Investigazioni a distanza. Trovare persone che non vogliono essere trovate

Maria Cattini | 02/05/2025 | Open source intelligence

Come funzionano le investigazioni a distanza sui crimini di guerra

Il lato invisibile dei conflitti: quando il giornalismo non può essere sul campo

In certi angoli del mondo, documentare la verità è un'impresa pericolosa, a volte impossibile. Guerre, repressioni, censura. Quando non è possibile essere fisicamente presenti, entra in gioco un nuovo approccio: **le investigazioni a distanza**.

Non parliamo di semplici ricerche online, ma di un **metodo rigoroso e strutturato** che permette di identificare persone, eventi e responsabilità anche in **assenza di accesso diretto al luogo dei fatti**.

> "*L'obiettivo non è solo trovare informazioni. È costruire un caso per l'accountability.*"

Da un dettaglio minuscolo parte tutto

Un nome, una foto, una voce registrata.

Può bastare per dare il via a un'indagine. Ma serve metodo, rigore e una buona dose di creatività.

Le prime domande da porsi:

• Chi può essere in pericolo (testimoni, colleghi, fonti)?
• Qual è la strategia per raccogliere prove in modo sicuro?
• Come documentare e archiviare tutto senza lasciare tracce?

Il team deve essere organizzato, con **ruoli chiari**, **VPN attive**, **dispositivi separati** per la ricerca. E soprattutto: ogni passo va pensato in funzione della **protezione di chi collabora all'indagine**.

Mentalità investigativa prima del toolset

Esistono centinaia di strumenti digitali, ma la differenza la fa l'approccio.

Chi investiga a distanza deve avere:

• Intuizione e problem solving
• Conoscenza del contesto geopolitico
• Familiarità con le piattaforme usate localmente
• Capacità di leggere tra le righe

□□ Le tecniche OSINT più usate includono:

• Ricerche avanzate su Google (con operatori booleani)
• Analisi dei social più usati nella regione target
• Ricostruzione dei contatti a partire da indizi indiretti

□□La chiave? Mappare le reti

Chi non vuole essere trovato... **lascia tracce indirette**. Familiari, colleghi, gruppi WhatsApp, follower. Mappare questa rete può:

• Svelare relazioni e movimenti
• Individuare coordinatori e comandanti
• Ricostruire catene di comando in contesti militari

□□ Capire la struttura di un gruppo (acronimi, gradi, simboli) può fare la differenza tra un nome isolato e **un'intera rete di responsabilità**.

⚖ Etica prima di tutto: "Do no harm"

Seguire una regola ferrea: **non fare danni**.

Significa:

• Non agire sotto copertura
• Non mettere a rischio chi condivide informazioni
• Evitare strumenti non trasparenti o rischiosi (es. riconoscimento facciale)

□□□□ Ogni dato raccolto deve essere valutato in base a:

• Chi lo ha generato
• Come viene salvato
• Chi potrebbe accedervi (anche in futuro)

Spesso, la scelta più responsabile è **non pubblicare tutto**. La sicurezza delle persone viene prima della notizia.

□□Verificare prima di accusare

Ogni informazione raccolta va verificata.

I 3 pilastri della verifica OSINT:

1. Geolocalizzazione – Dove è avvenuto l'evento
2. Cronolocalizzazione – Quando è successo
3. Contesto – Chi, come, perché

□□ Video e immagini possono essere confrontati con mappe satellitari, metadati, orari del tramonto...

Tutto serve a dimostrare **che un fatto è avvenuto davvero**.

Analisi specialistiche per casi solidi

Dopo la verifica, arriva l’analisi.

Spesso intervengono esperti di:

• Armi e munizionamenti
• Analisi forense digitale
• Dinamiche di propaganda e comunicazione

Le tecniche includono:

• Analisi spaziale (mappe interattive)
• Analisi video e frame-by-frame
• Mappatura di account e network

Lo scopo? **Costruire un dossier credibile**. Non per accusare, ma per documentare. E portare il caso davanti a chi ha gli strumenti per decidere.

Il diritto di replica non è un optional

Un punto etico fondamentale: **anche il presunto responsabile ha diritto di rispondere**.

Offrire il “diritto di replica”:

• Dà più forza al dossier
• Evita strumentalizzazioni
• Dimostra professionalità e imparzialità

L’indagine non è un processo. È un **racconto verificato di fatti**, aperto al confronto.

Archiviare è salvare la memoria

I contenuti online **possono sparire in pochi minuti**.

Per questo, chi indaga deve:

• Salvare l’URL originale
• Fare screenshot
• Scaricare contenuti digitali
• Estrarre codice sorgente della pagina

Ogni passaggio va **documentato e salvato in modo sicuro**, anche per eventuali usi legali futuri.

E non dimenticare di proteggere te stesso

Indagare su crimini di guerra significa **esporsi a materiale traumatico**. Anche a distanza.

>
> "*Parlate con i vostri team. Supportatevi. E se serve, chiedete aiuto.*"

La cura psicologica non è un lusso. È parte del lavoro.

In sintesi: un lavoro invisibile che fa la differenza

“Trovare persone che non vogliono essere trovate” è un’arte che mescola investigazione, rigore tecnico, sensibilità etica e resilienza.

