

Prima di condividere un video di guerra: cinque controlli OSINT da fare

Maria Cattini | 09/07/2026 | Open source intelligence

Un video di guerra arriva quasi sempre con una frase già pronta.

È successo adesso.

Oppure:

Questo mostra l'attacco di ieri.

Oppure ancora:

Guardate cosa hanno fatto.

Il problema è che il video, da solo, non dice tutto questo.

Un video mostra immagini, suoni, movimenti, oggetti, luoghi, persone, mezzi, esplosioni, fumo, edifici, strade, cartelli, uniformi, luci. Ma la frase che lo accompagna aggiunge quasi sempre qualcosa: un luogo, una data, un responsabile, una causa, una conseguenza, una certezza.

Nel lavoro OSINT bisogna separare queste due cose.

Da una parte c'è il contenuto visivo.

Dall'altra c'è il claim, cioè l'affermazione che qualcuno sta facendo su quel contenuto.

Prima di condividere un video di guerra, la domanda non dovrebbe essere:

Sembra vero?

La domanda utile è:

Che cosa posso verificare davvero?

Questa guida non serve a trasformare chi legge in investigatore professionista. Serve a ridurre un errore molto comune: rilanciare un video solo perché è forte, emotivo, urgente o coerente con ciò

che già pensiamo.

1. Trova la fonte più vicina all'originale

Il primo controllo è la provenienza.

Non chiederti subito se il video è vero. Chiediti prima da dove arriva.

Un video può passare da:

- una persona che lo ha registrato;
- un canale Telegram locale;
- un account X che aggrega contenuti;
- una pagina Facebook;
- un gruppo WhatsApp;
- una testata giornalistica;
- un profilo OSINT;
- un account anonimo;
- un repost senza contesto;
- uno screenshot trasformato di nuovo in video.

Ogni passaggio può aggiungere o perdere informazioni.

Il video originale potrebbe avere una didascalia diversa. Potrebbe essere stato tagliato. Potrebbe essere stato pubblicato ore o anni prima. Potrebbe riferirsi a un altro Paese. Potrebbe essere stato usato correttamente dalla prima fonte e male da chi lo rilancia.

Il controllo minimo è questo:

1. cerca se il post che stai guardando indica una fonte;
2. apri la fonte indicata, non fermarti al repost;
3. controlla se quella fonte indica a sua volta un'altra origine;
4. cerca una versione precedente del video usando parole chiave, frame e reverse search;
5. annota dove ti fermi.

Se non riesci a risalire a una fonte più vicina all'originale, non significa automaticamente che il video sia falso. Significa che la catena è debole.

E una catena debole non va presentata come certezza.

2. Controlla se il video è vecchio

Molti video di guerra non sono falsi nel senso tecnico del termine.

Sono veri, ma fuori contesto.

Un bombardamento reale può essere attribuito a un altro fronte. Un'esplosione di anni prima può essere presentata come avvenuta ieri. Un video girato durante un'esercitazione può essere rilanciato come combattimento. Una scena di un conflitto può essere usata per commentarne un altro.

Per questo il secondo controllo riguarda il tempo.

Ci sono alcune domande semplici:

- qual è la prima data in cui trovo questo video online?
- la data del post coincide con la data dell'evento dichiarato?
- ci sono versioni precedenti con un'altra descrizione?

- qualcuno lo ha già verificato o smentito?
- il meteo, la luce, gli abiti, la vegetazione o il contesto sono coerenti con la data indicata?

La reverse image search può aiutare, ma non basta.

Con un video conviene estrarre alcuni fotogrammi chiari: un'inquadratura con edifici, strade, mezzi, cartelli, fumo, montagne, insegne o elementi distintivi. Poi si cercano quei fotogrammi con strumenti diversi: Google Lens, Yandex, Bing Visual Search o altri motori disponibili.

Il punto non è trovare "la risposta" in un solo strumento.

Il punto è capire se quel materiale era già apparso altrove.

Se trovi lo stesso video pubblicato due anni prima, il problema è chiuso: il video non può documentare l'evento di oggi. Se trovi immagini simili ma non identiche, devi essere più prudente: potrebbero essere riprese dello stesso luogo in momenti diversi, o contenuti diversi confusi tra loro.

