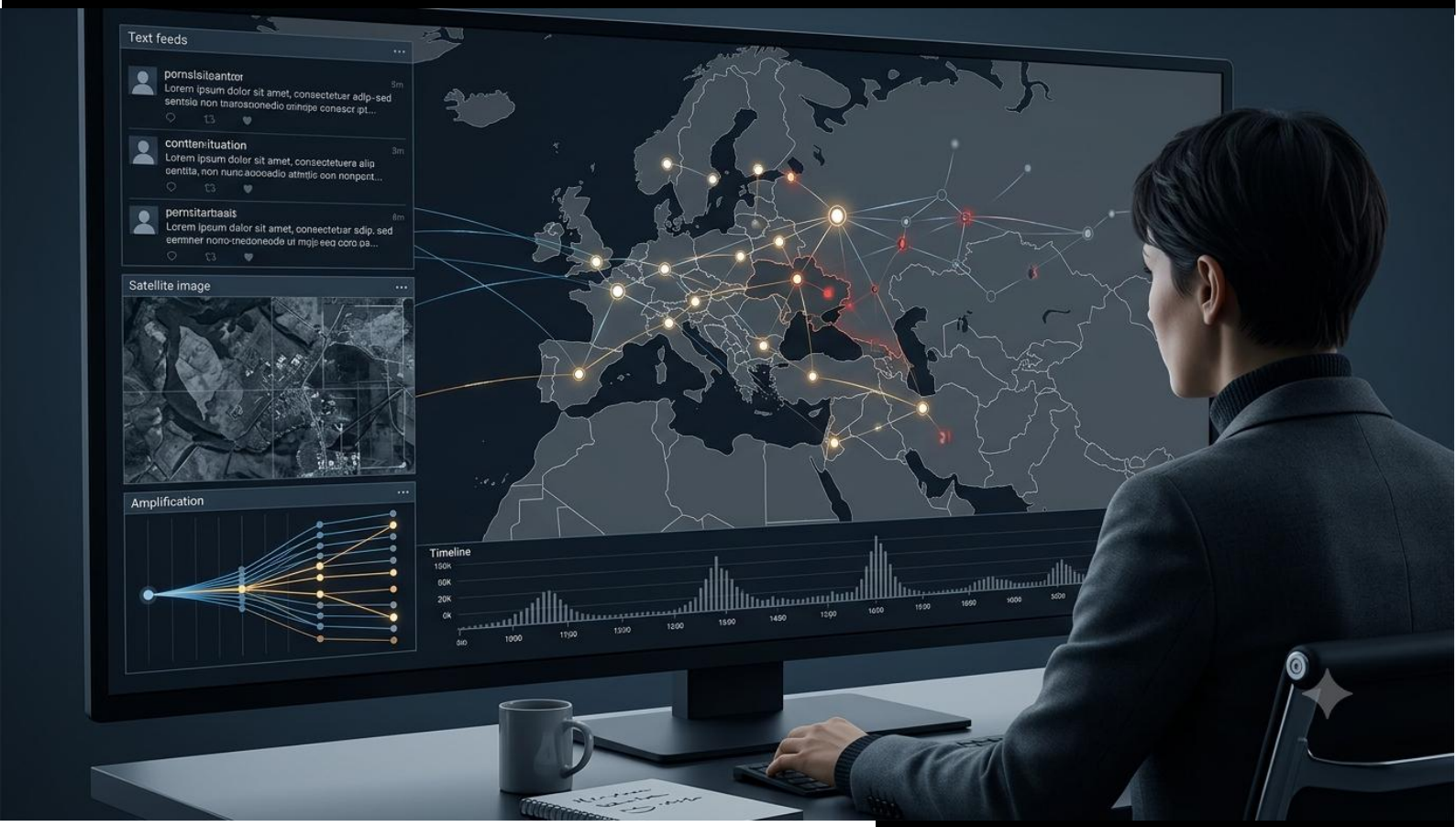
Contro-OSINT
la nuova frontiera dell’inganno



Giovanni Conio

27/06/2026

Contro-OSINT - la nuova frontiera dell'inganno

Le fonti aperte non sono uno spazio neutrale. Nell'ambiente informativo contemporaneo, ciò che è pubblicamente accessibile può essere selezionato, manipolato o costruito per orientare il lavoro degli analisti. La sfida non è più soltanto raccogliere informazioni, ma riconoscere quando l'OSINT diventa parte del "campo di battaglia", dell'inganno.

Come ribadito più volte, negli ultimi anni l'OSINT ha assunto un ruolo crescente nell'analisi dei conflitti, nella sicurezza, nel giornalismo investigativo, nella corporate intelligence e nel monitoraggio delle crisi. Immagini satellitari commerciali, video pubblicati sui social media, tracciamenti navali e aerei, registri pubblici, documenti ufficiali, comunicati, mappe digitali e contenuti generati dagli utenti hanno ampliato in modo significativo la quantità di informazioni disponibili.