Ma dietro ogni profilo identificato, ogni rete mappata, ogni video verificato… c’è **la possibilità concreta di ottenere giustizia**.

Come funzionano le investigazioni a distanza sui crimini di guerra

Il lato invisibile dei conflitti: quando il giornalismo non può essere sul campo

In certi angoli del mondo, documentare la verità è un'impresa pericolosa, a volte impossibile. Guerre, repressioni, censura. Quando non è possibile essere fisicamente presenti, entra in gioco un nuovo approccio: **le investigazioni a distanza**.

Non parliamo di semplici ricerche online, ma di un **metodo rigoroso e strutturato** che permette di identificare persone, eventi e responsabilità anche in **assenza di accesso diretto al luogo dei fatti**.

"*L’obiettivo non è solo trovare informazioni. È costruire un caso per l’accountability.*"

Da un dettaglio minuscolo parte tutto

Un nome, una foto, una voce registrata.

Può bastare per dare il via a un’indagine. Ma serve metodo, rigore e una buona dose di creatività.

Le prime domande da porsi:

• Chi può essere in pericolo (testimoni, colleghi, fonti)?
• Qual è la strategia per raccogliere prove in modo sicuro?
• Come documentare e archiviare tutto senza lasciare tracce?

Il team deve essere organizzato, con **ruoli chiari**, **VPN attive**, **dispositivi separati** per la ricerca. E soprattutto: ogni passo va pensato in funzione della **protezione di chi collabora all’indagine**.

Mentalità investigativa prima del toolset

Esistono centinaia di strumenti digitali, ma la differenza la fa l'approccio.

Chi investiga a distanza deve avere:

• Intuizione e problem solving
• Conoscenza del contesto geopolitico
• Familiarità con le piattaforme usate localmente
• Capacità di leggere tra le righe

Le tecniche OSINT più usate includono:

• Ricerche avanzate su Google (con operatori booleani)
• Analisi dei social più usati nella regione target
• Ricostruzione dei contatti a partire da indizi indiretti

La chiave? Mappare le reti

Chi non vuole essere trovato... **lascia tracce indirette**. Familiari, colleghi, gruppi WhatsApp, follower. Mappare questa rete può:

• Svelare relazioni e movimenti
• Individuare coordinatori e comandanti
• Ricostruire catene di comando in contesti militari

Capire la struttura di un gruppo (acronimi, gradi, simboli) può fare la differenza tra un nome isolato e **un'intera rete di responsabilità**.

⚖ Etica prima di tutto: "Do no harm"

Seguire una regola ferrea: **non fare danni**.

Significa:

• Non agire sotto copertura
• Non mettere a rischio chi condivide informazioni
• Evitare strumenti non trasparenti o rischiosi (es. riconoscimento facciale)

Ogni dato raccolto deve essere valutato in base a:

• Chi lo ha generato
• Come viene salvato
• Chi potrebbe accedervi (anche in futuro)

Spesso, la scelta più responsabile è **non pubblicare tutto**. La sicurezza delle persone viene prima della notizia.

Verificare prima di accusare

Ogni informazione raccolta va verificata.

I 3 pilastri della verifica OSINT:

1. Geolocalizzazione – Dove è avvenuto l'evento
2. Cronolocalizzazione – Quando è successo
3. Contesto – Chi, come, perché

Video e immagini possono essere confrontati con mappe satellitari, metadati, orari del tramonto... Tutto serve a dimostrare **che un fatto è avvenuto davvero**.

Analisi specialistiche per casi solidi

Dopo la verifica, arriva l'analisi.

Spesso intervengono esperti di:

• Armi e munizionamenti
• Analisi forense digitale
• Dinamiche di propaganda e comunicazione

□□ Le tecniche includono:

• Analisi spaziale (mappe interattive)
• Analisi video e frame-by-frame
• Mappatura di account e network

Lo scopo? **Costruire un dossier credibile**. Non per accusare, ma per documentare. E portare il caso davanti a chi ha gli strumenti per decidere.

□□Il diritto di replica non è un optional

Un punto etico fondamentale: **anche il presunto responsabile ha diritto di rispondere**.

Offrire il "diritto di replica":

• Dà più forza al dossier
• Evita strumentalizzazioni
• Dimostra professionalità e imparzialità

□□ L'indagine non è un processo. È u**racconto verificato di fatti**, aperto al confronto.

□□Archiviare è salvare la memoria

I contenuti online **possono sparire in pochi minuti**.

Per questo, chi indaga deve:

• Salvare l'URL originale
• Fare screenshot
• Scaricare contenuti digitali
• Estrarre codice sorgente della pagina

□□ Ogni passaggio va**documentato e salvato in modo sicuro**, anche per eventuali usi legali futuri.

□□E non dimenticare di proteggere te stesso

Indagare su crimini di guerra significa **esporsi a materiale traumatico**. Anche a distanza.

> □□
> "*Parlate con i vostri team. Supportatevi. E se serve, chiedete aiuto.*"

La cura psicologica non è un lusso. È parte del lavoro.

□□In sintesi: un lavoro invisibile che fa la differenza

"Trovare persone che non vogliono essere trovate" è un'arte che mescola investigazione, rigore tecnico, sensibilità etica e resilienza.

Ma dietro ogni profilo identificato, ogni rete mappata, ogni video verificato… c’è **la possibilità concreta di ottenere giustizia**.