3. Verifica il luogo, non solo la didascalia

La geolocalizzazione è uno dei passaggi più importanti e più fraintesi.

Geolocalizzare non significa indovinare un Paese guardando una bandiera, una lingua o un'uniforme. Significa trovare elementi visivi che collegano il video a un luogo verificabile.

Possono aiutare:

- cartelli stradali;
- insegne commerciali;
- forma degli edifici;
- incroci;
- ponti;
- montagne;
- coste;
- minareti, chiese, monumenti;
- linee elettriche;
- disposizione delle strade;
- fermate, binari, rotatorie;
- segni su veicoli o mezzi pubblici;
- profili delle colline;
- ombre e orientamento della luce.

Una sola corrispondenza raramente basta.

Un cartello può essere generico. Un edificio può assomigliare a molti altri. Una strada può essere stata ripresa da un'angolazione difficile. Una scritta può indicare lingua o area, ma non prova da sola il punto esatto.

Il controllo migliore combina più elementi.

Per esempio:

- il cartello indica una città;
- la curva della strada coincide con la mappa;
- un edificio alto ha la stessa forma;
- una montagna sullo sfondo ha lo stesso profilo;
- la direzione del fumo o della luce non contraddice l'inquadratura;
- altri post locali parlano dello stesso evento nella stessa area.

In quel caso puoi dire qualcosa di più solido:

Il luogo è compatibile con questa area.

Oppure, se la corrispondenza è forte:

Il video sembra essere stato girato in questo punto.

Ma evita frasi più forti di ciò che hai verificato.

Non scrivere "confermato" se hai solo una somiglianza.

4. Ricostruisci la sequenza temporale

Anche quando un video è autentico e il luogo è corretto, resta una domanda:

Quando è stato girato?

La data di pubblicazione non è la data di registrazione.

Un video può essere caricato ore dopo. Può essere stato ricevuto da un'altra persona. Può essere stato salvato, tagliato, compresso, rilanciato. Può arrivare da un archivio o da un gruppo chiuso.

Per questo serve una piccola timeline.

Non deve essere complicata. Può bastare una tabella:

Ora / data	Fonte	Che cosa mostra o afferma	Livello di certezza
08:13	primo post trovato	video senza luogo chiaro	basso
08:25	canale locale	afferma che è in città X	medio
08:40	testata locale	segnala esplosione nella stessa zona	medio
09:10	autorità / comunicato	conferma evento, ma non il video	medio

Questa tabella evita un errore molto comune: mescolare prove diverse come se confermassero tutte la stessa cosa.

Un comunicato può confermare che c'è stato un attacco in una città. Non conferma automaticamente che quel video mostri quell'attacco.

Un post locale può confermare che molte persone hanno sentito esplosioni. Non conferma automaticamente chi abbia colpito.

Una mappa può confermare che il luogo esiste. Non conferma la data.

Nel lavoro OSINT ogni elemento sostiene solo una parte della frase.

Il punto è non chiedere a una prova più di quanto possa dare.

5. Scrivi una conclusione stretta

Il quinto controllo riguarda il modo in cui condividi.

Anche dopo aver verificato fonte, data, luogo e contesto, potresti non avere abbastanza elementi per dire tutto.

Allora la conclusione deve essere stretta.

Esempi di conclusioni prudenti:

Il video risulta già online prima dell'evento indicato, quindi non può riferirsi all'attacco di oggi.

Il luogo sembra compatibile con l'area indicata, ma la data di registrazione non è verificata.

Il video mostra un'esplosione, ma non consente da solo di stabilire chi l'abbia causata.

La fonte originale non è stata identificata: il contenuto va trattato come non verificato.

Queste frasi sono meno spettacolari di "confermato".

Ma sono più corrette.

In guerra, la velocità è parte del problema. La propaganda, la confusione, la paura, il desiderio di conferma e l'orrore delle immagini spingono tutti nella stessa direzione: condividere prima di capire.

Il metodo OSINT serve a fare il contrario.

Rallentare abbastanza da non trasformare un segnale in prova.

Errori comuni da evitare

Credere che un account famoso basti

Un account molto seguito può essere utile per scoprire un video, ma non sostituisce la verifica. Anche account competenti possono rilanciare materiale incompleto, non contestualizzato o corretto dopo alcune ore.