Questa trasformazione ha prodotto un effetto rilevante: una parte del lavoro intelligence, un tempo riservata ad apparati specializzati, oggi può essere alimentata anche da dati pubblici, verificabili e condivisibili. Ma questa (apparente) apertura contiene un rischio.

Se un numero crescente di analisti, osservatori e decisori utilizza fonti aperte per comprendere eventi complessi, allora quelle stesse fonti diventano un bersaglio. O, più precisamente, diventano un ambiente nel quale un attore ostile può tentare di introdurre segnali falsi, manipolare il contesto, saturare il campo informativo, orientare l'attenzione o indurre conclusioni errate.

È qui che emerge il concetto di **contro-OSINT**.

> La contro-OSINT può essere intesa come l'insieme delle pratiche con cui un attore cerca di negare, degradare, manipolare o sfruttare l'intelligence da fonti aperte. Non si limita a nascondere informazioni. Può anche produrre informazioni apparentemente utili, ma costruite per ingannare chi osserva.

Un recente paper dell'**Observer Research Foundation** ha descritto la counter-OSINT come una dimensione crescente del panorama di minaccia contemporaneo, legata alla competizione informativa, alla sicurezza nazionale e alla necessità per gli apparati di intelligence di adattarsi a un ambiente in cui la distinzione tra segnale e rumore è sempre più problematica.

Il punto centrale è questo: l'OSINT non è automaticamente affidabile solo perché è pubblica.

La fine dell'innocenza delle fonti aperte

Per lungo tempo, una parte della "cultura" OSINT ha enfatizzato il valore della trasparenza: fonti aperte, dati verificabili, analisi replicabili, collaborazione distribuita. Questo valore resta importante. L'OSINT ha dimostrato di poter contribuire alla verifica di eventi complessi, alla documentazione di conflitti, all'individuazione di incongruenze nelle narrative ufficiali e alla costruzione di assessment fondati su evidenze pubbliche.

Tuttavia, la crescente centralità delle fonti aperte ha modificato il comportamento degli attori strategici.

Quando un attore sa di essere osservato, può adattarsi all'osservazione.

Può occultare. Può simulare. Può diffondere materiale selezionato. Può alimentare tracce ambigue. Può creare account apparentemente indipendenti. Può rilasciare immagini, video o dati in tempi e modalità funzionali a una narrativa. Può sfruttare la velocità dei social media per far circolare una versione prima che vi sia tempo per verificarla. Può produrre rumore sufficiente a rendere costosa la separazione, la cernita, tra informazione rilevante e informazione ingannevole.

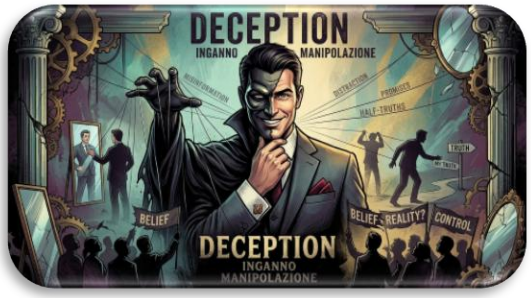
In questo senso, la fonte aperta diventa parte del terreno operativo.

Non è più soltanto ciò che l'analista osserva. È anche ciò che l'avversario può usare per farsi osservare nel modo desiderato.

Dalla disinformazione alla deception analitica

Ritengo sia importante distinguere la contro-OSINT dalla semplice disinformazione.

La disinformazione punta spesso a influenzare un pubblico ampio: opinione pubblica, media, comunità politiche, gruppi sociali, elettorati o mercati.



La contro-OSINT può essere più specifica: mira a influenzare chi analizza.

Il suo obiettivo non è necessariamente convincere tutti. Può essere sufficiente orientare il lavoro di una comunità di osservatori, produrre incertezza, rallentare la verifica, generare ipotesi concorrenti deboli ma rumorose, indurre un errore di attribuzione o far apparire un evento più certo, più incerto, più grave o più irrilevante di quanto sia.

La deception analitica non lavora solo sul falso. Lavora anche sull'ambiguità. Come?

- ✓ Un contenuto può essere autentico ma decontestualizzato.
- ✓ Una fonte può essere reale ma orientata.
- ✓ Un dato può essere corretto ma incompleto.
- ✓ Una sequenza temporale può essere vera ma selezionata.
- ✓ Un'immagine può essere geolocalizzata correttamente ma interpretata in modo fuorviante.
- ✓ Una narrativa può contenere fatti verificabili e, proprio per questo, risultare più persuasiva.

