok come fonte di prova

Dopo il colpo di stato del 2021, la repressione è stata documentata da cittadini attraverso **Facebook Live e TikTok**. Molti video, geolocalizzati con metodi OSINT, sono entrati nei dossier delle Nazioni Unite come **evidenze di violazioni dei diritti umani**, segnalando un ribaltamento: l'open source come fonte giudiziaria.

SIGINT e geopolitica: da monopolio statale a "mercato privato"

Il **Signals Intelligence**, un tempo esclusiva di NSA, GCHQ o Mossad, oggi è "democratizzato". Alcuni casi:

• Sudan, 2023: durante i combattimenti a Khartoum, agenzie private hanno usato radio-scanners commerciali per monitorare le comunicazioni militari. Alcuni dati sono trapelati su canali OSINT, fornendo prove sugli spostamenti dei generali.
• Mar Nero: flotte commerciali di AIS spoofing detection (Automatic Identification System) hanno rivelato manovre sospette di petroliere russe che aggiravano le sanzioni, un compito tradizionalmente riservato a satelliti militari.
• BaltiTech in Lituania ha sviluppato sistemi di intercettazione low-cost per monitorare traffico satellitare LEO. Questi strumenti, accessibili anche a università e centri civili, dimostrano come il SIGINT sia ormai parte di un mercato aperto.

Quando i media sul campo sono deboli o controllati dal potere politico, **l'intelligence open source diventa la principale lente sul reale**.
Un esempio lampante è l'**Etiopia durante la guerra nel Tigray**: mentre i giornalisti indipendenti erano espulsi, OSINT e SIGINT hanno fornito quasi tutte le informazioni sulla crisi umanitaria.
Il problema: senza corrispondenti e fact-checking radicati, l'ecosistema si affida a **fonti digitali**, più rapide ma anche più manipolabili.

OSINT + SIGINT integrati

• All-Source Analysis (ASA): metodologia che integra OSINT, SIGINT, HUMINT e GEOINT per compensare i limiti delle singole fonti.
• AI e NLP (Natural Language Processing): usati per scandagliare milioni di post sui social in tempo reale. Ad esempio, software come Palantir Gotham o Dataminr filtrano segnali da rumore con algoritmi di machine learning.
• COTS Satellites (Commercial Off-The-Shelf): immagini satellitari di alta qualità acquistabili sul mercato (Planet, Maxar, Capella Space) che hanno rivoluzionato la sorveglianza strategica.
• AIS e ADS-B tracking: sistemi civili per monitorare navi e velivoli, oggi sfruttati da analisti OSINT per studiare traffici sospetti (armi, petrolio, contrabbando).

C'è però un paradosso: **più OSINT e SIGINT diventano accessibili, più rischiamo di credere che "tutto sia verificabile"**.
In realtà, ogni dato aperto può essere manipolato, falsificato o decontestualizzato. Senza media locali robusti e senza un ecosistema di verifica multilivello, persino la migliore intelligence open-source rischia di diventare un **miraggio di accuratezza**.

Caratteristica	OSINT (Open Source Intelligence)	SIGINT (Signals Intelligence)
Accessibilità	Aperto e disponibile a ricercatori, ONG, cittadini, media.	Tradizionalmente riservato a governi e militari, ma sempre più disponibile tramite soluzioni commerciali.
Costi	Relativamente bassi: accesso a dati social, piattaforme open, satelliti commerciali (Planet, Maxar).	Elevati: antenne dedicate, satelliti, infrastrutture di intercettazione. Alcuni sistemi COTS hanno abbattuto i costi.
Velocità	Immediata: i social e i droni civili permettono verifiche in tempo reale.	Dipende da capacità tecniche e autorizzazioni. I dati sono spesso classificati.
Rischi	Manipolazione di fonti, fake news, overload informativo, bias linguistici.	Violazioni legali/etiche, cyber intrusion, rischi diplomatici.
Opportunità	Documentazione indipendente (guerre, disastri, traffici illeciti). Supporto a giornalismo investigativo e giustizia internazionale.	Tracciamento di reti militari, traffico marittimo/aereo sospetto, attività clandestine.
Valore aggiunto	Democratizzazione dell'intelligence, trasparenza, verifiche open.	Profondità tecnica e capacità di intercettare segnali non pubblici.

3 casi OSINT replicabili da un analista indipendente

1. Geolocalizzare un video di conflitto • Strumenti: Google Earth Pro, Mapillary, Sentinel Hub.• Processo: analisi dei dettagli (cartelli stradali, ombre, architettura) → confronto con mappe satellitari → verifica di coordinate.• Applicazione: confermare la provenienza di un filmato di guerra o di proteste civili.
2. Tracciare una nave sospetta nel Mediterraneo Strumenti: MarineTraffic (AIS), VesselFinder, OSINT Combine tools.
3. Processo: seguire i movimenti di una petroliera con flag di comodo → confrontare con news di embargo → incrociare rotte e attività sospette.
4. Applicazione: documentare triangolazioni di carburante o violazioni di sanzioni.
5. Verificare la presenza di sistemi militari in un'area Strumenti: immagini satellitari commerciali (Planet, Maxar, Copernicus Sentinel).
6. Processo: analisi di immagini a intervalli → rilevamento di pattern (veicoli corazzati, piste d'atterraggio improvvisate).
7. Applicazione: monitoraggio indipendente di buildup militari vicino a confini contesi.