Confondere il video con la didascalia

Il video può essere reale e la didascalia falsa. Oppure il video può mostrare un evento reale, ma in un altro luogo o in un altro momento.

Usare un solo fotogramma

Un frame può essere utile, ma può anche ingannare. Meglio estrarre più fotogrammi: uno con il

luogo, uno con dettagli, uno con oggetti o mezzi, uno con eventuali insegne.

Fidarsi solo dei metadati

Molti video pubblicati sui social perdono metadati. Altri possono essere compressi, scaricati e ricaricati. Se ci sono metadati, sono un indizio da valutare, non una prova totale.

Cercare solo la conferma

Se vuoi dimostrare a tutti i costi che il video è vero, troverai segnali che sembrano confermarlo. Il controllo migliore cerca anche l'ipotesi opposta: dove potrebbe essere stato girato prima? chi lo ha già pubblicato? quali elementi non tornano?

Checklist rapida prima di condividere

Prima di condividere un video di guerra, chiediti:

1. Ho trovato la fonte più vicina all'originale?
2. Ho controllato se il video era già online prima?
3. Ho verificato il luogo con più di un elemento visivo?
4. Ho separato data di pubblicazione e data di registrazione?
5. Ho distinto ciò che il video mostra da ciò che la didascalia afferma?
6. Ho cercato fonti indipendenti sullo stesso evento?
7. Ho scritto una conclusione prudente?
8. Ho evitato di indicare responsabili se il video non lo dimostra?
9. Ho salvato link, screenshot, data e ora dei controlli?
10. Se non ho verificato abbastanza, ho evitato di rilanciare come certezza?

La regola finale

Un video di guerra può essere una prova importante.

Ma non diventa prova solo perché è drammatico.

Diventa utile quando si può ricostruire una catena minima: fonte, data, luogo, contesto, limiti.

Se manca un pezzo, non bisogna inventarlo.

Bisogna dirlo.

Nel dubbio, la formula migliore è spesso la più semplice:

Video non ancora verificato.

Non è una sconfitta.

È una forma di responsabilità.

Un video di guerra arriva quasi sempre con una frase già pronta.

È successo adesso.

Oppure:

Questo mostra l'attacco di ieri.

Oppure ancora:

Guardate cosa hanno fatto.

Il problema è che il video, da solo, non dice tutto questo.

Un video mostra immagini, suoni, movimenti, oggetti, luoghi, persone, mezzi, esplosioni, fumo, edifici, strade, cartelli, uniformi, luci. Ma la frase che lo accompagna aggiunge quasi sempre qualcosa: un luogo, una data, un responsabile, una causa, una conseguenza, una certezza.

Nel lavoro OSINT bisogna separare queste due cose.

Da una parte c'è il contenuto visivo.

Dall'altra c'è il claim, cioè l'affermazione che qualcuno sta facendo su quel contenuto.

Prima di condividere un video di guerra, la domanda non dovrebbe essere:

Sembra vero?

La domanda utile è:

Che cosa posso verificare davvero?

Questa guida non serve a trasformare chi legge in investigatore professionista. Serve a ridurre un errore molto comune: rilanciare un video solo perché è forte, emotivo, urgente o coerente con ciò che già pensiamo.

1. [Trova la fonte più vicina all'originale](#)

Il primo controllo è la provenienza.

Non chiederti subito se il video è vero. Chiediti prima da dove arriva.

Un video può passare da:

- una persona che lo ha registrato;
- un canale Telegram locale;
- un account X che aggrega contenuti;
- una pagina Facebook;
- un gruppo WhatsApp;
- una testata giornalistica;
- un profilo OSINT;
- un account anonimo;
- un repost senza contesto;
- uno screenshot trasformato di nuovo in video.

Ogni passaggio può aggiungere o perdere informazioni.

Il video originale potrebbe avere una didascalia diversa. Potrebbe essere stato tagliato. Potrebbe essere stato pubblicato ore o anni prima. Potrebbe riferirsi a un altro Paese. Potrebbe essere stato usato correttamente dalla prima fonte e male da chi lo rilancia.