Per l'analista, il problema non è soltanto chiedersi se un'informazione sia vera o falsa. Il problema è chiedersi quale funzione svolga dentro un ambiente informativo competitivo.

Le quattro domande decisive

Per affrontare la contro-OSINT, l'analista deve aggiungere alla normale valutazione della fonte alcune domande di secondo livello.

La prima domanda è: **chi produce il dato?**

Non sempre è possibile rispondere con certezza, ma è necessario distinguere tra fonte primaria, fonte secondaria, amplificatore, aggregatore, account anonimo, canale istituzionale, media locale, soggetto privato o attore con possibili interessi operativi.

La seconda domanda è: **perché il dato emerge proprio ora?**

Il timing è spesso parte dell'informazione. Un video pubblicato in una fase critica, un documento diffuso alla vigilia di una decisione, una fuga di notizie durante un negoziato o una sequenza di post coordinati possono avere una funzione che va oltre il contenuto apparente.

La terza domanda è: **a chi è destinato il dato?**

Non tutte le informazioni pubbliche parlano allo stesso pubblico. Alcune mirano ai media. Altre agli analisti. Altre ai decisori. Altre ancora agli avversari, agli alleati, ai mercati o a comunità specifiche.

La quarta domanda è: **quale comportamento vuole produrre?**

Questa è la domanda più importante. Una traccia informativa può cercare di provocare allarme, rassicurazione, confusione, ritardo, attribuzione errata, sovrastima, sottostima o polarizzazione del giudizio.

In sintesi: Queste domande spostano l'OSINT da semplice raccolta a vera analisi intelligence.

Gli indicatori di contro-OSINT

Non esiste un indicatore unico di deception. Esistono però dei segnali che dovrebbero aumentare la cautela analitica.

Tra questi:

- ✓ comparsa simultanea di contenuti simili su canali diversi;
- ✓ account apparentemente indipendenti che rilanciano la stessa narrativa;
- ✓ contenuti tecnicamente verificabili ma privi di contesto;
- ✓ immagini o video pubblicati con ritardo non spiegato;
- ✓ metadati assenti, incoerenti o alterati;
- ✓ geolocalizzazioni corrette ma interpretazioni forzate;
- ✓ fonti anonime che si presentano come insider;
- ✓ eccessiva coerenza narrativa tra fonti formalmente diverse;
- ✓ dati che sembrano confermare in modo troppo perfetto una sola ipotesi;
- ✓ assenza di elementi disconfermanti in un quadro apparentemente complesso;
- ✓ forte pressione temporale alla condivisione o alla conclusione;
- ✓ uso di linguaggio emotivo per accompagnare materiale tecnico;
- ✓ improvvisa centralità di un tema prima marginale.

Questi elementi non provano automaticamente una manipolazione. Ma indicano che l'analista deve rallentare il giudizio, aumentare la verifica e formulare ipotesi alternative.

Metodo prima dello strumento

Il tema della contro-OSINT si collega direttamente ai contenuti del mio ***Manuale per l'analisi intelligence***: l'analisi non è accumulo di informazioni, ma disciplina del ragionamento.

In particolare, il Manuale offre almeno cinque agganci metodologici fondamentali:

1. Valutazione delle fonti

La contro-OSINT rende insufficiente una valutazione superficiale della fonte. Non basta chiedersi se una fonte sia nota, accessibile o apparentemente credibile. Occorre valutare attendibilità, motivazione, prossimità all'evento, catena di diffusione, possibili interessi e coerenza con altre evidenze.

> Nel contesto OSINT, la fonte non è solo un contenitore di informazione. È parte del problema analitico.

2. Distinzione tra dato, informazione e intelligence

Una delle distinzioni centrali nel Manuale è quella tra dato grezzo, informazione organizzata e intelligence come prodotto valutativo utile al decisore.

La contro-OSINT sfrutta proprio la confusione tra questi livelli.

Un video non è ancora intelligence. Un'immagine geolocalizzata non è ancora spiegazione.

Un documento diffuso online non è ancora assessment. Un trend social non è ancora indicatore strategico.

> Il passaggio dal dato alla valutazione richiede metodo, corroborazione e controllo delle ipotesi.

3. Bias cognitivi

La deception funziona perché sfrutta vulnerabilità cognitive.

La contro-OSINT può attivare confirmation bias, ancoraggio, disponibilità, overconfidence, effetto gregge, urgenza decisionale e attrazione per la narrativa più coerente.

> Un contenuto che conferma ciò che l'analista si aspettava di trovare è particolarmente pericoloso. Non perché sia necessariamente falso, ma perché viene verificato con minore severità.

Nel Manuale insisto molto sulla necessità di riconoscere i bias non come difetti individuali occasionali, ma come condizioni strutturali del ragionamento sotto incertezza. La contro-OSINT li sfrutta deliberatamente.