Il controllo minimo è questo:

1. cerca se il post che stai guardando indica una fonte;
2. apri la fonte indicata, non fermarti al repost;
3. controlla se quella fonte indica a sua volta un'altra origine;
4. cerca una versione precedente del video usando parole chiave, frame e reverse search;
5. annota dove ti fermi.

Se non riesci a risalire a una fonte più vicina all'originale, non significa automaticamente che il video sia falso. Significa che la catena è debole.

E una catena debole non va presentata come certezza.

2. Controlla se il video è vecchio

Molti video di guerra non sono falsi nel senso tecnico del termine.

Sono veri, ma fuori contesto.

Un bombardamento reale può essere attribuito a un altro fronte. Un'esplosione di anni prima può essere presentata come avvenuta ieri. Un video girato durante un'esercitazione può essere rilanciato come combattimento. Una scena di un conflitto può essere usata per commentarne un altro.

Per questo il secondo controllo riguarda il tempo.

Ci sono alcune domande semplici:

- qual è la prima data in cui trovo questo video online?
- la data del post coincide con la data dell'evento dichiarato?
- ci sono versioni precedenti con un'altra descrizione?
- qualcuno lo ha già verificato o smentito?
- il meteo, la luce, gli abiti, la vegetazione o il contesto sono coerenti con la data indicata?

La reverse image search può aiutare, ma non basta.

Con un video conviene estrarre alcuni fotogrammi chiari: un'inquadratura con edifici, strade, mezzi, cartelli, fumo, montagne, insegne o elementi distintivi. Poi si cercano quei fotogrammi con strumenti diversi: Google Lens, Yandex, Bing Visual Search o altri motori disponibili.

Il punto non è trovare "la risposta" in un solo strumento.

Il punto è capire se quel materiale era già apparso altrove.

Se trovi lo stesso video pubblicato due anni prima, il problema è chiuso: il video non può documentare l'evento di oggi. Se trovi immagini simili ma non identiche, devi essere più prudente: potrebbero essere riprese dello stesso luogo in momenti diversi, o contenuti diversi confusi tra loro.

3. Verifica il luogo, non solo la didascalia

La geolocalizzazione è uno dei passaggi più importanti e più fraintesi.

Geolocalizzare non significa indovinare un Paese guardando una bandiera, una lingua o un'uniforme. Significa trovare elementi visivi che collegano il video a un luogo verificabile.

Possono aiutare:

- cartelli stradali;
- insegne commerciali;
- forma degli edifici;
- incroci;
- ponti;
- montagne;
- coste;
- minareti, chiese, monumenti;
- linee elettriche;
- disposizione delle strade;
- fermate, binari, rotatorie;
- segni su veicoli o mezzi pubblici;
- profili delle colline;
- ombre e orientamento della luce.

Una sola corrispondenza raramente basta.

Un cartello può essere generico. Un edificio può assomigliare a molti altri. Una strada può essere stata ripresa da un'angolazione difficile. Una scritta può indicare lingua o area, ma non prova da sola il punto esatto.

Il controllo migliore combina più elementi.

Per esempio:

- il cartello indica una città;
- la curva della strada coincide con la mappa;
- un edificio alto ha la stessa forma;
- una montagna sullo sfondo ha lo stesso profilo;
- la direzione del fumo o della luce non contraddice l'inquadratura;
- altri post locali parlano dello stesso evento nella stessa area.

In quel caso puoi dire qualcosa di più solido:

Il luogo è compatibile con questa area.

Oppure, se la corrispondenza è forte:

Il video sembra essere stato girato in questo punto.

Ma evita frasi più forti di ciò che hai verificato.

Non scrivere "confermato" se hai solo una somiglianza.

4. Ricostruisci la sequenza temporale

Anche quando un video è autentico e il luogo è corretto, resta una domanda:

Quando è stato girato?

La data di pubblicazione non è la data di registrazione.

Un video può essere caricato ore dopo. Può essere stato ricevuto da un'altra persona. Può essere stato salvato, tagliato, compresso, rilanciato. Può arrivare da un archivio o da un gruppo chiuso.

Per questo serve una piccola timeline.

Non deve essere complicata. Può bastare una tabella:

Ora / data	Fonte	Che cosa mostra o afferma	Livello di certezza
08:13	primo post trovato	video senza luogo chiaro	basso
08:25	canale locale	afferma che è in città X	medio
08:40	testata locale	segnala esplosione nella stessa zona	medio
09:10	autorità / comunicato	conferma evento, ma non il video	medio

Questa tabella evita un errore molto comune: mescolare prove diverse come se confermassero tutte la stessa cosa.

Un comunicato può confermare che c'è stato un attacco in una città. Non conferma automaticamente che quel video mostri quell'attacco.

Un post locale può confermare che molte persone hanno sentito esplosioni. Non conferma automaticamente chi abbia colpito.

Una mappa può confermare che il luogo esiste. Non conferma la data.

Nel lavoro OSINT ogni elemento sostiene solo una parte della frase.

Il punto è non chiedere a una prova più di quanto possa dare.

5. Scrivi una conclusione stretta

Il quinto controllo riguarda il modo in cui condividi.

Anche dopo aver verificato fonte, data, luogo e contesto, potresti non avere abbastanza elementi per dire tutto.

Allora la conclusione deve essere stretta.

Esempi di conclusioni prudenti:

Il video risulta già online prima dell'evento indicato, quindi non può riferirsi all'attacco di oggi.

Il luogo sembra compatibile con l'area indicata, ma la data di registrazione non è verificata.

Il video mostra un'esplosione, ma non consente da solo di stabilire chi l'abbia causata.

La fonte originale non è stata identificata: il contenuto va trattato come non verificato.

Queste frasi sono meno spettacolari di "confermato".

Ma sono più corrette.

In guerra, la velocità è parte del problema. La propaganda, la confusione, la paura, il desiderio di conferma e l'orrore delle immagini spingono tutti nella stessa direzione: condividere prima di capire.

Il metodo OSINT serve a fare il contrario.

Rallentare abbastanza da non trasformare un segnale in prova.

Errori comuni da evitare

Credere che un account famoso basti

Un account molto seguito può essere utile per scoprire un video, ma non sostituisce la verifica. Anche account competenti possono rilanciare materiale incompleto, non contestualizzato o corretto dopo alcune ore.

Confondere il video con la didascalia

Il video può essere reale e la didascalia falsa. Oppure il video può mostrare un evento reale, ma in un altro luogo o in un altro momento.

Usare un solo fotogramma

Un frame può essere utile, ma può anche ingannare. Meglio estrarre più fotogrammi: uno con il luogo, uno con dettagli, uno con oggetti o mezzi, uno con eventuali insegne.

Fidarsi solo dei metadati

Molti video pubblicati sui social perdono metadati. Altri possono essere compressi, scaricati e ricaricati. Se ci sono metadati, sono un indizio da valutare, non una prova totale.

Cercare solo la conferma

Se vuoi dimostrare a tutti i costi che il video è vero, troverai segnali che sembrano confermarlo. Il controllo migliore cerca anche l'ipotesi opposta: dove potrebbe essere stato girato prima? chi lo ha già pubblicato? quali elementi non tornano?

Checklist rapida prima di condividere

Prima di condividere un video di guerra, chiediti:

1. Ho trovato la fonte più vicina all'originale?
2. Ho controllato se il video era già online prima?
3. Ho verificato il luogo con più di un elemento visivo?
4. Ho separato data di pubblicazione e data di registrazione?
5. Ho distinto ciò che il video mostra da ciò che la didascalia afferma?
6. Ho cercato fonti indipendenti sullo stesso evento?
7. Ho scritto una conclusione prudente?
8. Ho evitato di indicare responsabili se il video non lo dimostra?
9. Ho salvato link, screenshot, data e ora dei controlli?

10. Se non ho verificato abbastanza, ho evitato di rilanciare come certezza?

La regola finale

Un video di guerra può essere una prova importante.

Ma non diventa prova solo perché è drammatico.

Diventa utile quando si può ricostruire una catena minima: fonte, data, luogo, contesto, limiti.

Se manca un pezzo, non bisogna inventarlo.

Bisogna dirlo.

Nel dubbio, la formula migliore è spesso la più semplice:

Video non ancora verificato.

Non è una sconfitta.

È una forma di responsabilità.