4. Analysis of Competing Hypotheses (ACH)

L'ACH è uno strumento particolarmente utile contro la deception.

In presenza di un flusso OSINT ambiguo, l'analista dovrebbe evitare di chiedersi soltanto: "questa evidenza conferma la mia ipotesi?". Dovrebbe chiedersi: "quale ipotesi tende a escludere questa evidenza?".

Quando una serie di elementi conferma troppo facilmente una sola spiegazione, l'ACH aiuta a introdurre disciplina: confronto tra ipotesi, evidenze diagnostiche, elementi disconfermanti, ipotesi alternative.

Nel caso della contro-OSINT, una delle ipotesi da inserire esplicitamente nella matrice dovrebbe essere proprio: "il flusso informativo è stato (volutamente) manipolato o selezionato per orientare l'analisi".

5. Indicatori e allarme (I&W)

La contro-OSINT richiede anche un "sistema di indicatori". Non basta reagire caso per caso. Occorre monitorare segnali ricorrenti di possibile manipolazione informativa.

Gli indicatori possono riguardare anomalie nella diffusione, incoerenze temporali, ricorrenze narrative, amplificazione coordinata, improvvise convergenze tra fonti, assenza di corroborazione indipendente, pressione alla rapidità e selettività del materiale diffuso.

In questo modo, l'analista non si limita a "scoprire" la deception dopo il danno. Costruisce un sistema di allerta metodologico.

Una griglia pratica per l'analista

Per integrare la contro-OSINT nel processo analitico, può essere utile adottare una griglia in tre livelli.

Livello 1 Verifica del contenuto	**Livello 2** Valutazione della fonte	**Livello 3** Funzione informativa
Il contenuto è autentico? È databile? È geo localizzabile? È coerente con il contesto? È stato modificato? È completo o selettivo?	Chi lo pubblica? La fonte è primaria o derivata? Ha precedenti di affidabilità? Ha interessi evidenti? È collegata ad altri canali? È parte di una rete di amplificazione?	Perché emerge ora? Quale narrativa sostiene? Quale ipotesi rafforza? Quale ipotesi indebolisce? Quale pubblico vuole raggiungere? Quale comportamento può indurre?

Il terzo livello è quello più spesso trascurato. Ed è proprio lì che la contro-OSINT tende a operare.

Implicazioni per la cultura intelligence

La crescita della contro-OSINT impone un cambio di prospettiva.

L'OSINT resta una risorsa fondamentale. Ma deve essere trattata come un "ambiente competitivo", non come un deposito neutrale di dati.

Questo significa che la formazione degli analisti deve includere non solo strumenti di raccolta, ma anche:

- ✓ deception analysis;
- ✓ source criticism (valutazione delle fonti/informazioni);
- ✓ information behaviour analysis (analisi del comportamento informativo);
- ✓ riconoscimento dei bias e utilizzo di tecniche di analisi strutturata (ad es. ACH);
- ✓ indicatori di manipolazione;
- ✓ gestione del livello di confidenza;
- ✓ comunicazione dei caveat al decisore.

> La vera competenza OSINT non consiste nel trovare rapidamente informazioni pubbliche. Consiste nel capire quando quelle informazioni sono utili, quando sono incomplete, quando sono manipolate e quando stanno cercando di manipolare chi le analizza.

Conclusione

La contro-OSINT segna una nuova fase della competizione informativa. Le fonti aperte non scompaiono. Anzi, diventano sempre più centrali. Ma proprio per questo diventano anche più vulnerabili alla deception.

Per l'analista, la sfida non è abbandonare l'OSINT, ma professionalizzarla. Non basta cercare. Occorre verificare. Non basta raccogliere. Occorre interpretare. Non basta confermare. Occorre mettere alla prova le ipotesi.

Nel contesto contemporaneo, la domanda decisiva non è più soltanto: cosa posso sapere attraverso le fonti aperte?

La domanda diventa: chi vuole che io sappia questo, in questo momento, e con quali conseguenze sul mio giudizio?

È questa domanda che trasforma l'OSINT da pratica di raccolta a disciplina intelligence.

Ed è questa domanda che deve entrare stabilmente nella formazione degli analisti.

Checklist contro-OSINT per analisti

1. Il contenuto è autentico, databile e contestualizzabile?
2. La fonte è primaria, secondaria o amplificatrice?
3. Esistono conferme indipendenti?
4. Il contenuto emerge in un momento strategicamente rilevante?
5. La narrativa appare troppo coerente o troppo conveniente?
6. Ci sono elementi disconfermanti?
7. Quale ipotesi rafforza questa informazione?
8. Quale ipotesi alternativa potrebbe spiegare la stessa evidenza?
9. Il flusso informativo mostra segnali di coordinamento?
10. Quale comportamento potrebbe voler indurre nel decisore o nell'analista?